Ruijie Reyee RG-EG Series Routers

ReyeeOS 2.324 Configuration Guide

Document Version: V1.0
Date: January 26, 2025

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://reyee.ruijie.com
- Technical Support Website: https://reyee.ruijie.com/en-global/support
- Case Portal: https://www.ruijienetworks.com/support/caseportal
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Online Robot/Live Chat: https://reyee.ruijie.com/en-global/rita

Conventions

1. GUI Symbols

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

2. Signs

The signs used in this document are described as follows:

Warning

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

Caution

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

Note

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

Specification

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

3. Note

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

Contents

1 Change Description

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

1.1 ReyeeOS 2.324

1.1.1 Hardware Change

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

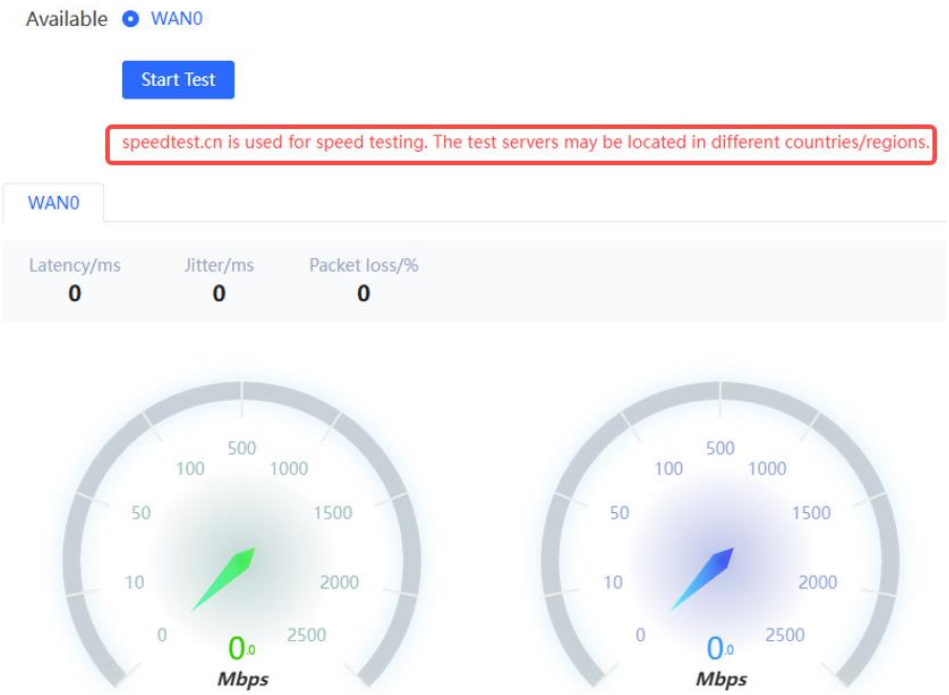
Model	Hardware Version
RG-EG210G-E	1.xx
RG-EG105G-V2	1.xx
RG-EG105G-P V2	1.xx, 2.xx
RG-EG210G-P	1.xx, 2.xx
RG-EG209GS	1.xx
RG-EG305GH-P-E	1.xx
RG-EG310GH-P-E	1.xx
RG-EG310GH-E	1.xx
RG-EG105G-V3	1.xx
RG-EG105G-P-V3	1.xx
RG-EG210G-P-V3	1.xx
RG-EG1510XS	1.xx

1.1.2 Software Feature Change

Compared to ReyeeOS 2.324, the software feature changes in this version are as follows:

1. Changed feature - Prompt added on the speed test page

Since ReyeeOS 2.324, the following prompt has been added on the speed test page. For details, see 4.4 Configuring Speed Test.


Available
WAN0
Start Test
speedtest.cn is used for speed testing. The test servers may be located in different countries/regions.
WAN0
Latency/ms
0
Jitter/ms
0
Packet loss/%
0
500
100
1000
50
1500
10
2000
0
2500
0
Mbps
500
100
1000
50
1500
10
2000
0
2500
0
Mbps

2 Login

2.1 Configuration Environment Requirements

2.1.1 PC

- Browser: 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 or format error may occur if an unsupported browser is used.
- Resolution: 1024 x 768 or a higher resolution is recommended. If other resolutions are used, the page fonts and formats may not be aligned, the GUI is less artistic, or other exceptions may occur.

2.2 Default Configuration

Table 2-1 Default Web Configuration

Item	Default
IP address	192.168.110.1
Password	The default password is "admin".

2.3 Login to Web Interface

2.3.1 Connecting to the Router

You can open the management page and complete Internet access configuration only after connecting a client to the router in either of the following ways:

- Wired Connection

Connect a local area network (LAN) port of the router to the network port of the PC, and set the IP address of the PC. See Section 2.3.2 Configuring the IP Address of the Management Client for details.

- Wireless Connection

Connect the LAN port to the uplink port on the AP and power on the AP. On a mobile phone or laptop, search for wireless network **@Ruijie-m***XXXX* (XXXX is the last four digits of the MAC address of each device). In this mode, you do not need to set the IP address of the management client, and you can skip the operation in Section 2.3.2 Configuring the IP Address of the Management Client.

2.3.2 Configuring the IP Address of the Management Client

Configure an IP address for the management client in the same network segment as the default IP address of the device (The default device IP address is 192.168.110.1, and the subnet mask is 255.255.255.0.) so that the

management client can access the device. For example, set the IP address of the management client to 192.168.110.200.

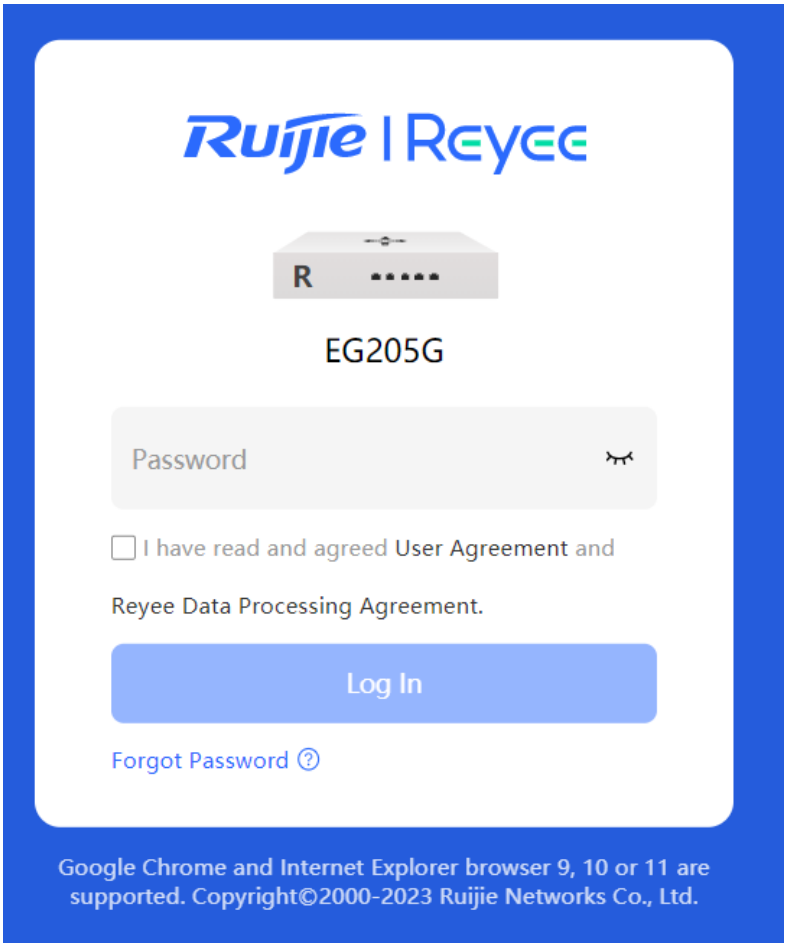
2.3.3 Login

Enter the IP address (192.168.110.1 by default) of the router 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 obtains a new dynamic IP address, the new IP address can be used to access the web management system of the device as long as the management client and the device are in the same network segment of a LAN.

(1) On the web page, enter the password and click **Log In** to enter 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.

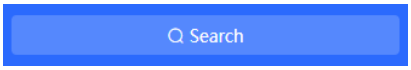
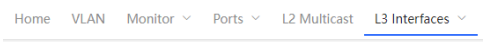
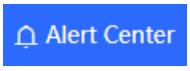
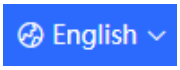
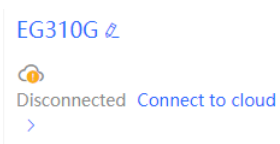
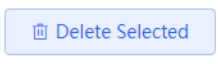
If you forget the IP address or password, hold down the **Reset** button on the device panel for more than 5 seconds when the device is connected to the power supply to restore factory settings. After restoration, you can use the default IP address and password to log in.

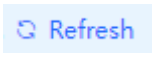
Caution

Restoring factory settings will delete the existing configuration and you are required to configure the device again at your next login. Therefore, exercise caution when performing this operation.

2.3.4 Frequently-Used Controls on the Web Page

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

Control	Description
	**Monitor**: Click it to view the topology of the self-organizing network and monitor device traffic trend, client traffic usage, device port status, and so on. **Config**: Click it to configure all functions available on the local device.
	Click it to search or select features for quick configuration.
	The navigation bar is arranged horizontally on the top when the device acts as the slave device, and vertically on the left when the device acts as the master device.
	Click it to access the alert list.
	Click it to change the language.
	Click it to log out of the web management system.
	Click it to connect the device to the cloud by scanning the QR code for remote management.
	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.

Control	Description
	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 access the corresponding page.

2.4 Work Mode

The device can work in router mode and AC mode. The system menu pages and configuration function scope vary depending on the work mode. By default, the EG router works in router mode. To modify the work mode, see Section 4.1 Switching the Work Mode.

2.4.1 Router Mode

The device supports routing functions such as route-based forwarding and network address translation (NAT), VPN, and behavior management. It can allocate addresses to downlink devices, forward network data based on routes, and perform NAT operations.

In the router mode, the device can access the network through Point-to-Point Protocol over Ethernet (PPPoE) dialing, dynamic IP address, and static IP address. It can also directly connect to a fiber-to-the-home (FTTH) network cable or an uplink device to provide network access and manage downlink devices.

2.4.2 AC Mode

The device supports Layer 2 forwarding only. The device does not provide the routing and Dynamic Host Configuration Protocol (DHCP) server functions. By default, the WAN interface obtains IP addresses through DHCP. The AC mode is applicable to the scenario where the network is working normally. In AC mode, the device serves as the management controller to access the network in bypass mode and manage the AP.

2.5 Configuration Wizard (Router Mode)

2.5.1 Getting Started

(1) Power on the device. Connect the WAN interface of the device to an uplink device using an Ethernet cable, or connect the device to the optical modem directly.

(2) Configure the Internet connection type according to requirements of the local Internet Service Provider (ISP). Otherwise, the Internet access may fail due to improper configuration. You are advised to contact your local ISP to confirm the Internet connection type:

- Figure out whether the Internet connection type is PPPoE, DHCP mode, or static IP address mode.
- In the PPPoE mode, a username, a password, and possibly a service name are needed.

- In the static IP address mode, an IP address, a subnet mask, a gateway, and a DNS server need to be configured.

2.5.2 Configuration Steps

1. Adding a Device to Network

You can manage and configure all devices in the network in batches by default. Please verify the device count and network status before configuration.

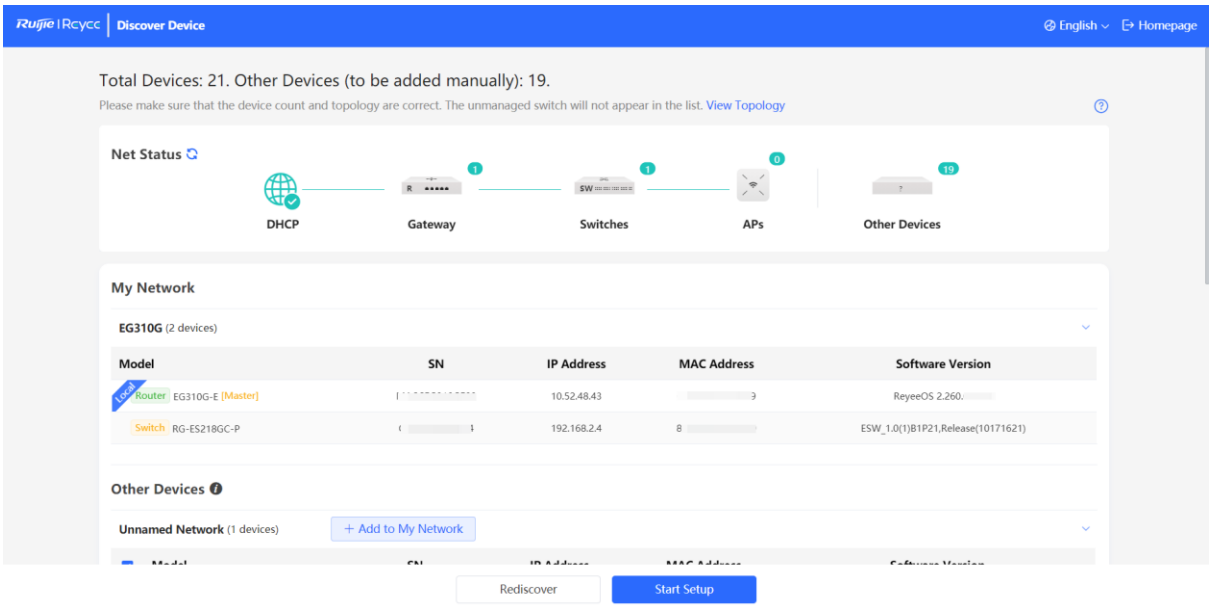
Note

New devices will join in a network automatically after being powered on. You only need to verify the device count.

If a new device is detected not in the network, click **Add to My Network** and enter its management password to add the device manually.

Note

If there is a firewall device in the network, the **Firewall Port Config** page appears. Select the corresponding port for configuration.



2. Creating a Network Project

Click **Start Setup** to configure the Internet connection type and management password.

(1) **Internet**: Configure the Internet connection type according to the requirements of the local ISP.

- **DHCP**: The router detects whether it can obtain an IP address via DHCP by default. If the router connects to the Internet successfully, you can click **Next** without entering an account.
- **PPPoE**: Click **PPPoE**, and enter the username, password, and service name. Click **Next**.

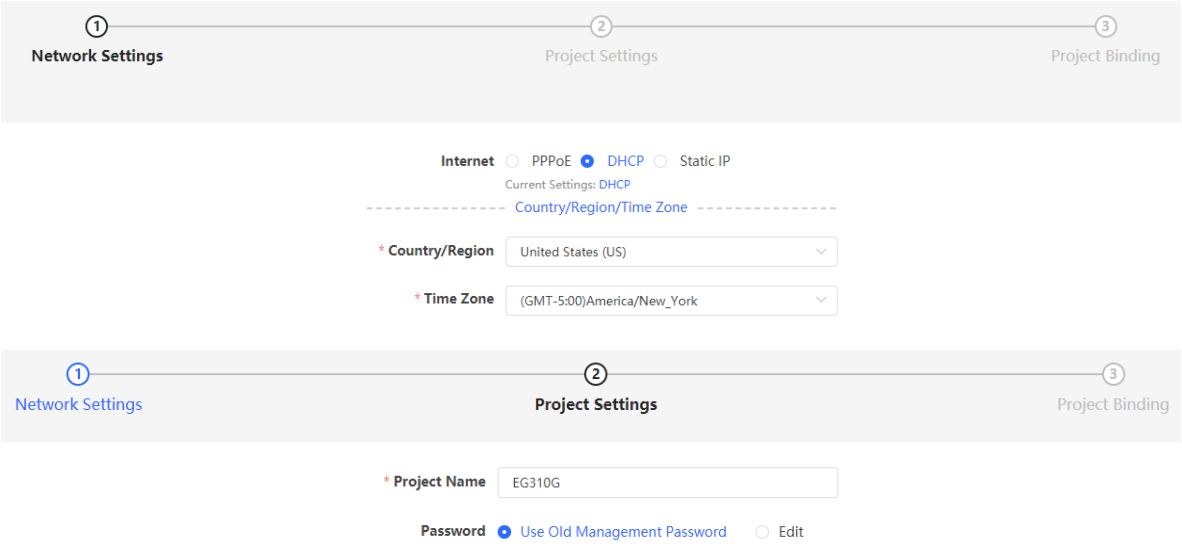
- **Static IP**: Enter the IP address, subnet mask, gateway, and DNS server, and click **Next**.

(2) **Country/Region**: You are advised to select the actual country or region.

(3) **Time Zone**: Set the system time. The network time server is enabled by default to provide the time service. You are advised to select the actual time zone.

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

(5) **Management Password**: The password is used for logging in to the management page.



Click **Create Network & Connect**. The device will deliver the initialization and check the network connectivity.

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

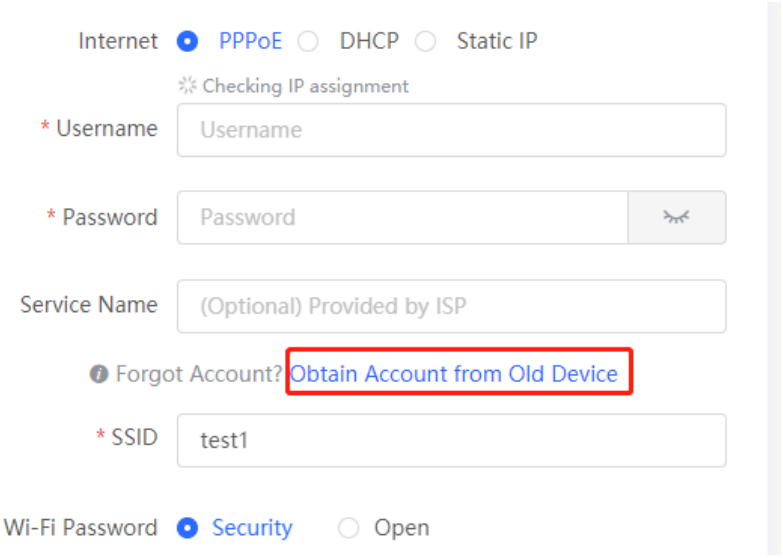
Note

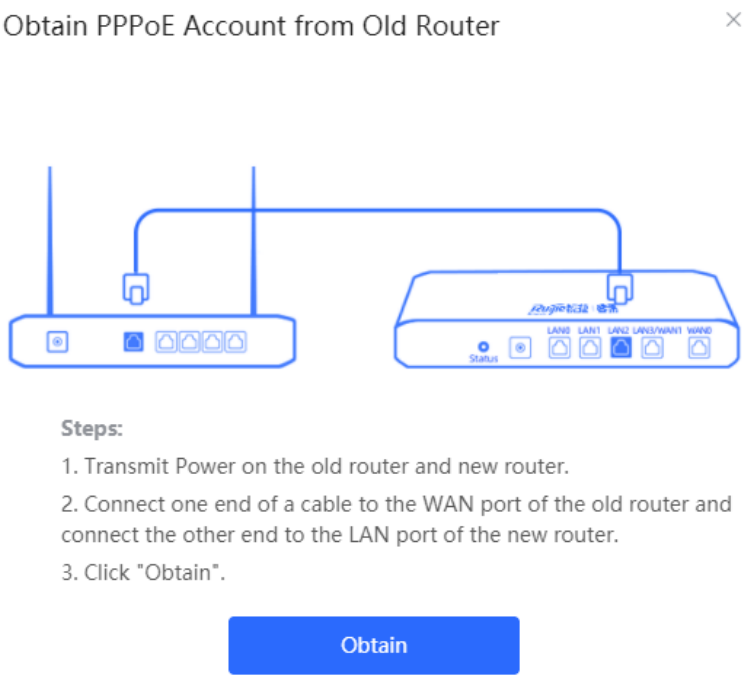
- If your device is not connected to the Internet, click **Exit** to exit the configuration wizard.
- Please log in again with the new password if you change the management password.

2.5.3 Forgetting the PPPoE Account

(1) Consult your local ISP.

(2) If you replace the old router with a new one, click **Obtain Account from Old Device**. Connect the old and new routers to a power supply and start them. Insert one end of an Ethernet cable into the WAN interface of the old router and connect the other end to a LAN port of the new router, and click **Obtain**. The new router automatically fetches the PPPoE account of the old router. Click **Save** to make the configuration take effect.





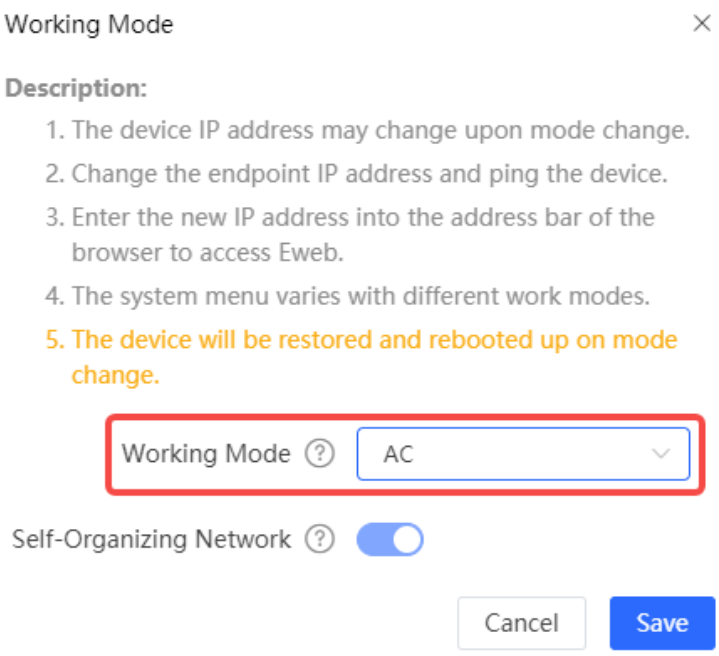
2.6 Configuration Wizard (AC Mode)

2.6.1 Getting Started

- Power on the device and connect the device to an uplink device.
- Make sure that the device can access the Internet.

2.6.2 Configuration Steps

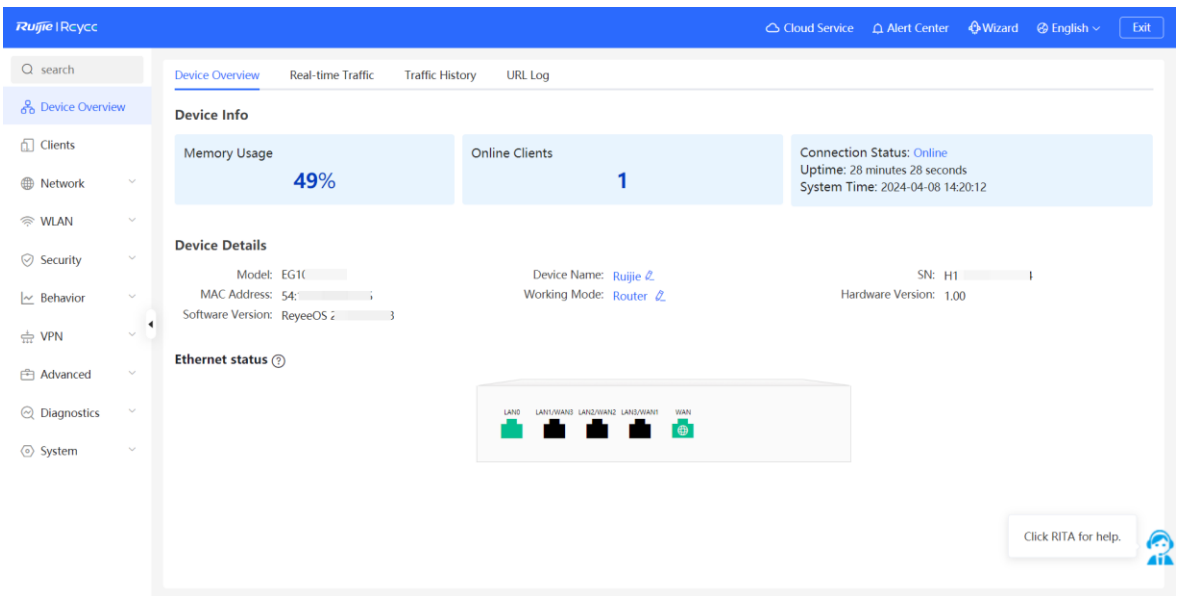
(1) On the work mode setting page, change the work mode from router mode to AC mode. For details, see Section 4.1 Switching the Work Mode.



(2) After mode switching, the device will restart. After restart, the WAN interface on the device obtains an IP address through DHCP and accesses the network by using a dynamic IP address. The default Internet connection type is DHCP mode. You can use the default value or manually configure a static IP address for the WAN interface. For details, see Section 2.5.2 Configuration Steps.

2.7 Switching the Work Mode

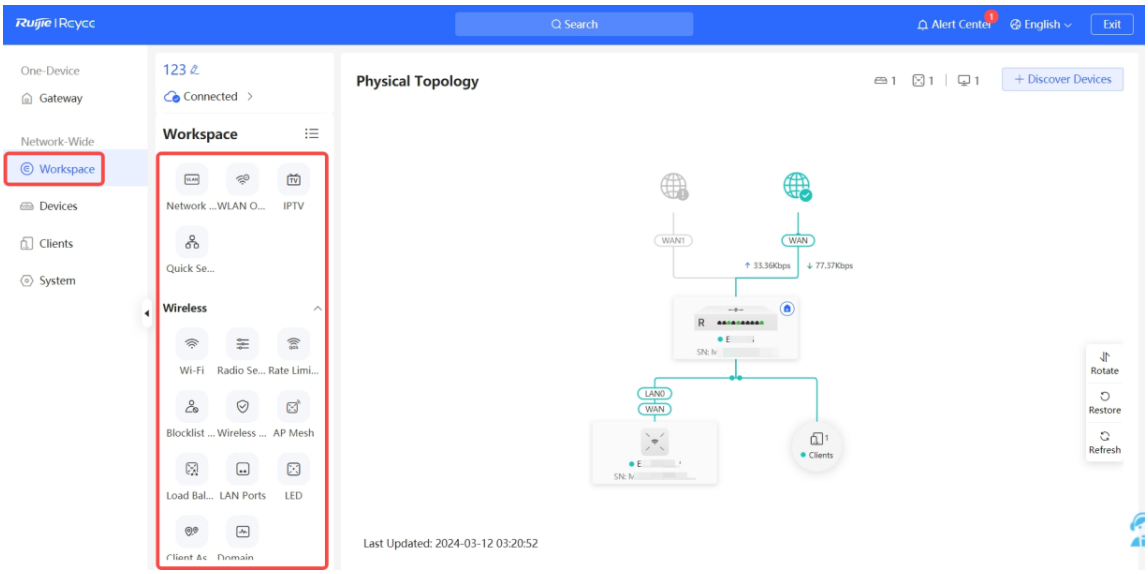
When the self-organizing network discovery function is disabled, which is enabled by default, the web interface will switch to the local device mode. For details, see 4.1 Switching the Work Mode.



When the self-organizing network discovery function is enabled, you can switch the web interface between network-wide mode and local device mode.

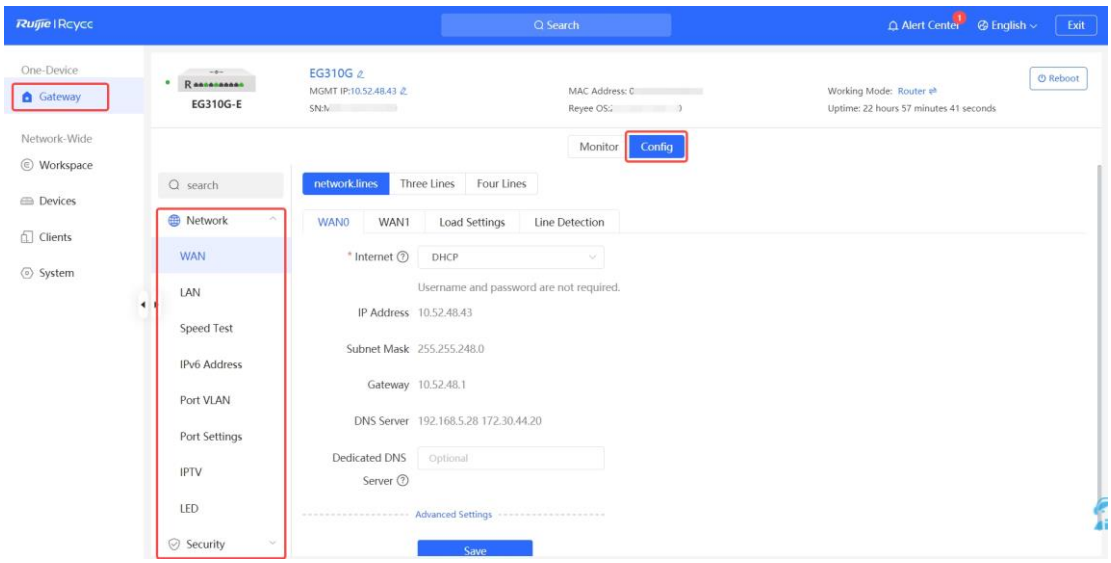
- Network-wide mode: You can view and configure all devices on the network from a network perspective.

  Click **Workspace** in the left navigation bar to access the corresponding functions for network-wide configuration in the secondary menu.

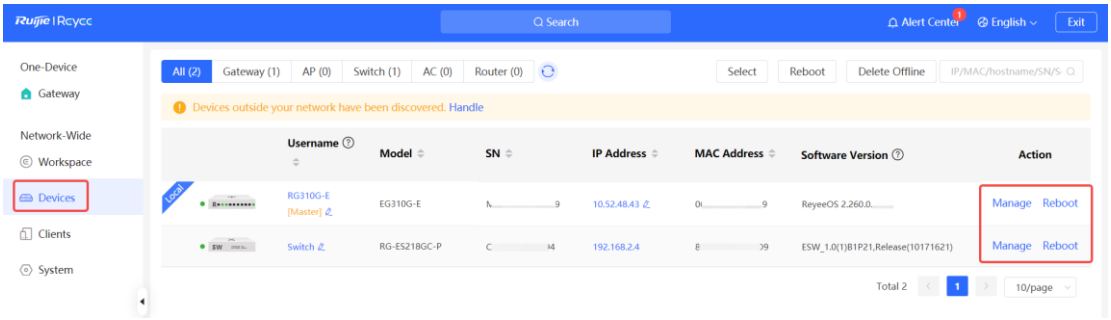


- Local device mode: You can configure only one device on the network. The configuration and management of an individual device can be accessed as follows:

  - Method 1: Choose **Gateway** > **Config** under the **One-Device** menu. On the displayed page, you can access the corresponding functions for single-device configuration in the secondary menu. This method only supports configuring gateway devices on the network.



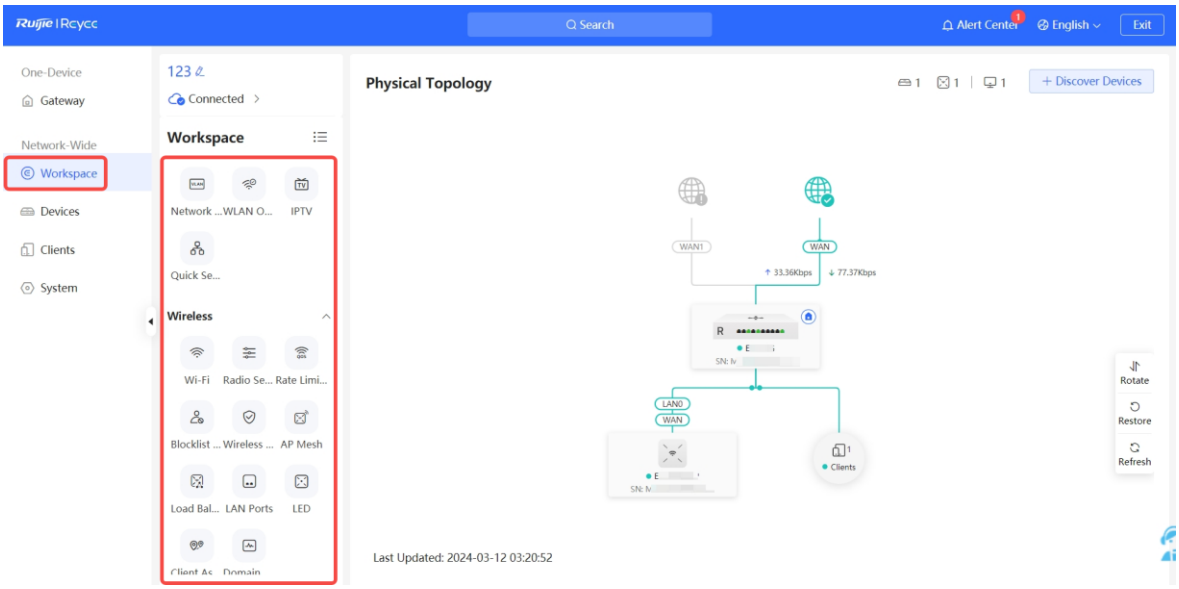
  - Method 2: Choose **Network-Wide** > **Devices**. In the device list, click the **Manage** button next to the target device. This method supports configuring any type of device on the network.


Ruijie | Reyee
Search
Alert Center
English
Exit
One-Device
Gateway
Network-Wide
Workspace
Devices
Clients
System
All (2)
Gateway (1)
AP (0)
Switch (1)
AC (0)
Router (0)
Select
Reboot
Delete Offline
IP/MAC/hostname/SN/S
Devices outside your network have been discovered. Handle
Username
Model
SN
IP Address
MAC Address
Software Version
Action
Local
RG310G-E
[Master]
EG310G-E
10.52.48.43
ReyeeOS 2.260.0
Manage
Reboot
Switch
RG-ES218GC-P
192.168.2.4
ESW_1.0(1)B1P21,Release(10171621)
Manage
Reboot
Total 2
1
10/page

3 Network-Wide Monitoring

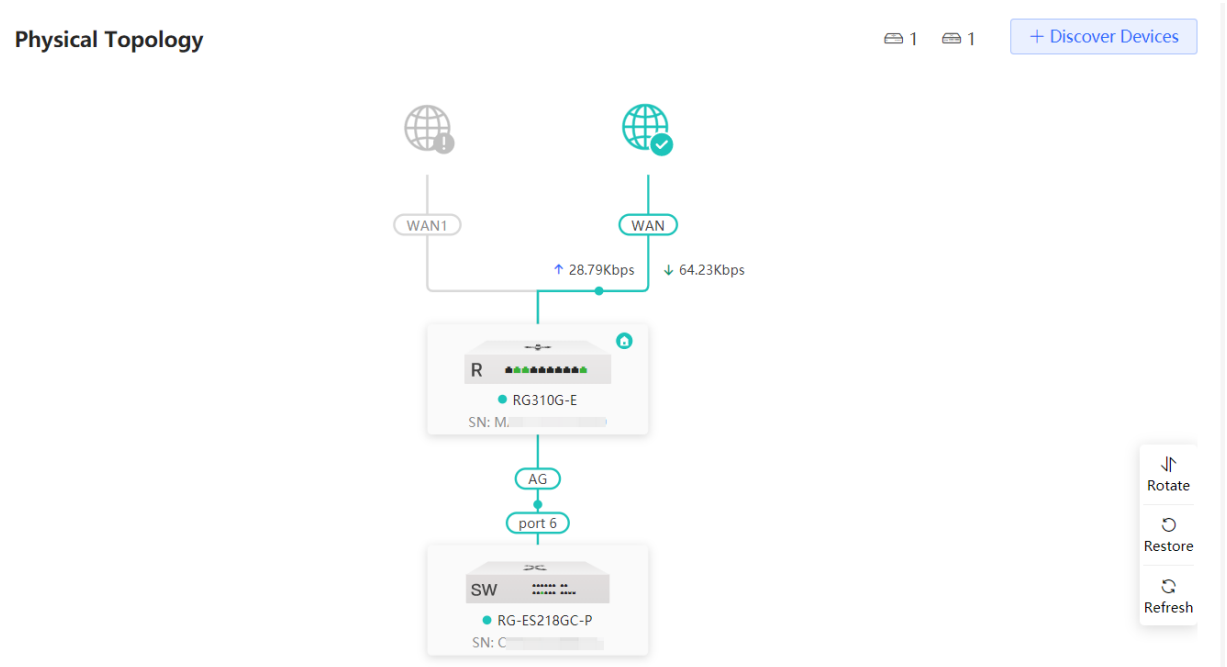
Choose **Network-Wide > Workspace > Physical Topology**.

The **Workspace** page displays the current network topology, uplink and downlink real-time traffic, network connection status. On the current page, you can monitor, configure, and manage the network status of the entire network.

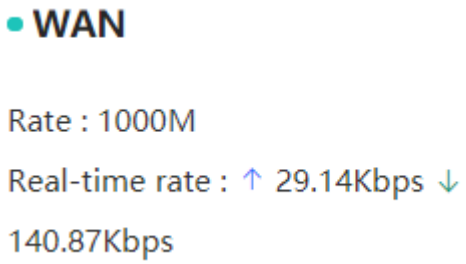


3.1 Viewing Networking Information

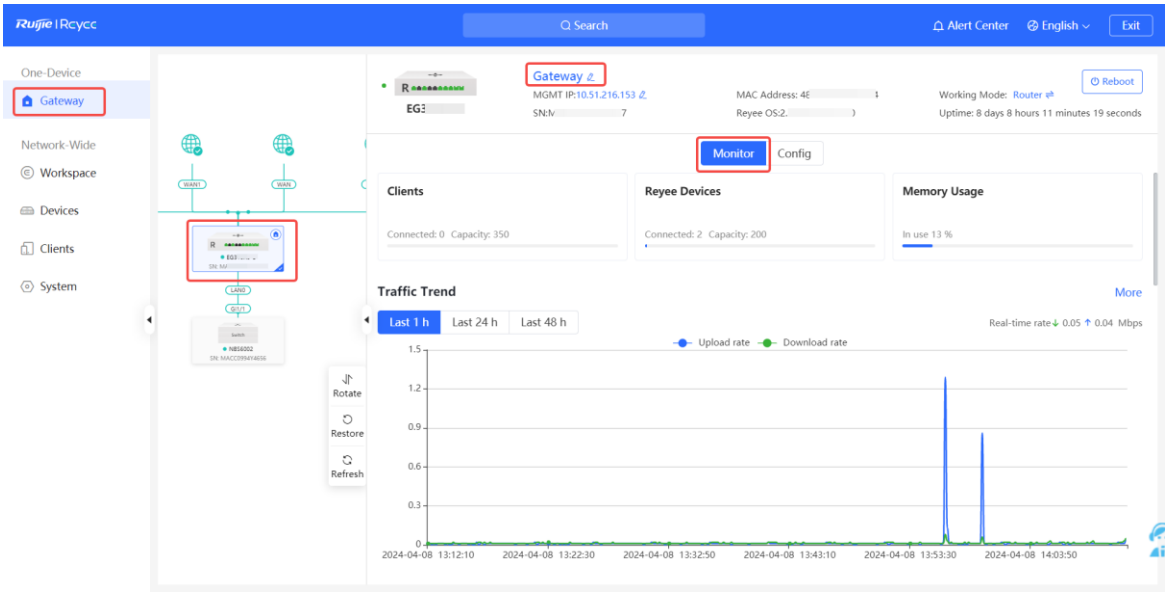
The networking topology contains information about online devices, connected port numbers, device SNs, and uplink and downlink real-time traffic.



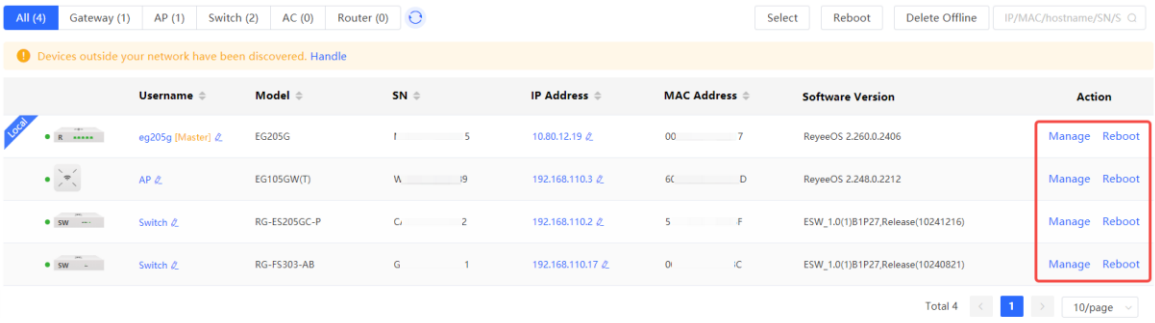
- Click the traffic data to view the bandwidth and real-time rates.



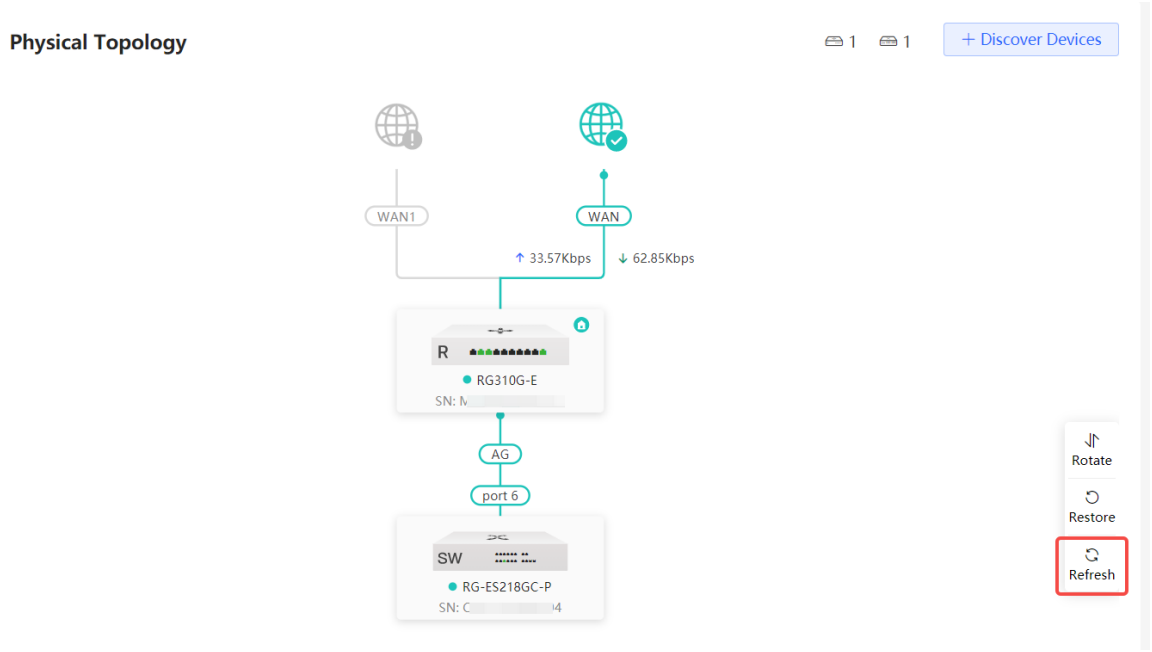
- Click a device in the topology to view the running status and configuration of the device and configure device functions. By default, the product model is used as the device name. Click to modify the device name so that the description can distinguish devices from one another.



- Choose **Network-Wide** > **Devices** to view the devices on the current network. Click **Manage** to monitor the device status and perform configuration. Click **Reboot** to reboot the device.



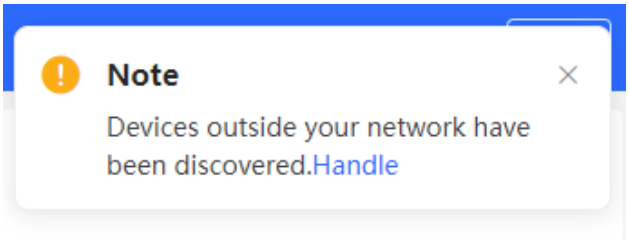
- The update time is displayed in the lower-left corner of the topology view. Click **Refresh** to update the topology to the latest state. It takes some time to update the topology data. Please wait patiently.



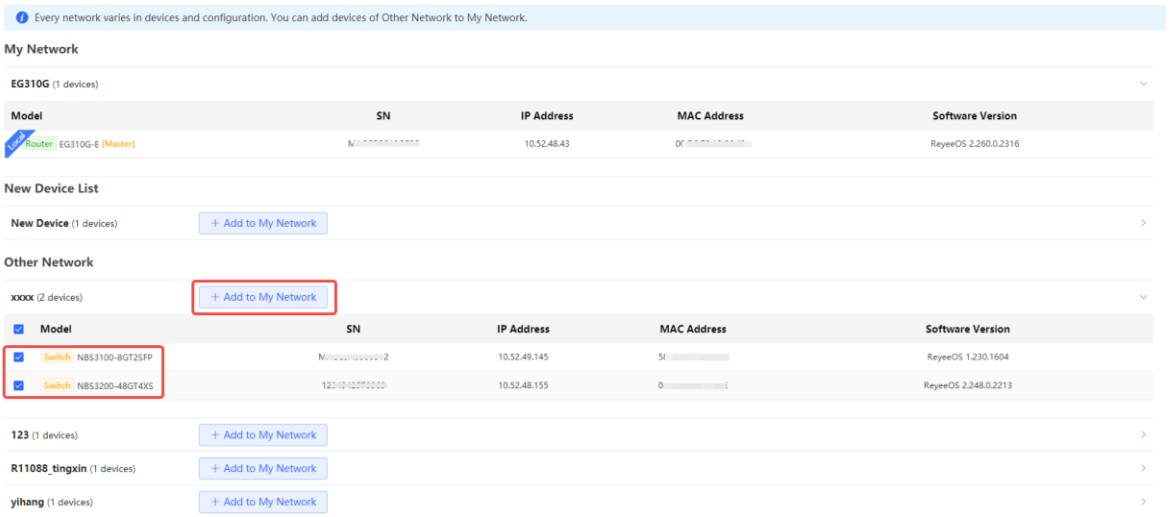
3.2 Adding Networking Devices

3.2.1 Wired Connection

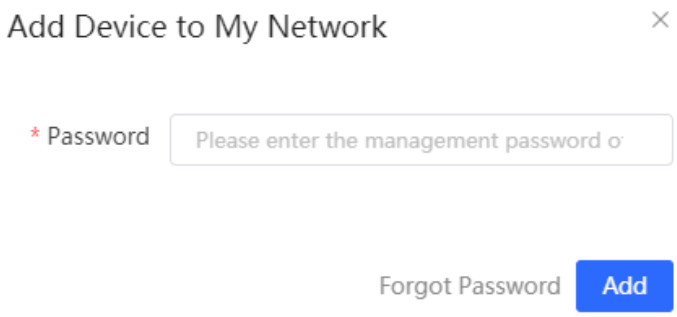
(1) When a new device is connected to the network via a wired connection, the system will display a prompt message indicating the presence of a new device and other unconnected devices. You can click **Handle** to add the new device and other unconnected devices to the network.



(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 is newly delivered from factory. If the device has a password, enter the management password of the device. Device addition fails if the password is incorrect.



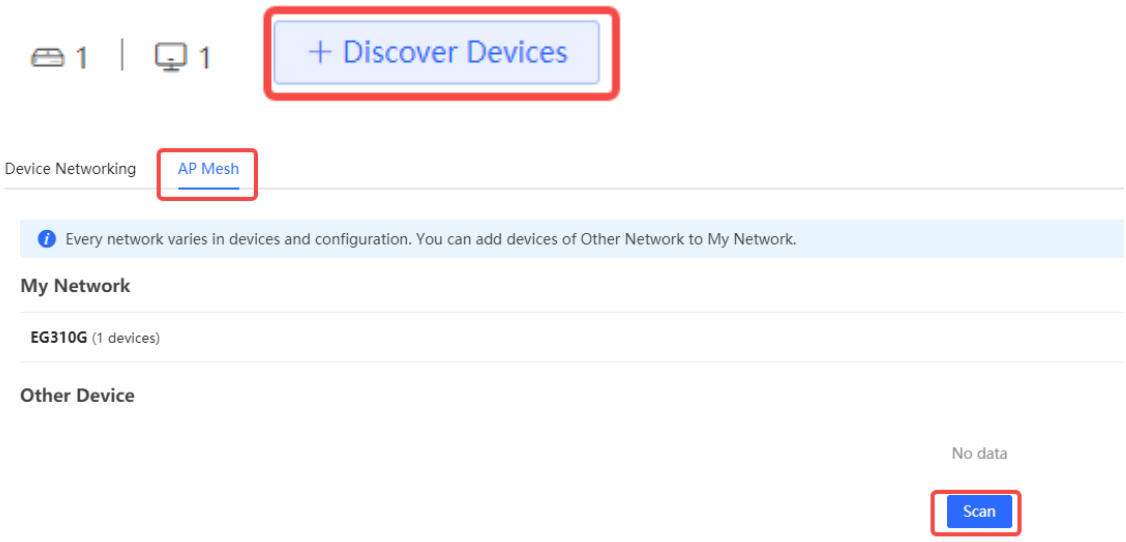
3.2.2 AP Mesh

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 Section 5.10 Enabling Reyee Mesh) The AP should be powered on nearby. It may fail to be scanned in case of long distance or obstacle blocking.
- You can scan to discover new APs on the AP Mesh page only when there are APs supporting the AP Mesh function on the network.

(1) After powering on the new AP and placing it within the range of an existing AP's Wi-Fi signal, log in to the web interface of the new AP. On the **Overview** page in network-wide management mode, click the topology view in the top right corner, and then click **+ Discover Devices**. Select the **AP Mesh** tab and scan for nearby APs that are not connected to the network via an Ethernet 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.

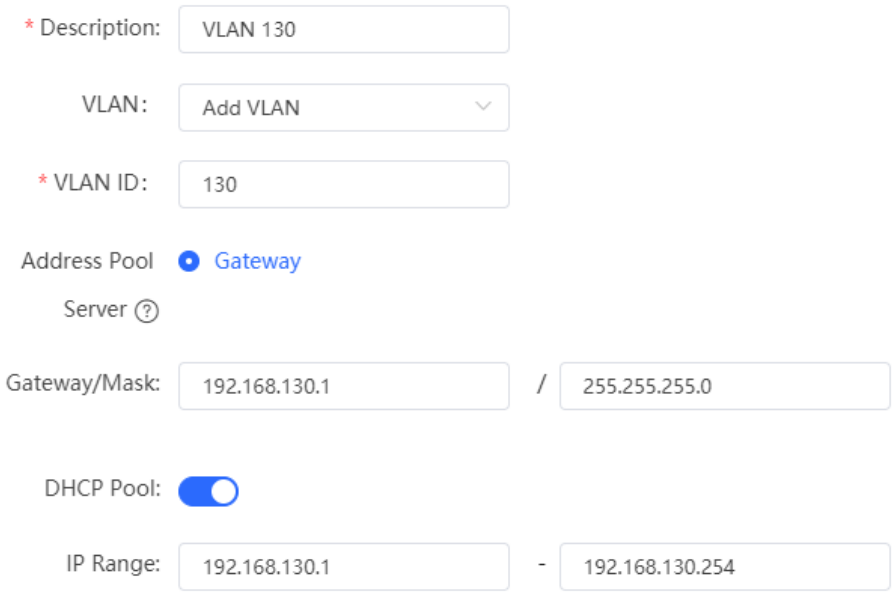
3.3 Configuring the Service Network

3.3.1 Configuring the Wired Network

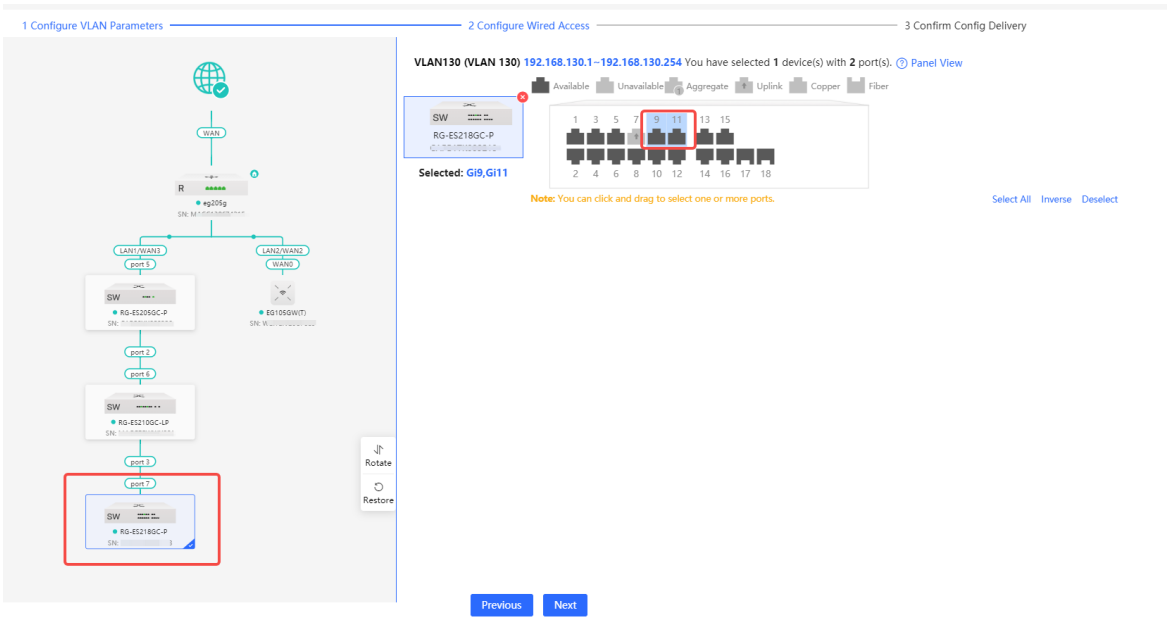
Choose **Network-Wide > Workspace > Network Planning**

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

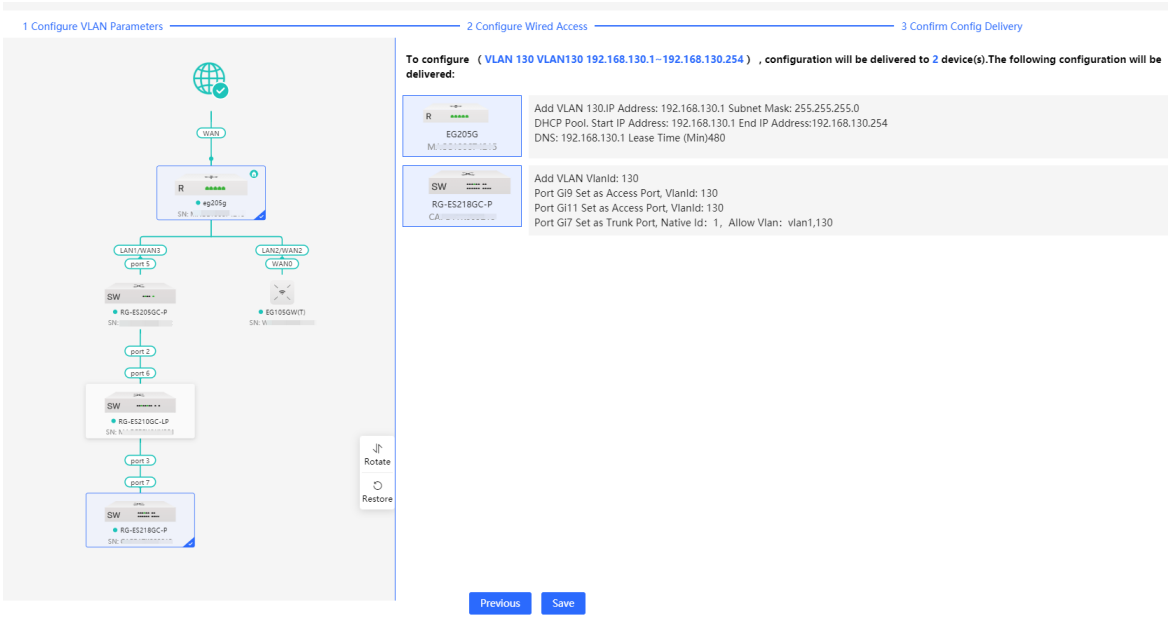
(2) Configure a VLAN for wired access, specify the address pool server for access clients in this VLAN, and determine whether to create a new DHCP address pool. By default, the gateway is used as the address pool server to allocate addresses to access clients. If an access switch is available in this networking, you can select this switch 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**.



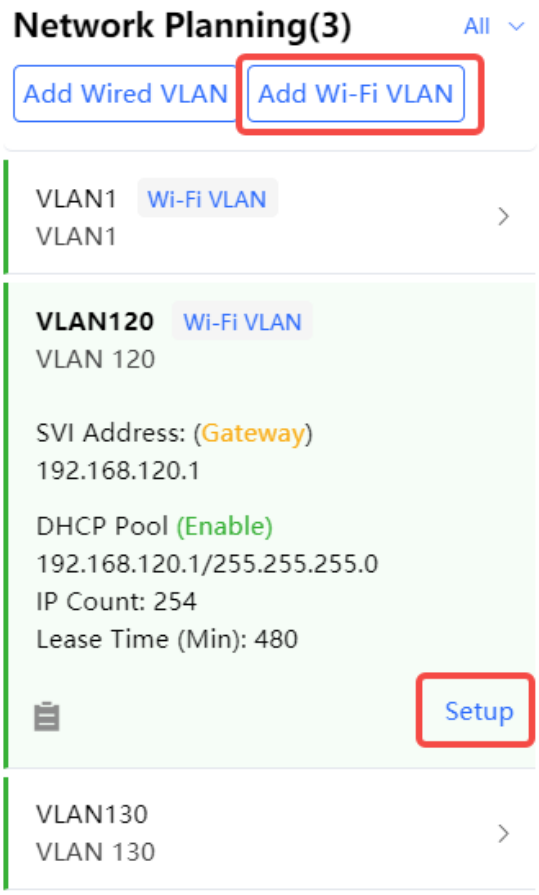
(4) Confirm that the configuration items to be delivered are correct and then click **Save**. Wait a moment for the configuration to take effect.



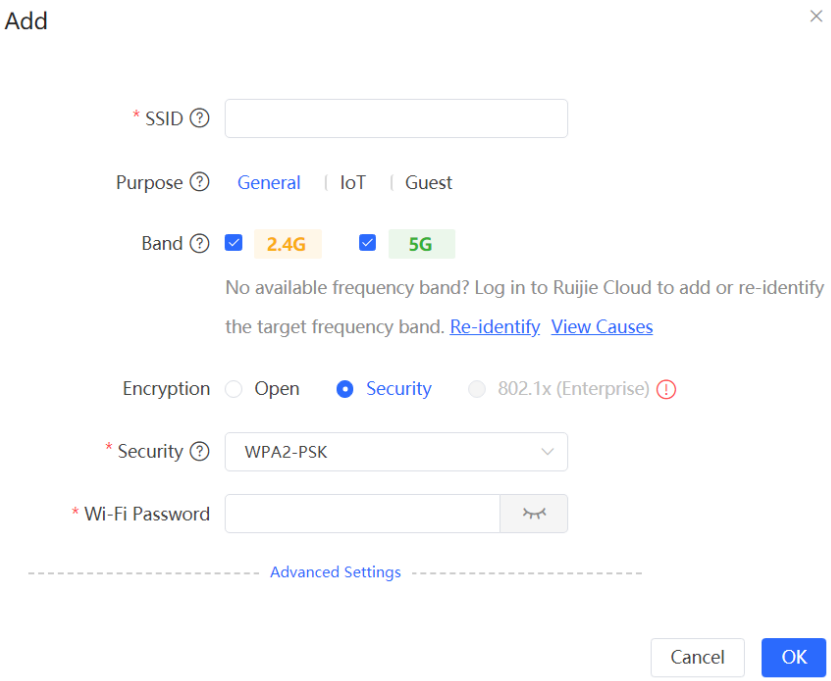
3.3.2 Configuring the Wireless Network

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

(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.



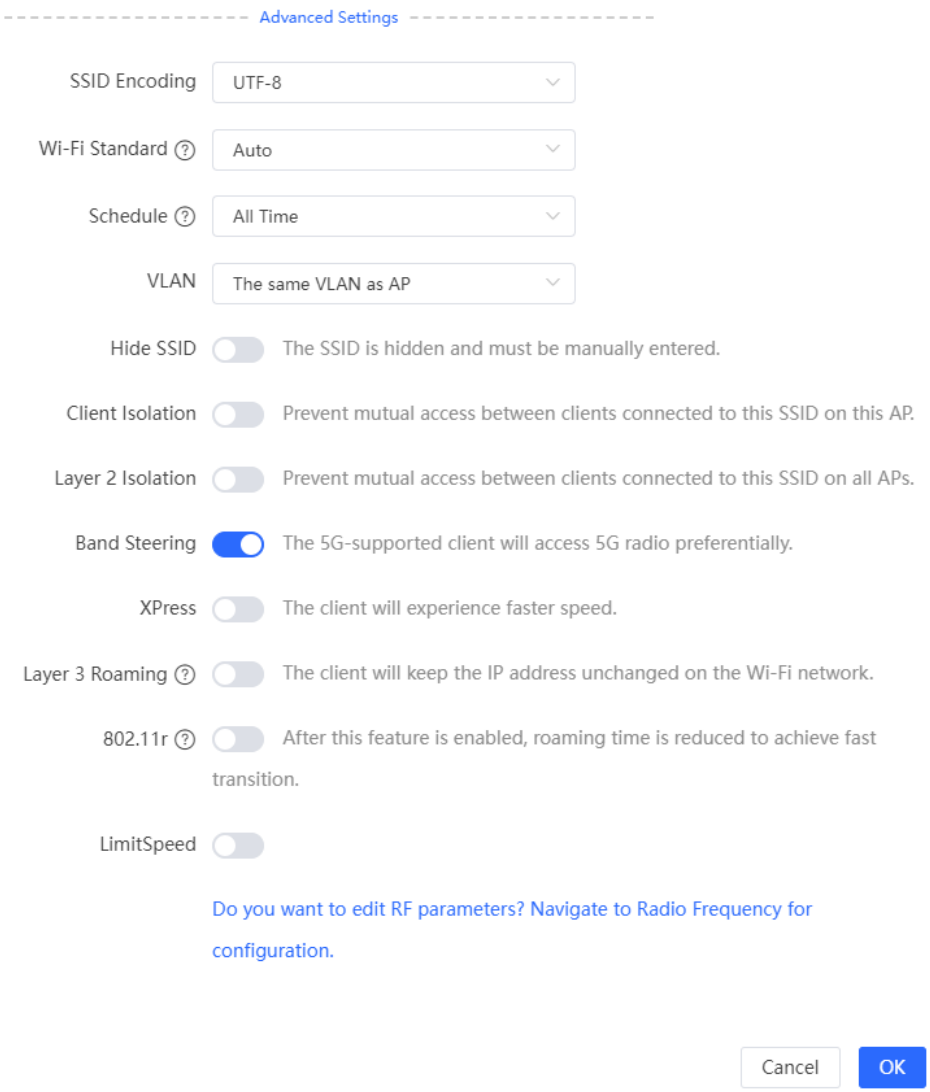
(2) Set the SSID, Wi-Fi password, and applicable bands. Click **Next**.



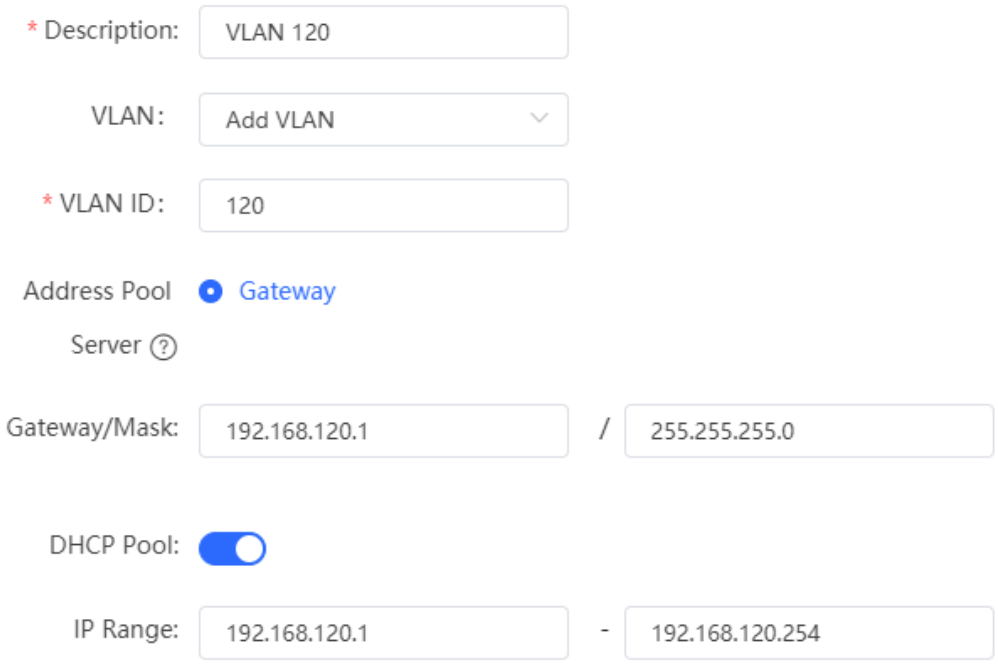
Applicable bands include 2.4 GHz, 5 GHz, and 2.4 GHz + 5 GHz.

Encryption modes include: **Open**, **Security**, and **802.1x (Enterprise)**. When the encryption mode is set to **Security**, you need to set the Wi-Fi password.

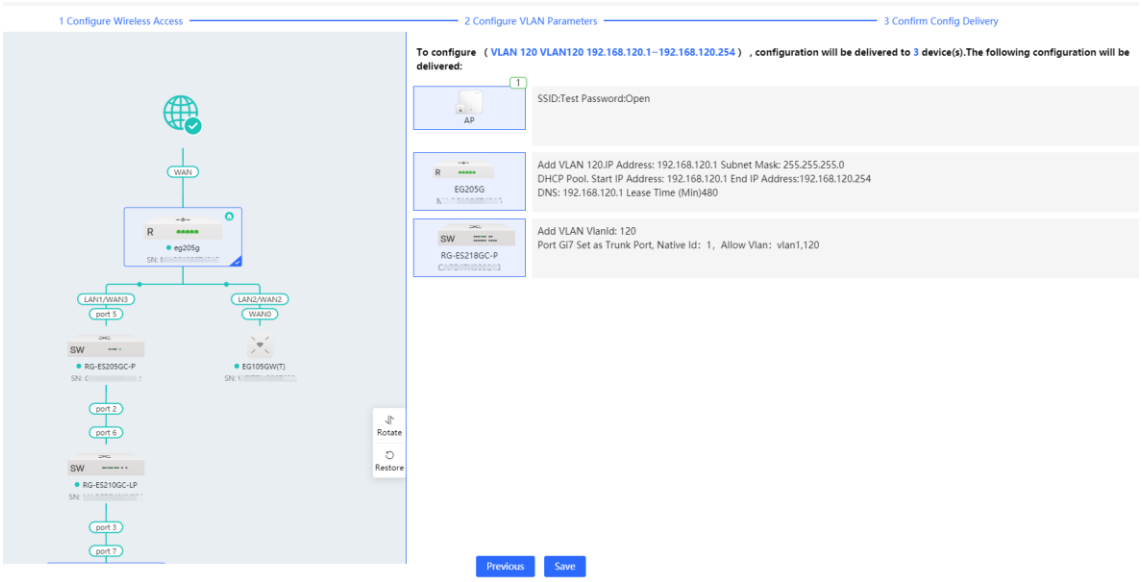
Click **Advanced Settings** to configure the advanced parameters, including Wi-Fi Standard, Wireless Schedule, Hide SSID, Client Isolation and so on.



(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. By default, the gateway is used as the address pool server to allocate addresses to access clients. If an access switch is available in this networking, you can select this switch 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.



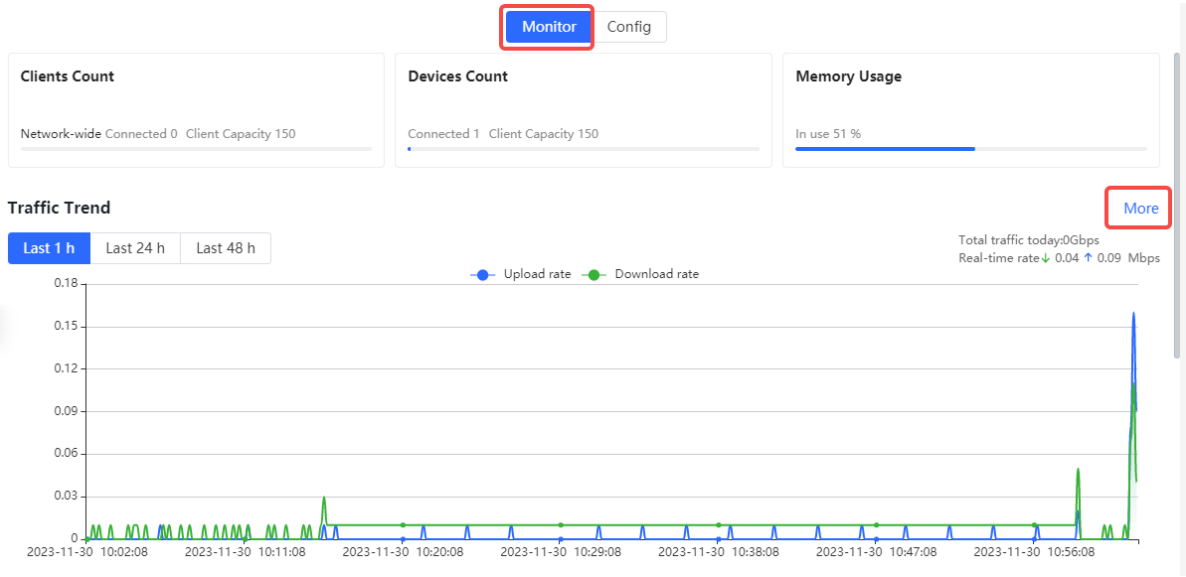
3.4 Supporting Traffic Monitoring

Traffic monitoring can be carried out based on ports, users, and applications. The real-time or historical uplink traffic, downlink traffic, and number of sessions can be displayed.

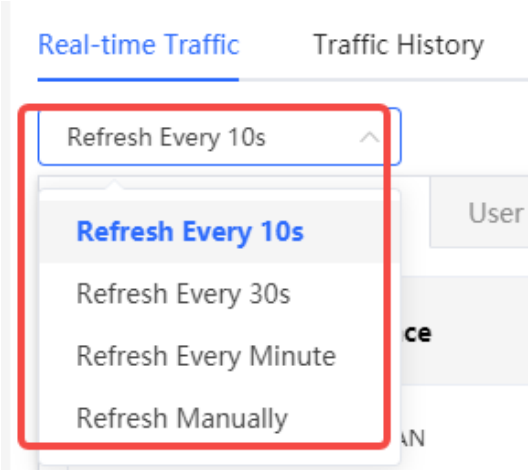
3.4.1 Viewing Real-Time Traffic

Choose **One-Device > Gateway > Monitor**.

Click **More** to the right of **Traffic Trend** to access the gateway's monitoring details page. On the page that is displayed, click the **Real-time Traffic** tab.

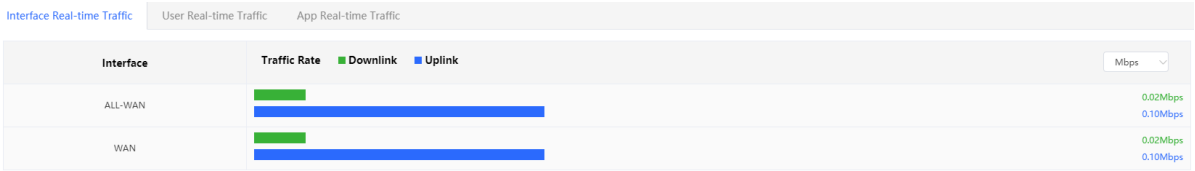


Select a refresh frequency to set the frequency of real-time traffic refresh.



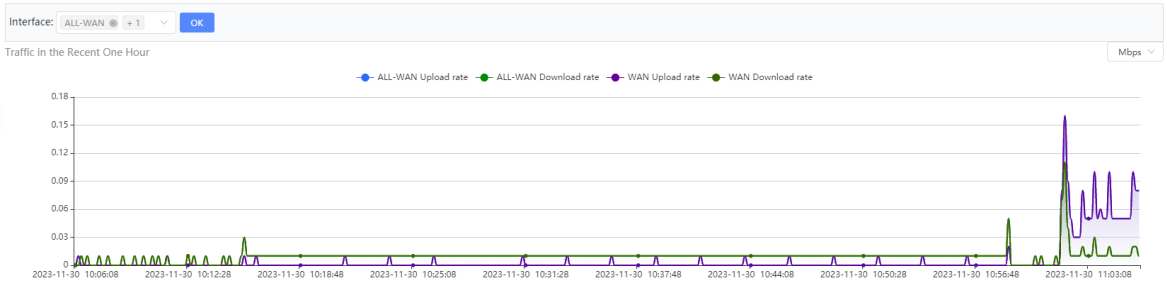
1. Viewing Real-time Traffic of an Interface

Click the **Interface Real-Time Traffic** tab to view the uplink or downlink traffic of an interface or the entire device.



- View traffic in the recent one hour

  Select an interface or **ALL-WAN** in the **Interface** drop-down menu. You can view the traffic and sessions of the interface or device in the last one hour, including the sessions of the excluded WAN interface.

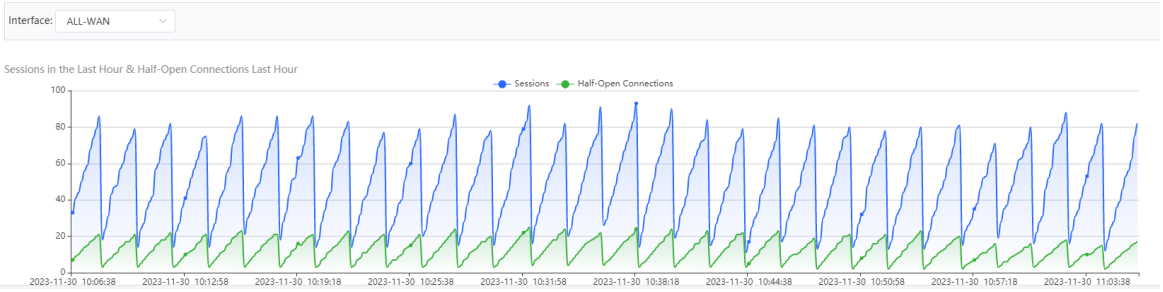


Note

Uplink traffic and downlink traffic are color-coded in the figure. You can move the cursor over a curve to view uplink traffic and downlink traffic at a certain time.

- View the number of sessions and half-open connections in the last one hour

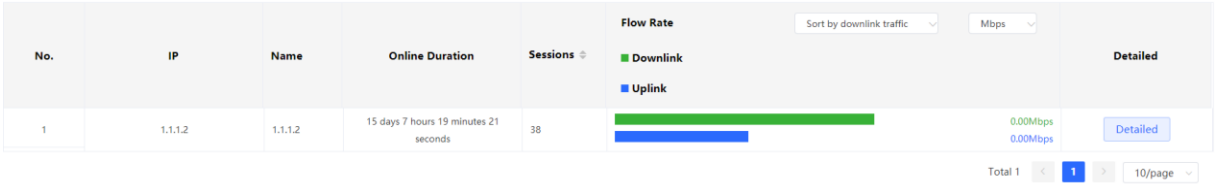
  Select an interface or **ALL-WAN** in the **Interface** drop-down menu to check the number of sessions and half-open connections in the last one hour (including the session information of the excluded WAN interface).



2. Viewing Real-time Traffic of a Client

Click the **User Real-Time Traffic** tab to view the IP address, name, online duration, number of sessions, and uplink and downlink traffic of each client.

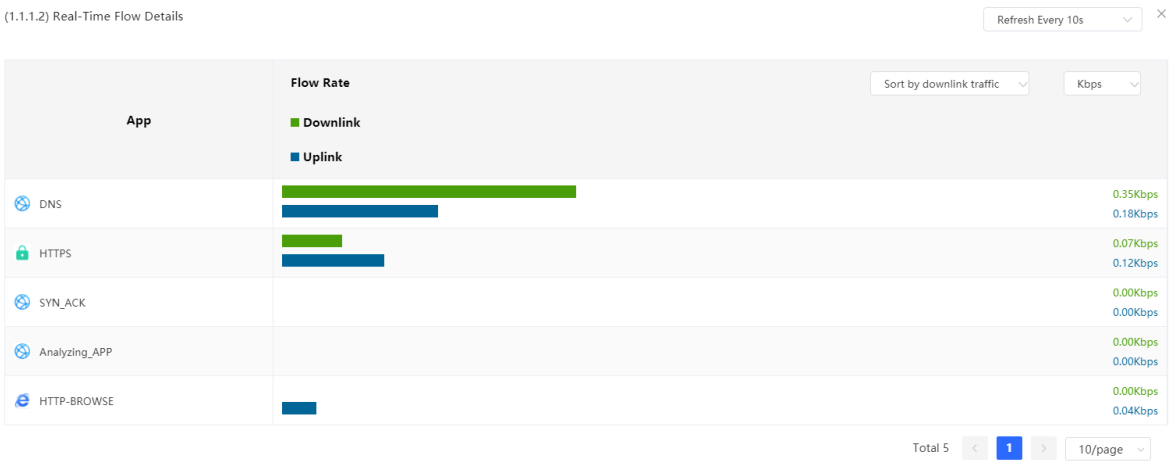
If there are multiple clients, the system displays traffic data by downlink traffic in descending order by default. The sorting mode can be switched based on uplink traffic or downlink traffic. You can set the traffic unit, number of items to be displayed on the current page, paging display, and other functions based on service requirements.



Click **Detailed**. The system displays the uplink and downlink traffic rates of various applications used by the current client. You can set the sorting mode (by downlink traffic or uplink traffic), unit, and other parameters based on service requirements.

Note

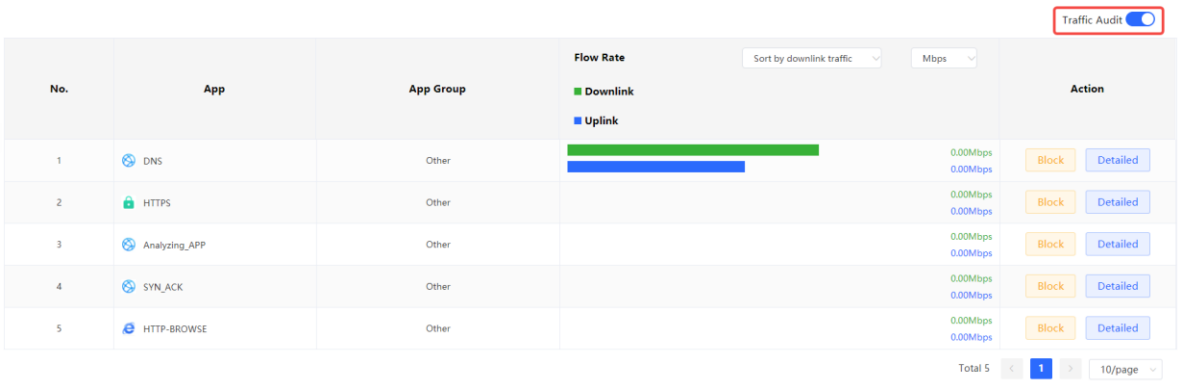
To view real-time traffic of a client, ensure that the **Traffic Audit** function is enabled on the **App Real-time Traffic** page.



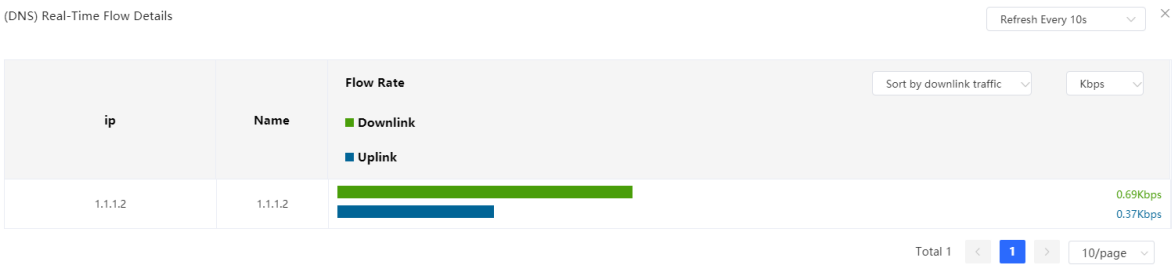
3. Viewing Real-time Traffic of an App

Click the **App Real-Time Traffic** tab and enable **Traffic Audit**. You can view the name, application group, uplink traffic, and downlink traffic of each app.

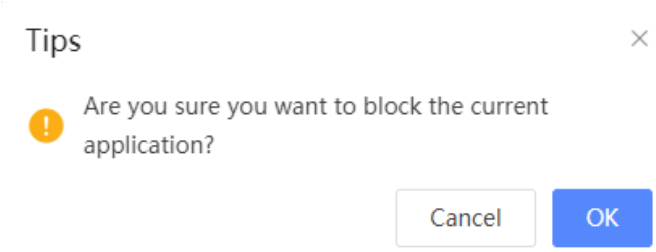
If there are multiple apps, the system displays traffic data by downlink traffic in descending order by default. The sorting mode can be switched based on uplink traffic or downlink traffic. You can set the traffic unit, number of items to be displayed on the current page, paging display, and other functions based on service requirements.



Click **Detailed**. The details of the traffic used by each user of the current application are displayed in the pop-up dialog box. You can set the sorting mode (by downlink traffic or uplink traffic), unit, and other parameters based on service requirements.



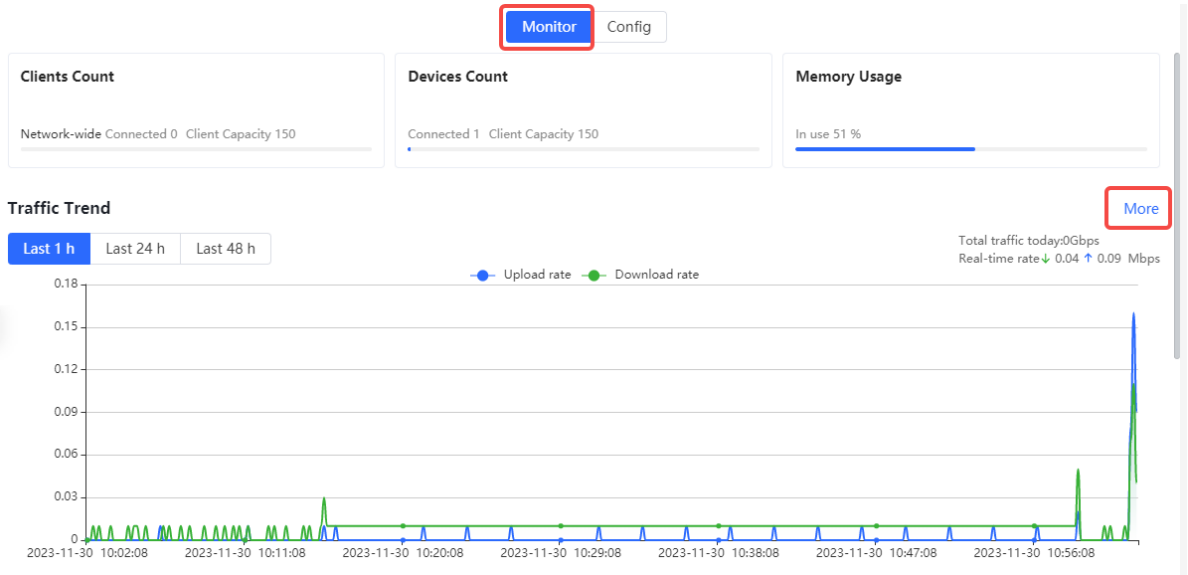
Click **Block**. In the displayed message, click **OK** to block the corresponding application.



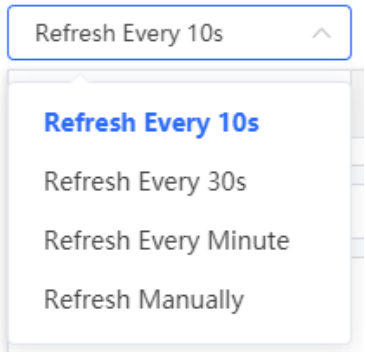
3.4.2 Viewing Historical Traffic

Choose **One-Device > Gateway > Monitor**.

Click **More** to the right of the **Traffic Trend** tab. On the gateway monitoring details page, click the **Traffic History** tab.



Select a refresh frequency to set the frequency of historical traffic refresh.



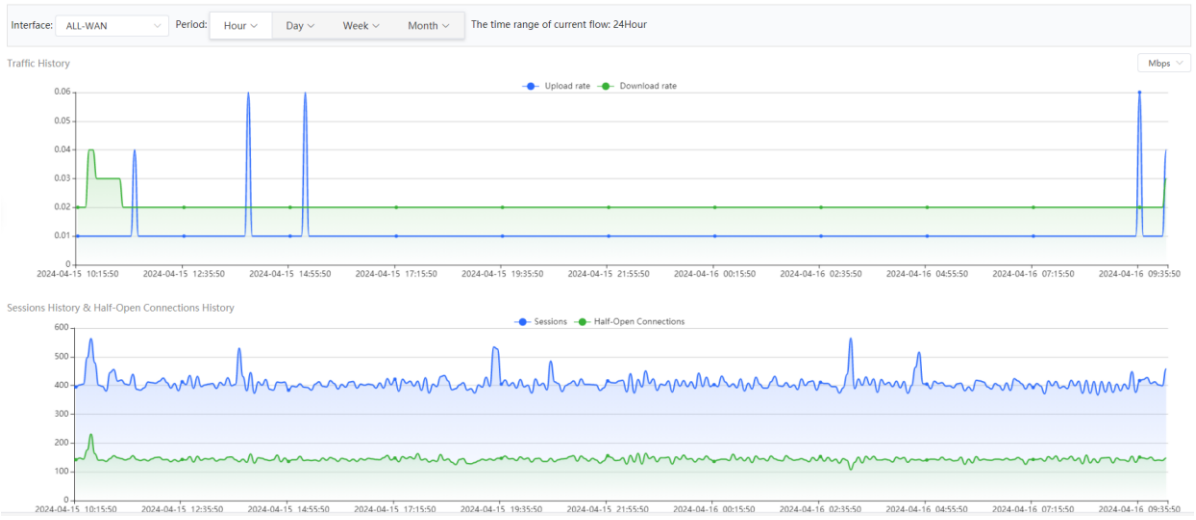
1. Viewing Historical Traffic of an Interface

(1) Click the **Traffic History** tab.

(2) Select an interface or ALL-WAN in the Interface drop-down menu.

(3) Select a time range.

(4) The system displays historical traffic, session, and half-open connection statistics of an interface or the device within a specified period.



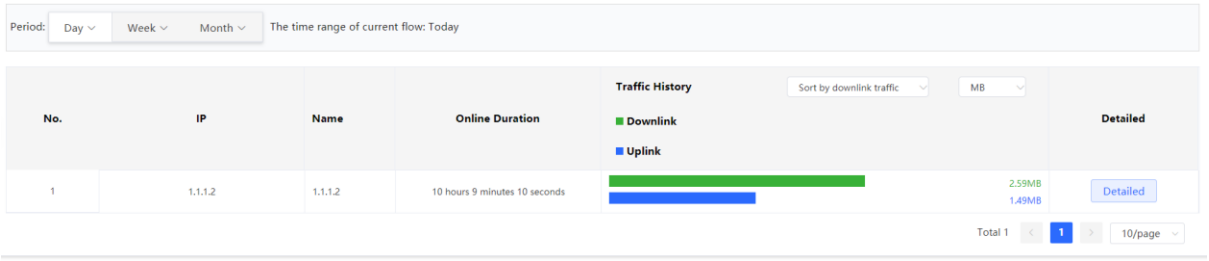
Note

Uplink traffic and downlink traffic are color-coded in the figure. You can move the cursor over a curve to view uplink traffic and downlink traffic at a certain time.

2. View Historical Traffic of a Client

Click the **User Traffic History** tab. Select a time range. You can view historical traffic data of clients today or this week on the **User Traffic History** page.

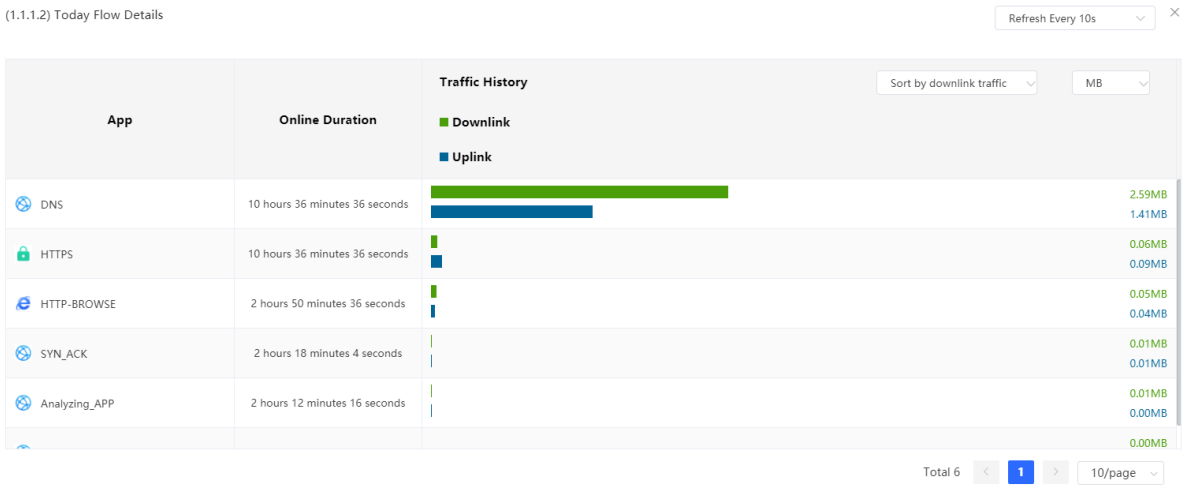
If there are multiple clients, the system displays the traffic data by downlink traffic in descending order by default. You can view the online duration, uplink traffic, and downlink traffic of each client in the time span. The sorting mode can be switched based on the uplink traffic or downlink traffic. You can set the traffic unit, number of items to be displayed on the current page, paging display, and other functions based on service requirements.



Click **Detailed**. The details of the current client's app usage, including the traffic size and online duration, are displayed in a pop-up dialog box. You can set the sorting mode (by downlink traffic or uplink traffic), unit, and other parameters based on service requirements.

Note

To view historical traffic of a client, ensure that the **Traffic Audit** function is enabled on the **App Real-Time Traffic** page.



3. View Historical Traffic of an App

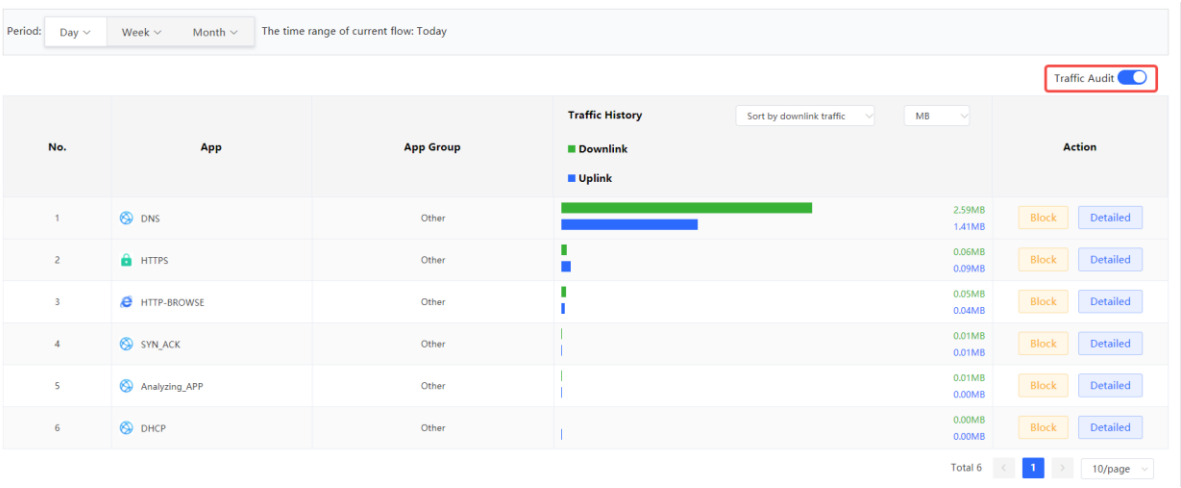
Click the **Traffic History** tab, enable the **Traffic Audit** function, and view the application historical traffic.

Note

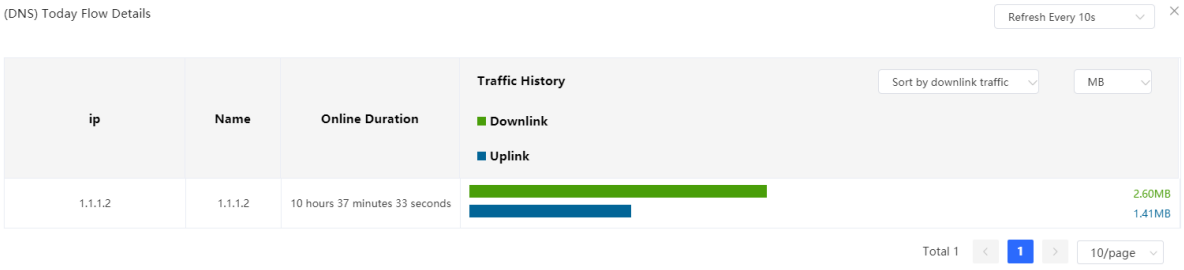
The status of **Traffic Audit** switch is consistent with that on the **App Real-Time Traffic** page. After it is enabled, the **App Real-Time Traffic** function and **App History Traffic** function are enabled.

On the **App History Traffic** page, you can view historical traffic of an application today or this week.

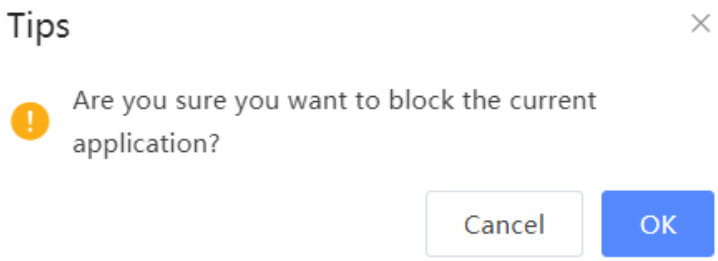
If there are multiple applications, the system displays traffic data by downlink traffic in descending order by default. You can view the name, application group, uplink traffic, and downlink traffic of each application in the time span. The sorting mode can be switched based on uplink traffic or downlink traffic. You can set the traffic unit, number of items to be displayed on the current page, paging display, and other functions based on service requirements.



Click **Detailed**. The system displays details about the traffic used by each client of the current application in a pop-up dialog box. You can set the sorting mode (by downlink traffic or uplink traffic), unit, and other parameters based on service requirements.



Click **Block**. In the displayed message, click **OK** to block the corresponding application.



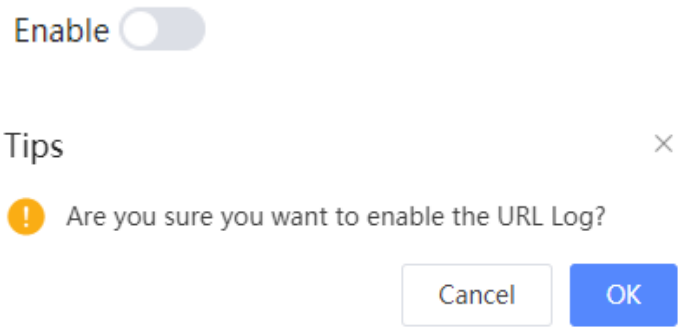
3.5 Supporting the URL Logging Function

URL logs record and display website domain names accessed by devices connected to LAN ports within a certain minute, access count, and audit results.

Choose **One-Device > Gateway > Monitor**.

Click **More** to the right of the **Traffic Trend** tab. On the page that is displayed, click the **URL Log** tab.

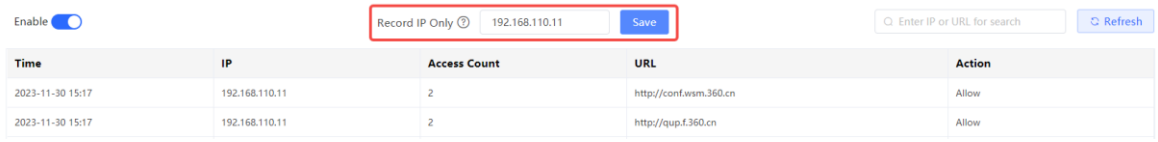
(1) Toggle on the **Enable** switch. On the pop-up dialog box, click **OK**.



(2) (Optional) Configure **record IP**.

The system records access records of all devices connected to LAN ports by default. If you need to view access records of a single device, set **record IP**.

Enter the device IP address in **record IP** and click **Save**.



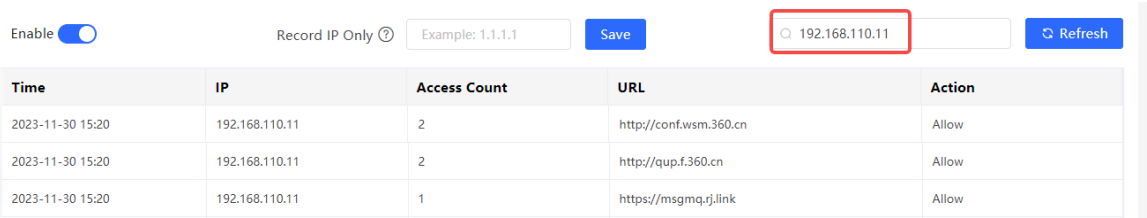
Note

If you need to restore access records of all devices connected to LAN ports, clear information in **Record IP Only** and click **Save**.

(3) Check access records.

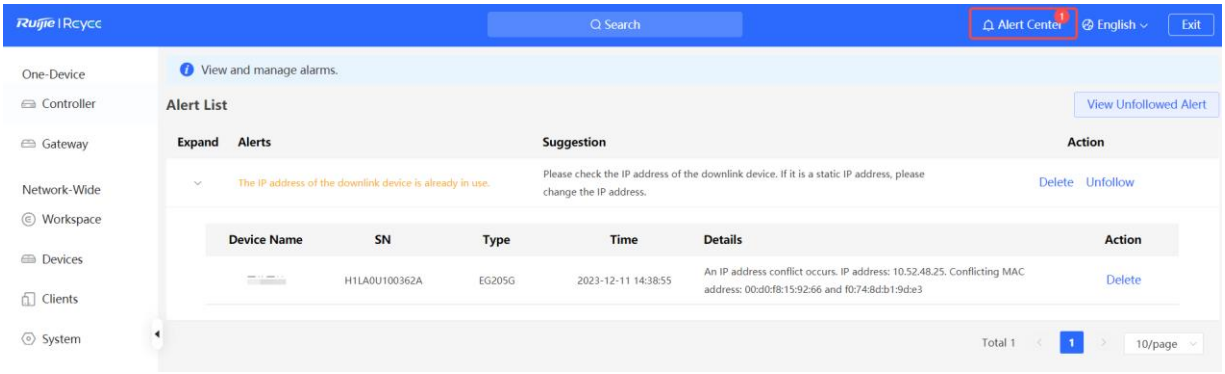
The system displays detailed access records, including the time, IP address.

You can search for access records by IP address or URL.



3.6 Processing Alerts

When a network exception occurs, the system generates an alert and provides suggested actions. Click **Alert Center** in the navigation bar to view the faulty device, alert details, and suggested actions. You can troubleshoot the fault based on the suggested actions.


Search
Alert Center
English
Exit
One-Device
Controller
Gateway
Network-Wide
Workspace
Devices
Clients
System
View and manage alarms.
Alert List
View Unfollowed Alert
Expand
Alerts
Suggestion
Action
The IP address of the downlink device is already in use.
Please check the IP address of the downlink device. If it is a static IP address, please change the IP address.
Delete
Unfollow
Device Name
SN
Type
Time
Details
Action
H1LA0U100362A
EG205G
2023-12-11 14:38:55
An IP address conflict occurs. IP address: 10.52.48.25. Conflicting MAC address: 00:d0:f8:15:92:66 and f0:74:8d:b1:9d:e3
Delete
Total 1
1
10/page

4 Network Settings

4.1 Switching the Work Mode

4.1.1 Work Mode

For details, see Section 2.4 Work Mode.

4.1.2 Self-Organizing Network Discovery

When setting the work mode, you can set whether to enable the self-organizing network discovery function. This function is enabled by default.

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 any device in the network to check information about all devices in the network. After this function is enabled, clients can maintain and manage the current network more efficiently. You are advised to keep this function enabled.

If the self-organizing network discovery function is disabled, the device will not be discovered in the network and it runs in standalone mode. 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.

Note

- In AC mode, the self-organizing network discovery function is enabled by default.
- After the self-organizing network discovery function is enabled, you can view the self-organizing role of the device on the Device Details page.
- The menus on the Web page vary depending on whether the self-organizing network discovery function is enabled. (For details, see Section 2.7 Switching the Work Mode.) Find the configuration entry for this function according to the instructions in Configuration Steps below.

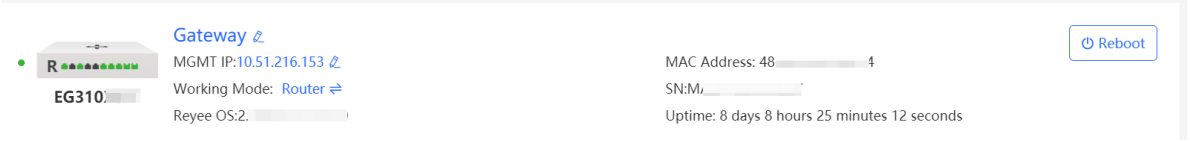
4.1.3 Configuration Steps

Choose **One-Device** > **Gateway**.

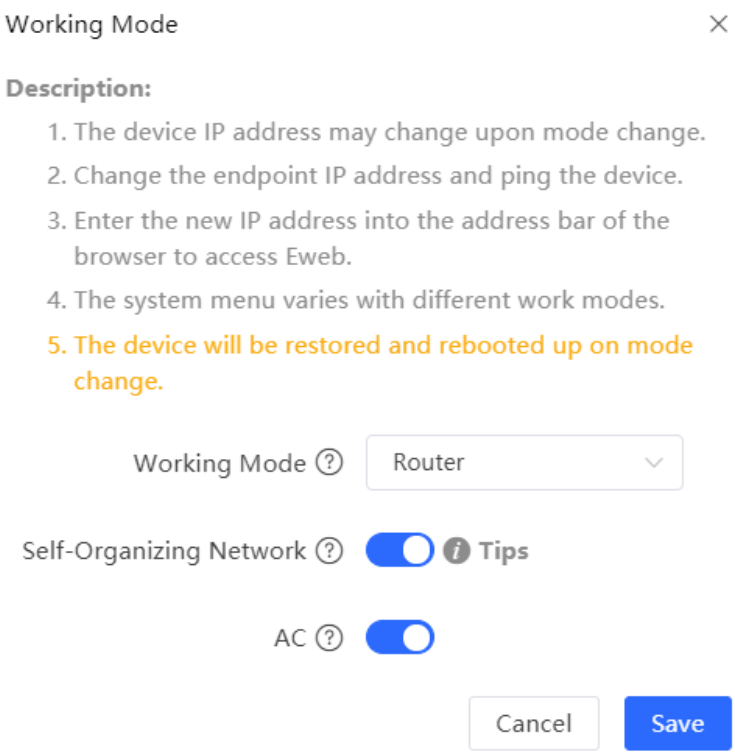
Click the current work mode to edit the work mode.

Caution

After you switch the work mode, the device will restore factory settings and restart. Please proceed with caution.



AC function switch: If a device works in the router mode and the self-organizing network discovery function is enabled, you can enable or disable the AC function. After the AC function is enabled, the device in the router mode supports the virtual AC function and can manage downlink devices. If this function is disabled, the device needs to be elected as an AC in self-organizing network mode and then manage downlink devices.

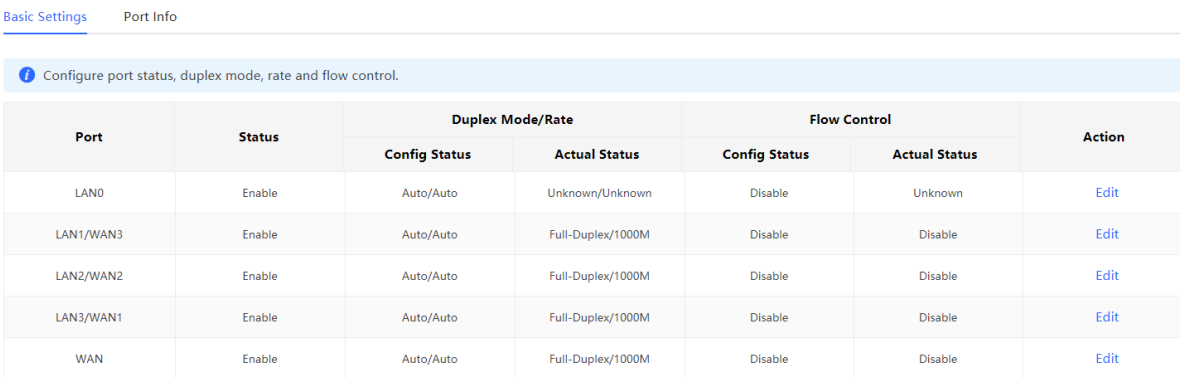


4.2 Port Settings

You can choose **Port Settings** to set port parameters and view the port information.

4.2.1 Setting the Port Parameters

Choose **One-Device > Gateway > Config > Network > Port Settings > Basic Settings**.



Port	Status	Duplex Mode/Rate		Flow Control		Action
		Config Status	Actual Status	Config Status	Actual Status	
LAN0	Enable	Auto/Auto	Unknown/Unknown	Disable	Unknown	Edit
LAN1/WAN3	Enable	Auto/Auto	Full-Duplex/1000M	Disable	Disable	Edit
LAN2/WAN2	Enable	Auto/Auto	Full-Duplex/1000M	Disable	Disable	Edit
LAN3/WAN1	Enable	Auto/Auto	Full-Duplex/1000M	Disable	Disable	Edit
WAN	Enable	Auto/Auto	Full-Duplex/1000M	Disable	Disable	Edit

(1) Choose the target port and click **Edit**.

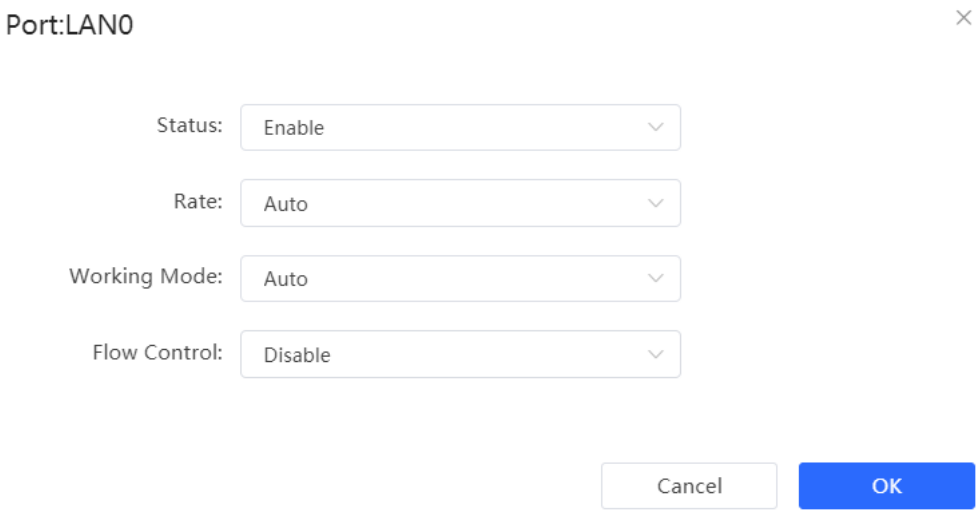


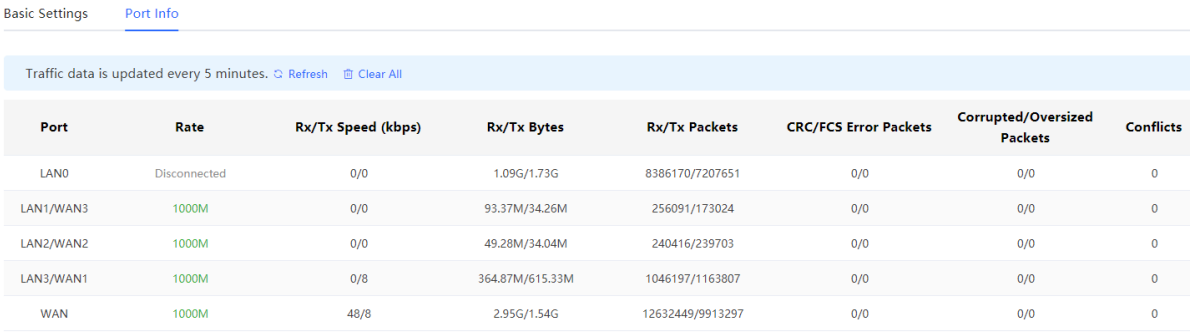
Table 4-1 Port Configuration Parameters

Parameter	Description
Status	Enable or disable the port.
Rate	Set the data transmission rate of the port. The options are **Auto**, **10M**, **100M**, and **1000M**. When selecting the port rate, ensure that the connected device can communicate at the same rate. If a device only supports a rate of 100 Mbps, but the port rate is set to 1000 Mbps, communication may fail due to rate mismatch.
Working Mode	Set the working mode of the port: ● **Auto**: The port automatically detects the working mode of the connected device and automatically selects the full-duplex or half-duplex mode based on the connected device. ● **Full-duplex**: In full-duplex mode, a port can send and receive data simultaneously, achieving bidirectional communication. ● **Half-duplex**: In half-duplex mode, a port can only send or receive data, but not both.
Flow Control	When wired ports of the device work in different rates, data blocking may occur, leading to slow network speed. Enabling port flow control helps relieve the data congestion.

(2) Set the port parameters and click **OK**.

4.2.2 Viewing the Port Information

Choose **One-Device > Gateway > Config > Network** > **Port Settings** > **Port Info**.



Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
LAN0	Disconnected	0/0	1.09G/1.73G	8386170/7207651	0/0	0/0	0
LAN1/WAN3	1000M	0/0	93.37M/34.26M	256091/173024	0/0	0/0	0
LAN2/WAN2	1000M	0/0	49.28M/34.04M	240416/239703	0/0	0/0	0
LAN3/WAN1	1000M	0/8	364.87M/615.33M	1046197/1163807	0/0	0/0	0
WAN	1000M	48/8	2.95G/1.54G	12632449/9913297	0/0	0/0	0

4.3 Configuring the WAN Ports

Choose **One-Device > Gateway > Config > Network** > **WAN**.

You can configure multi-line access for the device to allow multiple lines to work simultaneously. After you switch to multi-line access, you need to specify the egress provider of the lines and set the load balancing mode, in addition to setting basic network parameters for the WAN interfaces.

Caution

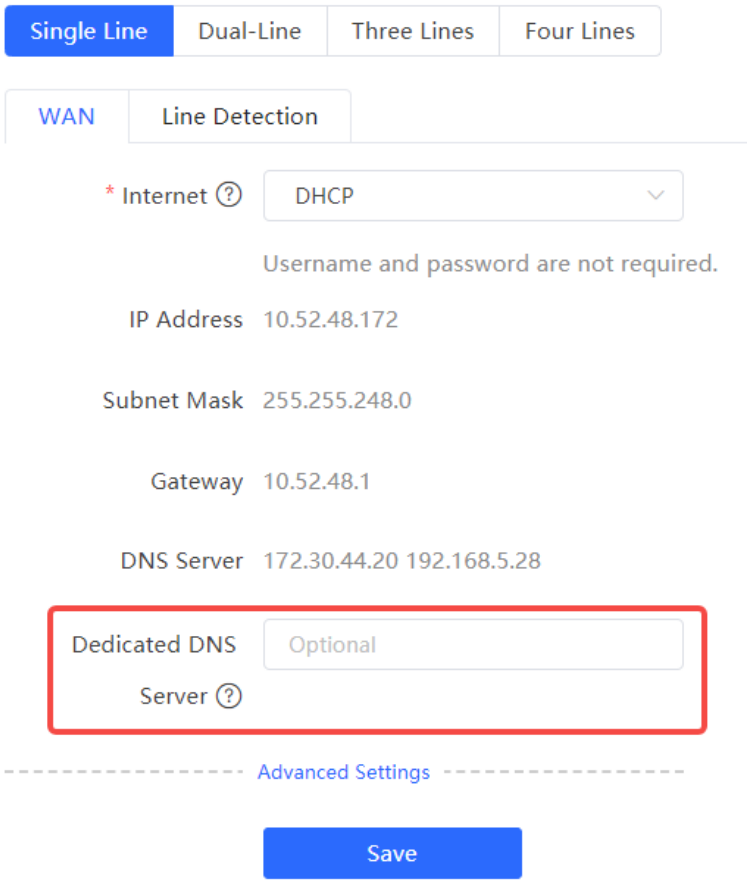
The number of lines supported varies with the product. The actual configuration prevails.

4.3.1 Configuring the Internet Access Mode

Choose **One-Device > Gateway > Config > Network** > **WAN**.

The device can access the WAN in one of the following three methods: static IP, DHCP, and PPPoE dialing. Select a proper method based on the actual broadband line type. For details, see Section 2.5 Configuration Wizard (Router Mode).

When the Internet access mode is not **DHCP** or **PPPoE**, you can specify a DNS server to ensure that the device can correctly parse domain names and access Internet resources, thereby improving the access speed and security.

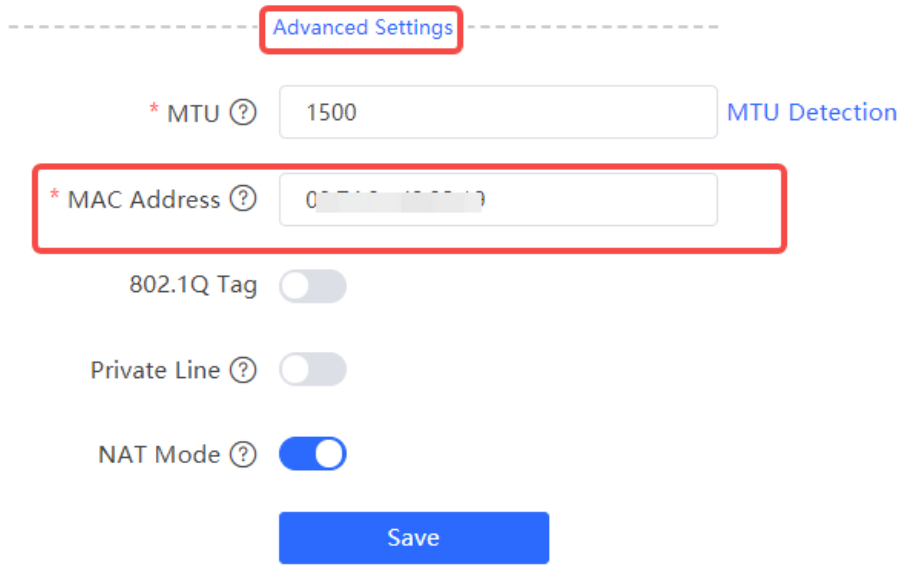


4.3.2 Modifying the MAC Address

Choose **One-Device > Gateway > Config > Network > WAN**.

Sometimes, the provider restricts Internet access of devices with unknown MAC addresses out of security considerations. In this case, you can change the MAC addresses of the WAN interfaces to valid MAC addresses.

Select the target WAN interface. Click **Advanced Settings**, enter a MAC address, and click **Save**. You do not need to modify the default MAC address unless otherwise specified.

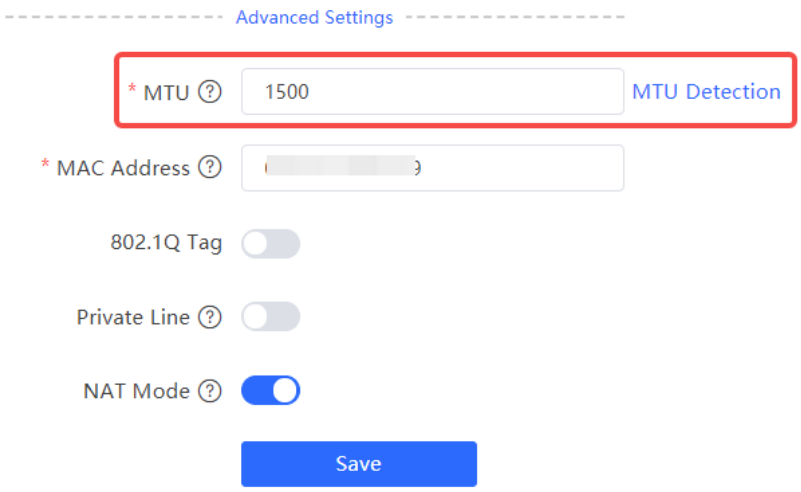


4.3.3 Modifying the MTU

Choose **One-Device > Gateway > Config > Network > WAN**.

1. Modifying the MTU

MTU specifies the maximum transmission unit allowed to pass a WAN interface. By default, the MTU of a WAN interface is 1500 bytes. Sometimes, large data packets are limited in transmission speed or prohibited in the ISP network, leading to slow network speed or even network disconnection. If this occurs, you can click **Advanced Settings**, set the MTU to a smaller value.

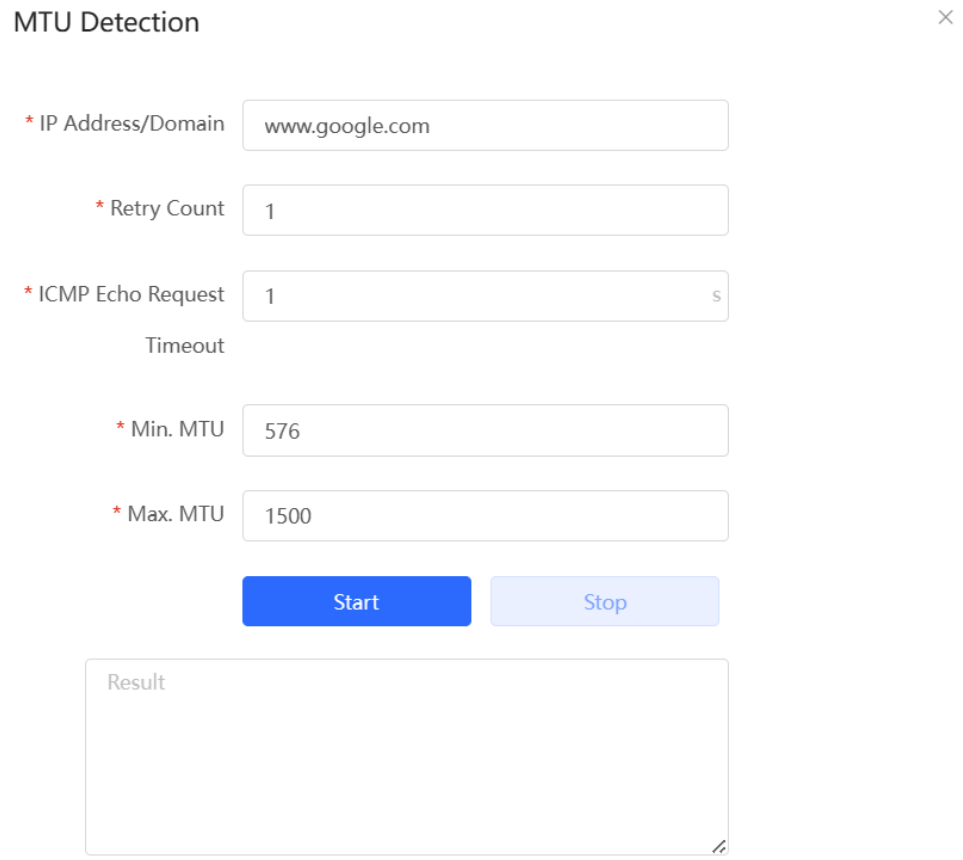


If the MTU value is unknown, click **MTU Detection** to configure the one-click MTU detection, and adjust the MTU settings based on the results obtained from MTU detection.

2. Detecting the MTU

Click **MTU Detection** to configure the one-click MTU detection to determine the MTU between two communication devices.

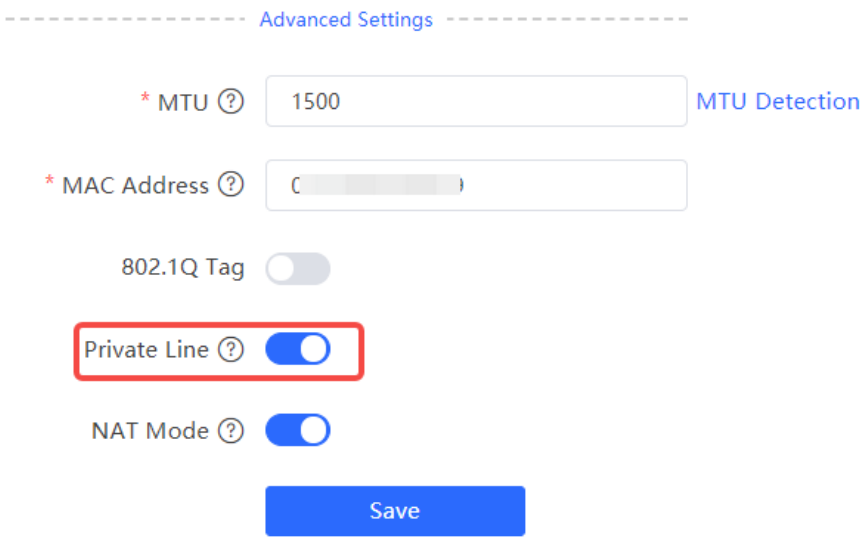
Enter the destination IP/domain name, retry count, ICMP echo request timeout, minimum MTU, maximum MTU, and click **Start** to start the detection.



4.3.4 Configuring the Private Line

Choose **One-Device > Gateway > Config > Network > WAN**.

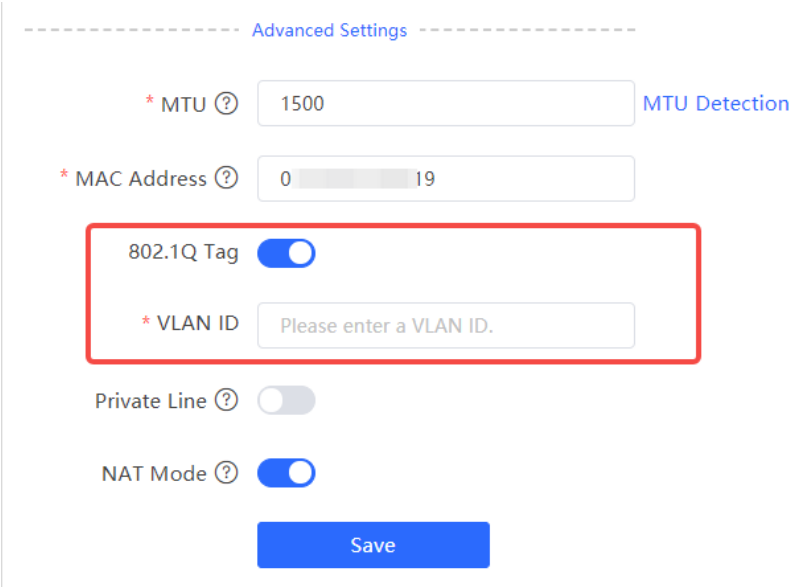
Click **Advanced Settings**, turn on **Private Line** and determine whether to set the current WAN line as a private line. Generally, private lines are used for access to specific internal networks but not the Internet. Private lines provide higher network security.



4.3.5 Configuring the VLAN Tag

Choose **One-Device > Gateway > Config > Network > WAN**.

Some ISPs require that packets transmitted to their networks carry VLAN IDs. In this case, you can click **Advanced Settings**, enable the **802.1Q Tag** function and set a **VLAN ID** and **Priority** for the WAN interface. By default, the VLAN tag function is disabled. You are advised to keep the VLAN tag function disabled unless otherwise specified.

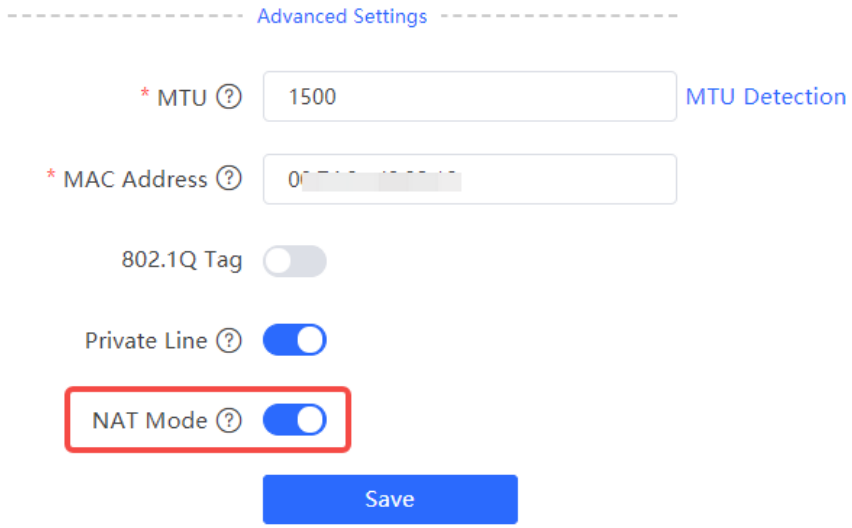


4.3.6 Configuring NAT Mode

Choose **One-Device > Gateway > Config > Network > WAN**.

When an intranet needs to communicate with an extranet, Network Address Translation (NAT) must be configured to convert the private IP address into a globally unique IP address, so that the private network can access the public network.

Click **Advanced Settings**, toggle on **NAT Mode** to enable the NAT mode. When the NAT mode is disabled, this router operates in router mode to forward data packets, enabling mutual access between hosts connected to the LAN and the WAN interfaces of this router.



Caution

Disabling NAT mode may potentially impact the functionality of the self-organizing network (SON) feature.

4.3.7 Configuring the Multi-Line Load Balancing Mode

Choose **One-Device** > **Gateway** > **Config** > **Network** > **Single Line/Dual-Line/Three Lines/Four Lines** > **WAN** > **Load Settings**.

When multiple links are available, some traffic is forwarded along the link selected based on the address library and the remaining traffic is distributed to other links in load balancing mode.

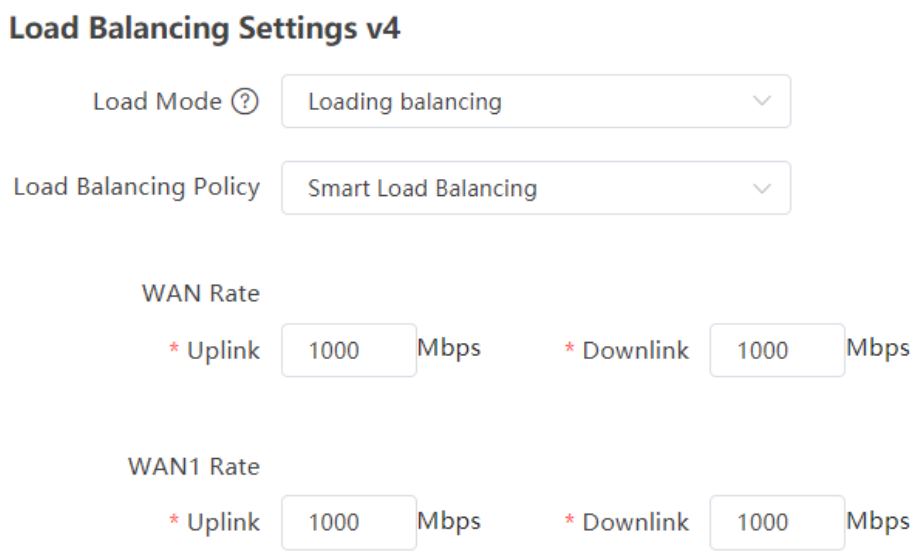
Table 4-2 Load balancing modes

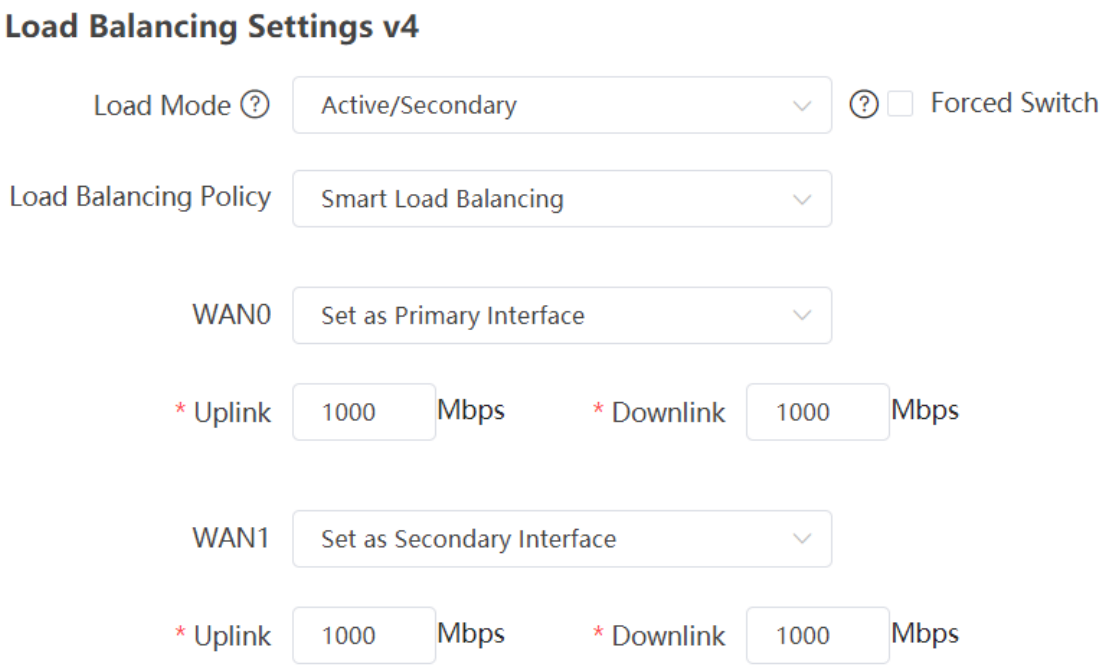
Load Balancing Mode	Description
Loading balancing	The traffic will be distributed across multiple links according to the weight of each WAN interface. Larger traffic will be distributed to the WAN interface with a higher weight. When you select this mode, you must specify the weight of each WAN interface. For example, if the weight of WAN and WAN 1 ports is set to 3 and 2 respectively, then, 60% of the total traffic will be routed over WAN and 40% over WAN 1.

Load Balancing Mode	Description
Active/Secondary	All traffic is routed over the primary interface. Once the primary interface fails, traffic will be switched over to the secondary interface. If there are multiple primary or secondary interfaces, the weight of these interfaces must be set. (See balanced mode.)
Forced Switch	With **Load Mode** switched from **Load balancing** to **Active/Secondary**, if **Forced Switch** is not selected, traffic of new connections will be routed through the specified primary interface, while the egress for the traffic of existing connections remains unchanged. When **Forced Switch** is selected, traffic of both new and existing connections will be routed to the primary interface.

The system supports IPv4 and IPv6 multi-link load balancing. IPv4 multi-link load balancing is enabled by default, while IPv6 multi-link load balancing needs to be enabled manually.

1. Configuring IPv4 Multi-Link Balancing





(1) Select a load balancing mode from the **Load Mode** drop-down list.

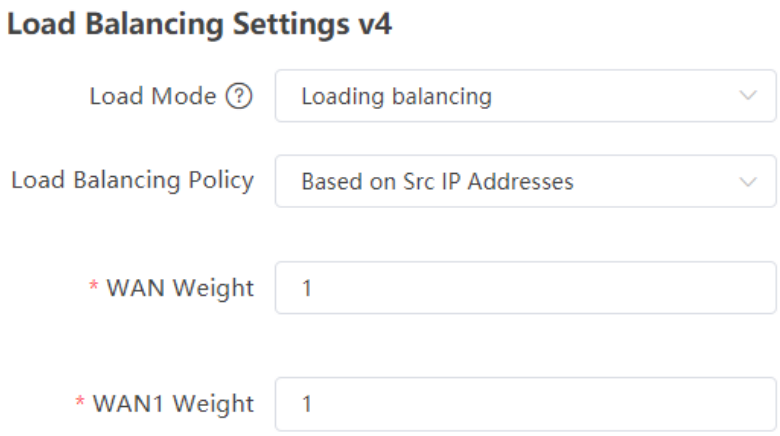
(2) Select a loading balancing policy from the **Load Balancing Policy** drop-down list.

Table 4-3 Description of Load Balancing Policies (IPv4)

Load Balancing Policy	Description
Based on Connections	After you enable this policy, the traffic is routed over multiple links based on the links. Packets with the same source IP address, destination IP address, source port, destination port, and protocol are routed over the same link.
Based on Src IP Address	After you enable this policy, the traffic is routed over multiple links based on the source IP address. The traffic from the same user (same source IP address) will be routed to the same interface. This policy prevents traffic from the same user from being routed to different links, lowering the risks of network access exceptions.
Based on Src and Dest IP Address	After you enable this policy, the traffic is routed over multiple links based on the source IP address and destination. The traffic of the same source IP address and destination IP address will be routed to the same interface.
Smart Load Balancing	After you enable this feature, the traffic is routed over multiple links based on the link bandwidth, the actual loads of the links, application recognition and traffic prediction.

(3) Set the uplink and downlink bandwidths or the weight for each WAN interface.

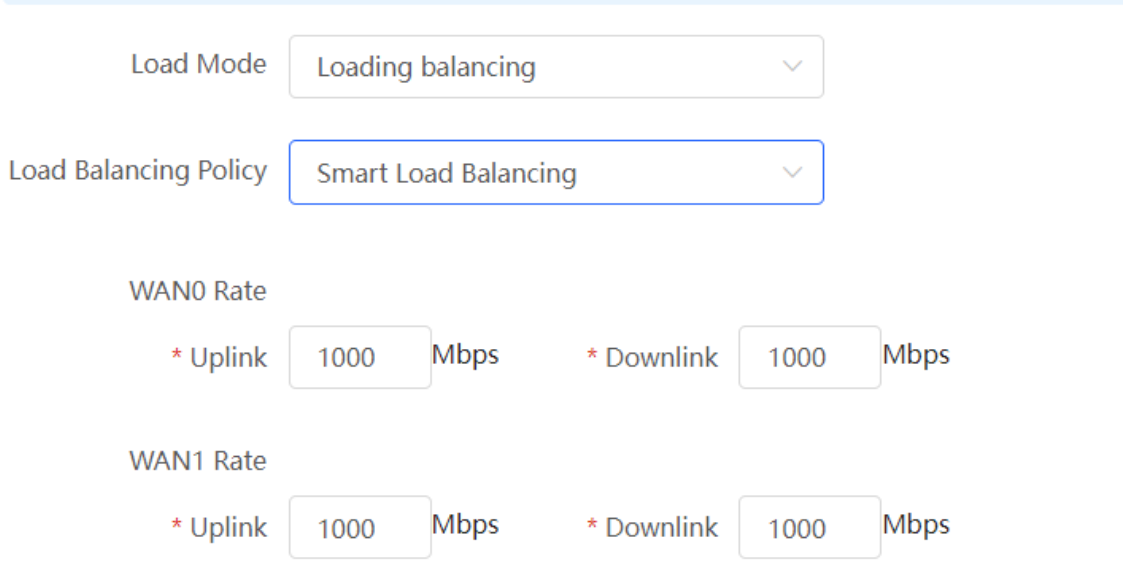
- When the load balancing policy is set to **Based on Connections**, **Based on Src IP Address**, or **Based on Src and Dest IP Address**, a weight must be set for each WAN interface.



Note

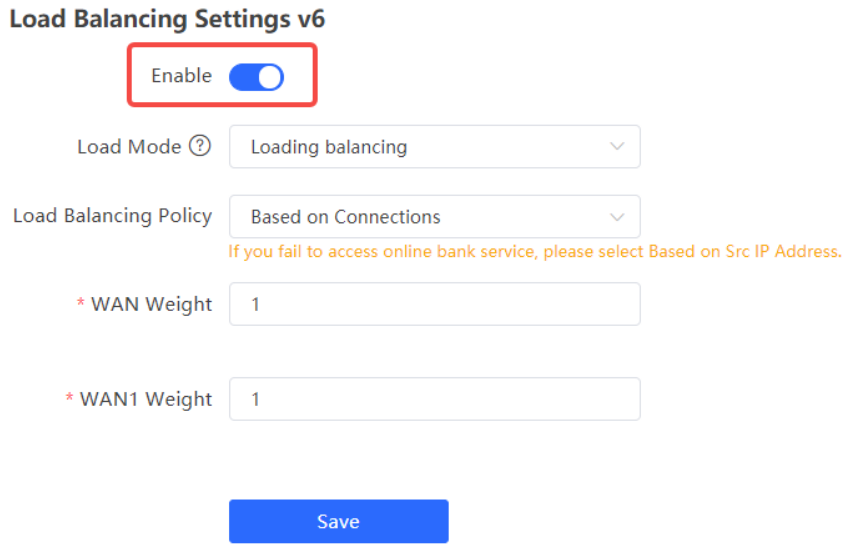
The higher the value of the weight, the more traffic is directed to the WAN interface.

- When the load balancing policy is set to **Smart Load Balancing**, the uplink and downlink bandwidths must be set for each WAN interface.



(4) Click **Save**.

2. Configuring IPv6 Multi-Link Balancing



(1) Toggle on **Enable** to enable the IPv6 multi-link load balancing mode.

(2) Select a load balancing mode from the **Load Mode** drop-down list.

(3) Select a loading balancing policy from the **Load Balancing Policy** drop-down list.

Table 4-4 Description of Load Balancing Policies (IPv6)

Load Balancing Policy	Description
Based on Connections	After you enable this policy, the traffic is routed over multiple links based on the links. Packets with the same source IP address, destination IP address, source port, destination port, and protocol are routed over the same link.
Based on Src IP Address	After you enable this policy, the traffic is routed over multiple links based on the source IP address. The traffic from the same user (same source IP address) will be routed to the same interface. This policy prevents traffic from the same user from being routed to different links, lowering the risks of network access exceptions.
Based on Src and Dest IP Address	After you enable this policy, the traffic is routed over multiple links based on the source IP address and destination. The traffic of the same source IP address and destination IP address will be routed to the same interface.

(4) Set a weight for each WAN interface.

The valid range of weight is 1 to 100000.

Note

The higher the value of the weight, the more traffic is directed to the WAN interface.

(5) Click **Save**.

4.3.8 Configuring Link Detection

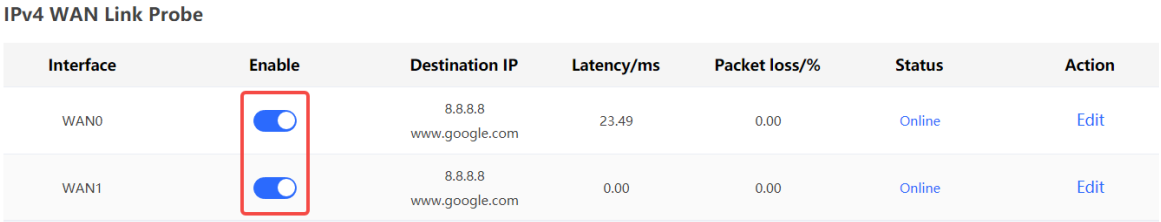
Choose **One-Device > Gateway > Config > Network** > **Single Line/Dual-Line/Three Lines/Four Lines** > **Line Detection**.

After configuring multiple WAN interfaces, use the link detection function to check whether lines are connected to the external network. If the network is down, the system does not select a route based on the interface, such as load balancing, policy-based routing, and ISP routing.

The system supports IPv4 and IPv6 WAN link detection, which can be enabled separately.

1. Configuring IPv4 WAN Link Detection

(1) On the **IPv4 WAN Link Probe** page, select a WAN interface, and toggle on **Enable** to enable IPv4 WAN link detection.



(2) In the WAN interface list, select a WAN interface for link detection, and click **Edit**.

(3) Configure the parameters of the link detection function, and click **OK**.

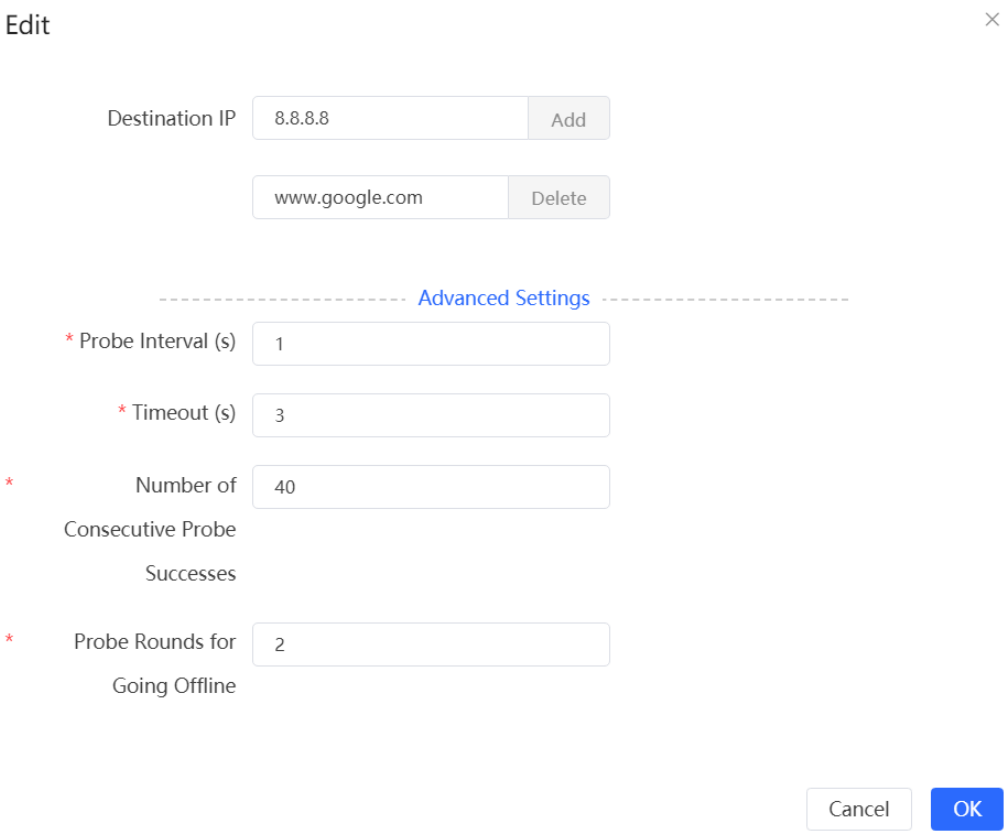


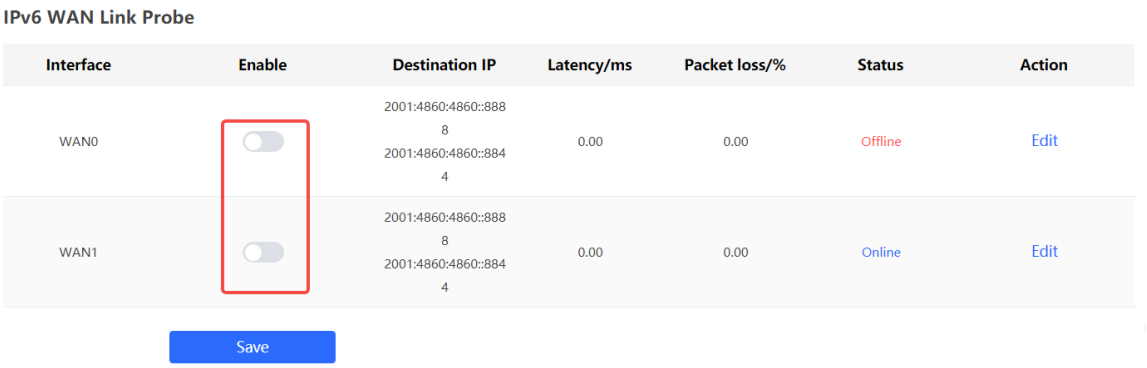
Table 4-5 Description of Link Detection (IPv4)

Parameter	Description
Destination IP	The destination IP address to which the system sends ping messages. You can set up to three destination IP addresses. The system sends ping messages to one of the IP addresses randomly during detection.
Probe Interval (s)	Interval for the system to perform connectivity detection. The default value is 1 second.
Timeout (s)	The maximum timeout period during which the device waits for a response after sending a ping message to the destination IP address. If no response is received within this time, the probe packet is marked as timed out. The default value is 3 seconds.
Number of Consecutive Probe Successes	The system periodically sends a ping message to a detection destination IP address at the specified interval. If the ping succeeds and the number of consecutive successful pings reaches the set number of **Number of Consecutive Probe Successes**, the WAN interface is set to be online.
Probe Rounds for Going Offline	The system periodically sends a ping message to a detection destination IP address at the specified interval. If the ping fails and the number of consecutive unsuccessful pings reaches the set number of **Probe Rounds for Going Offline**, the WAN interface is set to be offline.

(4) Click **OK**.

2. Configuring IPv6 WAN Link Detection

(1) On the **IPv6 WAN Link Detection** page, toggle on **Enable** to enable IPv6 WAN link detection.



(2) In the WAN interface list, select a WAN interface for link detection, and click **Edit**.

(3) Configure the link detection parameters, and click **OK**.

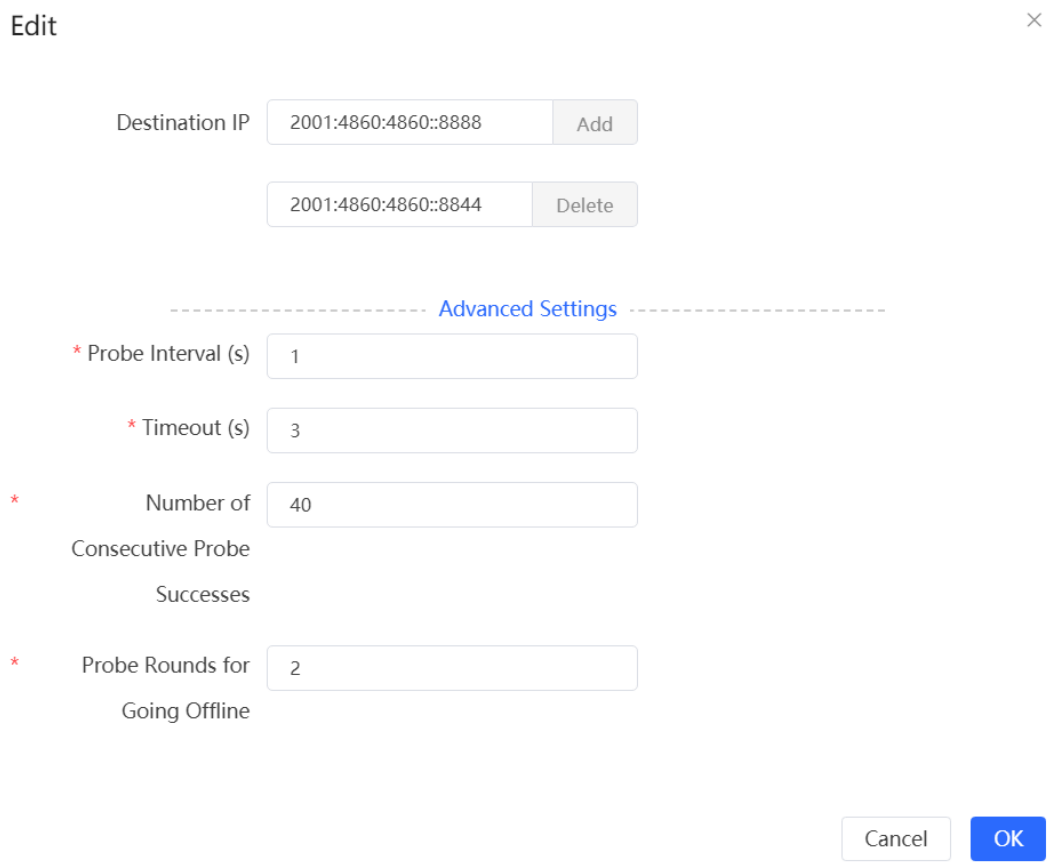


Table 4-6 Description of Link Detection (IPv6)

Parameter	Description
Destination IP	The destination IP address (IPv6) to which the system sends ping messages. You can set up to three destination IP addresses. The system sends ping messages to one of the IP addresses randomly during detection.
Probe Interval (s)	Interval for the system to perform connectivity detection. The default value is 1 second.
Timeout (s)	The maximum timeout period during which the device waits for a response after sending a ping message to the destination IP address. If no response is received within this time, the probe packet is marked as timed out. The default value is 3 seconds.
Number of Consecutive Probe Successes	The system periodically sends a ping message to a detection destination IP address at the specified interval. If the ping succeeds and the number of consecutive successful pings reaches the set number of **Number of Consecutive Probe Successes**, the WAN interface is set to be online.

Parameter	Description
Probe Rounds for Going Offline	The system periodically sends a ping message to a detection destination IP address at the specified interval. If the ping fails and the number of consecutive unsuccessful pings reaches the set number of **Probe Rounds for Going Offline**, the WAN interface is set to be offline.

(4) Click **Save**.

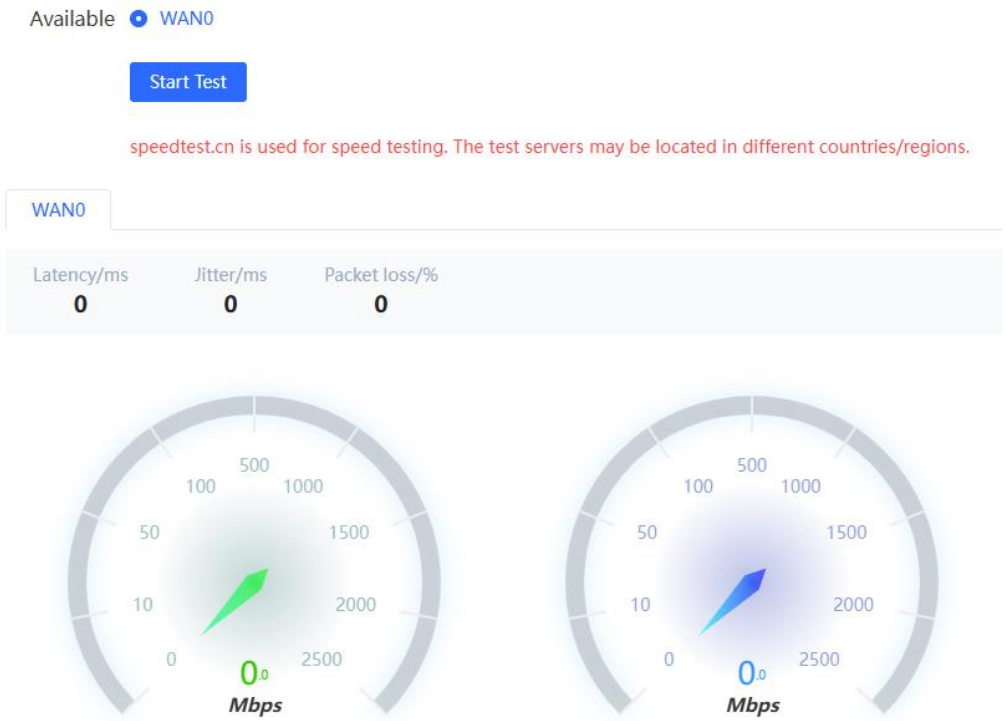
4.4 Configuring Speed Test

Note

Only RG-EG3XX series devices (such as RG-EG310GH-E) and RG-EG1510XS support this function.

You can use the rate test function to easily monitor the transmission rate of individual ports. In the case of ports with low transmission rates, you can identify and address potential issues to ensure that service quality remains high.

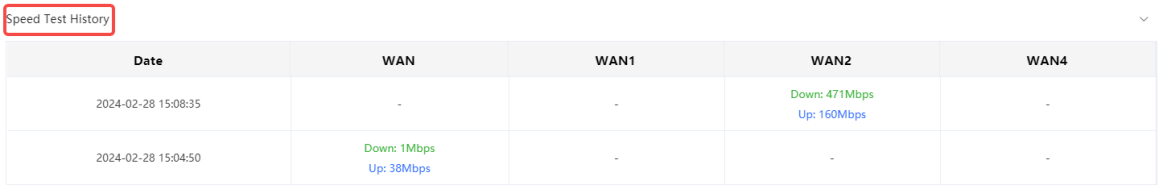
Choose **One-Device > Gateway > Config > Network** > **Speed Test**.



(1) Select the WAN interface to be tested. You can click **Select All** to select all WAN interfaces for the rate test.

(2) Click **Start Test**.

(3) After the rate test is complete, the system will display the test results, including latency, jitter, and packet loss.

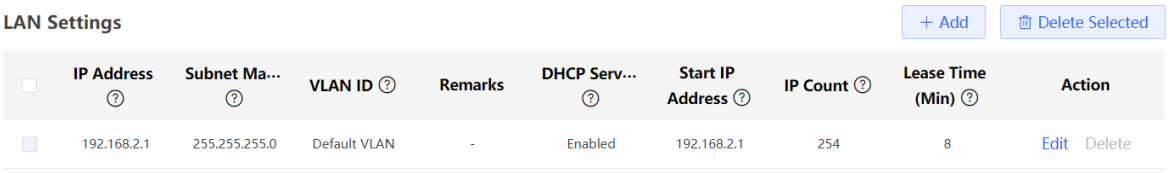


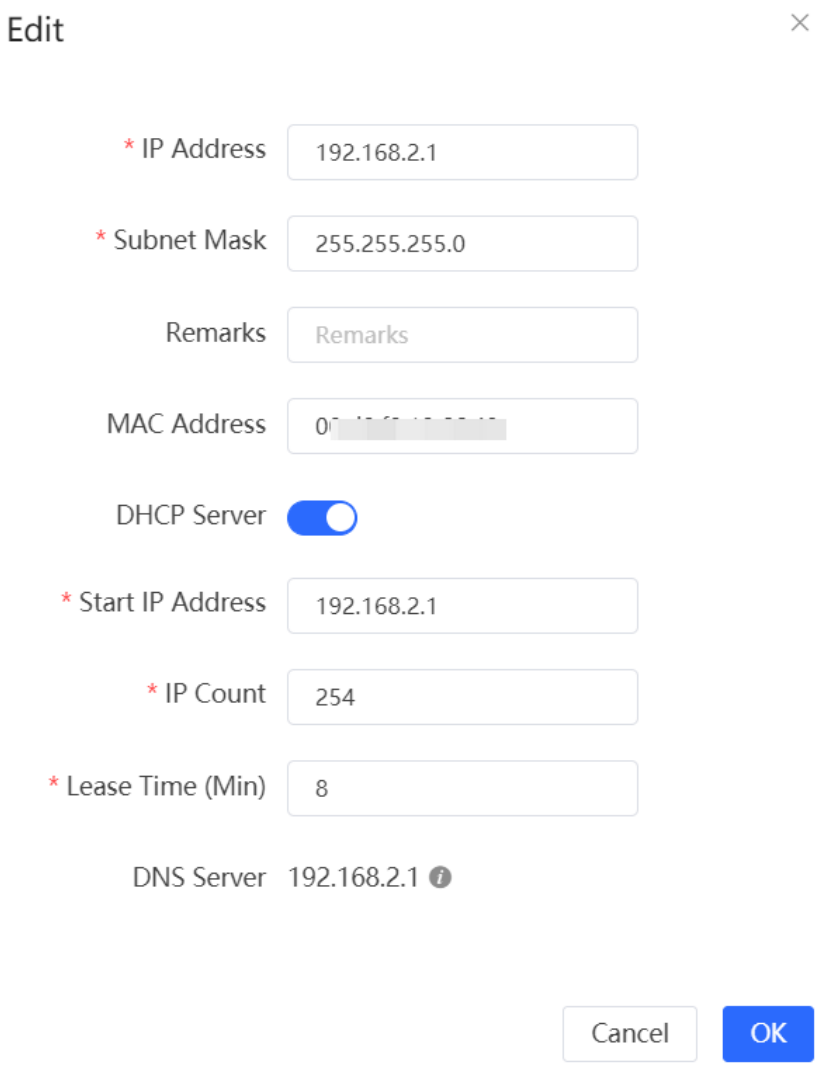
4.5 Configuring the LAN Ports

4.5.1 Modifying the LAN Port IP Address

Choose **One-Device** > **Gateway** > **Config** > **Network** > **LAN** > **LAN Settings**.

Click **Edit**. In the dialog box that appears, enter the IP address and subnet mask, and then click **OK**. After you modify the LAN port IP address, you need to enter the new IP address in the browser to log in to the device again before you can configure and manage this device.



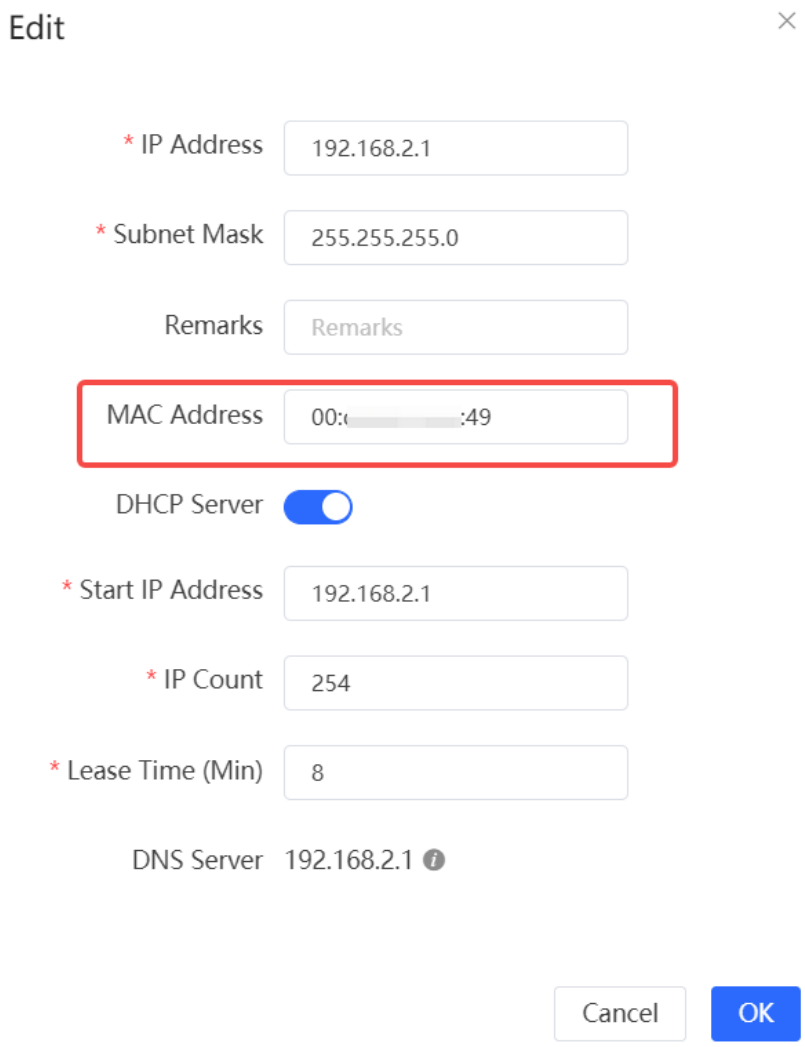


4.5.2 Modifying the MAC Address

Choose **One-Device** > **Gateway** > **Config** > **Network** > **LAN** > **LAN Settings**.

If a static Address Resolution Protocol (ARP) entry (binding between IP address and MAC address of the gateway) is configured to prevent ARP attacks to clients in the LAN, the gateway IP address remains unchanged but its MAC address changes when the gateway is replaced. As a result, the client may fail to learn the gateway MAC address. You can modify the static ARP entry of the client to prevent this problem. You can also change the LAN port MAC address of the new device to the MAC address of the original device to allow clients in the LAN to access the Internet normally.

Click **Edit**. In the dialog box that appears, enter the MAC address, and then click **OK**. You do not need to modify the default LAN port MAC address unless otherwise specified.



4.6 Configuring VLAN

4.6.1 VLAN Overview

Virtual Local Area Network (VLAN) is a communication technology that divides a physical LAN into multiple logical broadcast domains. Each VLAN has independent broadcast domains. Hosts in the same VLAN can directly communicate with each other, while hosts in different VLANs cannot as they are isolated at Layer 2. Compared with traditional Ethernet, VLAN has the following advantages:

- Control broadcast storms: Broadcast packets can only be forwarded inside a VLAN. This saves bandwidth as the performance of a VLAN is not affected by broadcast storms of other VLANs.
- Enhance LAN security: As a VLAN is divided into multiple broadcast domains, packets of different VLANs in a LAN are isolated. Different VLAN users cannot directly communicate, enhancing network security.
- Simplify network management: The VLAN technology can be used to divide the same physical network into different logical networks. When the network topology changes, you only need to modify the VLAN configuration, simplifying network management.

4.6.2 Creating a VLAN

Note

RG-EG1XX series devices, RG-EG2XX series devices, RG-EG3XX series devices and RG-EG1510XS support a maximum of 16, 32, 64 and 128 VLANs respectively.

Choose **One-Device** > **Gateway** > **Config** > **Network** > **LAN** > **LAN Settings**.

A LAN can be divided into multiple VLANs. Click **Add** and create a VLAN.

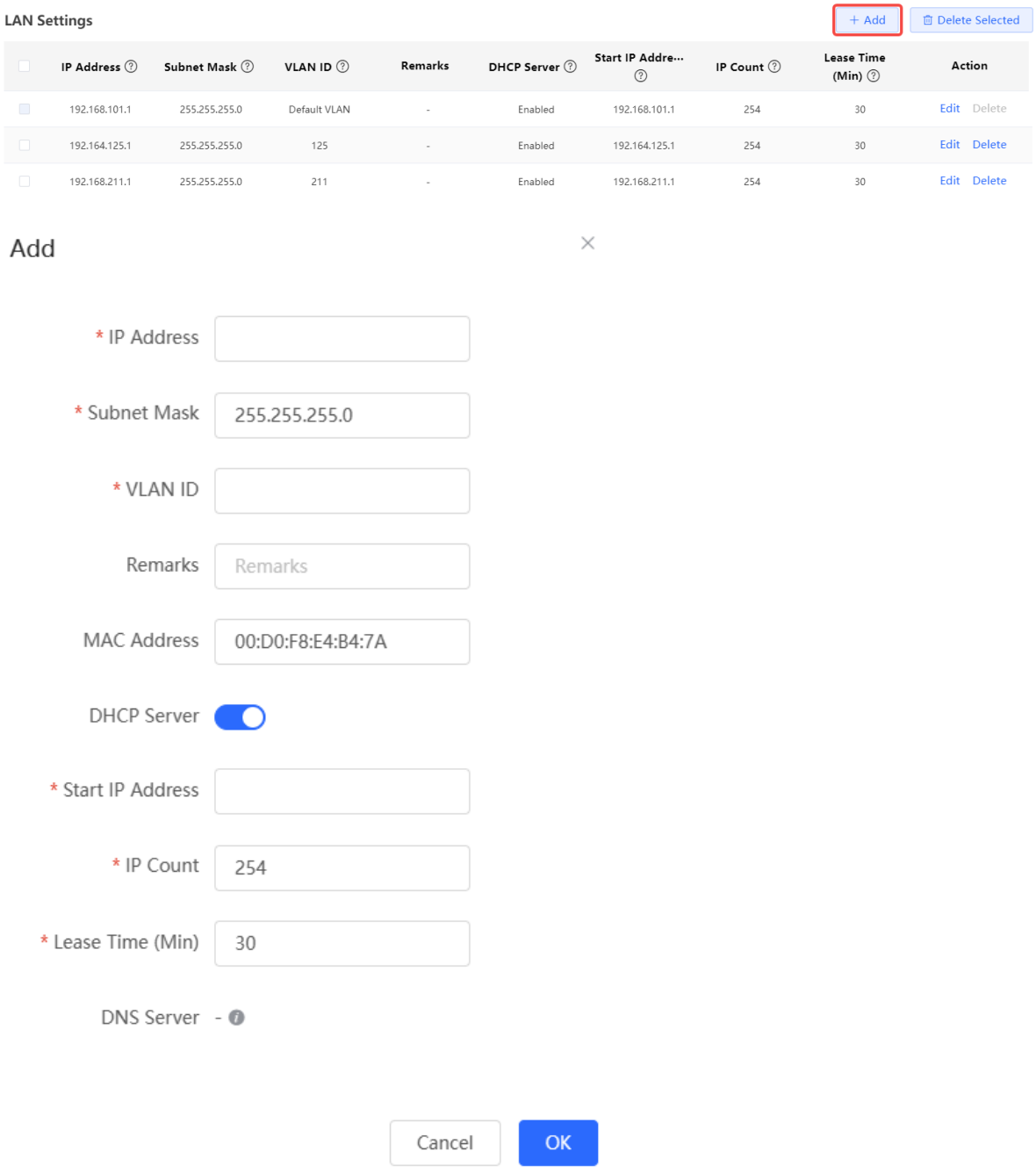


Table 4-7 VLAN Configuration

Parameter	Description
IP Address	Configure an IP address for the VLAN interface. This IP address is used as the default gateway for the LAN devices that need to access the Internet.
Subnet Mask	Configure an IP address subnet mask for the VLAN interface.
VLAN ID	Configure the VLAN ID.
Remarks	Enter the VLAN description.
MAC Address	Configure an MAC address for the VLAN interface.
DHCP Server	Enable the DHCP server function. After this function is enabled, devices in the LAN can automatically obtain IP addresses. You also need to specify the start address for IP address allocation by the DHCP server, the number of IP addresses that can be allocated, and the address lease. You can also configure DHCP Options. For details, see Section 4.9.3 Configuring the DHCP Server.

Caution

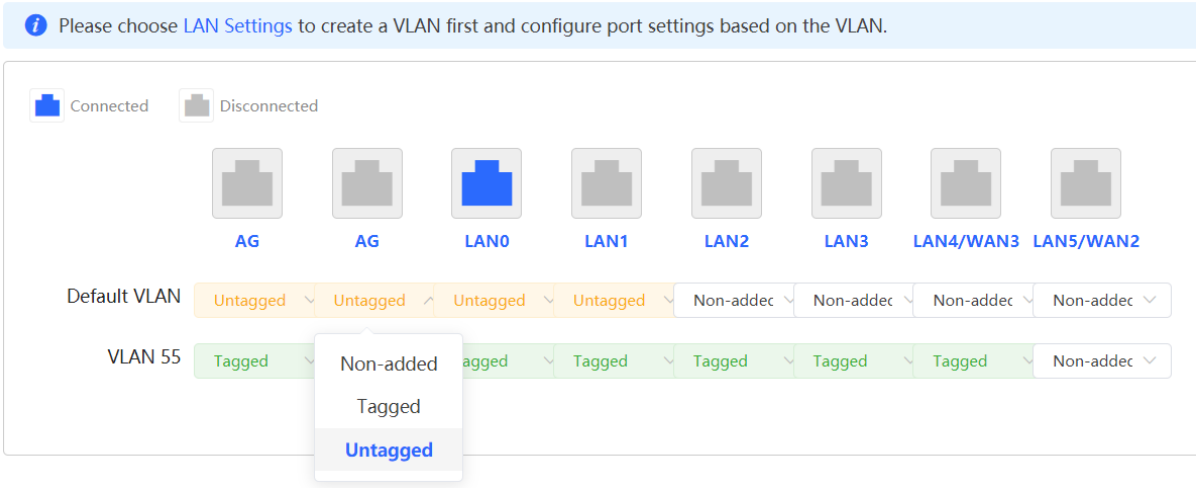
The VLAN configuration is associated with the uplink configuration. Exercise caution when you perform this operation.

4.6.3 Configuring a Port VLAN

Choose **One-Device** > **Gateway** > **Config** > **Network** > **Port VLAN**.

This page displays the VLAN division of the current port. Create VLANs on the **LAN Settings** page and then configure the port based on the VLANs on this page. For details, see Section 4.6.2 Creating a VLAN.

Click the check box under a port and select the relationship between VLAN and port from the drop-down list box.



- **Untagged**: Configure the VLAN as the native VLAN of the port. When the port receives packets from the specified VLAN, the port removes the VLAN ID before forwarding the packets. When the port receives packets without a VLAN ID, the port adds this VLAN ID to the packets before forwarding them. You can set only one VLAN of the port to **Untagged**.
- **Tagged**: Configure the port to allow packets with this VLAN ID to pass. This VLAN is not the native VLAN. When the port receives packets from the specified VLAN, it forwards the packets with the original VLAN ID.
- **Non-added**: Configure the port to deny packets with this VLAN ID to pass. For example, if you set VLAN 10 and VLAN 20 to **Non-added** for port 2, port 2 will not receive packets from VLAN 10 and VLAN 20.

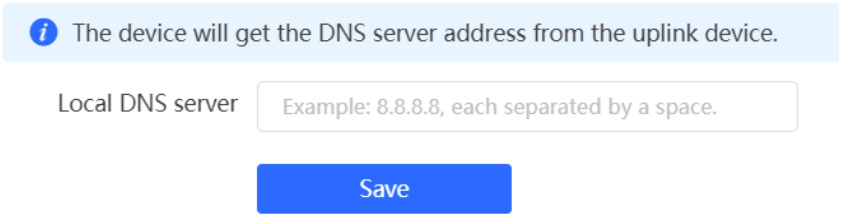
4.7 Configuring DNS

4.7.1 Local DNS

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **DNS** > **Local DNS**.

When the WAN interface runs DHCP or PPPoE protocol, the device automatically obtains the DNS server address. If the upper-layer device does not deliver the DNS server address or the DNS server needs to be changed, you can manually configure a new DNS server.

Local DNS server: Configure the DNS server address used by the local device. If multiple addresses exist, separate them with spaces.



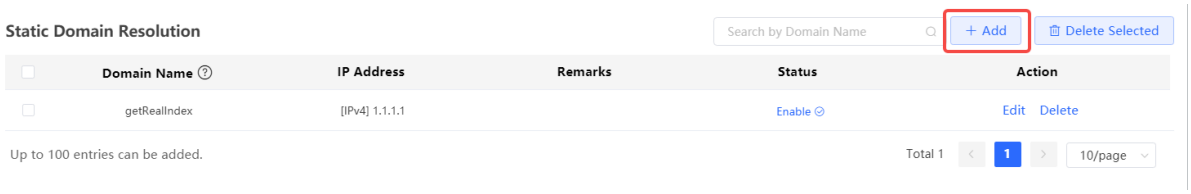
4.7.2 DNS Policy

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **DNS** > **DNS Policy**.

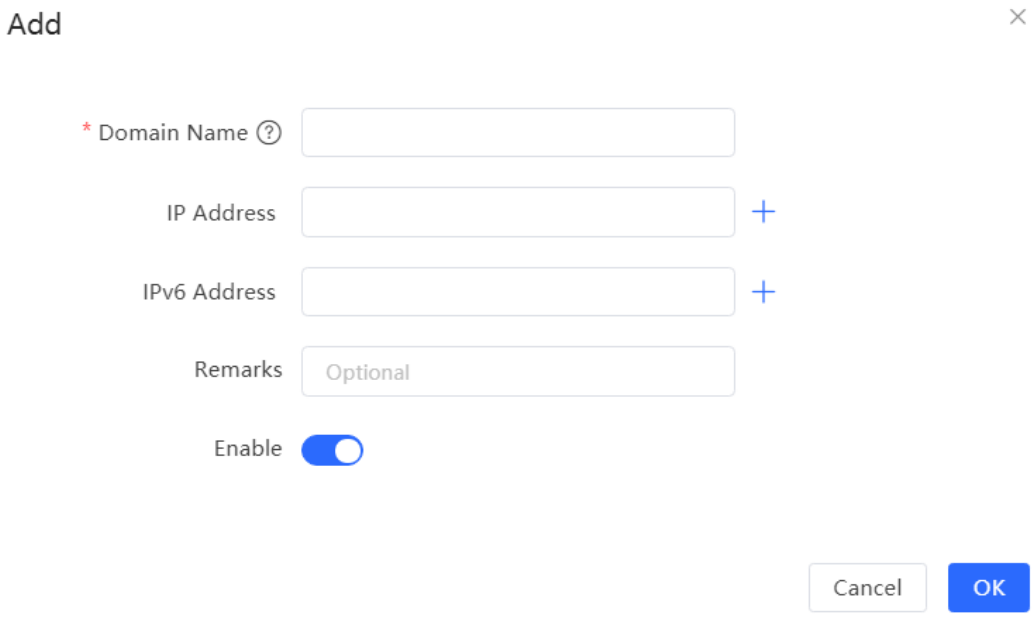
1. Static Domain Name Resolution

By configuring a DNS policy, you can resolve a specified domain name to the corresponding IP address, without relying on an external DNS server to perform domain name resolution. This can accelerate domain name resolution and mitigate security risks such as DNS hijacking.

(1) In the Static Domain Resolution section, click +Add.



(2) In the pop-up window that is displayed, enter the domain name and IP address.



(3) Toggle on **Enable**, and click **OK**.

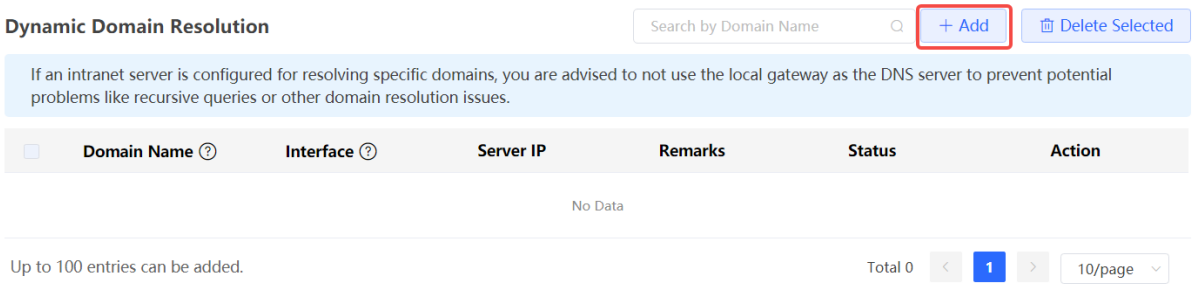
2. Dynamic Domain Name Resolution

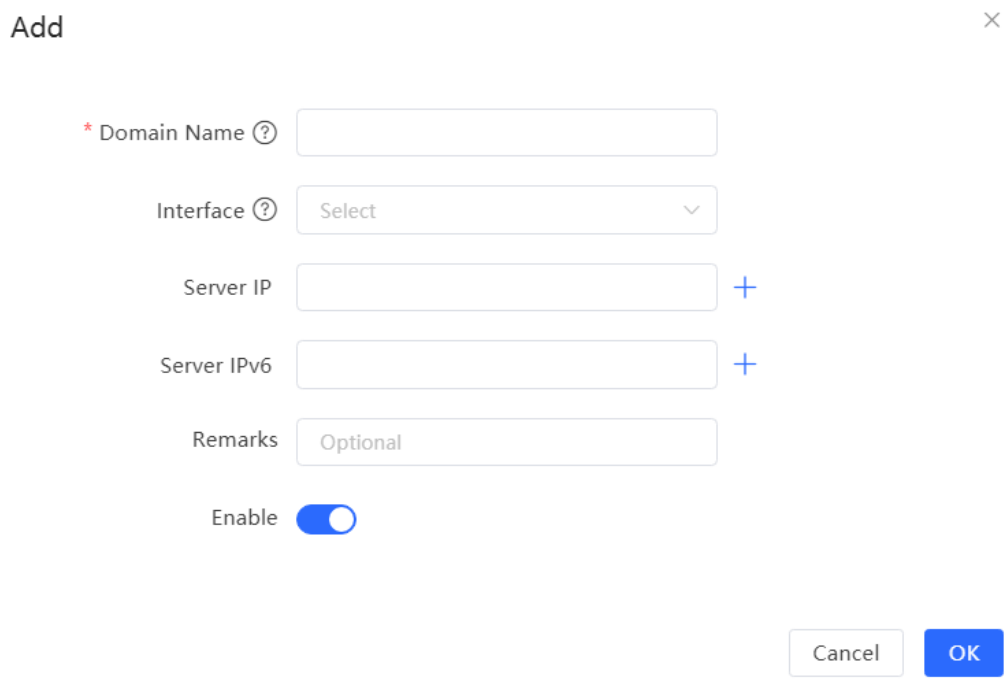
After a DNS server is configured, the specified interface uses the configured DNS server to resolve domain names.

In the **Dynamic Domain Resolution** section, click **+Add**. In the pop-up window that is displayed, enter the domain name, and select the interface. Enter the DNS server IP address and remarks if necessary, toggle on **Enable**, and click **OK**.

Caution

If an intranet server is configured for resolving specific domains, you are advised to not use the local gateway as the DNS server to prevent potential problems like recursive queries or other domain resolution issues.





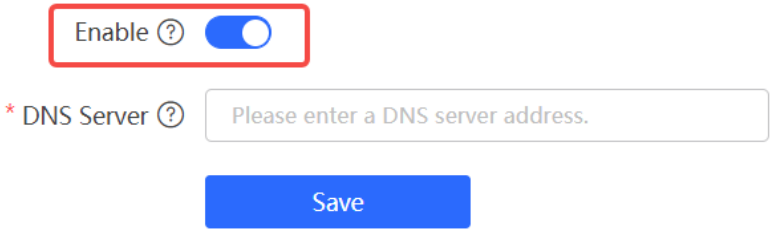
4.7.3 DNS Proxy

DNS proxy is optional configuration. By default, the device obtains the DNS server address from the upper-layer device.

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **DNS** > **DNS Proxy**.

DNS Proxy: By default, the DNS proxy is disabled, and the DNS address delivered by the ISP is used. If the DNS configuration is incorrect, the device may fail to parse domain names and network access will fail. It is recommended to keep the DNS proxy disabled.

DNS Server: Enable clients to access the Internet by using the DNS server address delivered by the upper-layer device. The default settings are recommended. After the DNS proxy is enabled, you need to enter the DNS server IP address. The DNS settings vary with the region. Consult the local ISP for details.



4.8 Configuring IPv6

4.8.1 IPv6 Overview

Internet Protocol Version 6 (IPv6) is the next-generation IP protocol designed by Internet Engineering Task Force (IETF) to substitute IPv4. It is used to compensate insufficient IPv4 network addresses.

4.8.2 IPv6 Basics

1. IPv6 Address Format

IPv6 extends 32-bit IPv4 address into 128 bits, providing wider address space than IPv4.

The basic format of an IPv6 address is X:X:X:X:X:X:X:X. It is represented as eight groups of four hexadecimal digits (0-9, A-F), each group representing16 bits. The groups are separated by colons (:). In this format, each X represents a group of four hexadecimal digits.

Samples of IPv6 addresses are 2001:ABCD:1234:5678:AAAA:BBBB:1200:2100, 800:0:0:0:0:0:0:1, and 1080:0:0:0:8:800:200C:417A.

The digit 0 in an IPv6 address can be suppressed as follows:

- Leading zeros in each 16-bit field are suppressed. For example, 2001:00CD:0034:0078:000A:000B:1200:2100 can be suppressed to 2001:CD:34:78:A:B:1200:2100.
- The long sequence of consecutive all-zero fields in some IPv6 addresses can be replaced with two colons (::). For example, 800:0:0:0:0:0:0:1 can be represented as 800::1. The two colons (::) can be used only when all the 16 bits in a group are 0s, and it can appear only once in an IPv6 address.

2. IPv6 Prefix

IPv6 addresses are typically composed of two logical parts:

- Network prefix: *n* bits, corresponding to the network ID in IPv4 addresses
- interface ID: (128 – *n*) bits, corresponding to the host ID in IPv4 addresses

A slash (/) is used to separate the length of network prefix from an IPv6 address. For example, 12AB::CD30:0:0:0:0/60 indicates that the 60-bit network prefix in the address is used for route selection. IPv6 prefixes can be obtained from the IPv6 DHCP server, along with IPv6 addresses. A downlink DHCP server can also automatically obtain IPv6 prefixes from its uplink DHCP server.

3. Special IPv6 Addresses

There are some special IPv6 addresses:

fe80::/8: loopback address, similar to the IPv4 address 169.254.0.0/16

fc00::/7: local address, similar to IPv4 addresses 10.0.0.0/8, 172.16.0.0/16, and 192.168.0.0/16

ff00::/12: multicast address, similar to the IPv4 address 224.0.0.0/8

4. NAT66

IPv6-to-IPv6 Network Address Translation (NAT66) is a process of converting the IPv6 address in the IPv6 data packet header into another IPv6 address. NAT66 can be implemented by converting the prefix in an IPv6 address in an IPv6 data packet header into another IPv6 address prefix. NAT66 enables mutual access between an internal network and an external public network.

4.8.3 IPv6 Address Allocation Modes

- Manual configuration: IPv6 addresses, prefixes, and other network parameters are configured manually.
- Stateless Address Autoconfiguration (SLAAC): The link-local address is generated based on the interface ID, and the IPv6 address is automatically allocated based on the prefix information in the Router Advertisement (RA) packet.

- Stateful address allocation (DHCPv6): Two DHCPv6 allocation methods are as follows:
  - Automatic DHCPv6 allocation: The DHCPv6 server automatically allocates IPv6 addresses, prefixes, and other network parameters.
  - Automatic allocation of DHCPv6 Prefix Delegations (PDs): The lower-layer network device submits a prefix allocation application to the upper-layer network device. The upper-layer network device allocates an appropriate address prefix to the lower-layer device. The lower-layer device further divides the obtained prefix (usually less than 64 bits) into 64-bit prefixed subnet segments and advertises the address prefixes to the user link directly connected to the IPv6 host through the RA packet, implementing automatic address configuration for hosts.

4.8.4 Enabling the IPv6 Function

Choose **One-Device > Gateway > Config > Network > IPv6 Address**.

Turn on **Enable** to enable the IPv6 function.

4.8.5 Configuring an IPv6 Address for the WAN Interface

Choose **One-Device** > **Gateway** > **Config** > **Network** > **IPv6 Address** > **WAN Settings**.

Caution

- When IPv6 is enabled, the MTU of the IPv4 WAN interface must be greater than 1280.
- If NAT66 is disabled, a public IPv6 address can access clients using the public IPv6 address on the intranet.

After you enable the IPv6 function, you can set related parameters on the **WAN Settings** tab. The number of **WAN** tabs indicates the number of WAN interfaces on the current device.

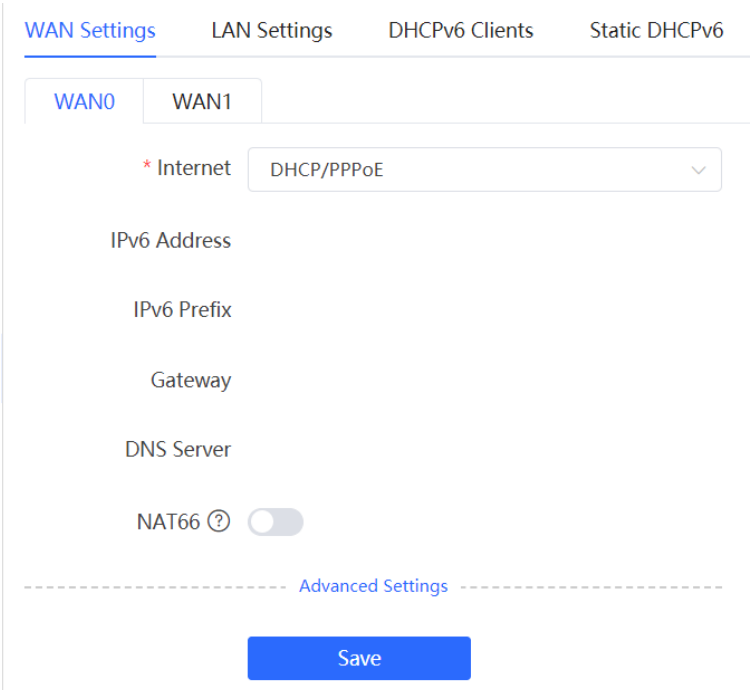


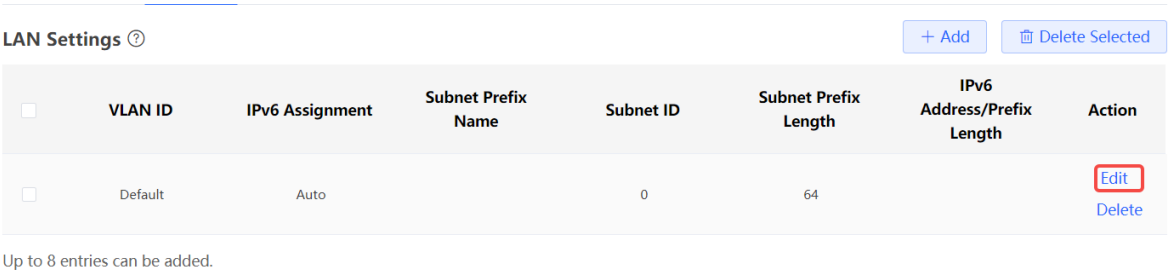
Table 4-8 IPv6 address configuration for WAN interface

Parameter	Description
Internet	Configure a method for the WAN interface to obtain an IPv6 address. ● **DHCP/PPPoE**: The current device functions as the DHCPv6 client, and it applies for an IPv6 address and prefix from the uplink network device. ● **Static IP**: You need to manually configure a static IPv6 address, gateway address, and DNS server. ● **Null**: The IPv6 function is disabled on the WAN interface.
IPv6 Address	When **Internet** is set to **DHCP/PPPoE**, the automatically obtained IPv6 address is displayed. When **Internet** is set to **Static IP**, you need to configure this parameter manually.
IPv6 Prefix	When **Internet** is set to **DHCP/PPPoE,** the IPv6 address prefix automatically obtained by the current device is displayed.
Gateway	When **Internet** is set to **DHCP/PPPoE**, the automatically obtained gateway address is displayed. When **Internet** is set to **Static IP**, you need to configure this parameter manually.
DNS Server	When **Internet** is set to **DHCP/PPPoE**, the automatically obtained DNS server address is displayed. When **Internet** is set to **Static IP**, you need to configure this parameter manually.
NAT66	If the current device cannot access the Internet through **DHCP/PPPoE** or cannot obtain the IPv6 prefix, you need to enable the NAT66 function to allocate IPv6 addresses to clients on the internal network.
Default Preference	Set the default route preference for the current line. A smaller value indicates a higher preference. For the same destination address, the route with the highest preference is selected as the optimal route.

4.8.6 Configuring an IPv6 Address for the LAN Port

Choose **One-Device** > **Gateway** > **Config** > **Network** > **IPv6 Address** > **LAN Settings**.

When the device accesses the Internet through DHCP, it can obtain LAN port IPv6 addresses from the uplink device and allocate IPv6 addresses to the clients in the LAN based on the IPv6 address prefix. If the uplink device cannot allocate an IPv6 address prefix to the device, you need to manually configure an IPv6 address prefix for the LAN port and enable the NAT66 function to allocate IPv6 addresses to the clients in the LAN. For details, see Section 4.8.5 Configuring an IPv6 Address for the WAN Interface.

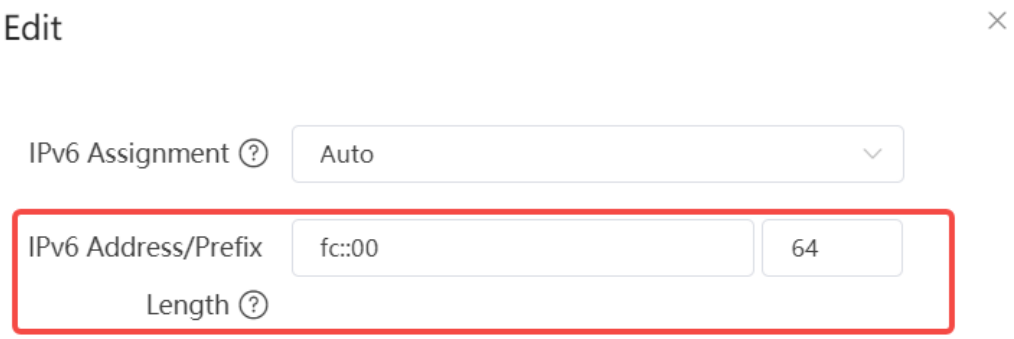


Click **Edit** next to the default VLAN, and set **IPv6 Address/Prefix Length** to a local address with no more than 64 bits. This address is also used as the IPv6 address prefix.

You can use either of the following methods to allocate IPv6 addresses to clients:

- **Auto**: Allocate IPv6 addresses to clients in DHCPv6 or SLAAC mode.
- **DHCPv6**: Allocate IPv6 addresses to clients through DHCPv6.
- **SLAAC**: Allocate IPv6 addresses to clients through SLAAC.
- **Null**: Do not allocate addresses to clients.

You should select an allocation method based on the protocol supported by clients on the internal network. If you are not sure about the supported protocol, select **Auto**.



Click **Advanced Settings** to configure more address attributes.

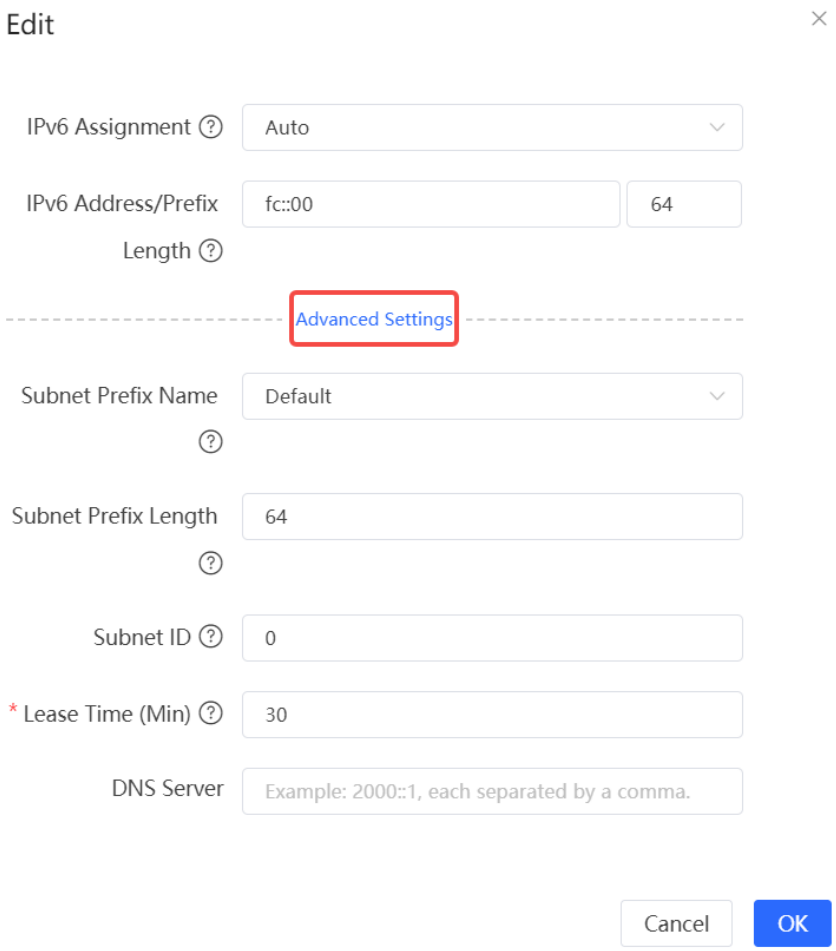


Table 4-9 IPv6 address configuration for LAN port

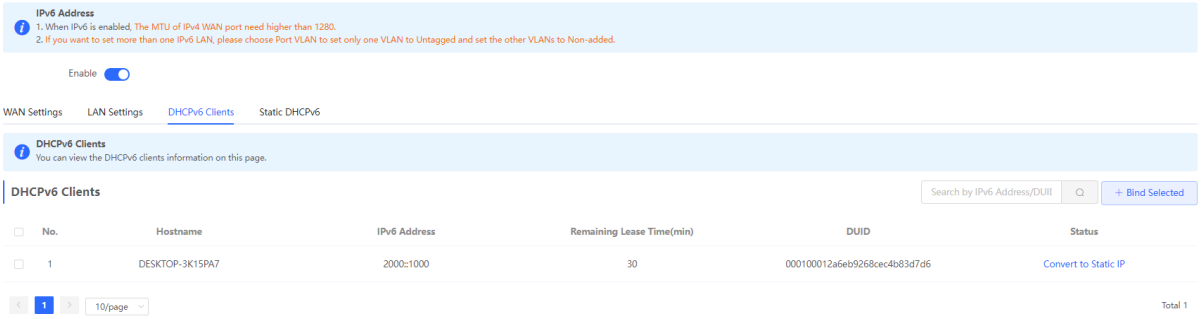
Parameter	Description
Subnet Prefix Name	Specify the interface from which the prefix is obtained, such as **WAN_V6** or **WAN1_V6**. By default, the device obtains prefixes from all interfaces.
Subnet Prefix Length	Specify the length of the subnet prefix. The value is in the range of 48 to 64.
Subnet ID	Configure the subnet ID in the hexadecimal format. The value 0 indicates auto increment.
Lease Time(Min)	Set the lease of the IPv6 address, in minutes.
DNS Server	Configure the IPv6 DNS server address.

4.8.7 Viewing the DHCPv6 Client

Choose **One-Device** > **Gateway** > **Config** > **Network** > **IPv6 Address** > **DHCPv6 Clients**.

When the device functions as a DHCPv6 server to allocate IPv6 addresses to clients, you can view the information about the client that obtains an IPv6 address from the device on the current page. The client information includes the host name, IPv6 address, remaining lease time, and DHCPv6 Unique Identifier (DUID).

Enter the DUID in the search bar and click to quickly find relative information of the specified DHCPv6 client.

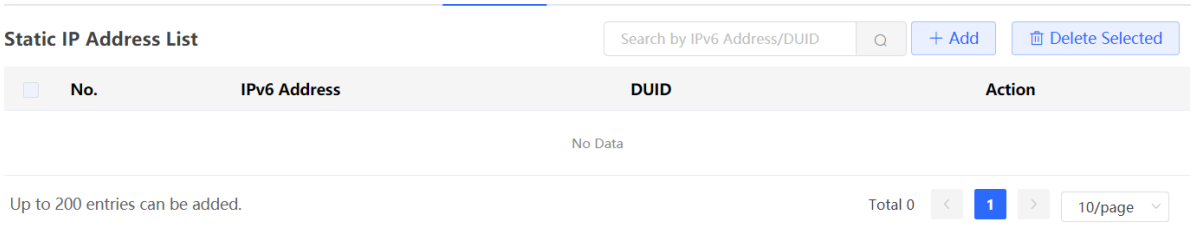


- Click **Convert to Static IP** to convert the IP binding of a client with an IP address to static binding. Then the DHCP server assigns a static IP address to the client.
- Click **Bind Selected** to convert the IP binding of multiple clients with IP addresses to static binding. Then the DHCP server assigns static IP addresses to the clients.

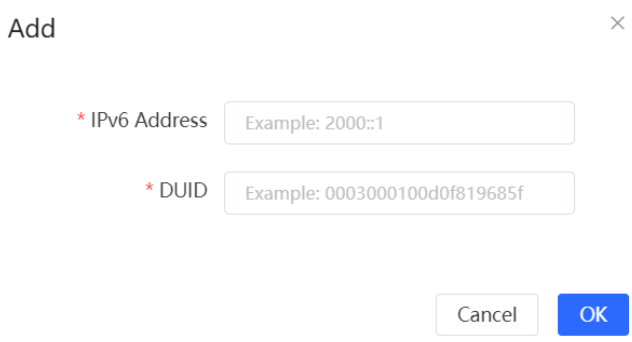
4.8.8 Configuring the Static DHCPv6 Address

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

Choose **One-Device** > **Gateway** > **Config** > **Network** > **IPv6 Address** > **Static DHCPv6**.



(1) Click **Add**.



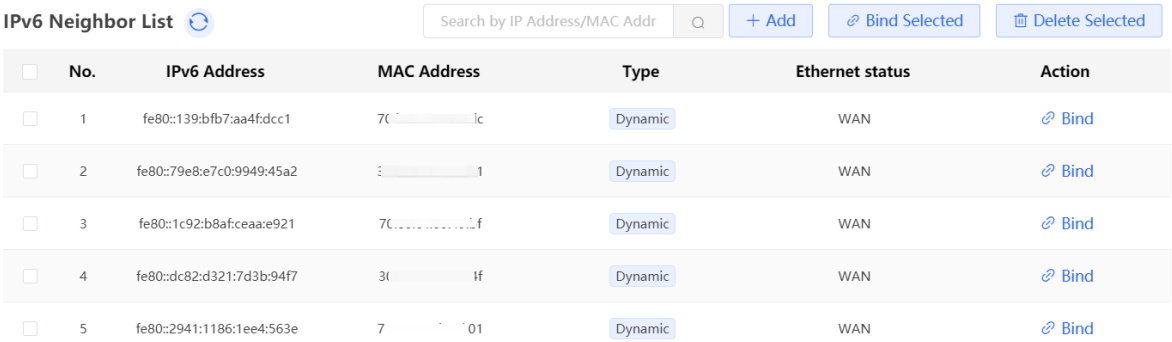
(2) Enter the IPv6 address and DUID.

(3) Click **OK**.

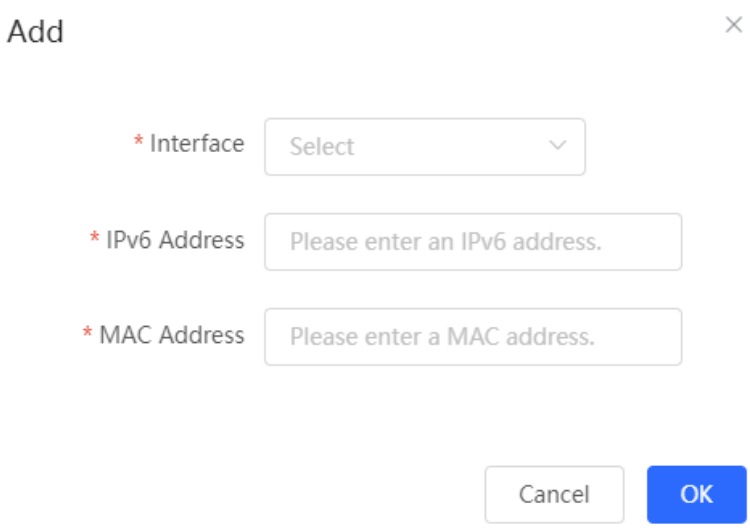
4.8.9 Configuring the IPv6 Neighbor List

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.

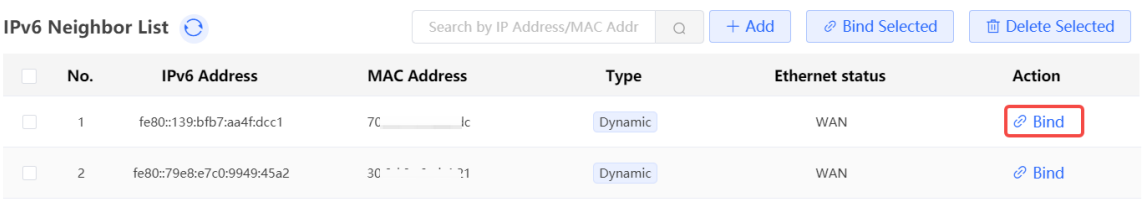
Choose **One-Device** > **Gateway** > **Config** > **Security** > **IPv6 Neighbor List**.



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



(2) Select the MAC address and IP address to be bound, and click **Bind** in the **Action** column to bind the IP address to the MAC address to prevent ND attacks.



4.9 Configuring a DHCP Server

4.9.1 DHCP Server Overview

After the DHCP server function is enabled in the LAN, the device can automatically deliver IP addresses to clients, so that clients connected to the LAN ports of the device or connected to Wi-Fi can access the Internet using the obtained addresses.

See Section 4.8.6 Configuring an IPv6 Address for the LAN Port for more information about the DHCPv6 server function.

4.9.2 Address Allocation Mechanism

The DHCP server allocates an IP address to a client in the following way:

(1) When the device receives an IP address request from a DHCP client, the device searches the DHCP static address allocation list. If the MAC address of the DHCP client is in the DHCP static address allocation list, the device allocates the corresponding IP address to the DHCP client.

(2) If the MAC address of the DHCP client is not in the DHCP static address allocation list or the IP address that the DHCP client applies is not in the same network segment as the LAN port IP address, the device selects an IP address not used from the address pool and allocates the address to the DHCP client.

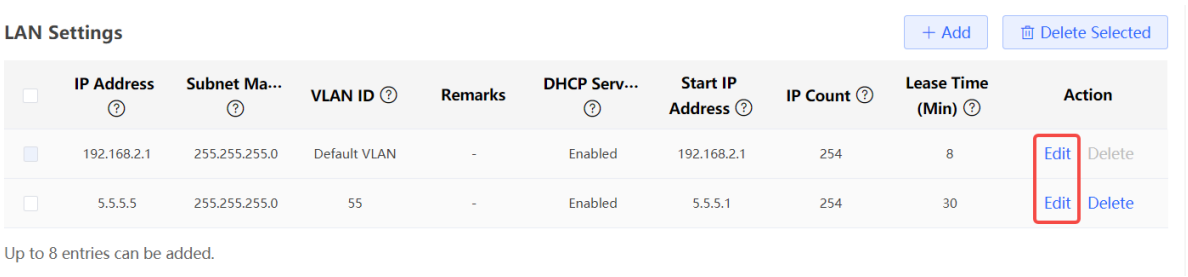
(3) If no IP address in the address pool is allocable, the client will fail to obtain an IP address.

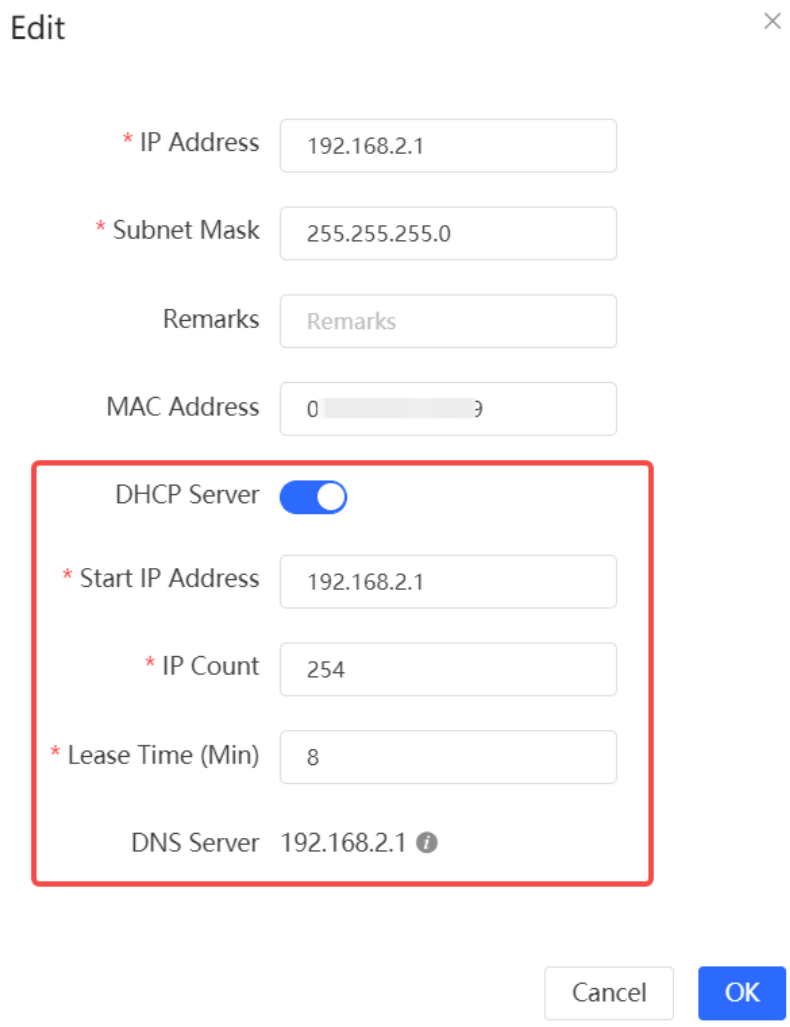
4.9.3 Configuring the DHCP Server

1. Configuring Basic Parameters

Choose **One-Device > Gateway > Config > Network > LAN > LAN Settings.**

Select the VLAN to which the DHCP function needs to be configured and click **Edit**.





DHCP Server: The DHCP server function is enabled by default in the router mode. You are advised to enable the function if the device is used as the sole router in the network. When multiple routers are connected to the upper-layer device through LAN ports, disable this function.

Caution

If the DHCP server function is disabled on all devices in the network, clients cannot automatically obtain IP addresses. You need to enable the DHCP server function on one device or manually configure a static IP address for each client for Internet access.

Start IP Address: Enter 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: Enter the number of IP addresses in the address pool.

Lease Time (Min): Enter the address lease term. When a client is connected, the leased IP address is automatically renewed. If a leased IP address is not renewed due to client disconnection or network instability,

the IP address will be reclaimed after the lease term expires. After the client connection is restored, the client can request an IP address again. The default lease term is 30 minutes.

2. Configuring DHCP Option

Choose **One-Device** > **Gateway** > **Config** > **Network** > **LAN** > **DHCP**.

The DHCP Option configuration is shared by all LAN ports. You can configure DHCP Option based on actual needs.

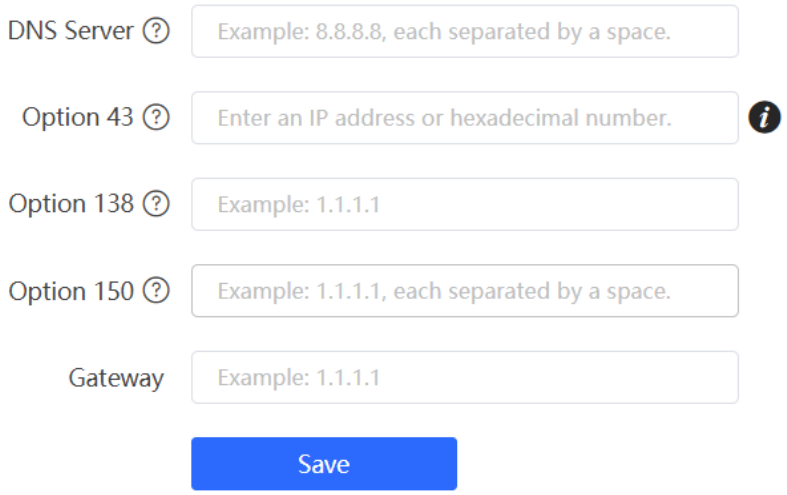


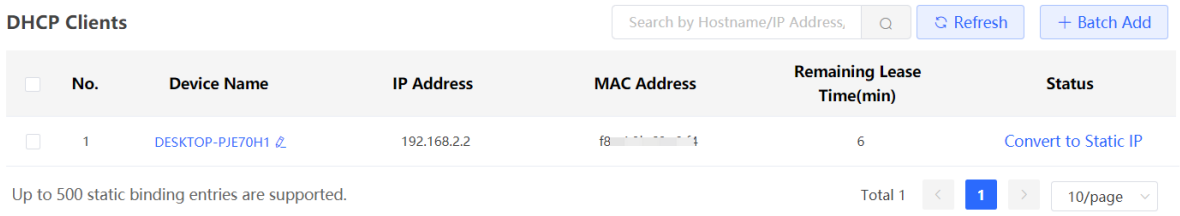
Table 4-10 DHCP Option configuration

Parameter	Description
DNS Server	Enter the DNS server address provided by the ISP.
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. The TFTP server allocates addresses to clients.
Gateway	Configure the IP address of the default gateway or default route that the DHCP server assigns to clients. The default gateway is the next hop address used by a client to send data packets to an external network. It is responsible for forwarding the data packets to the target network.

4.9.4 Viewing the DHCP Client

Choose **One-Device** > **Gateway** > **Config** > **Network** > **LAN** > **DHCP Clients**.

View the client addresses automatically allocated by thorough DHCP. Find the target client and click **Convert to Static IP** in the **Status** column, or select desired clients and click **Batch Add**. 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 Section 4.9.5 Configuring Static IP Addresses.

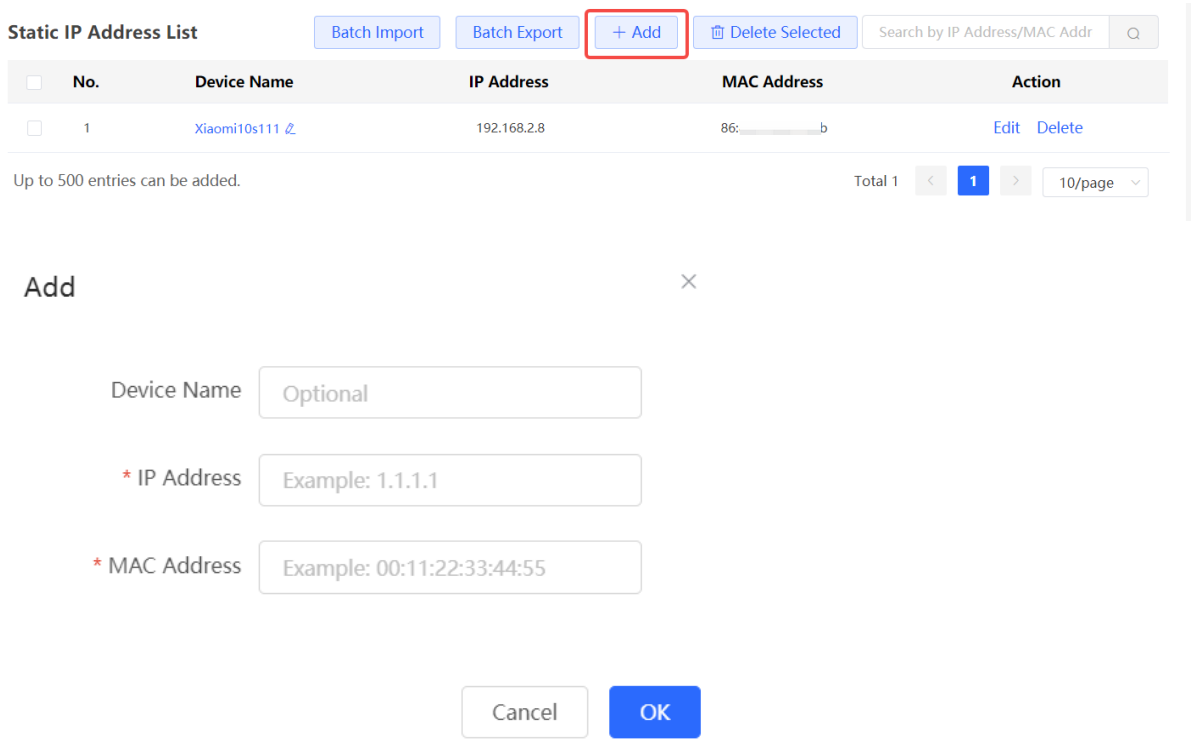


4.9.5 Configuring Static IP Addresses

Choose **One-Device** > **Gateway** > **Config** > **Network** > **LAN Static IP Addresses**.

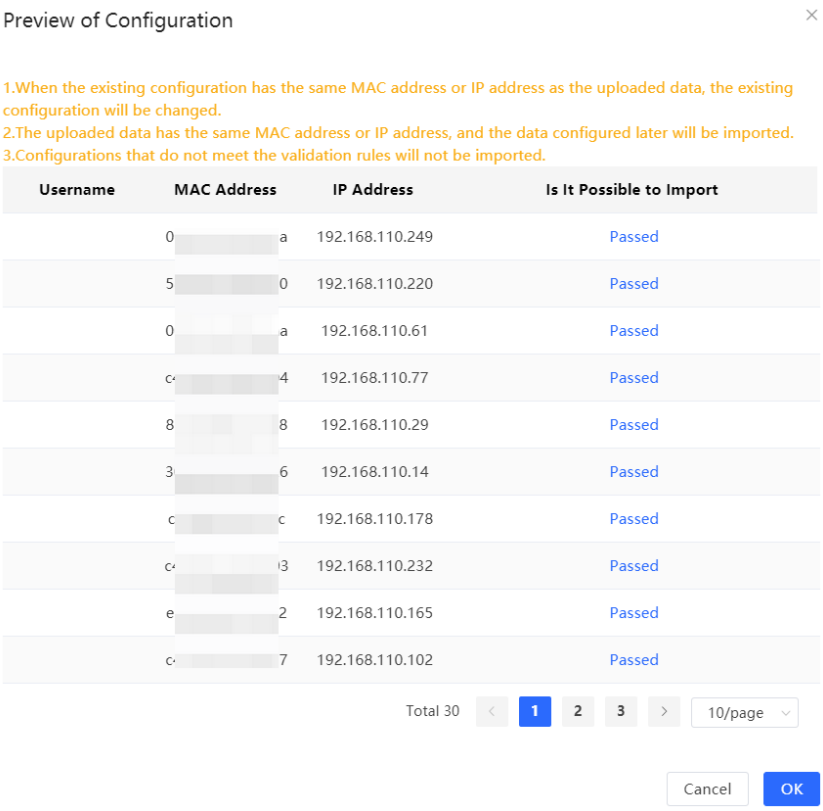
The page displays all configured static IP addresses.

Click **Add**. In the pop-up window, enter the device name, 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 client connects to the network.



Click **Batch Export** to export all existing static IP addresses.

Click **Batch Import** to import static IP addresses in the file to the device. The entries with the same MAC address as those in the list will be overwritten by the configurations in the file, and the other configurations in the list will not be changed. The other configurations in the file will be added to the list in the form of new entries.



4.10 Configuring Routes

4.10.1 Configuring Static Routes

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.

1. Configuring IPv4 Static Routing

Choose **One-Device > Gateway > Config > Advanced** > **Routing** > **Static Routing**.

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.

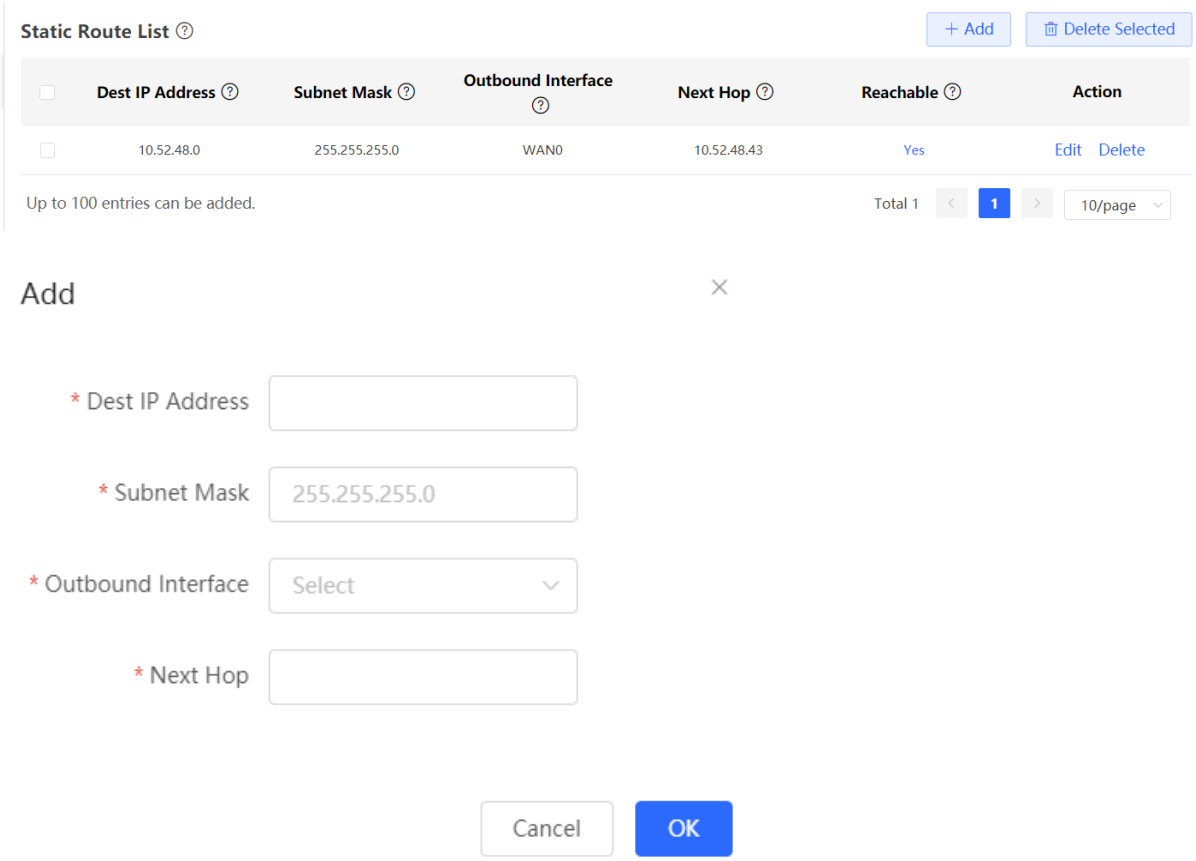
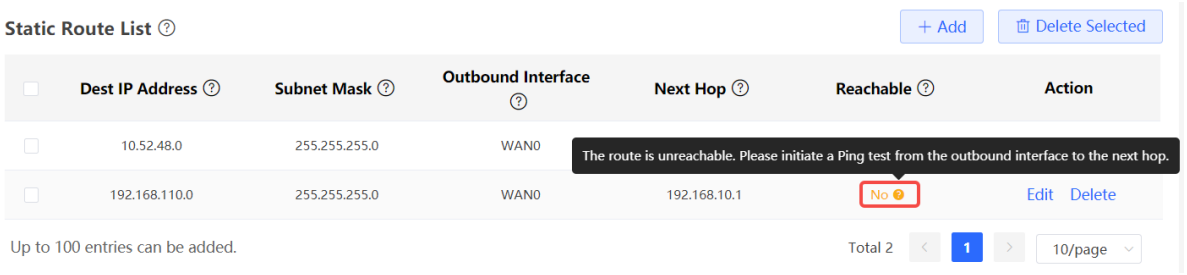


Table 4-11 Static route configuration

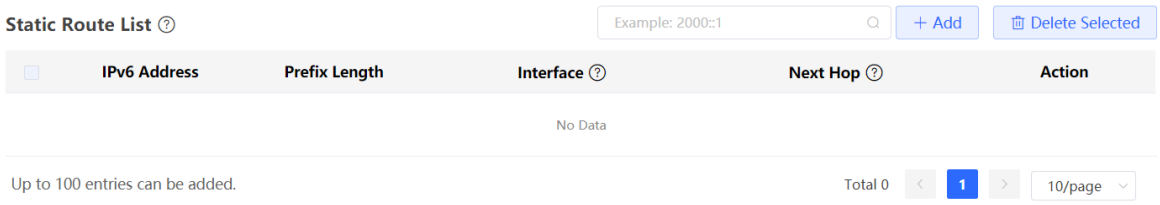
Parameter	Description
Dest IP Address	Specify the destination network to which the data packet is to be sent. The device matches the data packet based on the destination address and subnet mask.
Subnet Mask	Specify the subnet mask of the destination network. The device matches the data packet based on 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. If the outbound interface accesses the Internet through PPPoE dialing, you do not need to configure the next-hop address.

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.

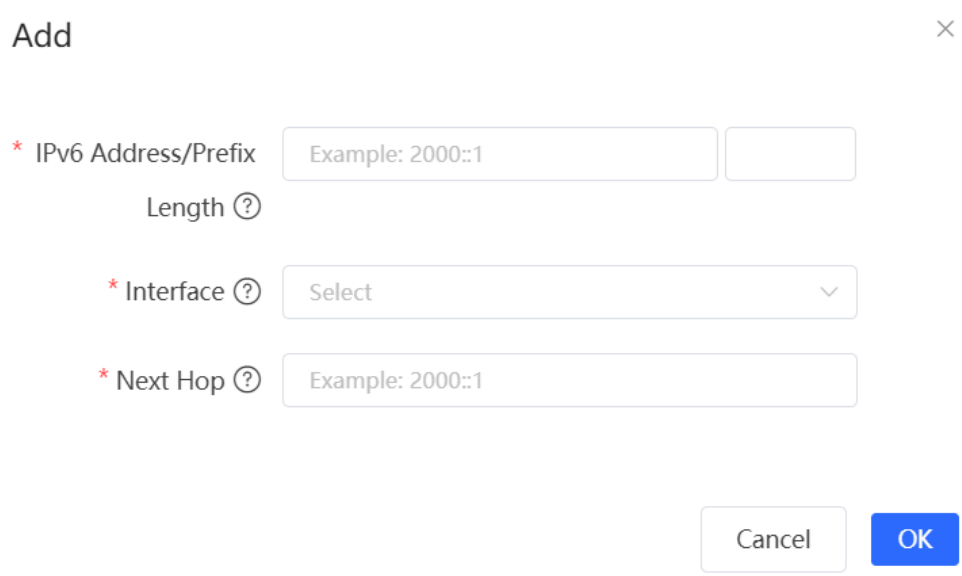


2. Configuring the IPv6 Static Route

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **IPv6 Static Routing**.



(1) Click **Add**.



(2) Configure an IPv6 static route of the device.

Table 4-12 Description of IPv6 Static Routing 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.

Parameter	Description
Next Hop	IP address of the next routing node to which the packet is sent.

(3) Click **OK**.

4.10.2 Configuring PBR

Policy-based routing (PBR) is a mechanism for routing and forwarding based on user-specified policies. When a router forwards data packets, it filters the packets according to the configured rules, and then forwards the matched packets according to the specified forwarding policy. The PBR feature enables the device to formulate rules according to specific fields (source or destination IP address and protocol type) in the data packets, and forward the data packets from a specific interface.

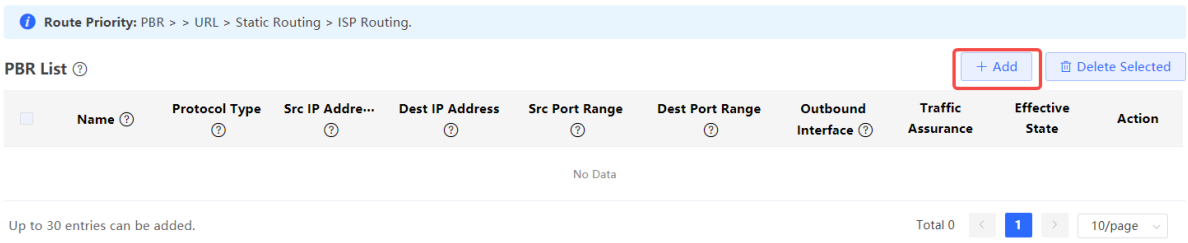
In a multi-line scenario, if the device is connected to the Internet and the internal network through different lines, the traffic will be evenly routed over the lines if no routing settings are available. In this case, access data to the internal network may be sent to the external network, or access data to the external network may be sent to the internal network, resulting in network exceptions. To prevent these exceptions, you need to configure PBR to control data isolation and forwarding on the internal and external networks.

The device can forward data packets using either of the following three policies: PBR, address-based routing, and static routing. When all the policies exist, PBR, static routing, and address-based routing have descending order in priority. For details on address-based routing, see Section 4.3.7 Configuring the Multi-Line Load Balancing Mode.

1. Configuring IPv4 PBR

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **PBR**.

Click **Add** to add a PBR rule.



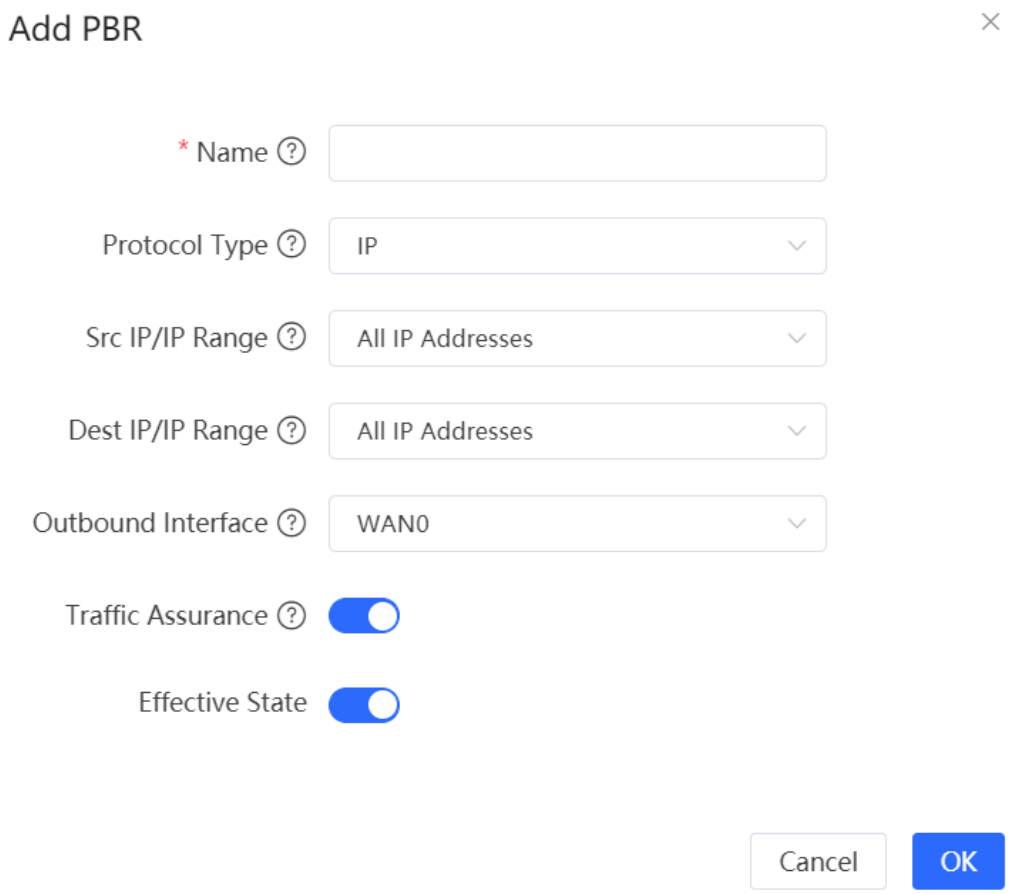


Table 4-13 Description of IPv4 PBR Configuration Parameters

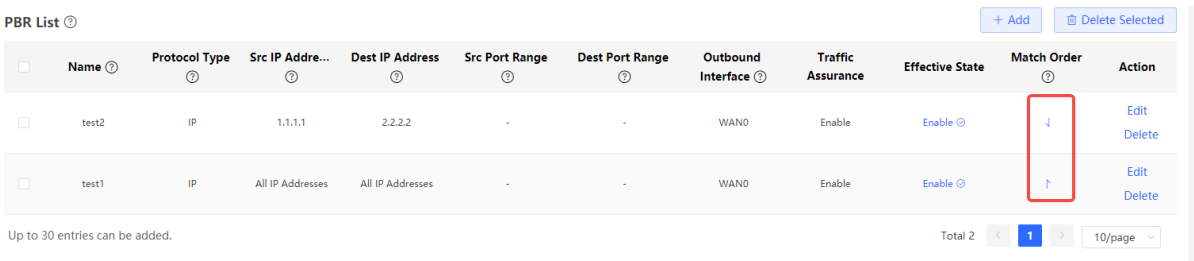
Parameter	Description
Name	Specify the name of the PBR rule, which uniquely identifies a PBR rule. The name must be unique for each rule.
Protocol Type	Specify the protocol to which the PBR rule is effective. You can set this parameter to **IP**, **ICMP**, **UDP**, **TCP**, or **Custom**.
Protocol Number	When **Protocol Type** is set to **Custom**, you need to enter the protocol number.
Src IP/IP Range	Configure the source IP address or IP address range for matching PBR entries. The default value is All IP Addresses. ● **All IP Addresses**: Match all the source IP addresses. ● **Custom**: Match the source IP addresses in the specified IP range.
Custom Src IP	When Src IP/IP Range is set to **Custom**, you need to enter a single source IP address or a source IP range.

Parameter	Description
Dest IP/IP Range	Configure the destination IP address or IP address range for matching PBR entries. The default value is All IP Addresses. ● **All IP Addresses**: Match all the destination IP addresses. ● **Custom**: Match the destination IP addresses in the specified IP range.
Custom Dest IP	When Dest IP/IP Range is set to Custom, you need to enter a destination source IP address or a destination IP range.
Src Port Range	This parameter is available only when Protocol Type is set to TCP or UDP. This parameter specifies the source port range for packet matching using PBR.
Dest Port Range	This parameter is available only when Protocol Type is set to TCP or UDP. This parameter specifies the destination port range for packet matching using PBR.
Outbound Interface	Specify the interface that forwards the data packet based on the hit PBR rule.
Traffic Assurance	When an outbound interface is unreachable, the traffic will be automatically routed to other reachable outbound interfaces.
Effective State	Turn on **Effective State** to specify whether to enable the PBR rule. If **Effective State** is turned off, this rule does not take effect.

Note

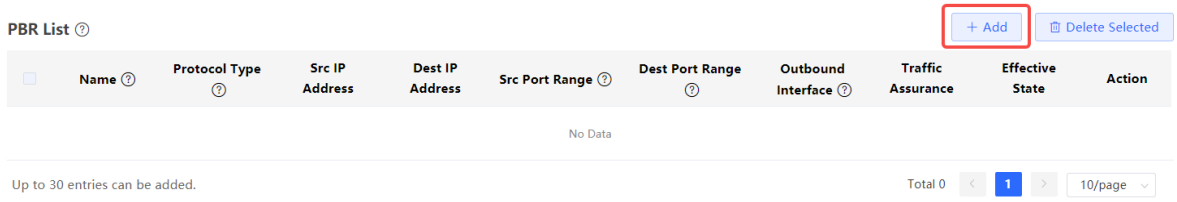
If you want to restrict the access device to access only the specified internal network, you can set the outbound interface in the corresponding route to the WAN interface in the private line network. For details on how to set the private line network, see Section 4.3.4 Configuring the Private Line.

All the created PBR policies are displayed in the PBR list, with the latest policy listed on the top. The device matches the policies according to their sorting in the list. You can manually adjust the policy matching sequence by clicking or in the **Match Order** column.



2. Configuring IPv6 PBR

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **IPv6 PBR**.



Click **Add** to add a PBR rule.

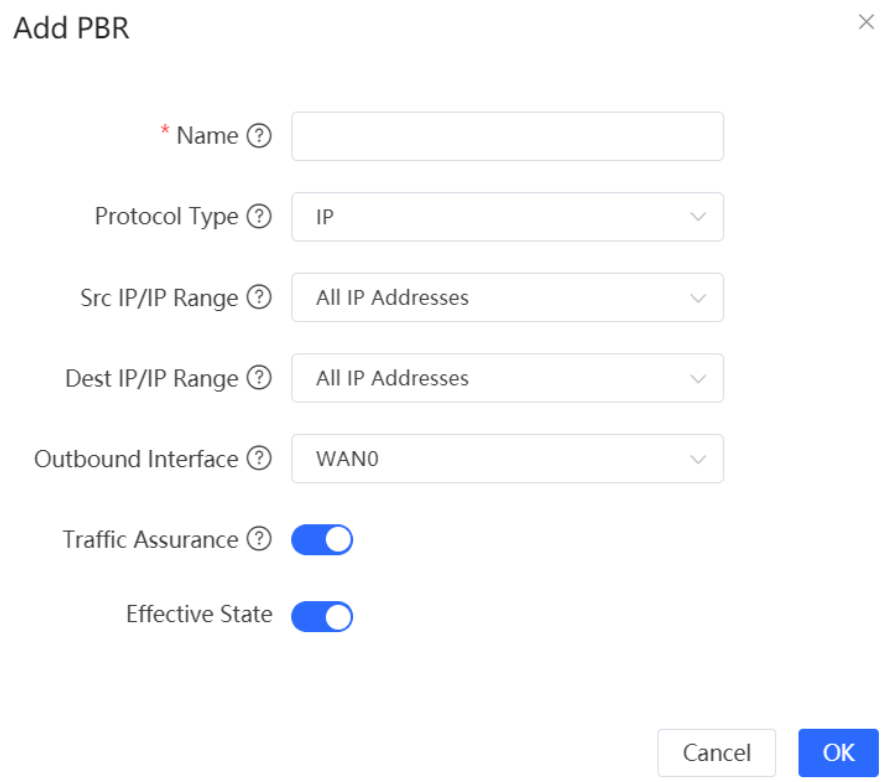


Table 4-14 Description of IPv6 PBR Configuration Parameters

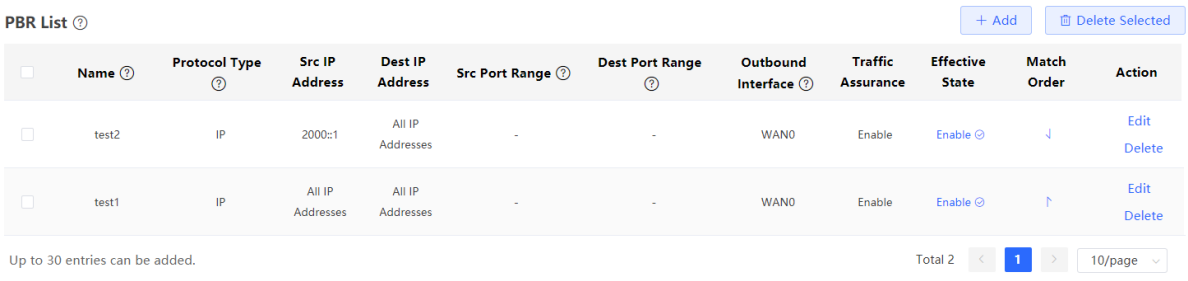
Parameter	Description
Name	Specify the name of the PBR rule, which uniquely identifies a PBR rule. The name must be unique for each rule.
Protocol Type	Specify the protocol to which the PBR rule is effective. You can set this parameter to **IP**, **ICMPv6**, **UDP**, **TCP**, or **Custom**.
Protocol Number	When **Protocol Type** is set to **Custom**, you need to enter the protocol number.
Src IP/IP Range	Configure the source IP address or IP address range for matching PBR entries. The default value is All IP Addresses. ● **All IP Addresses**: Match all the source IP addresses. ● **Custom**: Match the source IP addresses in the specified IP range.

Parameter	Description
Custom Src IP	When Src IP/IP Range is set to **Custom**, you need to enter a single source IP address or a source IP range.
Dest IP/IP Range	Configure the destination IP address or IP address range for matching PBR entries. The default value is All IP Addresses. ● **All IP Addresses**: Match all the destination IP addresses. ● **Custom**: Match the destination IP addresses in the specified IP range.
Custom Dest IP	When Dest IP/IP Range is set to Custom, you need to enter a destination source IP address or a destination IP range.
Src Port Range	This parameter is available only when Protocol Type is set to TCP or UDP. This parameter specifies the source port range for packet matching using PBR.
Dest Port Range	This parameter is available only when Protocol Type is set to TCP or UDP. This parameter specifies the destination port range for packet matching using PBR.
Outbound Interface	Specify the interface that forwards the data packet based on the hit PBR rule.
Traffic Assurance	When an outbound interface is unreachable, the traffic will be automatically routed to other reachable outbound interfaces.
Effective State	Turn on **Effective State** to specify whether to enable the PBR rule. If **Effective State** is turned off, this rule does not take effect.

Note

If you want to restrict the access device to access only the specified internal network, you can set the outbound interface in the corresponding route to the WAN interface in the private line network. For details on how to set the private line network, see Section 4.3.4 Configuring the Private Line.

All the created PBR policies are displayed in the PBR list, with the latest policy listed on the top. The device matches the policies according to their sorting in the list. You can manually adjust the policy matching sequence by clicking or in the **Match Order** column.



3. Typical Configuration Example

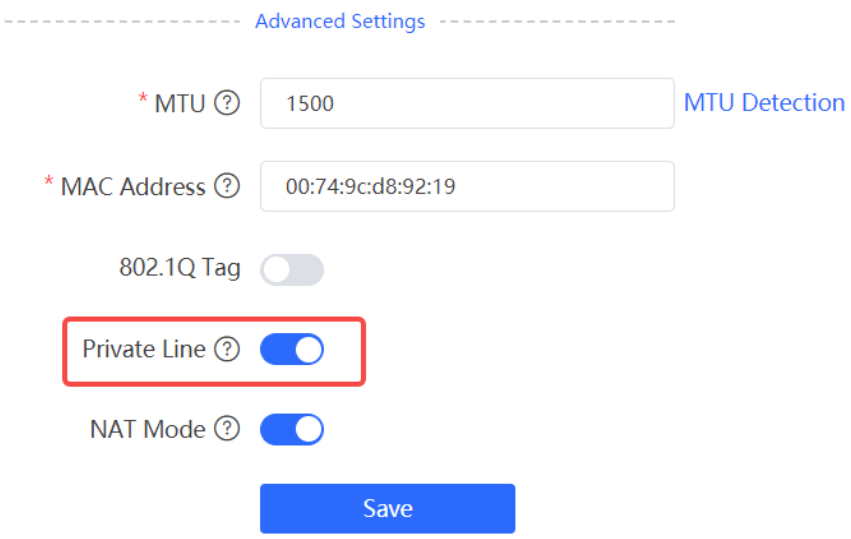
- Networking Requirements

Two lines with different bandwidths are deployed for an enterprise. Line A (WAN 1) is used for access to the Internet and Line B (WAN 2) is used for access to the specific internal network (10.1.1.0/24). The enterprise wants to configure PBR to guarantee correct data flows between the internal and external networks, isolate devices in the specified address range (172.26.31.1 to 172.26.31.200) from the external network, and allow these devices to access the specific internal network only.

- Configuration Roadmap
- Configure the private line.
- Add a PBR policy for access to the internal network.
- Add a PBR policy for access to the external network.
- Add a PBR policy to restrict specific devices to access the internal network only.
- Configuration Steps

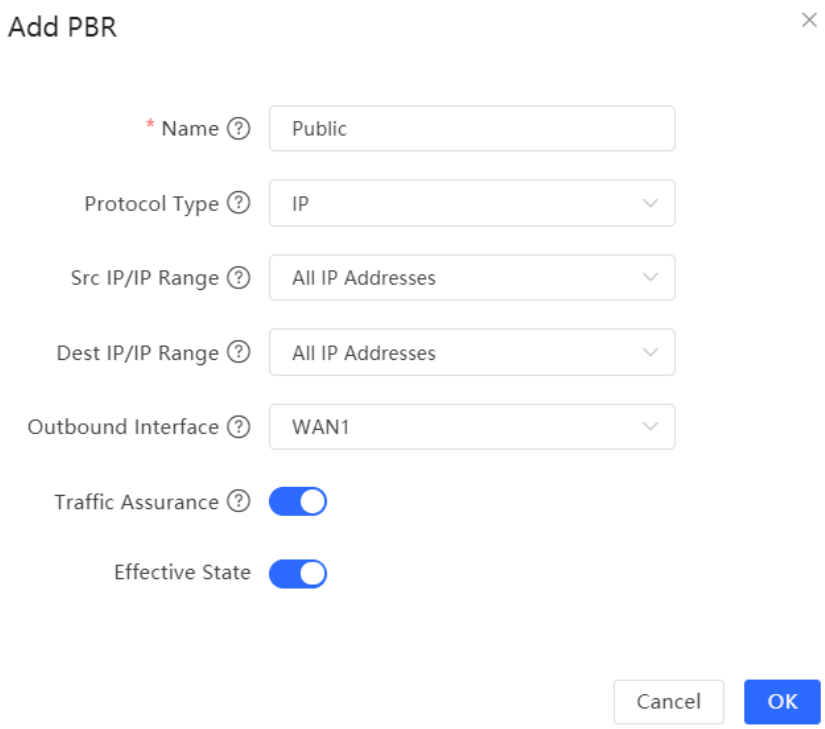
(1) Configure WAN 2 as the private line for the internal network.

When you configure networking parameters for WAN 2 port, click **Advanced Settings**, turn on **Private Line**, and click **Save**. For details, see Section 4.3.4 Configuring the Private Line.



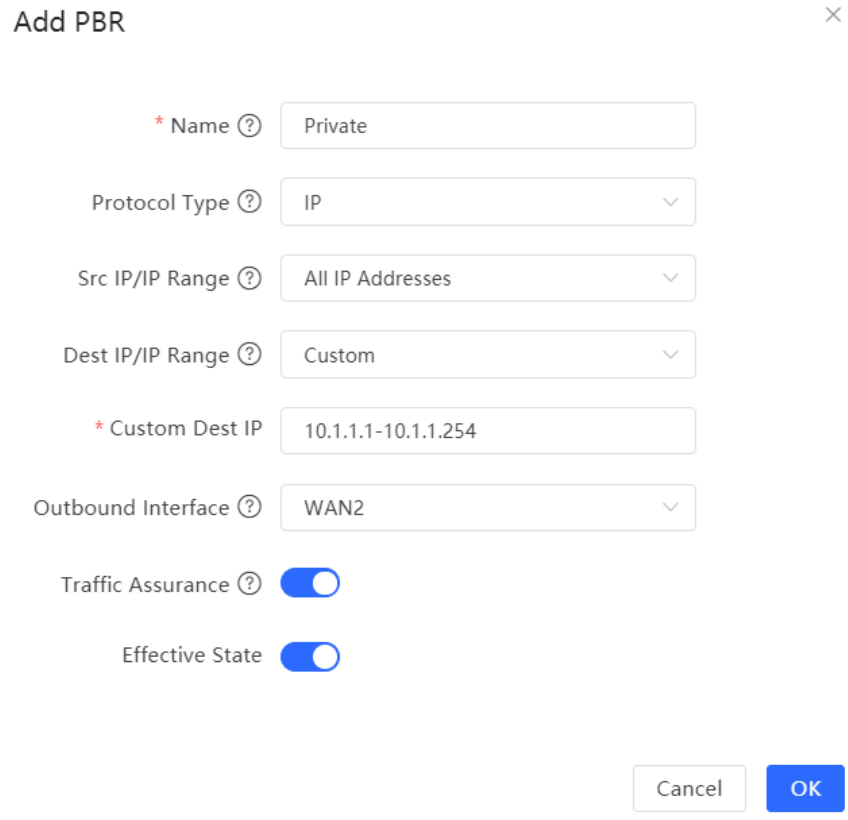
(2) Add a PBR policy to forward data packets destined to the external network through WAN 1 port.

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **PBR** and click **Add**. In the dialog box that appears, create a PBR policy and set **Outbound Interface** to **WAN1**.



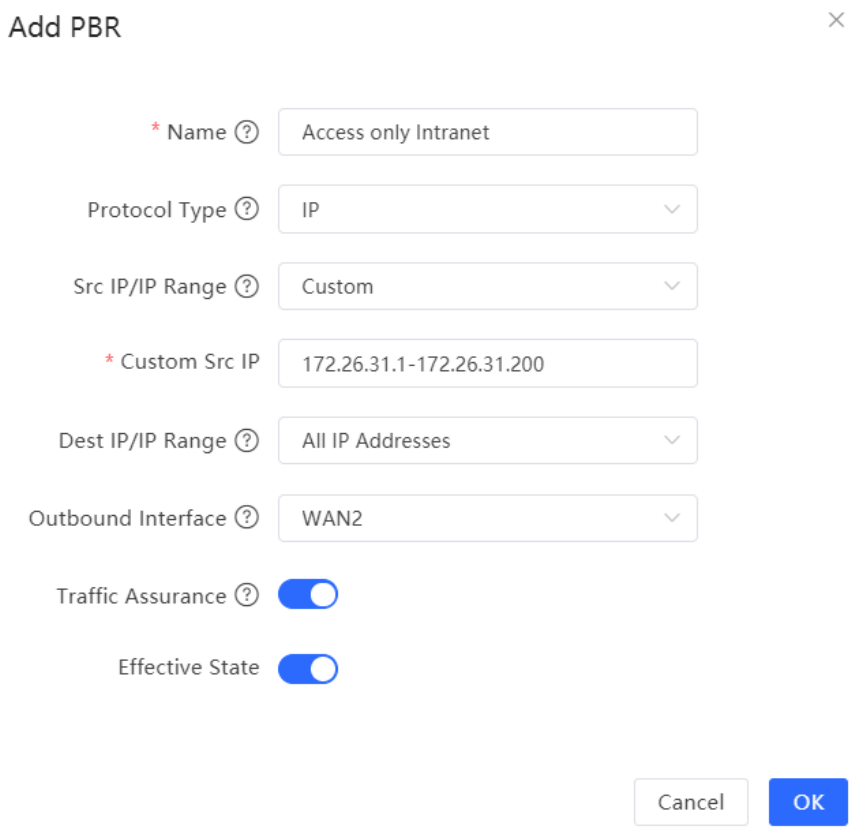
(3) Add a PBR policy to forward data packets destined to the internal network through WAN 2 port.

In this policy, set **Custom Dest IP** to 10.1.1.1-10.1.1.254 and **Outbound Interface** to WAN2.



(4) Add a PBR policy to restrict devices in the IP range 172.26.31.1 to 172.26.31.200 to access the internal private line only.

In this policy, set **Src IP/IP Range** to **Custom**, **Custom Src IP** to 172.26.31.1-172.26.31.200, and **Outbound Interface** to WAN2.



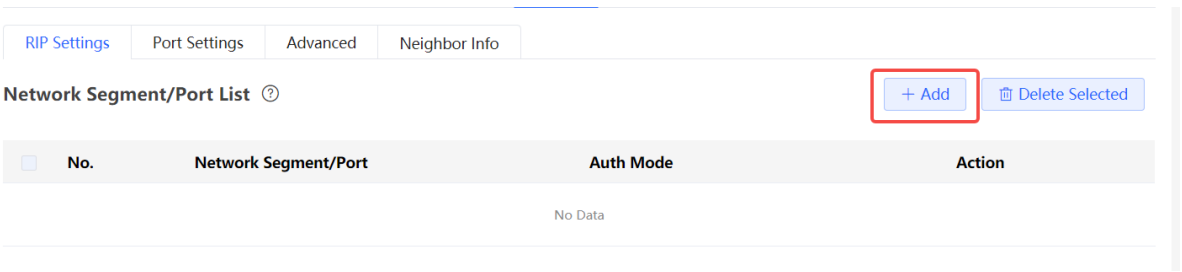
4.10.3 Configuring RIP

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.

1. Configuring RIP Basic Functions

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **RIP Settings**

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



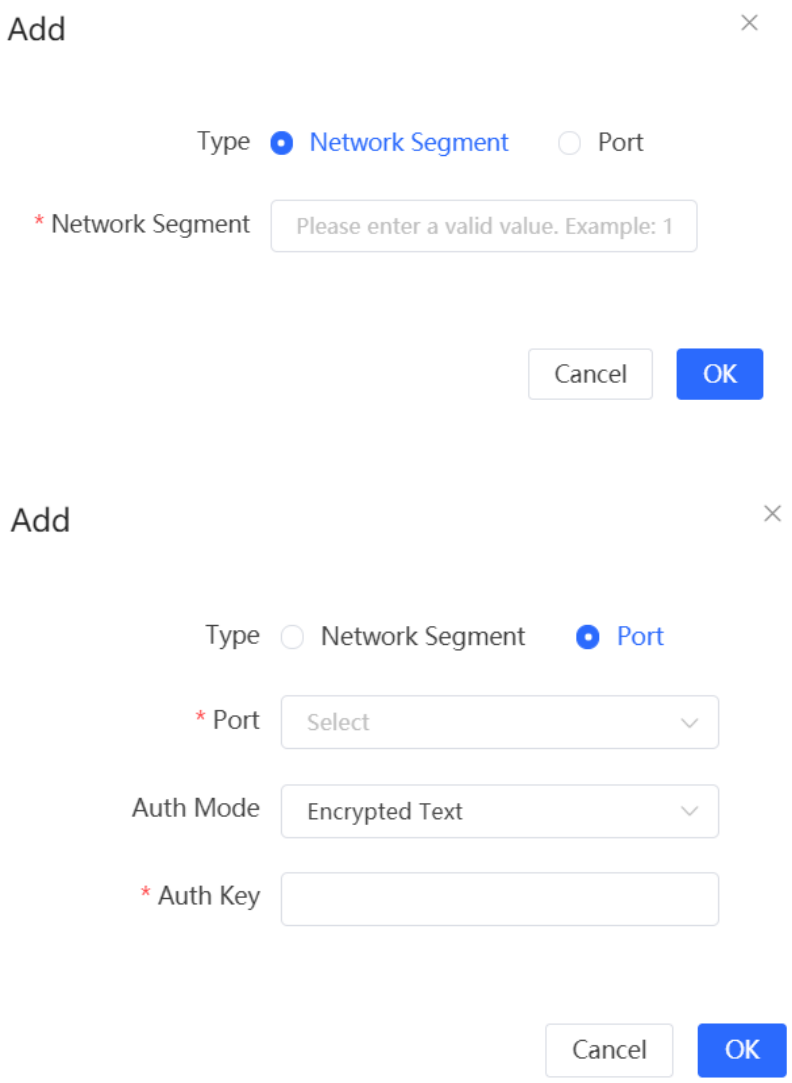


Table 4-15 RIP Configuration Parameters

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**.

Parameter	Description
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**.

2. Configuring the RIP Port

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **RIP Settings** > **Port Settings**

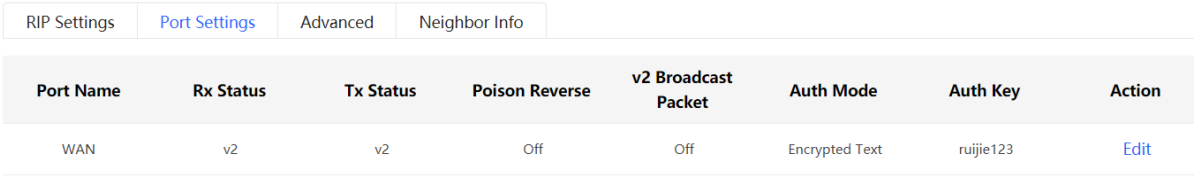


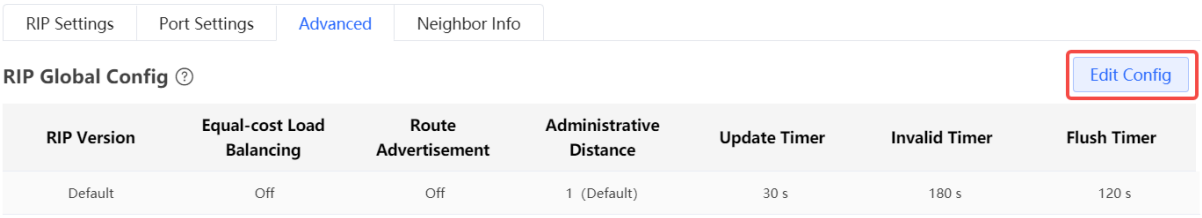
Table 4-16 Configuration Parameters in the Port List

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**.

Parameter	Description
Action	Click **Edit** to modify RIP settings of the port.

3. Configuring the RIP Global Configuration

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **RIP Settings** > **Advanced,** click **Edit Config**, and configure RIP global configuration parameters.



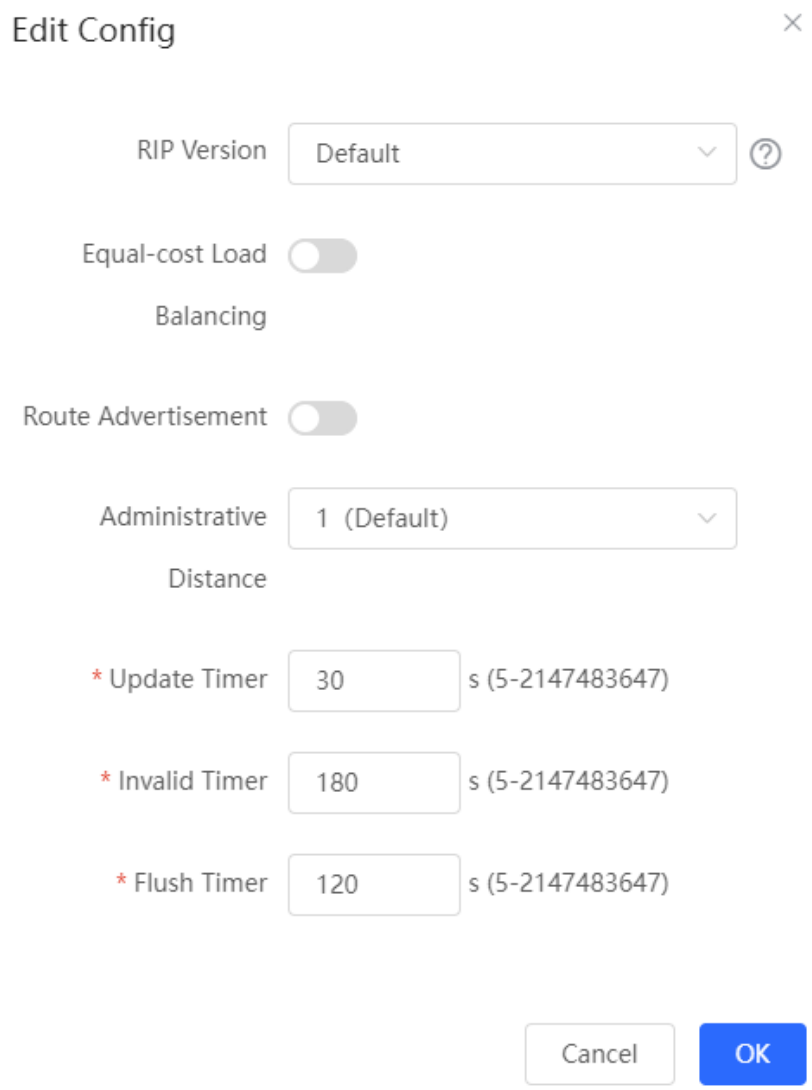


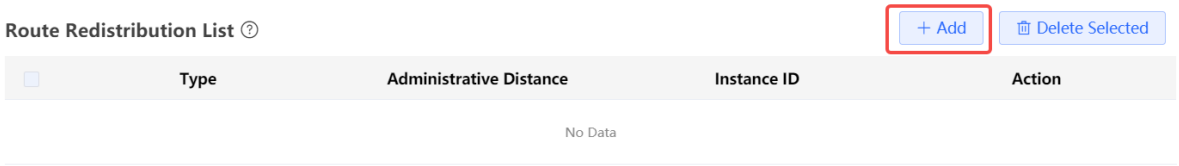
Table 4-17 RIP Global Configuration Parameters

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.
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.

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 **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **RIP Settings** > **Advanced**, click **Add** in **Route Redistribution List**, and select the type and administrative distance.



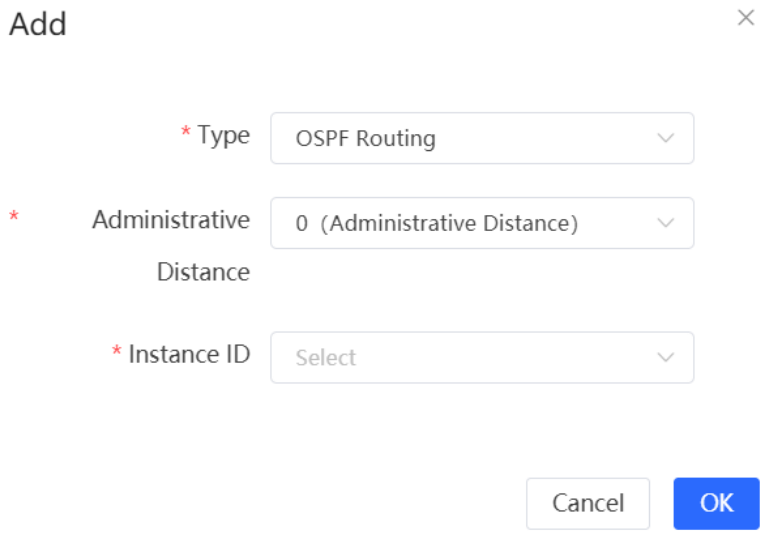


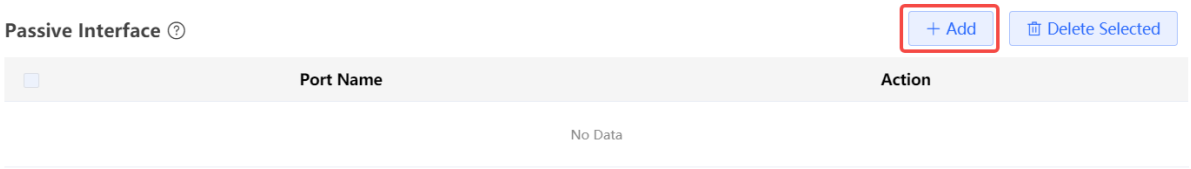
Table 4-18 RIP Route Redistribution Parameters

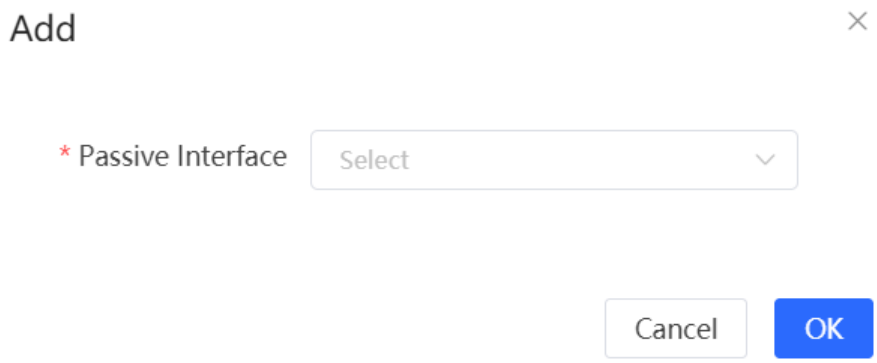
Parameter	Description
Type	Configure the type of routes that are learned by a routing protocol and then redistributed to RIP. The types include direct routes, OSPF routes, and static routes.
Administrative Distance	The device converts the metric of the routes learned from other routing protocols into the metric used by the target protocol so that the target protocol can select the optimal route. 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 redistributed. OSPFv2 needs to be enabled on the local device.

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 **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **RIP Settings** > **Advanced,** click **Add** in **Passive Interface** and select a passive interface.

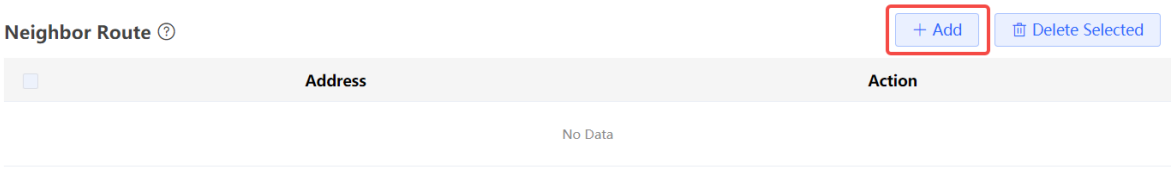


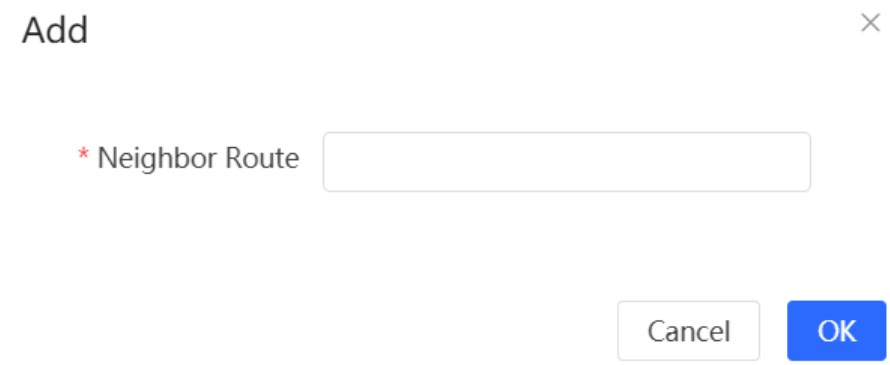


6. Configuring the Neighbor Route

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

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **RIP Settings** > **Advanced,** click **Add** in **Neighbor Route**, and enter the IP address of the neighbor router.

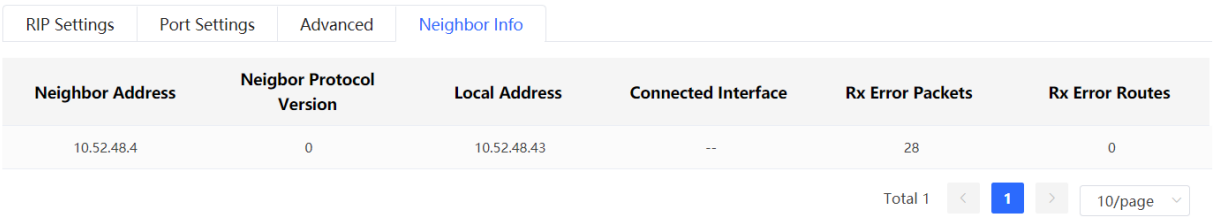




7. Viewing the Neighbor Information

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **RIP Settings** > **Neighbor Info**.

The neighbor list displays information about neighbors of the device, including the neighbor address, neighbor protocol version, local address, connected interface, number of received error packets, and number of received error routes.



4.10.4 Configuring RIPng

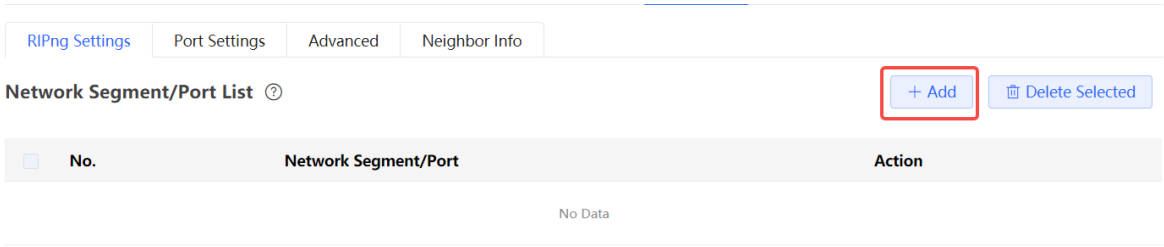
RIP Next Generation (RIPng) provides the routing function for IPv6 networks.

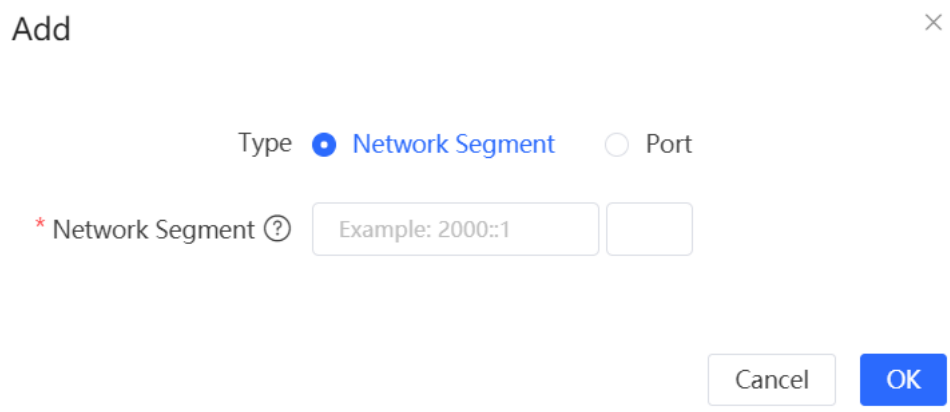
RIPng uses UDP port 512 to exchange the routing information.

1. Configuring RIPng Basic Functions

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **RIPng Settings**

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





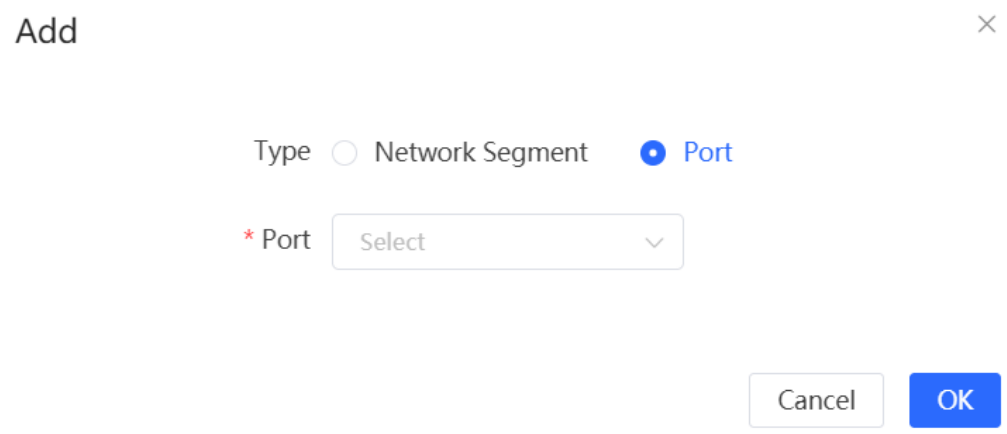


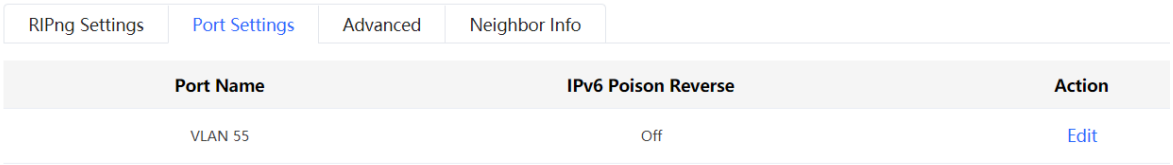
Table 4-19 RIPng Configuration Parameters

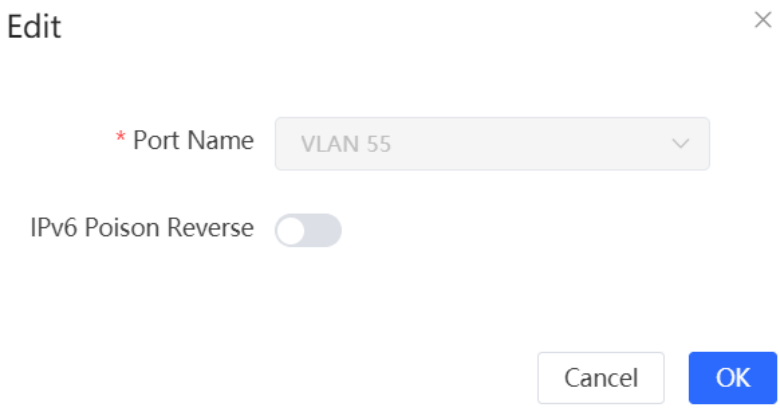
Parameter	Description
Type	● **Network Segment**: Enable RIP in the specified network segment. The IP addresses of this network segment are added to the RIP routing table, and the device and its RIP-enabled neighbor devices learn the routing table from each other. ● **Port**: Enable RIP on the specified 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**.

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.

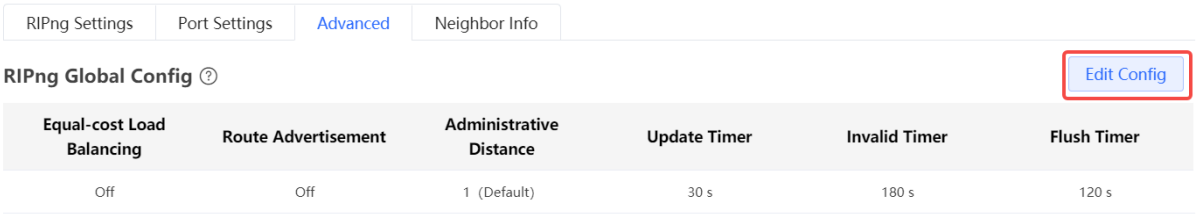
Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **RIPng Settings** > **Port Settings,** click **Edit**, and enable IPv6 poison reverse.





3. Configuring the RIPng Global Configuration

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **RIPng Settings** > **Advanced**, click **Edit Config** in **RIPng Global Config**, and configure RIPng global configuration parameters.



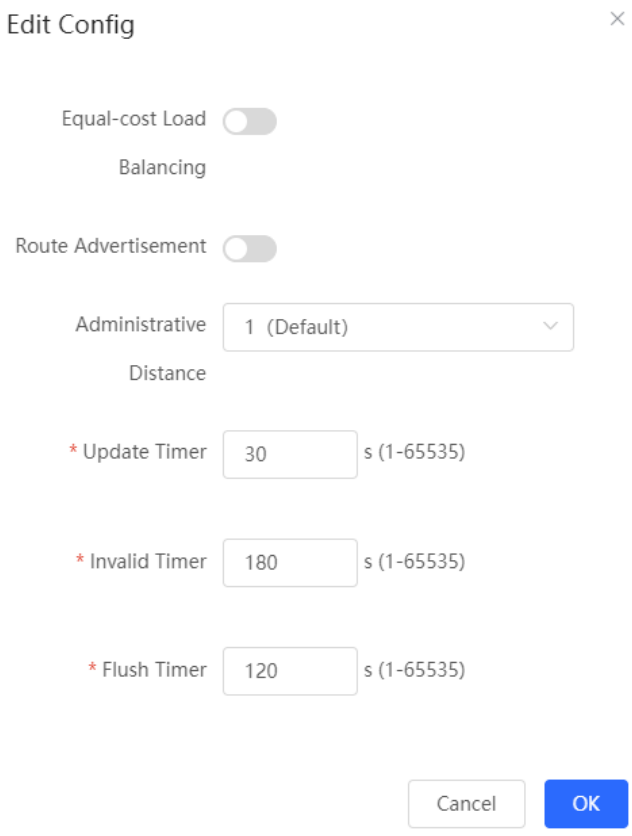


Table 4-20 RIPng Global Configuration Parameters

Parameter	Description
Equal-cost Load Balancing	After this function is enabled, equal-cost routes are automatically balanced and forwarded with a weight of 1:1.
Route Advertisement	After this function is enabled, the current device generates a default route and sends it to the neighbor.
Administrative Distance	Routes of other protocols are redistributed to the RIP domain so that RIP can communicate with other routing domains.
Update Timer	RIP update cycle. The routing information is updated every 30 seconds by default.
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.

4. Configuring the RIPng Route Redistribution List

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

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **RIPng Settings** > **Advanced**, click **Add** in **Route Redistribution List**, and configure RIPng route redistribution.

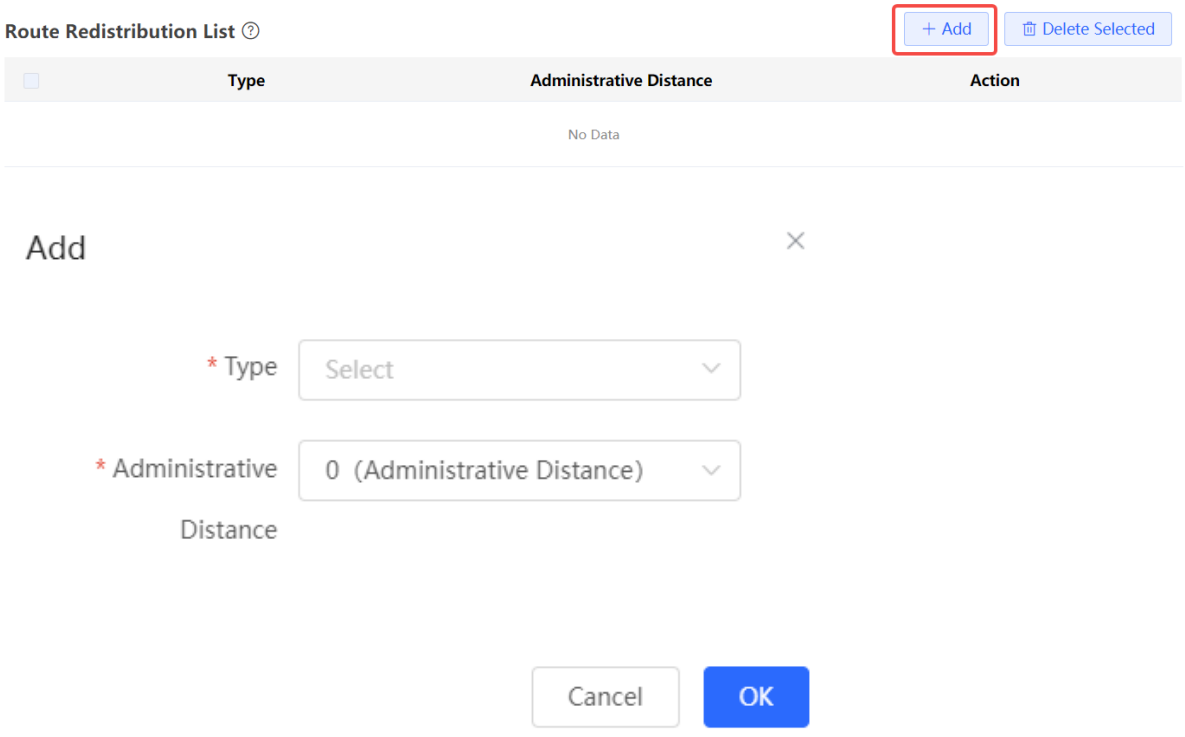


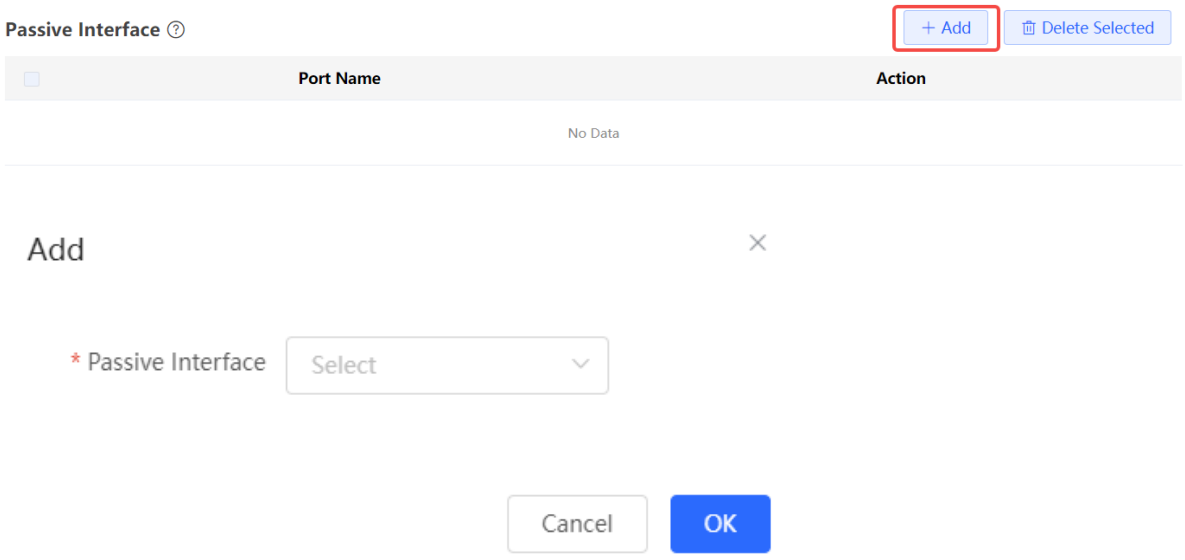
Table 4-21 RIP Route Redistribution Parameters

Parameter	Description
Type	Configure the type of routes that are learned by a routing protocol and then redistributed to RIP. The types include direct routes, OSPF routes, and static routes.
Administrative Distance	The device converts the metric of the routes learned from other routing protocols into the metric used by the target protocol so that the target protocol can select the optimal route. A smaller administrative distance indicates a higher priority. The default value is 0. The value ranges from 0 to 16.

5. Configuring the RIPng Passive Interface

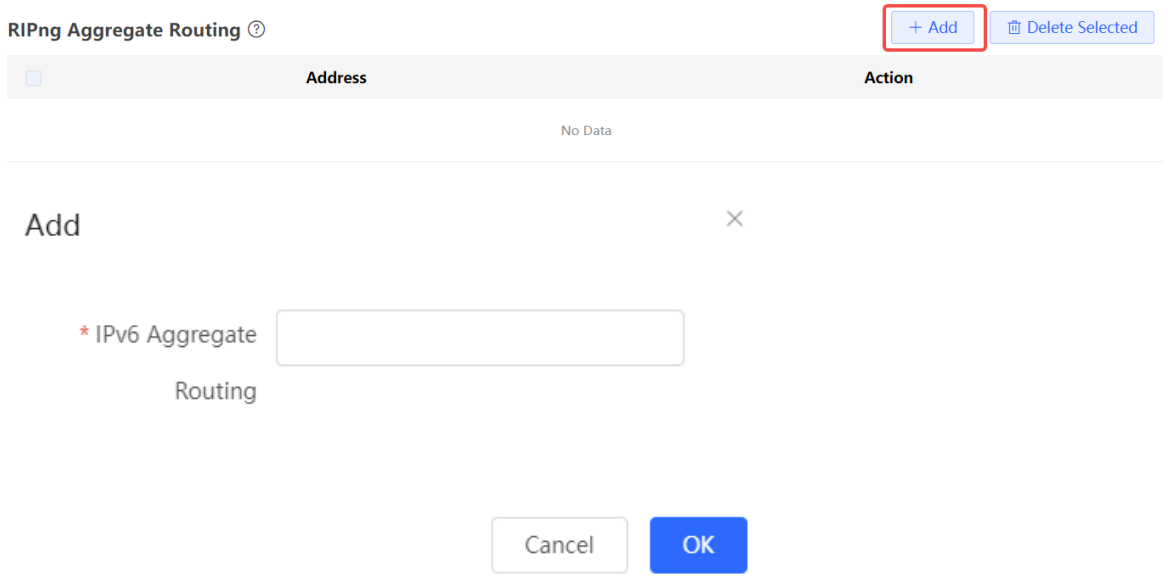
If an interface is configured as a passive interface, it will suppress RIPng update packets. If the connected peer device does not run RIP, you are advised to enable the passive interface.

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **RIPng Settings** > **Advanced,** click **Add** in **Passive Interface**, and select a passive interface.



6. Configuring the IPv6 Aggregate Route

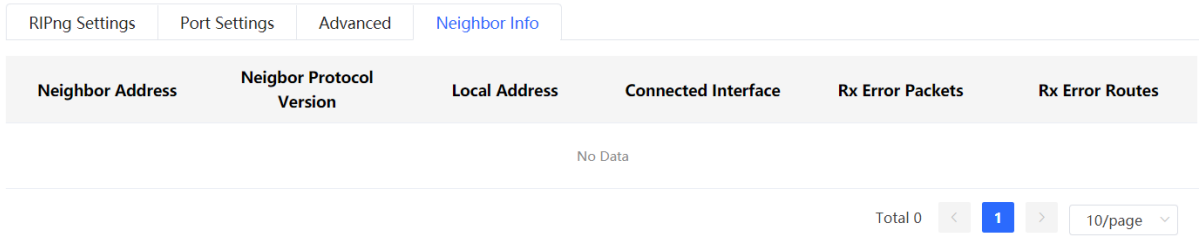
Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **RIPng Settings** > **Advanced**, click **Add** in **RIPng Aggregate Routing**, and enter the IPv6 address or length. The length of IPv6 address prefix ranges from 0 bit to 128 bits.



7. Viewing the Neighbor Information

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **RIP Settings** > **Neighbor Info**.

The neighbor list displays information about neighbors of the device, including the neighbor address, neighbor protocol version, local address, connected interface, number of received error packets, and number of received error routes.



4.10.5 OSPF v2

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

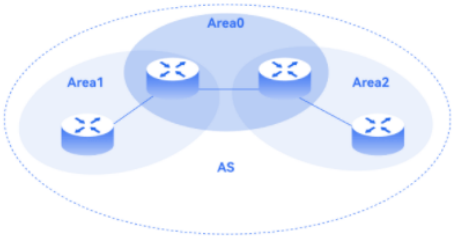
OSPF is a typical link-state routing protocol, which can solve the problems of slow route update, inaccurate measurement, and poor scalability in large networks. It is suitable for networks of various sizes, and even a network with up to thousands of devices.

Note

Only RG-EG105G-V3, RG-EG105G-P-V3, RG-EG210G-P-V3, RG-EG1510XS and RG-EG3XX series devices (such as RG-EG310GH-E) support this function.

1. Configuring OSPFv2 Basic Parameters

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **OSPFV2**, click **Start Setup**, and then configure an instance and an interface respectively.



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.

Start Setup

- Configure an instance

(1) Configure basic parameters for an instance.

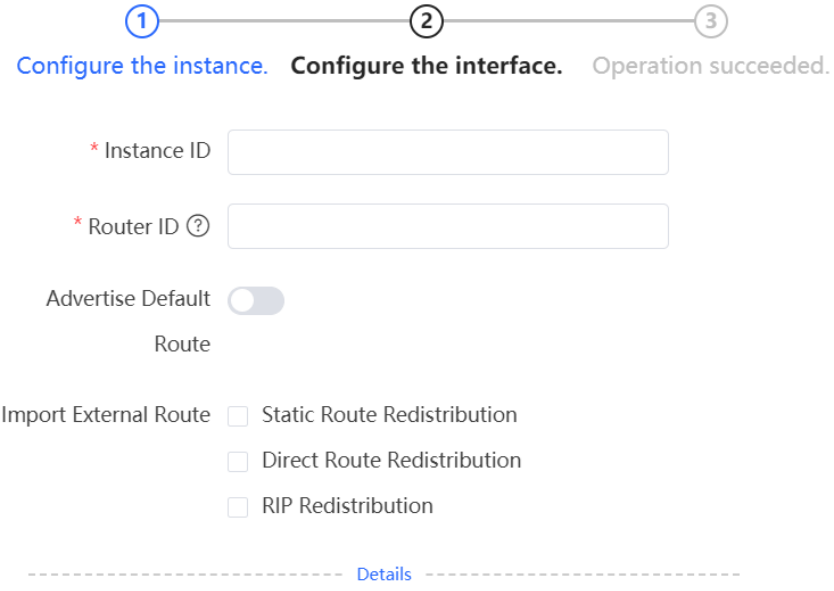


Table 4-22 Description of Basic OSPF Instance Configuration Parameters

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 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.

(2) Click **Details** to display detailed configurations.

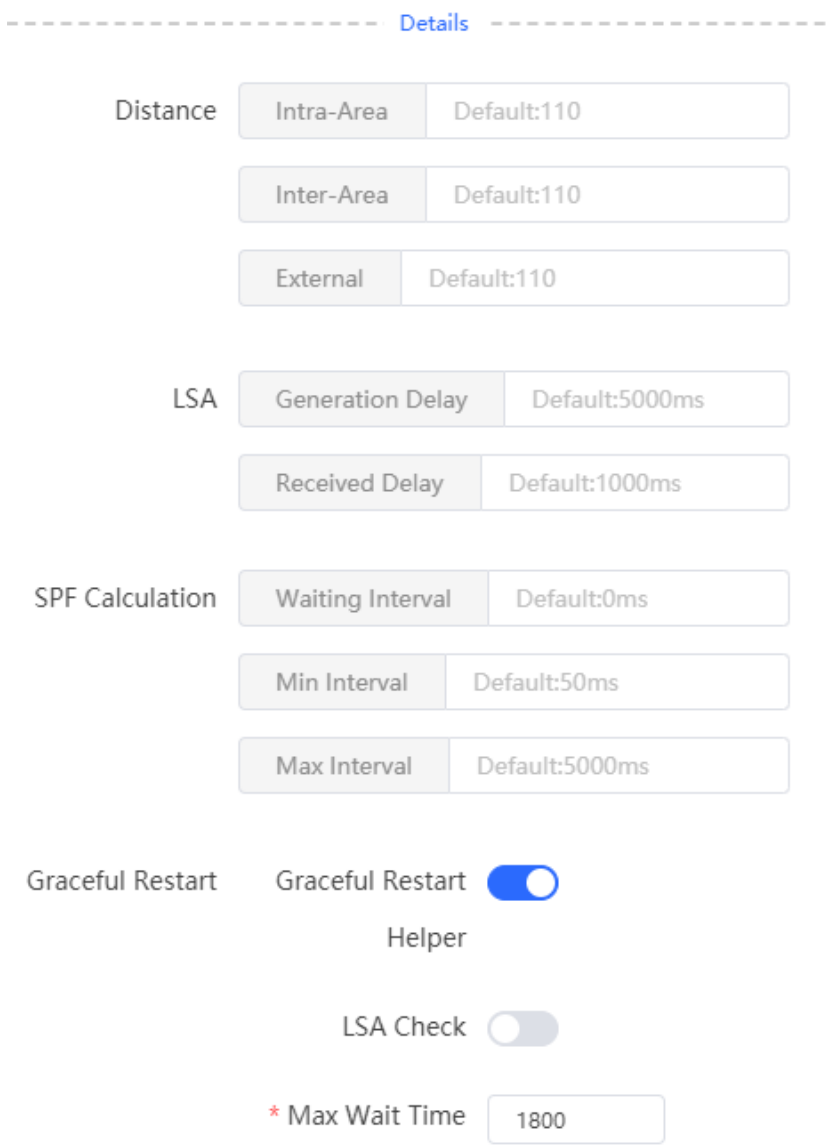


Table 4-23 Description of Detailed OSPF Instance Configuration Parameters

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.

- Configure an interface

(1) Configure basic parameters for an OSPFv2 interface.

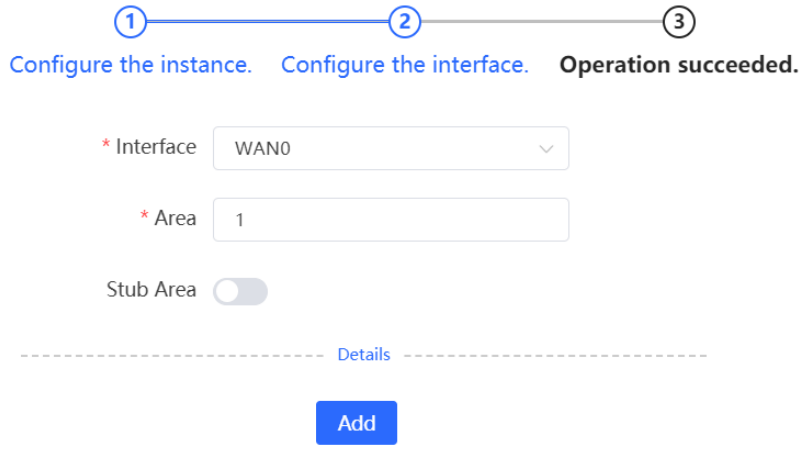


Table 4-24 Description of Basic OSPFv2 Interface Configuration Parameters

Parameter	Description
Interface	Select the OSPF-enabled L3 interface.
Area	Configure the area ID. Value range: 0-4294967295

Parameter	Description
Stub Area	If **Stub Area** is enabled, you need to configure the **Area Type** and **Inter-Route Isolation** ● **Area Type** ○ 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-Route Isolation** After this function is enabled, inter-area routes will not be imported to this area.

(2) Click **Details** to display detailed configurations.

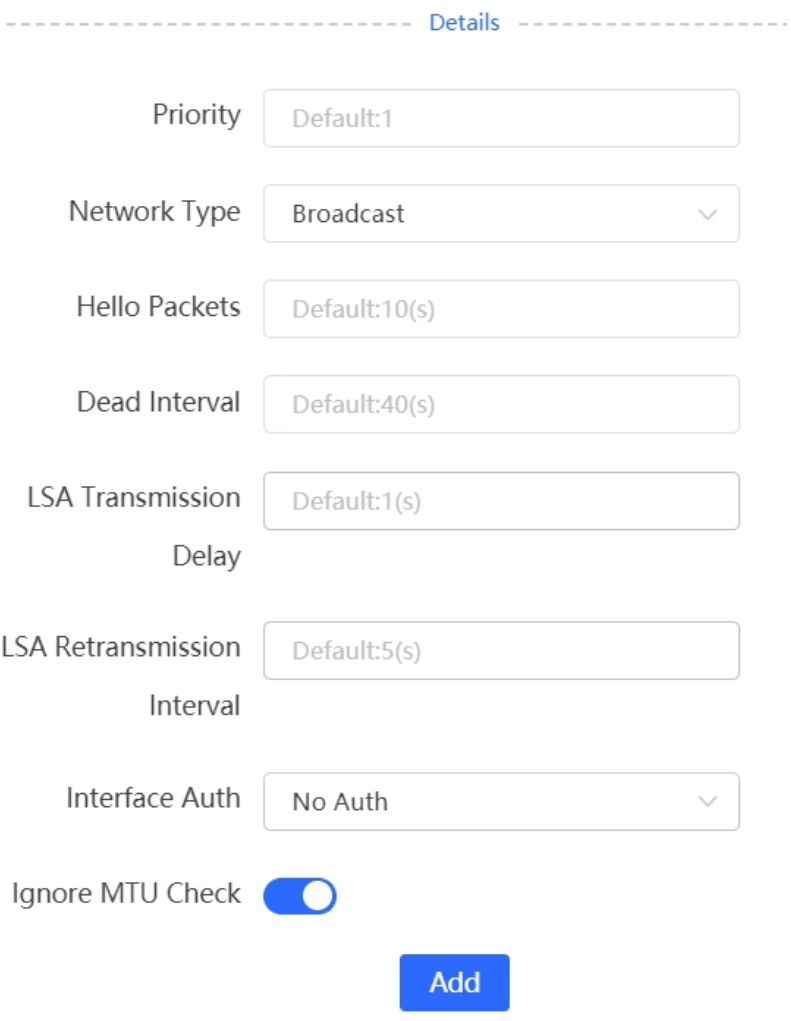
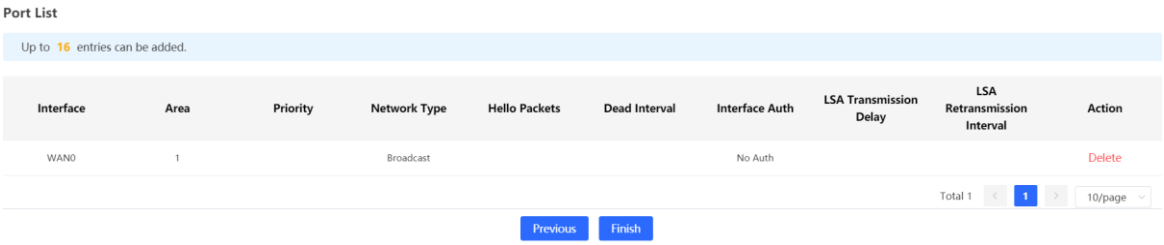


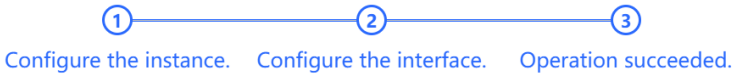
Table 4-25 Description of Detailed OSPFv2 Interface Configuration Parameters

Parameter	Description
Priority	A higher priority value indicates a greater chance of being elected as the DR or BDR. The default value is 1.
Network Type	OSPFv2 defines different network types, which affect the establishment of OSPF neighbor relationships, route update, and network convergence. The supported network types include broadcast, unicast, multicast, and non-broadcast multi-access (NBMA).
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	The purpose of ignoring MTU check is to ensure that OSPF-enabled routers can update routing information in time when the network topology changes. This function is enabled by default.

(3) Click **Add** to add an interface to **Interface List**.

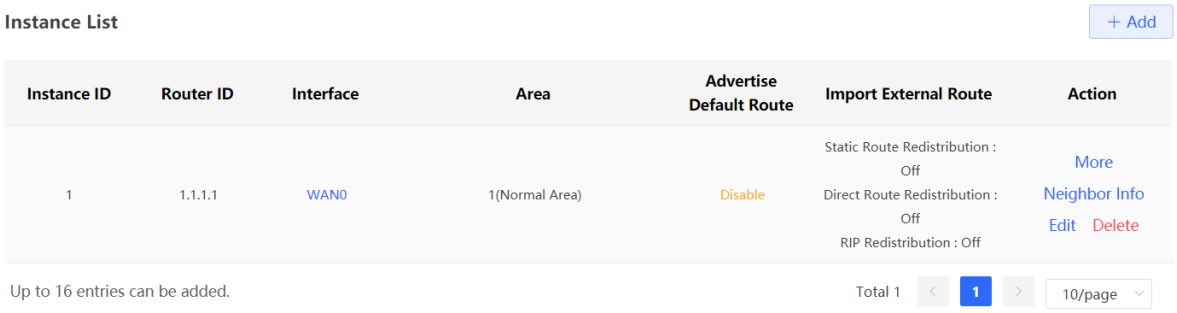


(4) Click **Finish**.



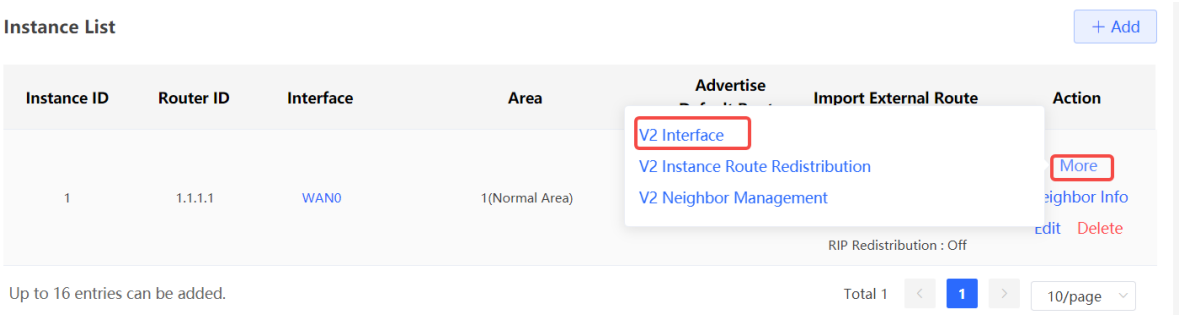
Operation succeeded.

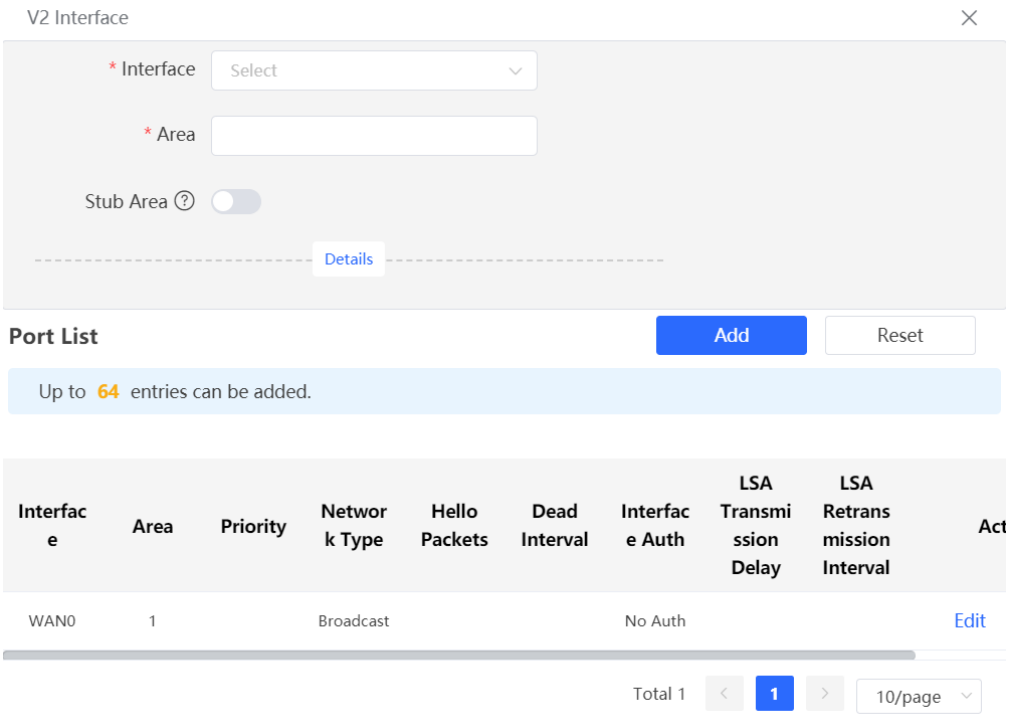
After you create an instance and an interface, choose **One-Device > Gateway > Advanced** > **Routing** > **OSPFV2** to check the current **Instance List**.



2. Adding an OSPFv2 Interface

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **OSPFV2**, select the instance to be configured in **Instance List**, and choose **More** > **V2 Interface**.



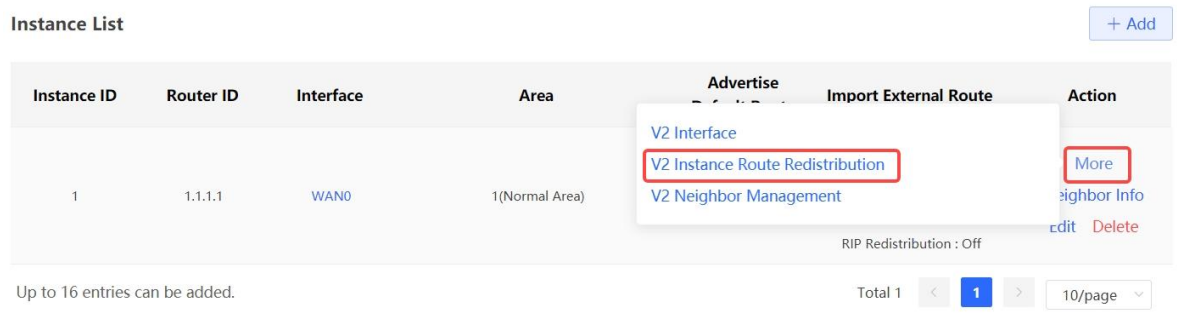


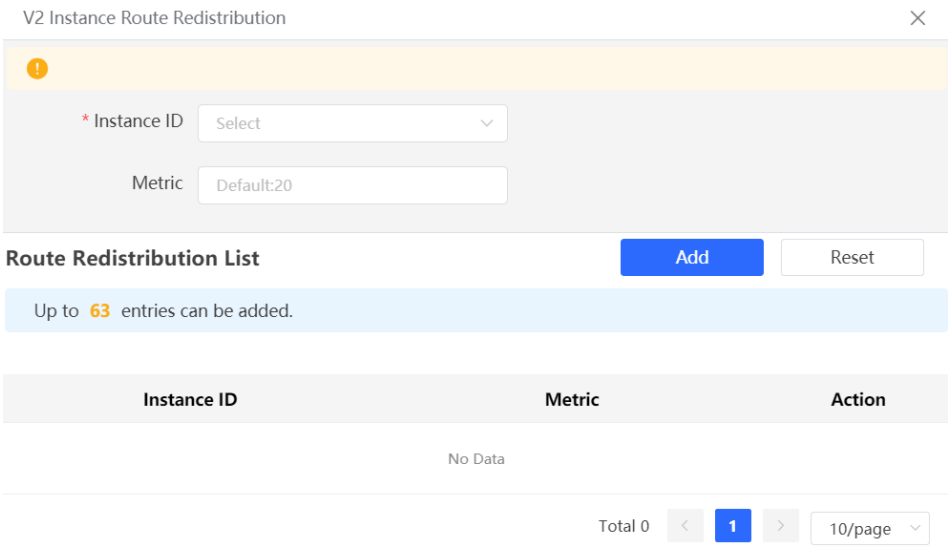
3. Redistributing OSPFv2 Instance Routes

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **OSPFV2**, select the instance to be configured in **Instance List**, and choose **More** > **V2 Instance Route Redistribution**.

Caution

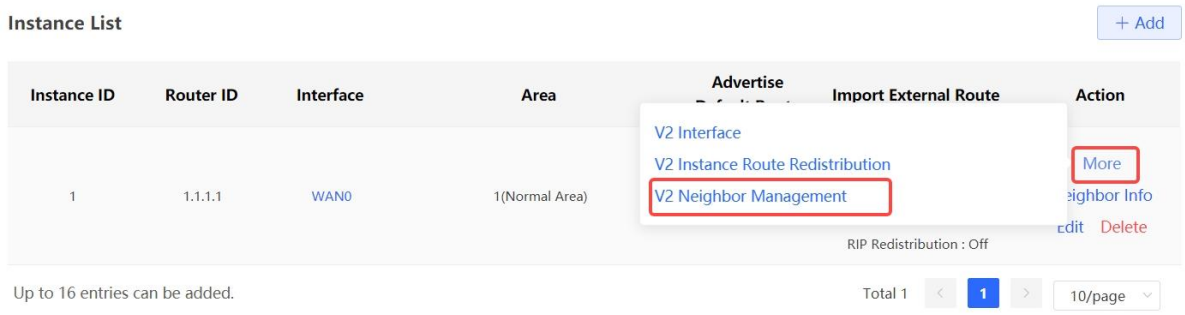
The instance ID cannot be selected for route redistribution.

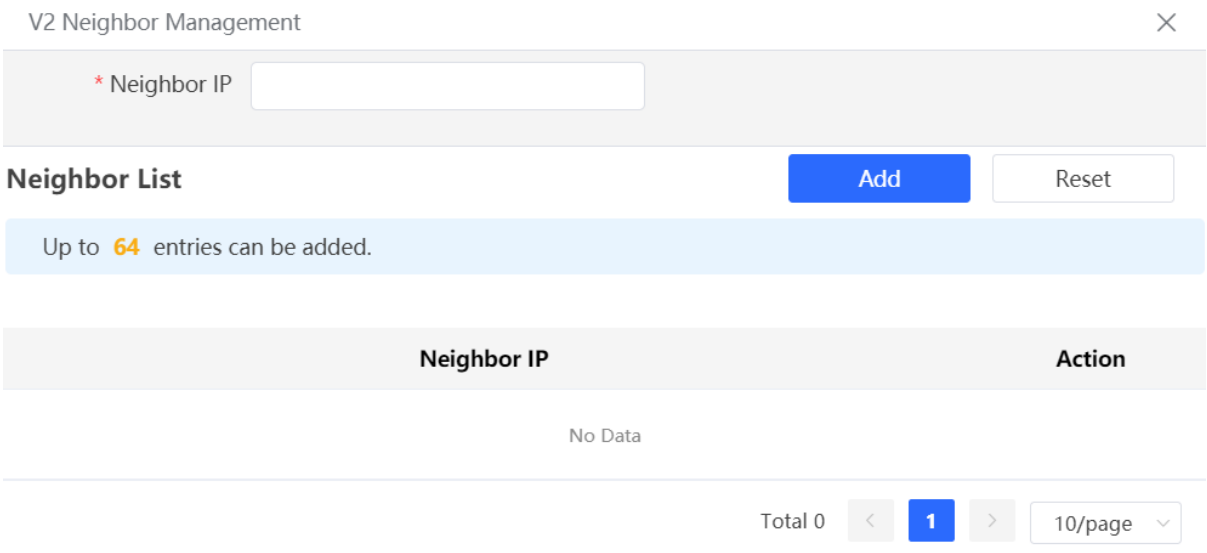




4. Managing OSPFv2 Neighbors

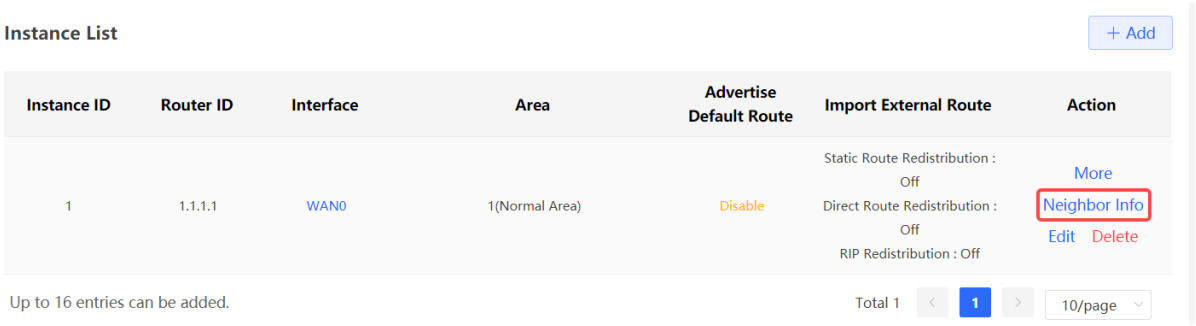
Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **OSPFV2**, select the instance to be configured in **Instance List**, and choose **More** > **V2 Neighbor Management**.

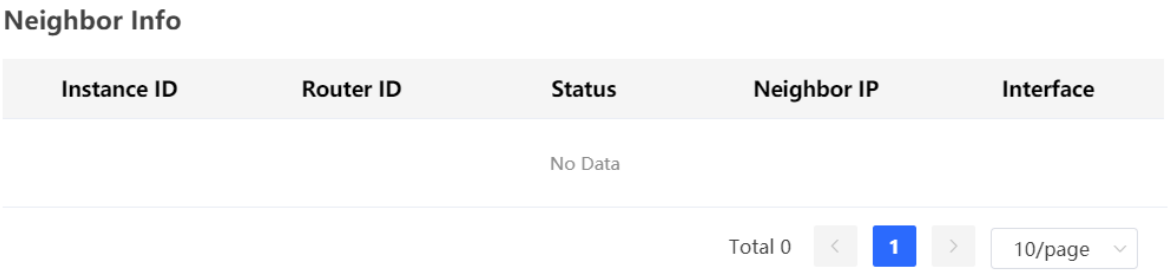




5. Viewing OSPFv2 Neighbor Information

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **OSPFV2**, select the instance to be configured in **Instance List**, and click **Neighbor Info**.





4.10.6 OSPF v3

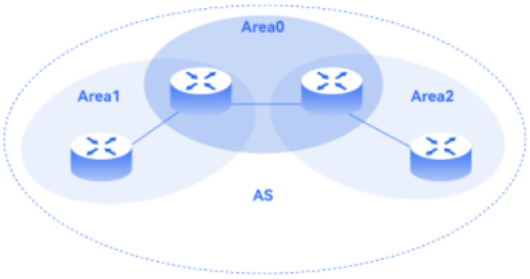
Open Shortest Path First (OSPF) can be applied to large-scale networks. IPv4 uses OSPFv2, and IPv6 uses OSPFv3.

Note

Only RG-EG105G-V3, RG-EG105G-P-V3, RG-EG210G-P-V3, RG-EG1510XS and RG-EG3XX series devices (such as RG-EG310GH-E) support this function.

1. Configuring OSPFv3 Basic Parameters

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **OSPFV3**, click **Start Setup**, and then configure an instance and an interface respectively.



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.

Start Setup

- Configure an instance

(1) Configure basic parameters for an instance.

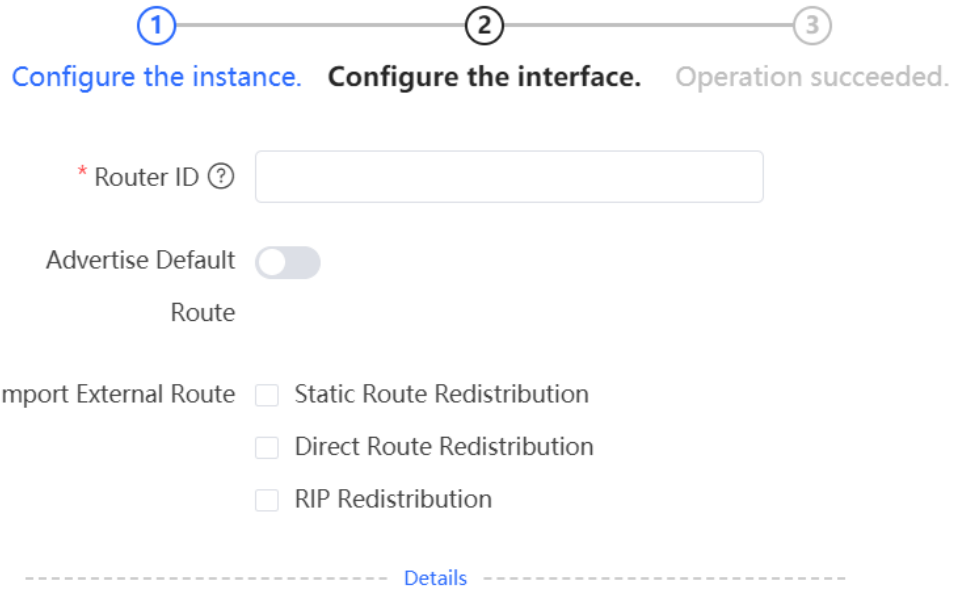


Table 4-26 Description of Basic OSPF Instance Configuration Parameters

Parameter	Description
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 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.

(2) Click **Details** to display detailed configurations.

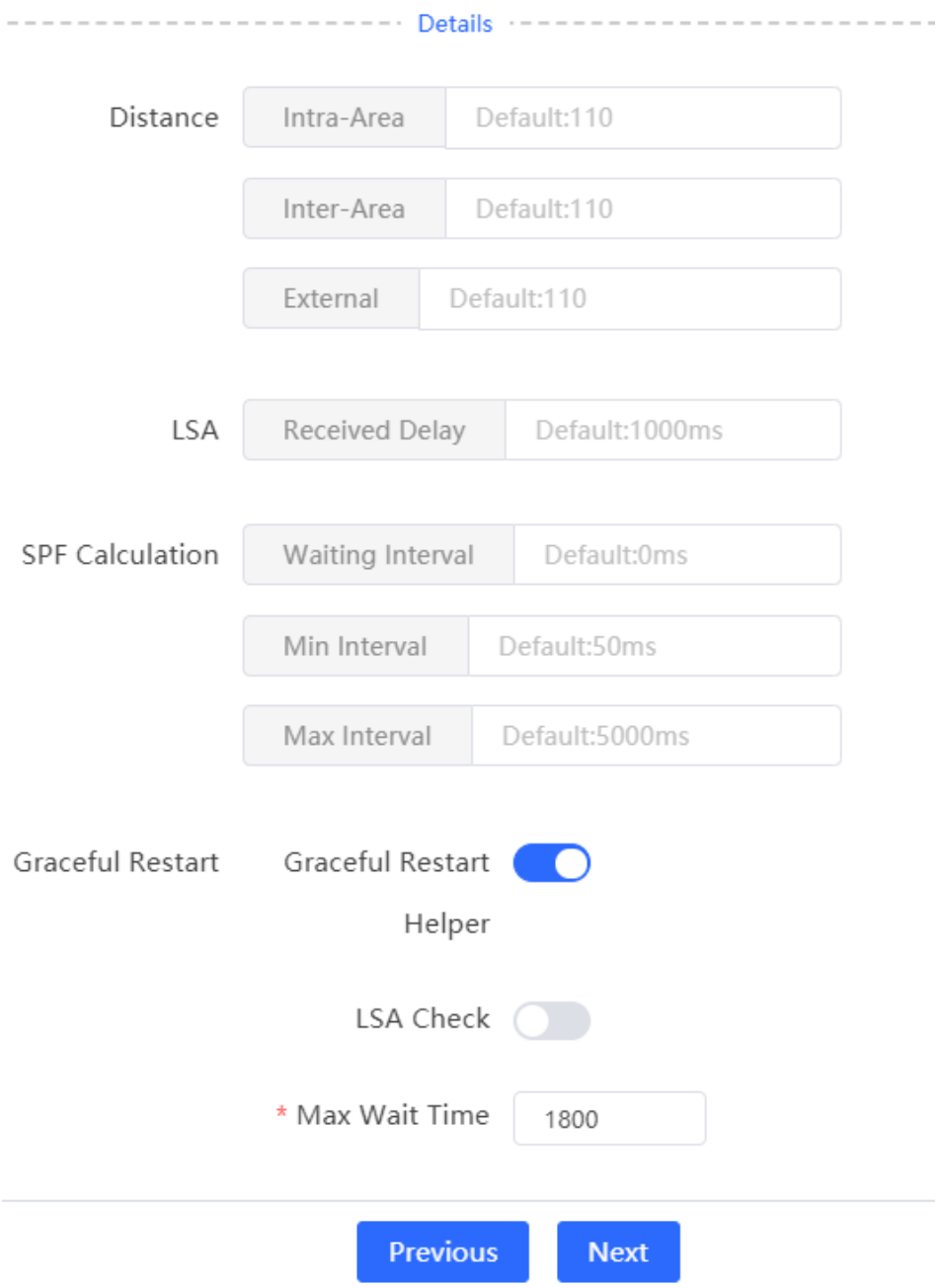


Table 4-27 Description of Detailed OSPF Instance Configuration Parameters

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.

- Configure an interface

(1) Configure basic parameters for an interface.

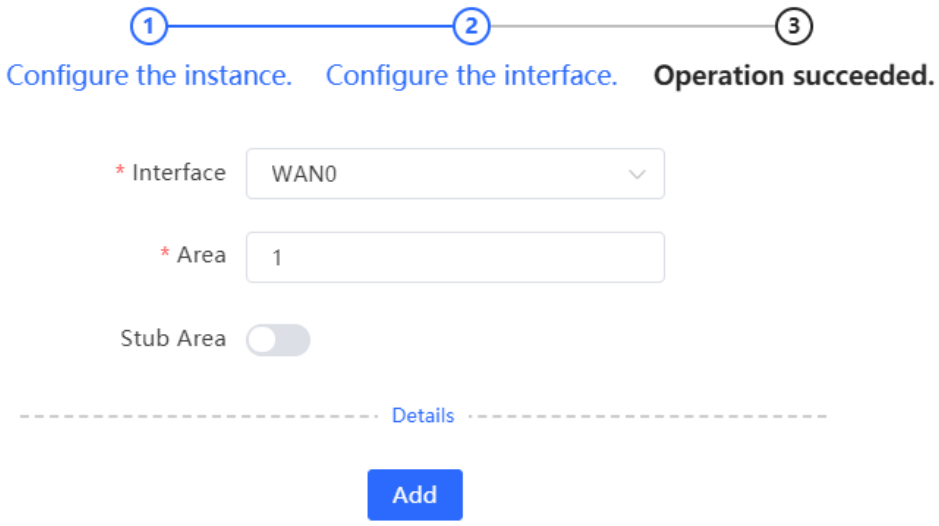


Table 4-28 Description of Basic OSPF Interface Configuration Parameters

Parameter	Description
Interface	Select the OSPF-enabled L3 interface.
Area	Configure the area ID. Value range: 0-4294967295

Parameter	Description
Stub Area	If **Stub Area** is enabled, you need to configure the **Area Type** and **Inter-Route Isolation** ● **Area Type** ○ 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-Route Isolation** After this function is enabled, inter-area routes will not be imported to this area.

(2) Click **Details** to display detailed configurations.

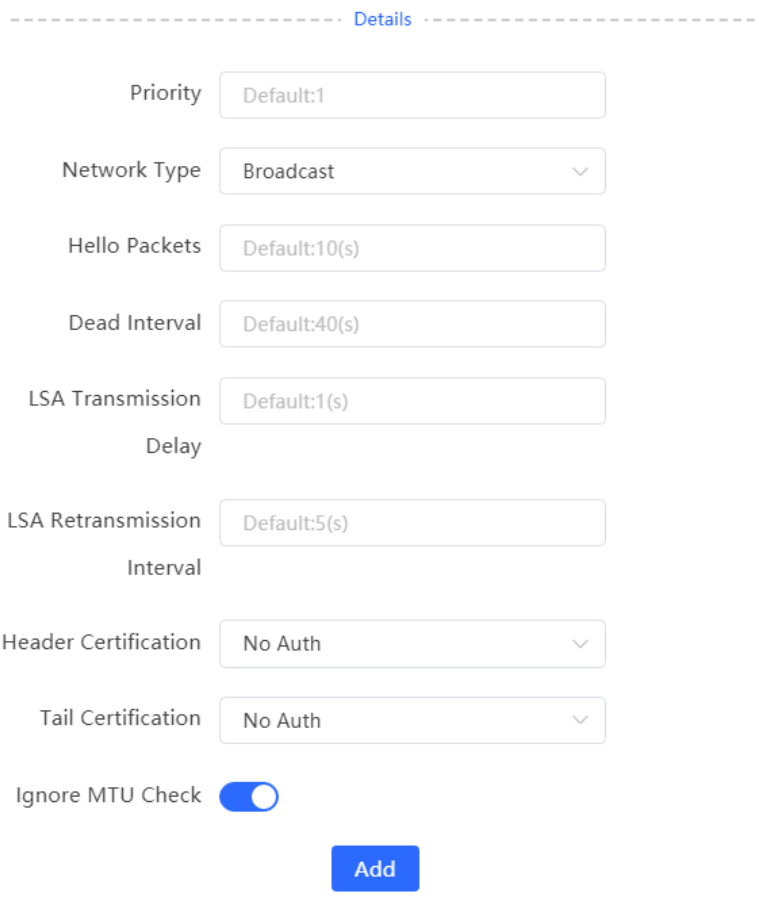
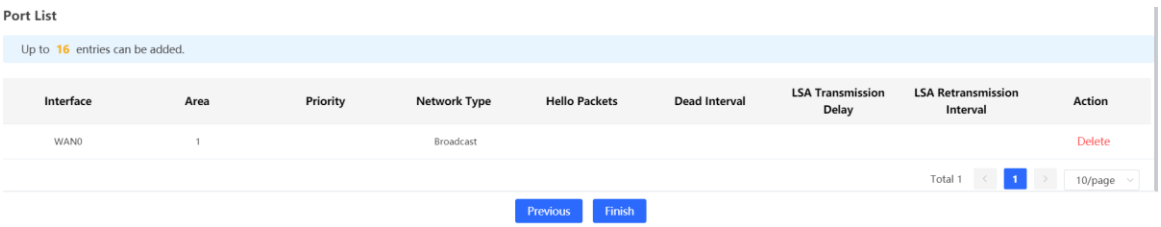


Table 4-29 Description of Detailed OSPF Interface Configuration Parameters

Parameter	Description
Priority	A higher priority value indicates a greater chance of being elected as the DR or BDR. The default value is 1.

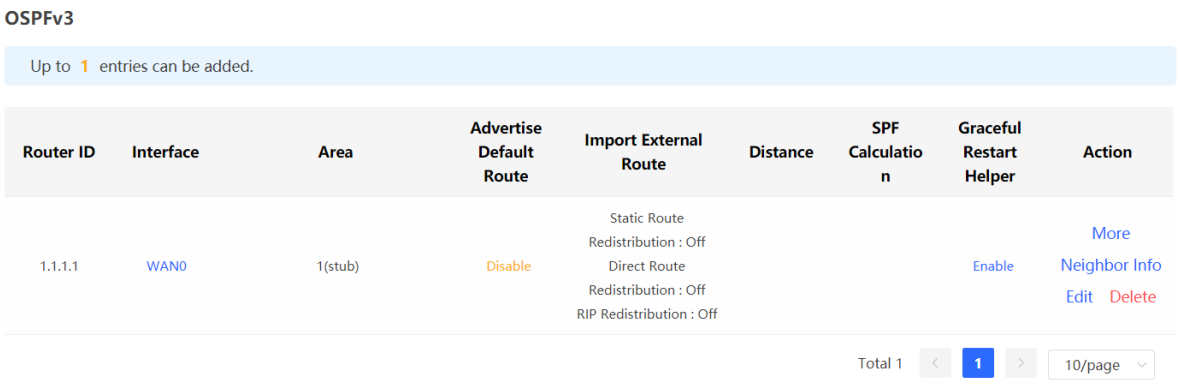
Parameter	Description
Network Type	OSPFv3 defines different network types, which affect the establishment of OSPF neighbor relationships, route update, and network convergence. The supported network types are broadcast and unicast.
Hello Packets	Interval for periodic transmission, which is used to discover 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.
Header Certification	The authentication field in the header of an OSPFv3 packet for verifying the integrity of the packet, including the header and payload. The supported authentication modes are as follows: ● **No Auth**: No authentication is performed by default. ● **MD5 Auth**: MD5 HMAC ● **SHA1 Auth**: SHA-1 HMAC ● **SHA256 Auth**: SHA-256 HMAC
Tail Certification	The authentication field added to the trailer of an OSPFv3 packet for verifying the authenticity of the packet and ensure that the packet is sent by an authorized sender and is not tampered with during transmission. The supported authentication modes are as follows: ● **No Auth**: No authentication is performed by default. ● **MD5 Auth**: MD5 HMAC ● **SHA256 Auth**: SHA-256 HMAC
Ignore MTU Check	The purpose of ignoring MTU check is to ensure that OSPF-enabled routers can update routing information in time when the network topology changes. This function is enabled by default.

(3) Click **Add** to add an interface to **Interface List**.



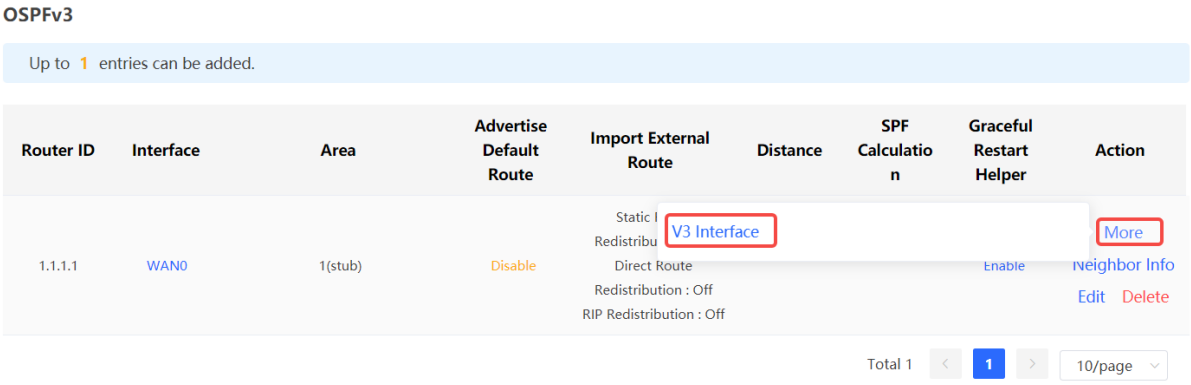
(4) Click **Finish**.

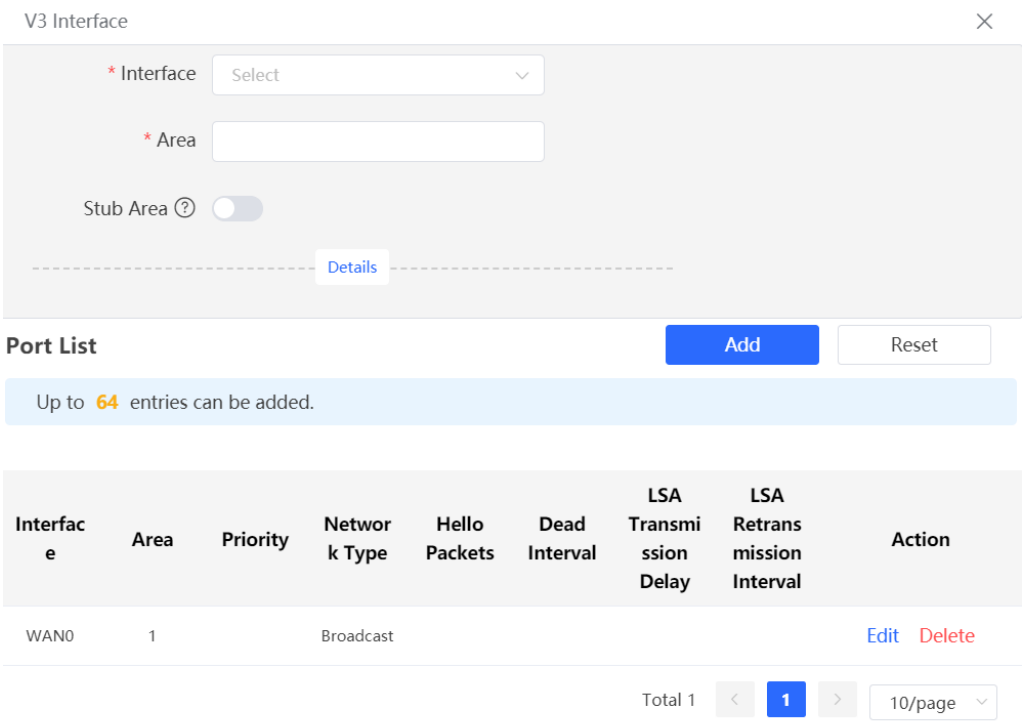
After you complete configuration, choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **OSPFV3** to check **Instance List**.



2. Adding an OSPFv3 Interface

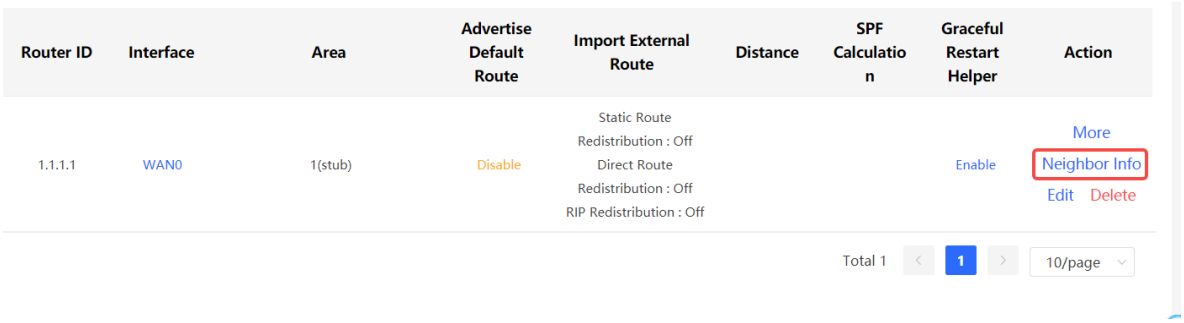
Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **OSPFV3**, select the instance to be configured in **Instance List**, and choose **More** > **V3 Interface**.

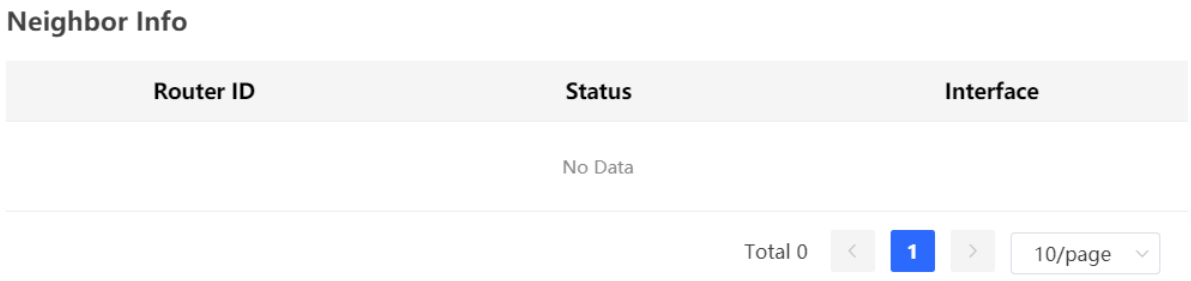




3. Viewing OSPFv3 Neighbor Information

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **OSPFV3**, select the instance to be configured in **Instance List**, and click **Neighbor Info**.



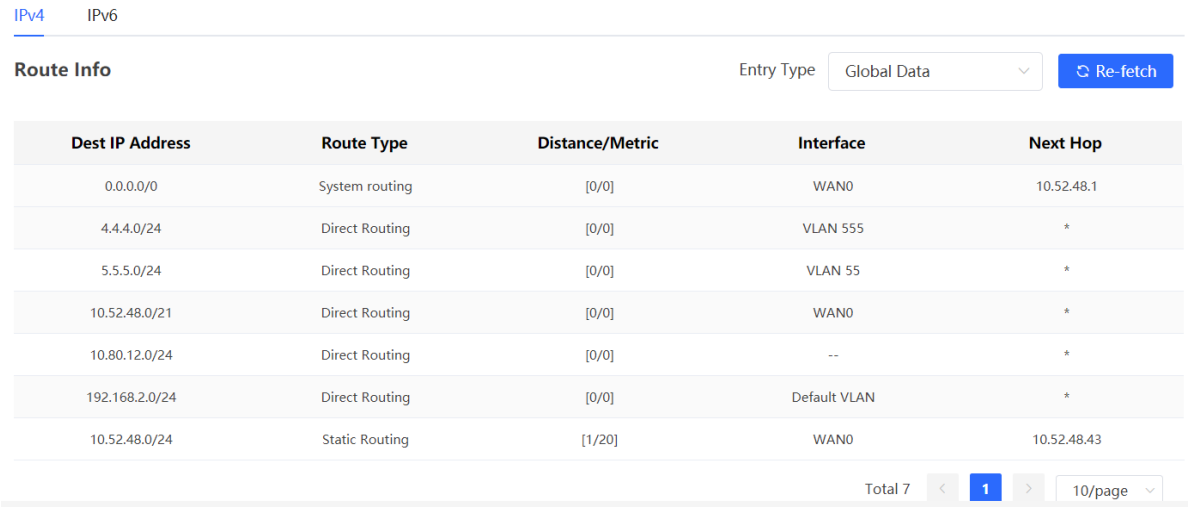


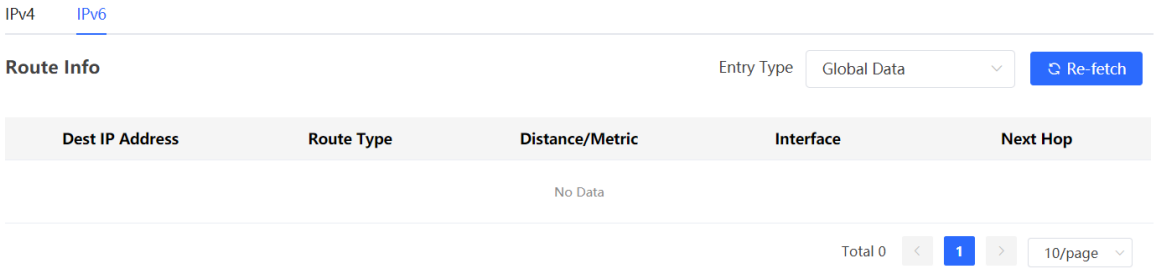
4.10.7 Viewing Routing Tables

Note

Only RG-EG105G-V3, RG-EG105G-P-V3, RG-EG210G-P-V3, RG-EG1510XS and RG-EG3XX series devices (such as RG-EG310GH-E) support this function.

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **Routing Table Info** to view IPv4 and IPv6 routing table details.

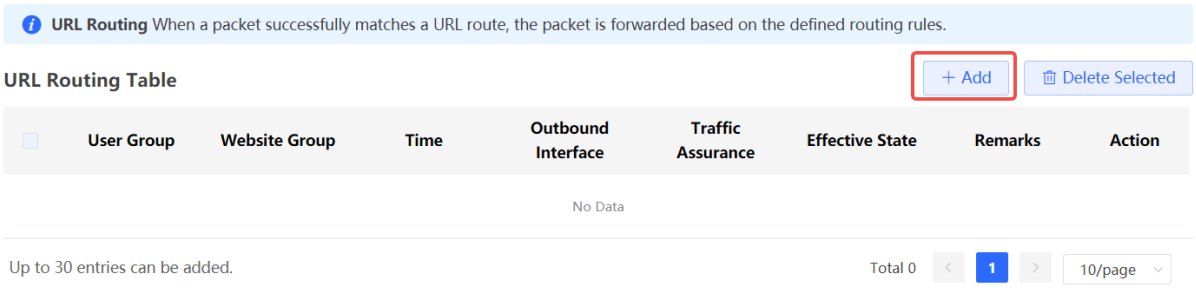




4.10.8 Set URL Route

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing Settings** > **URL Routing**.

Configure the outbound interface for accessing a website URL. When a data packet matches the URL route, the data packet is forwarded in the specified mode.



Click **Add**. In the dialog box that appears, set the type, website group, outbound interface, and managed time range, and then click Add to create a URL route.

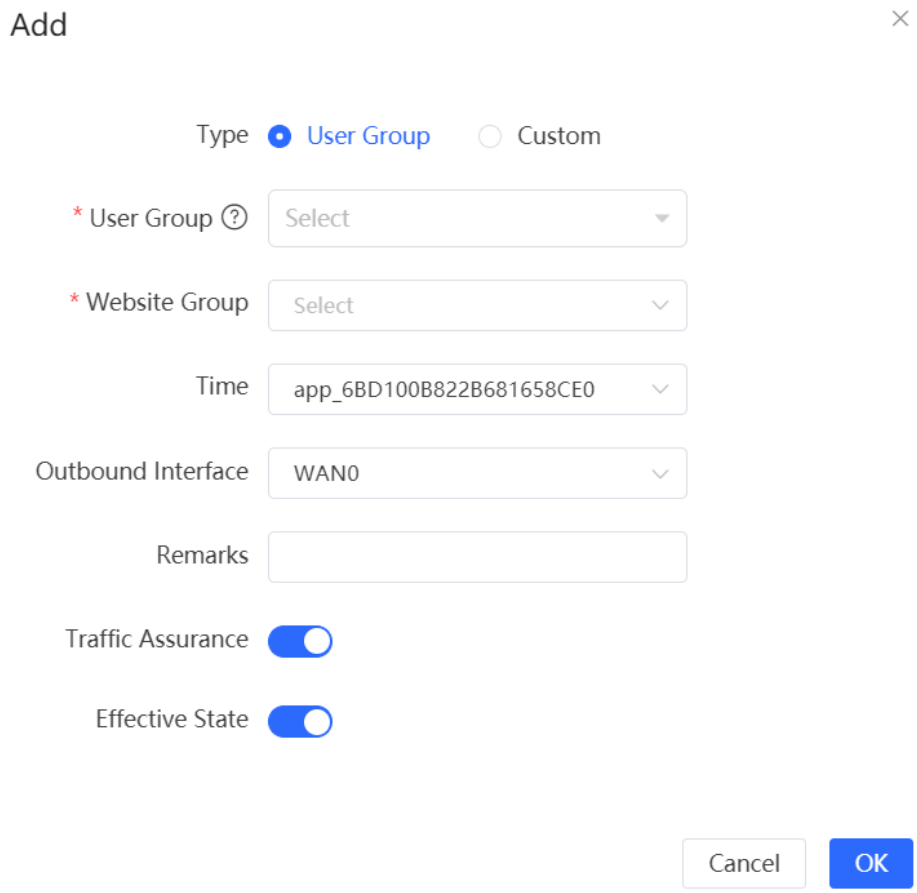


Table 4-30 URL Routing Configuration Parameters

Parameter	Description
Type	URL route type, which can be: ● **User group**: select the user group to which the route-policy applies. ● **Custom**: apply the route to users with IP addresses in the specified IP address range. You need to manually enter the IP address range.
User group	This parameter is required when type is set to user group. Select users to which the URL route applies from the user group list. The user group list is available in 8.2 User Management. If all members in a user group are selected, the configuration takes effect on the entire user group (including members added to the user group later).
IP Address Group	Configure this information when type is set to custom. Enter the IP address range managed by URL routing.
Website group	Set the website type for which URL routes need to be configured. Select a website group from the created website groups. For details on how to create or modify a website group, see 8.5 Website Management.

Parameter	Description
Managed time period	During the controlled period, when the managed client accesses the application in the website group, the packets are forwarded through the outbound interface. Select from the drop-down list. Time range defined in 8.3 Time Management, or select custom and manually configure a time range.
Outgoing interface	Specify the interface that forwards the data packet based on the hit PBR rule.
Remarks	Configuring the description of a URL route
Network disconnection protection	After this function is enabled, if the outbound interface is unreachable, traffic is automatically switched to another reachable outbound interface.
Effective status	Turn on status to specify whether to enable the PBR rule. If status is turned off, this rule does not take effect.

4.11 Configuring ARP Binding and ARP Guard

4.11.1 Overview

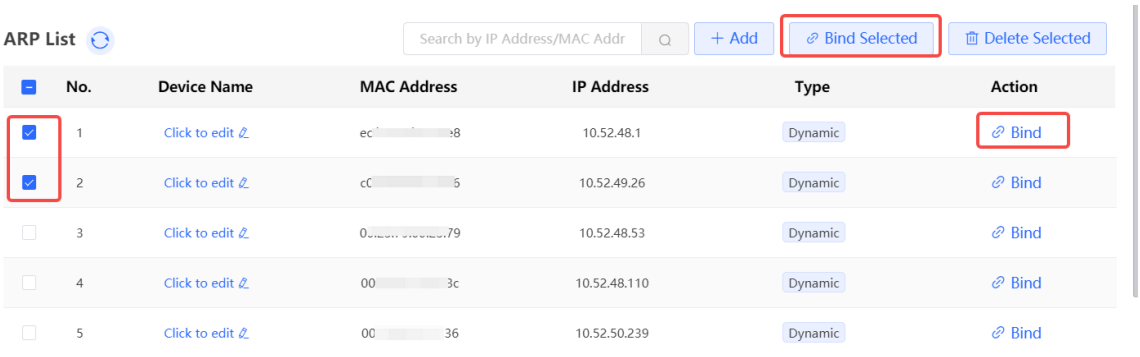
The device learns the IP address and MAC address of the network devices connected to its interfaces and generates the corresponding ARP entries. You can enable ARP guard and configure IP-MAC binding to restrict Internet access of LAN hosts and improve network security.

4.11.2 Configuring ARP Binding

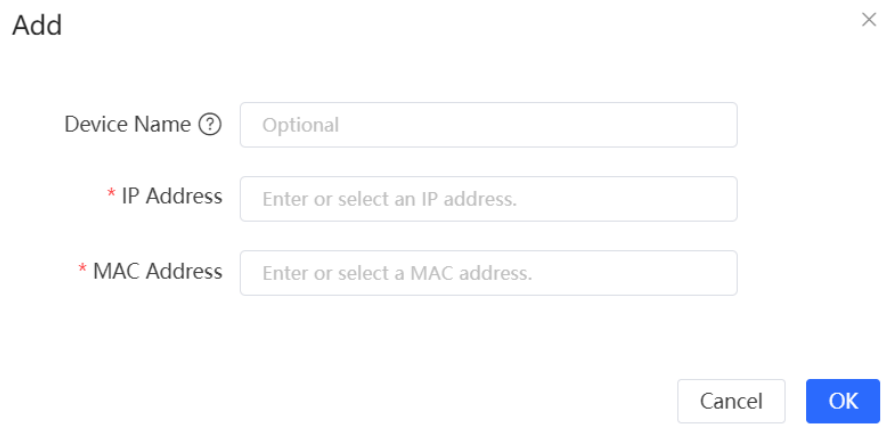
Choose **One-Device** > **Gateway** > **Config** > **Security** > **ARP List**.

Before you enable ARP guard, you must configure the binding between IP addresses and MAC addresses in either of the following ways:

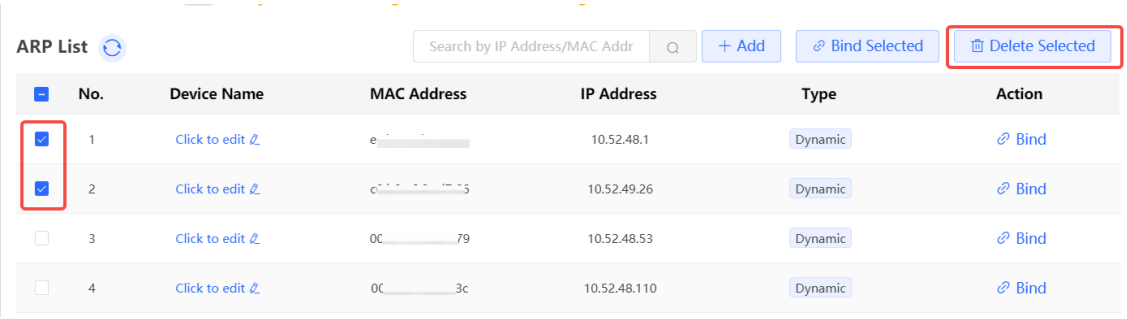
(1) Select a dynamic ARP entry in the ARP list and click **Bind**. You can select multiple entries to be bound at one time and click **Bind Selected** to bind them.



(2) Click **Add**, enter the device name, IP address and MAC address to be bound, and click **OK**. The input box can display existing address mappings in the ARP list. You can click a mapping to automatically enter the address mapping.



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

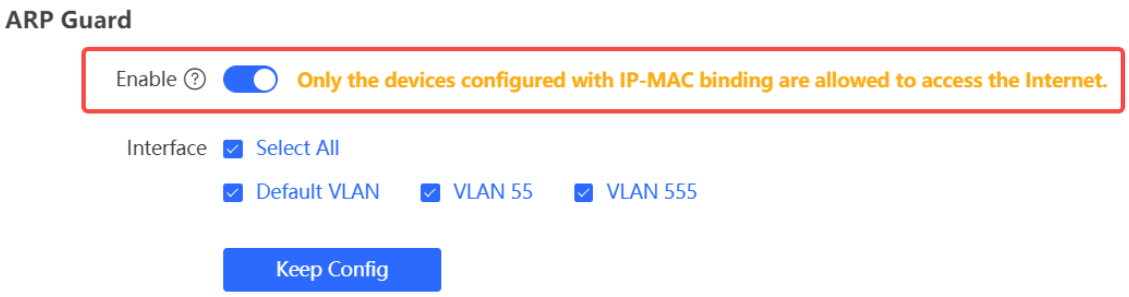


4.11.3 Configuring ARP Guard

After ARP guard is enabled, only LAN hosts with IP-MAC binding can access the external network. For details on how to configure ARP binding, see Section 4.11.2 Configuring ARP Binding.

(1) Choose **One-Device** > **Gateway** > **Config** > **Security** > **ARP List**.

(2) Turn on **Enable** in the **ARP Guard** section to enable ARP guard.



(3) Set the range for the function to take effect.

If you select **Select All**, the ARP guard function will take effect on all clients on the LAN. If you select a specified port, the ARP guard function will take effect only on clients connected to the port.

4.12 Configuring MAC Address Filtering

4.12.1 Overview

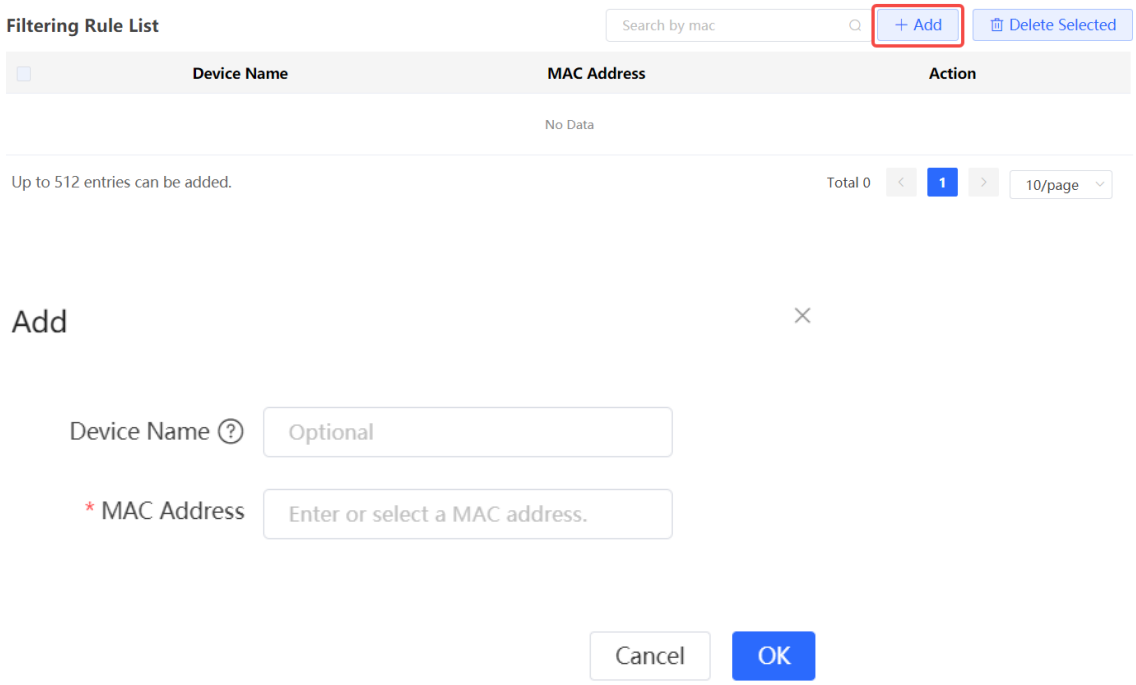
You can enable MAC address filtering and configure an **Allowlist** or **Blocklist** to effectively control Internet access from LAN hosts.

- **Allowlist**: Allow only hosts whose MAC addresses are in the filter rule list to access the Internet.
- **Blocklist**: Deny hosts whose MAC addresses are in the filter rule list from accessing the Internet.

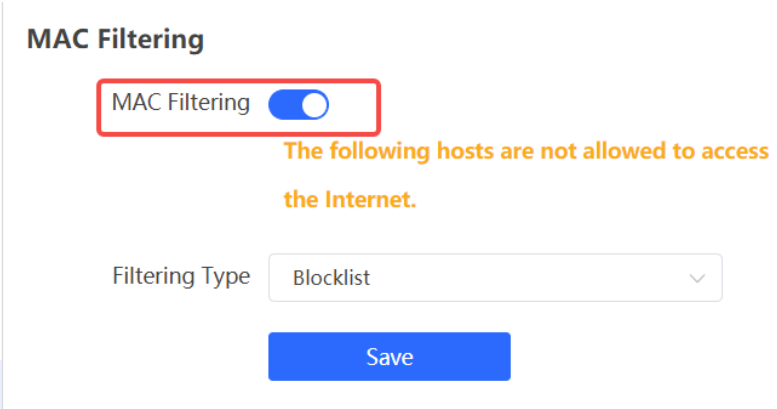
4.12.2 Configuration Steps

Choose **One-Device > Gateway > Config > Security > MAC Filtering**.

(1) In the Filtering Rule List pane, click **Add**. In the dialog box that appears, enter the MAC address and remarks. The input box can display existing address mappings in the ARP list. You can click a mapping to automatically enter the MAC address. Click **OK**. A filter rule is created.



(2) Turn on **MAC Filtering**, set **Filtering Type**, and click **Save**.



4.13 Configuring the PPPoE Server

4.13.1 Overview

Point-to-Point Protocol over Ethernet (PPPoE) is a network tunneling protocol that encapsulates PPP frames inside Ethernet frames. When the router functions as a PPPoE server, it provides the access service to LAN users and supports bandwidth management.

4.13.2 Global Settings

Choose **One-Device > Gateway > Config > Advanced > PPPoE Server > Global Settings**.

Set **PPPoE Server** to **Enable** and configure PPPoE server parameters.

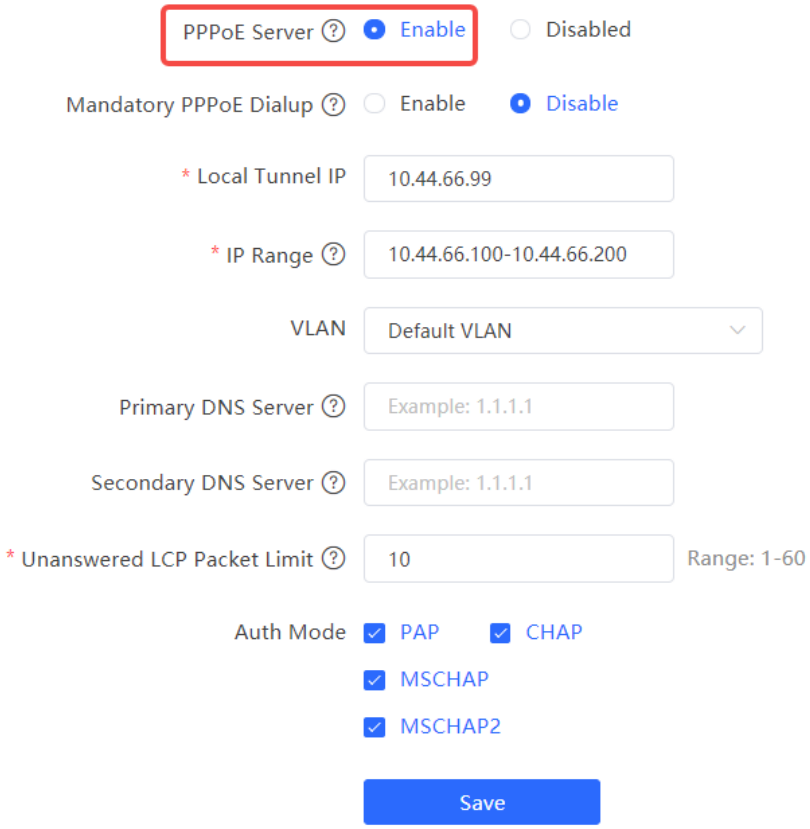


Table 4-31 PPPoE server configuration

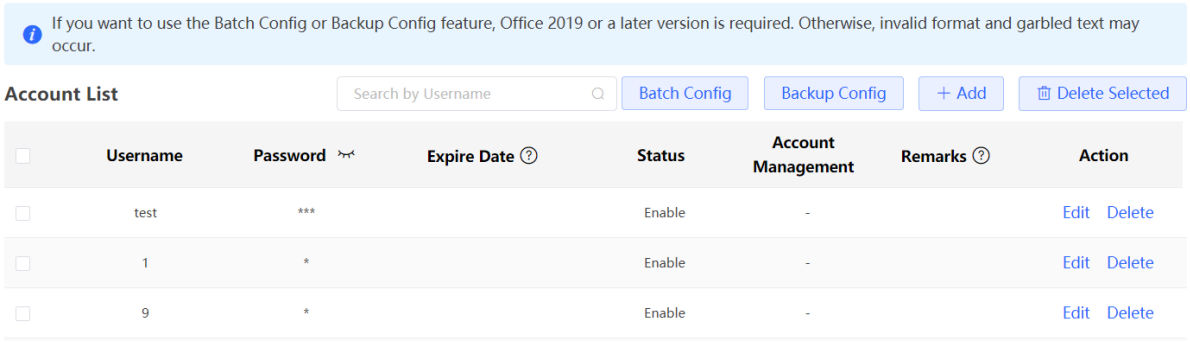
Parameter	Description
PPPoE Server	Specify whether to enable the PPPoE server function.
Mandatory PPPoE Dialup	Specify whether LAN users must access the Internet through dialing.
Local Tunnel IP	Set the point-to-point address of the PPPoE server.

Parameter	Description
IP Range	Specify the IP address range that can be allocated by the PPPoE server to authenticated users.
VLAN	Set the VLAN of the current PPPoE server.
Primary/Secondary DNS Server	Specify the DNS server address delivered to authenticated users.
Unanswered LCP Packet Limit	When the number of LCP packets not answered in one link exceeds the specified value, the PPPoE server automatically disconnects the link.
Auth Mode	Select at least one authentication mode from the following: PAP, CHAP, MSCHAP, and MSCHAP2.

4.13.3 Configuring a PPPoE User Account

Choose **One-Device > Gateway > Config > Advanced > PPPoE Server > Account Settings**.

Click **Add** to create a PPPoE authentication user account. The currently created PPPoE authentication user accounts are displayed in the **Account List** section. Find the target account and click **Edit** to modify the account information. Find the target account and click **Delete** to delete the account.



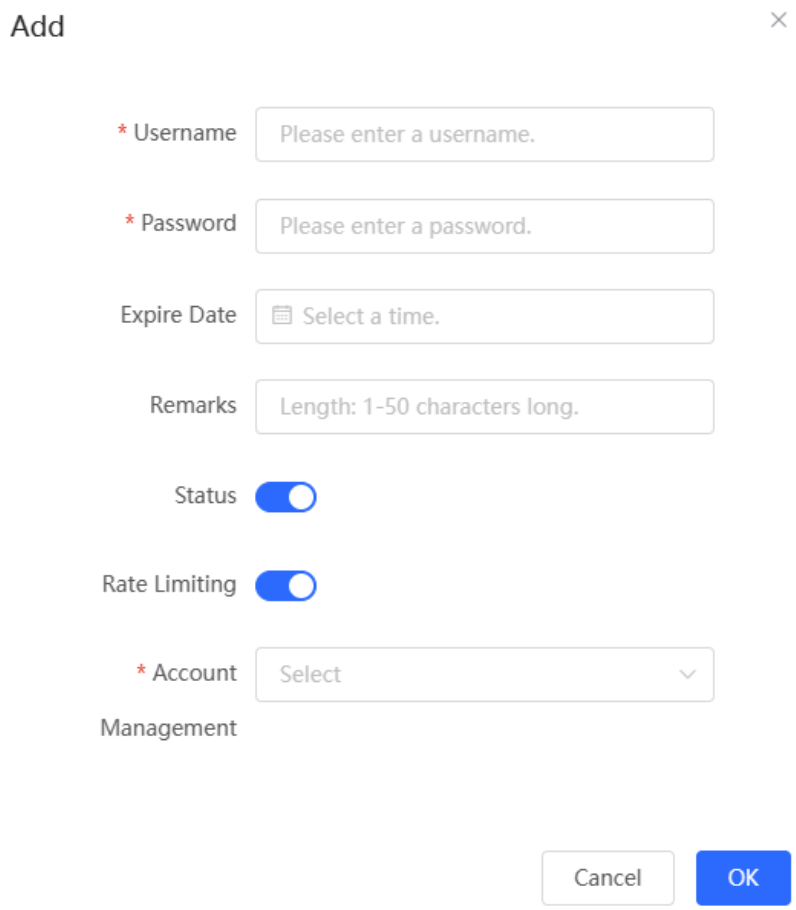


Table 4-32 PPPoE user account configuration

Parameter	Description
Username/Password	Set the username and password of the authentication account for Internet access through PPPoE dialing.
Expire Date	Set the expiration date of the authentication account. After the account expires, it can no longer be used for Internet access through PPPoE authentication.
Remark	Enter the account description.
Status	Specify whether to enable this user account. If the account is disabled, the account is invalid and cannot be used for Internet access through PPPoE authentication.
Rate Limiting	Specify whether to apply flow control on the account. If flow control is enabled, you need to configure flow control policies for the PPPoE authentication user. If smart flow control is disabled, Rate Limiting must be turned off. To turn on Rate Limiting, enable smart flow control first.

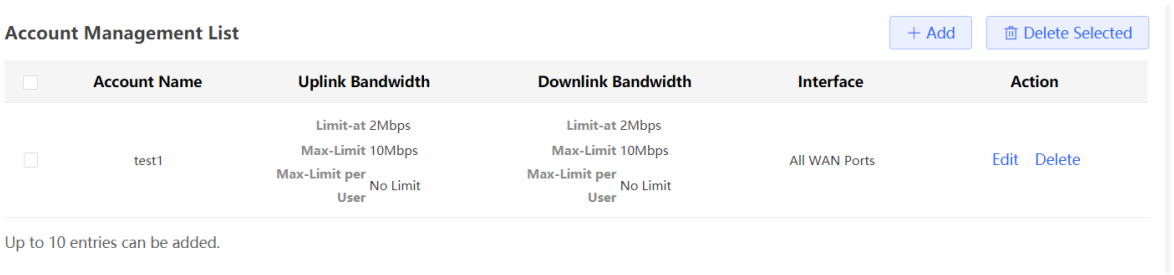
Parameter	Description
Account Management	After flow control is enabled, you need to configure a flow control package for the current account to restrict user bandwidth accordingly. For details on how to configure and view flow control packages, see Section 4.13.4 Configuring a Flow Control Package.

4.13.4 Configuring a Flow Control Package

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **PPPoE Server** > **Account Management**.

If smart flow control is disabled, the flow control package for the account does not take effect. Before you configure a flow control package, enable smart flow control first. For details on how to set smart flow control, see Section 8.6.2 Smart Flow Control.

Click **Add** to create a flow control package. The currently created flow control packages are displayed in the **Account Management List** section. You can modify or delete the packages.



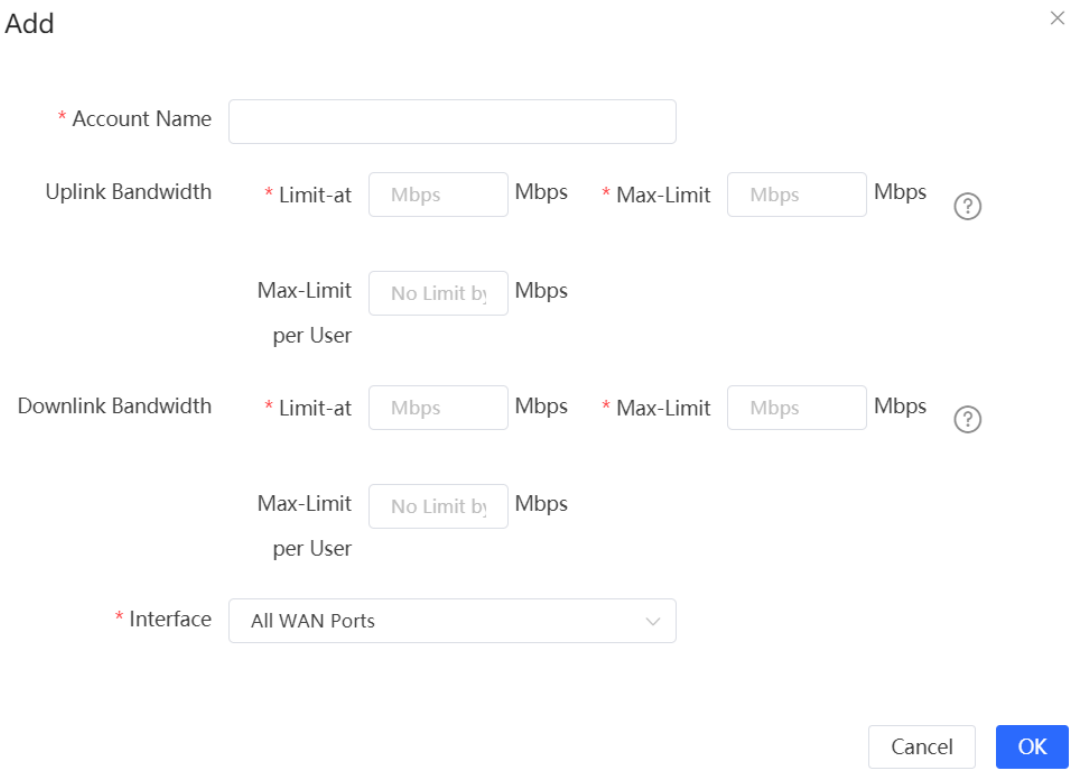


Table 4-33 PPPoE user flow control package configuration

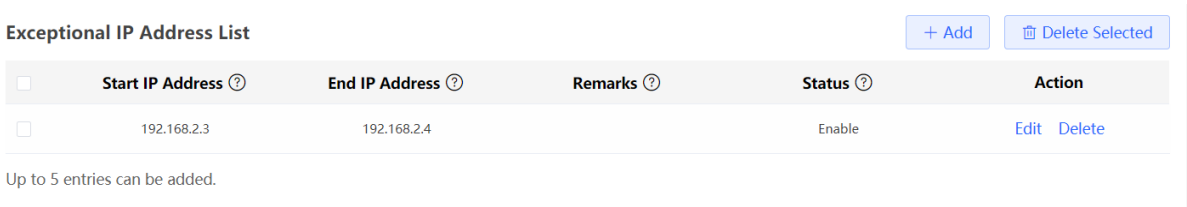
Parameter	Description
Account Name	Set the name of the flow control package. When you configure an authentication account, you can select a flow control package based on the name.
Uplink Bandwidth	The following uplink bandwidth options can be configured, all measured in Mbps. ● Limit-at: Guaranteed available uplink bandwidth for authenticated users when bandwidth resources are limited. ● Max-Limit: Maximum available uplink bandwidth for authenticated users when bandwidth resources are sufficient. ● Max-Limit per User: Maximum available uplink bandwidth for each user. This parameter is optional and the default value is no limit.
Downlink Bandwidth	The following downlink bandwidth options can be configured, all measured in Mbps. ● Limit-at: Guaranteed available downlink bandwidth for authenticated users when bandwidth resources are limited. ● Max-Limit: Maximum available downlink bandwidth for authenticated users when bandwidth resources are sufficient. ● Max-Limit per User: Maximum available downlink bandwidth for each user. This parameter is optional and the default value is no limit.
Interface	Specify the interface to which the flow control package applies.

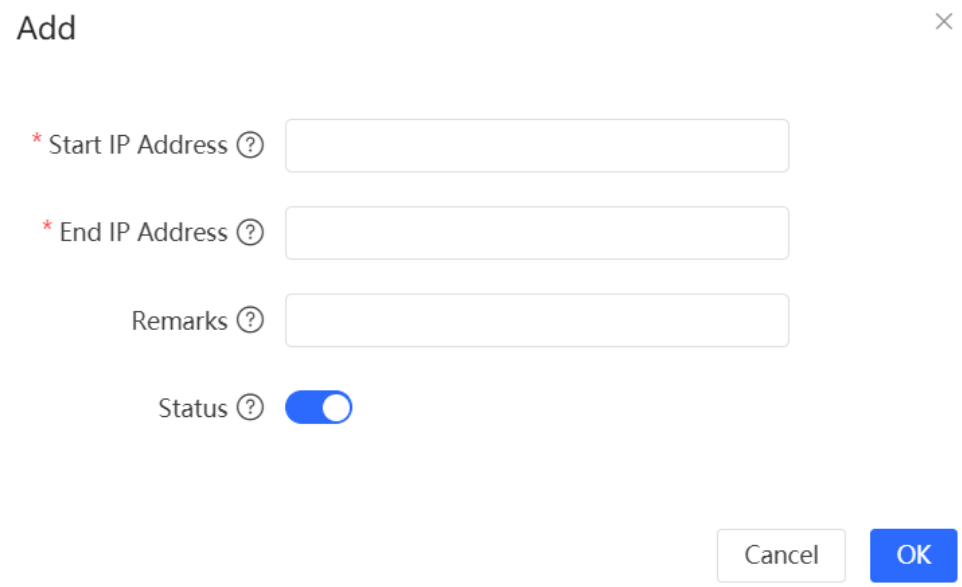
4.13.5 Configuring Exceptional IP Addresses

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **PPPoE Server** > **Exceptional IP Address**.

When the PPPoE server is enabled, if you want to allow some IP addresses in a specific VLAN to access the Internet without passing account and password authentication, you can configure these IP addresses as exceptional IP addresses.

The currently created exceptional IP addresses are displayed in the **Exceptional IP Address List** section. Click **Edit** to modify the exceptional IP address. Click **Delete** to delete the exceptional IP address.





- **Start IP Address/End IP Address**: Start and end of exceptional IP addresses.
- **Remark**: Description of an exceptional IP address.
- **Status**: Whether the exceptional IP address is effective.

4.13.6 Viewing Online Users

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **PPPoE Server** > **Online Clients**.

View the information of end users that access the Internet through PPPoE dialing. Click **Disconnect** to disconnect the user from the PPPoE server.

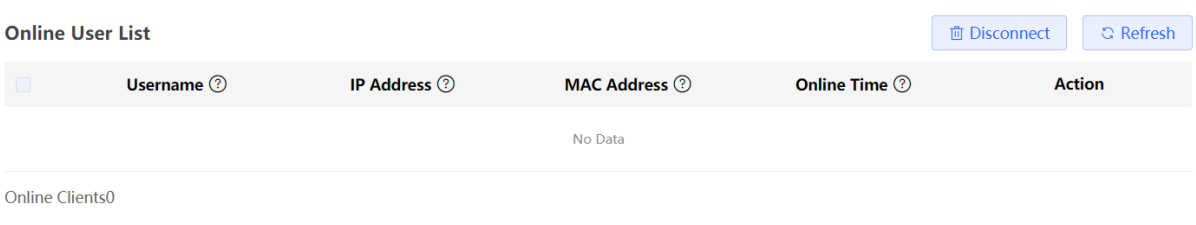


Table 4-34 PPPoE online user information

Parameter	Description
Username	Total number of online users that access the Internet through PPPoE dialing.
IP Address	IP address of the client.
MAC Address	MAC address of the client.
Online Time	Time when the user accesses the Internet.

4.14 Port Mapping

4.14.1 Overview

1. Port Mapping

The port mapping function can establish a mapping relationship between the IP address and port number of a WAN interface and the IP address and port number of a server in the LAN, so that all access traffic to a service port of the WAN interface will be redirected to the corresponding port of the specified LAN server. This function enables external users to actively access the service host in the LAN through the IP address and port number of the specified WAN interface.

Application scenario: Port mapping enables users to access the cameras or computers in their home network when they are in the enterprise or on a business trip.

2. NAT-DMZ

When an incoming data packet does not hit any port mapping entry, the packet is redirected to the LAN server according to the Demilitarized Zone (DMZ) rule. All data packets actively sent from the Internet to the device are forwarded to the designated DMZ host, thus realizing LAN server access of external network users. DMZ not only realizes the external network access service, but also ensures the security of other hosts in the LAN.

Application scenario: Configure port mapping or DMZ when an external network user wants to access the LAN server, for example, access a server deployed in the home network when the user is in the enterprise or on a business trip.

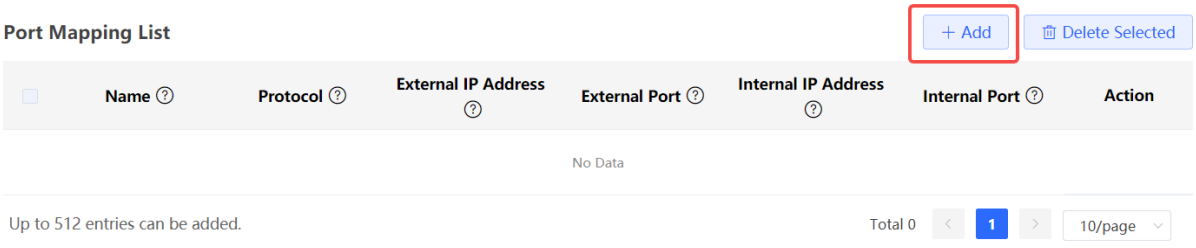
4.14.2 Getting Started

- Confirm the intranet IP address of the mapping device on the LAN and the port number used by the service.
- Confirm that the mapped service can be normally used on the LAN.

4.14.3 Configuration Steps

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Port Mapping** > **Port Mapping**.

Click **Add**. In the dialog box that appears, enter the rule name, service type, protocol type, external port/range, internal server IP address, and internal port/range. You can create a maximum of 50 port mapping rules.



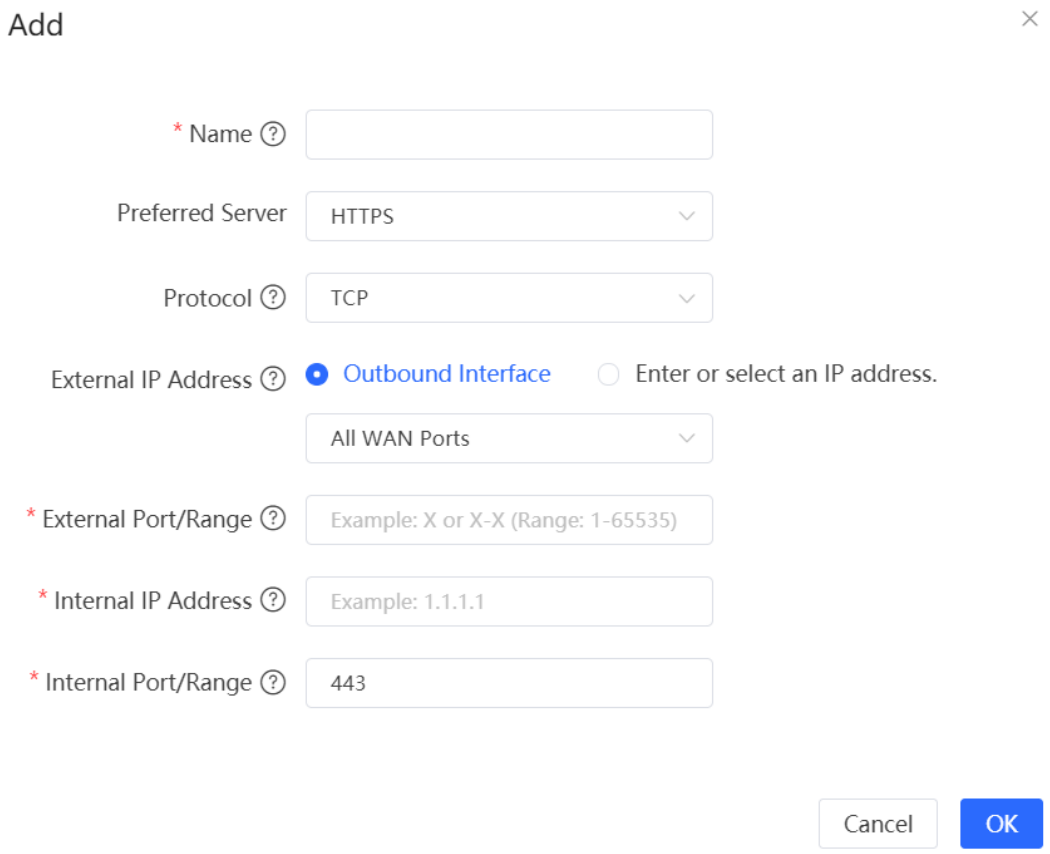


Table 4-35 Port mapping configuration

Parameter	Description
Name	Enter the description of the port mapping rule, which is used to identify the rule.
Preferred Server	Select the type of service to be mapped, such as HTTP or FTP. The internal port number commonly used by the service is automatically entered. If you are not sure about the service type, select **Custom**.
Protocol	Select the transmission layer protocol type used by the service, such as **TCP** or **UDP**. The value **ALL** indicates that the rule applies to both protocols. The value must comply with the client configuration of the service.
External IP Address	Specify the host address used for accessing the external network. You can set it to the following: ● **Outbound Interface**: You can select **All WAN Ports** or specify a WAN interface. ● **Enter or select an IP address**: Select or enter the IP address of a WAN interface.

Parameter	Description
External Port/Range	Specify the port number used for Internet access. You need to confirm the port number in the client software, such as the camera monitoring software. You can enter a port number or a port range, such as 1050-1060. If you enter a port range, the value of **Internal Port/Range** must also be a port range.
Internal IP Address	Specify the IP address of the internal server to be mapped to the WAN interface, that is, the IP address of the LAN device that provides Internet access, such as the IP address of the network camera.
Internal Port/Range	Specify the service port number of the internal server to be mapped to the WAN interface, that is, the port number of the application that provides Internet access, such as port 8080 of the Web service. You can enter a port number or a port range, such as 1050-1060. If you enter a port range, the number of ports must be the same as that specified in **External Port/Range**.

4.14.4 Verification and Test

Check whether the external network device can access services on the destination host using the external IP address and external port number.

4.14.5 Solution to Test Failure

(1) Modify the value of **External Port/Range** and use the new external port number to perform the test again. The possible cause is that the port is blocked by the firewall.

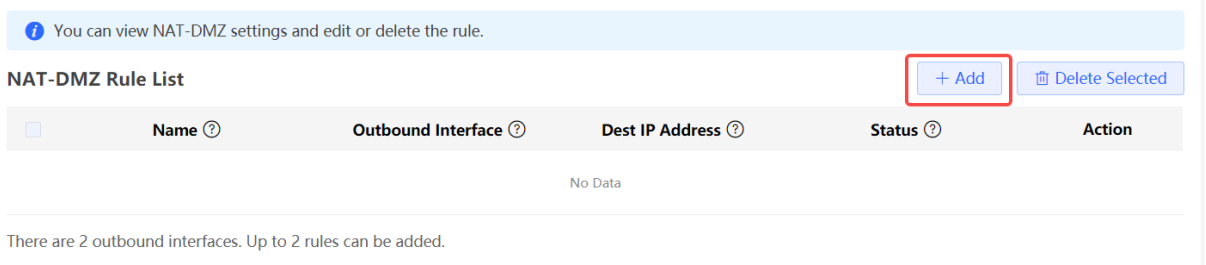
(2) Enable the remote access permission on the server. The possible cause is that remote access is displayed on the server, resulting in normal internal access but abnormal access across network segments.

(3) Configure DMZ rules. For details, see Section 4.14.6 Configuration Steps (DMZ). The possible cause is that the specified ports are incorrect or incomplete.

4.14.6 Configuration Steps (DMZ)

Choose **One-Device > Gateway > Config > Advanced > Port Mapping > NAT-DMZ**.

Click **Add**. Enter the rule name and internal server IP address, select the interface to which the rule applies, specify the rule status, and click **OK**. You can configure only one DMZ rule for an outbound interface.



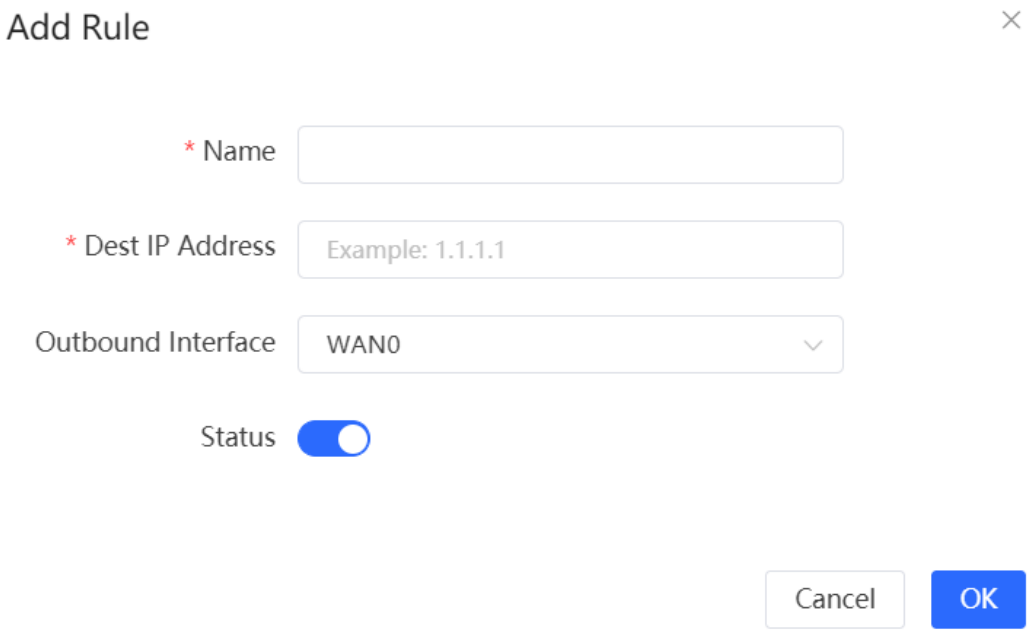


Table 4-36 DMZ rule configuration

Parameter	Description
Name	Enter the description of the mapping rule, which is identify the DMZ rule.
Dest IP Address	Specify the IP address of the DMZ host to which packets are redirected, that is, the IP address of the internal server that can be accessed from the Internet.
Outbound Interface	Specify the WAN interface in the DMZ rule. You can configure only one rule for a WAN interface.
Status	Specify whether the rule is effective. The rule is effective after you turn on **Status**.

4.15 UPnP

4.15.1 Overview

After the Universal Plug and Play (UPnP) function is enabled, the device can change the port used by the Internet access service according to the client request, implementing NAT. When a client on the Internet wants to access the internal resources on the LAN device, the device can automatically add port mapping entries to realize traversal of some services between internal and external networks. The following commonly used programs support the UPnP protocol: MSN Messenger, Thunder, BT, and PPLive.

Before you use the UPnP service, note that clients (PCs and mobile phones) used in combination also support UPnP.

Note

To implement automatic port mapping using UPnP, the following conditions must be met:

- UPnP is enabled on the device.
- The operating system of the LAN host supports UPnP and has UPnP enabled.
- The programs support UPnP and have UPnP enabled.

4.15.2 Configuring UPnP

Choose **One-Device > Gateway > Config > Advanced > UPnP**.

Turn on Enable to enable the UPnP function. Select a port from the drop-down list box of **Default Interface**. Click **Save** to make the configuration take effect.

If any relevant program converts the port automatically, the information is displayed in the **UPnP List** section.

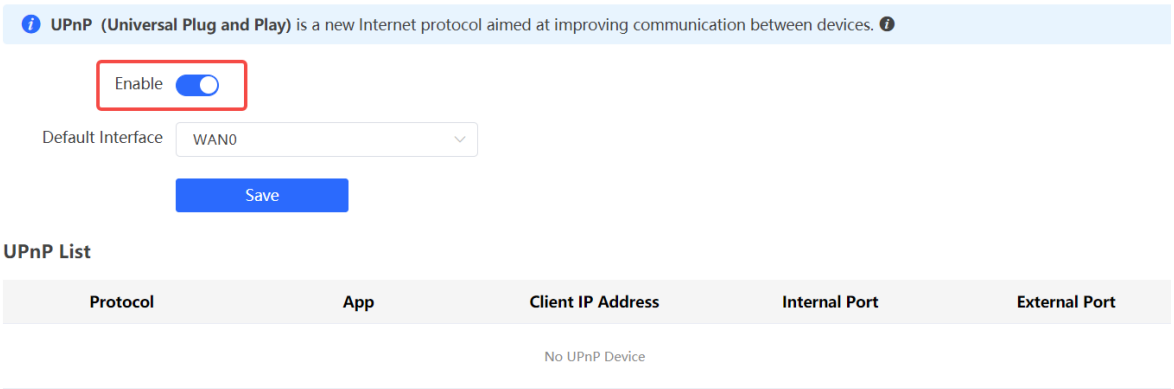


Table 4-37 UPnP configuration

Parameter	Description
Enable	Specify whether to enable UPnP. By default, UPnP is disabled.
Default Interface	Specify the WAN interface address bound to the UPnP service. By default, the default interface is a WAN interface. On the device with multiple WAN interfaces, you can manually select the WAN interface to bind or set this parameter to **Auto** to allow the device to select a WAN interface automatically.

4.15.3 Verifying Configuration

After the UPnP service is enabled, open a program that supports the UPnP protocol (such as Thunder or BitComet) on the client used with the device, and refresh the Web page on the device. If a UPnP entry is displayed in the UPnP list, a UPnP tunnel is created successfully.

4.16 Dynamic DNS

4.16.1 Overview

After the Dynamic Domain Name Server (DDNS) service is enabled, external users can use a fixed domain name to access service resources on the device over the Internet at any time, without the need to search for the WAN interface IP address. You need to register an account and a domain name on the third-party DDNS service provider for this service. The device supports No-IP DNS and Other DNS.

4.16.2 Getting Started

Before you use the DDNS service, register an account and a domain name on the DDNS or No-IP official website.

4.16.3 Configuring DDNS

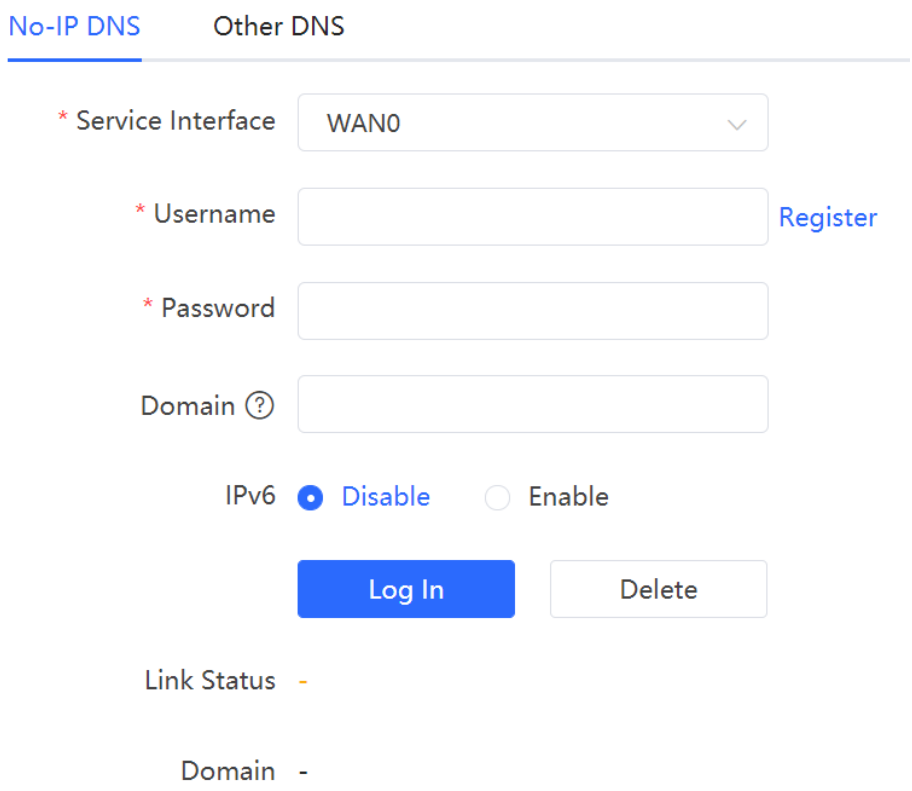
1. No-IP DNS

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Dynamic DNS** > **No-IP DNS**.

Enter the registered username and password and click Log In to initiate a connection request to the server. The binding between the domain name and WAN interface IP address of the device takes effect.

Click Delete to clear all the entered information and remove the server connection relationship.

The **Link Status** parameter specifies whether the server connection is established successfully. If you do not specify the domain name upon login, the domain name list of the current account is displayed after successful connection. All the domain names of this account are parsed to the WAN interface IP address.



Note

- Both No-IP DNS and other DNS support IPv6 connectivity.
- To ensure compatibility with the IPsec VPN functionality, you are advised to enable IPv6 when IPv6 is used for IPsec VPN connection.

Table 4-38 DDNS login information

Parameter	Description
Service Interface	One domain name can be parsed to only one IP address. Therefore, you need to specify the WAN interface bound to the domain name when multiple WAN interfaces are available. By default, the service interface is a WAN interface.
Username / Password	Enter the username and password of the account registered on the official website. If no registered account is available, click **Register** to switch to the official website and create a new account.
Domain	Specify the domain name bound to the service interface IP address. This parameter is optional for No-IP DNS. One account can be bound to multiple domain names. You can choose to bind only one domain name to the IP address of the current service interface. Only the selected domain name is parsed to the WAN interface IP address. If no domain name is specified, all the domain names of the current account are parsed to the WAN interface IP address.

2. Other DNS

Choose **One-Device > Gateway > Config > Advanced > Dynamic DNS > Other DNS**.

Select the service provider and service interface, enter the username and password for login, and click **Log In** to initiate a connection request to the server to make the binding relationship between the domain name and the device WAN interface IP address effective.

Clicking **Delete** will clear all input information and disconnect from the server.

The connection status indicates whether a connection has been successfully established with the server.

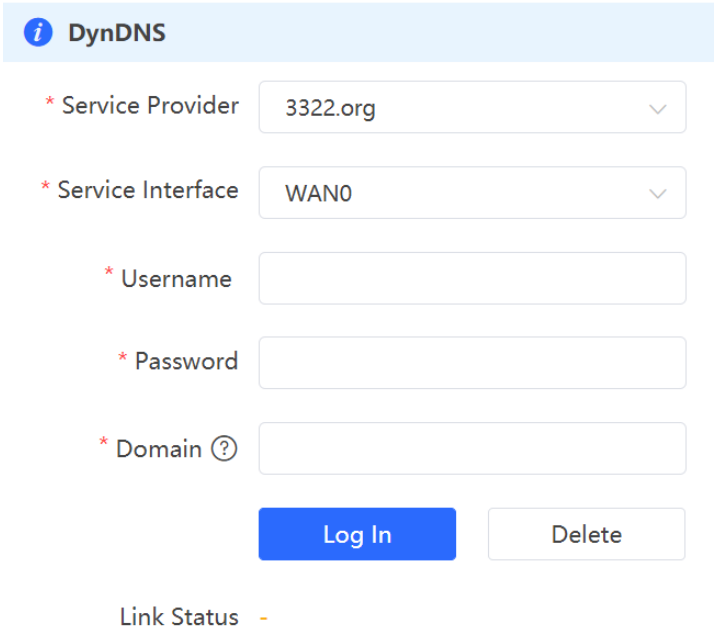


Table 4-39 DDNS Login Information

Parameter	Description
Service provider	An organization that provides dynamic domain name services, such as 3322.2org, cloudflare. com v4, and aliyun.
Service Interface	One domain name can be parsed to only one IP address. Therefore, you need to specify the WAN interface bound to the domain name when multiple WAN interfaces are available. By default, the service interface is a WAN interface.
Username / Password	Enter the username and password of the account registered on the official website.
Domain	Specify the domain name bound to the service interface IP address.

Note

- Both No-IP DNS and other DNS support IPv6 connectivity.
- To ensure compatibility with the IPsec VPN functionality, you are advised to enable IPv6 when IPv6 is used for IPsec VPN connection.

3. Verifying Configuration

If **Link Status** is displayed as **Connected**, the server connection is established successfully. After the configuration is completed, ping the domain name from the Internet. The ping succeeds and the domain name is parsed to the WAN interface IP address.

4.17 Connecting to IPTV

Caution

To connect to IPTV in the Chinese environment, switch the system language. For details, see Section 12.13 Switching System Language.

IPTV is a network television service provided by the ISP.

4.17.1 Getting Started

- Confirm that the IPTV service is activated.
- Check the local IPTV type: VLAN or IGMP. If the type is VLAN, confirm the VLAN ID. If you cannot confirm the type or VLAN ID, contact the local ISP.

4.17.2 Configuration Steps (VLAN Type)

Choose **One-Device > Gateway > Config > Network > IPTV > IPTV/VLAN**.

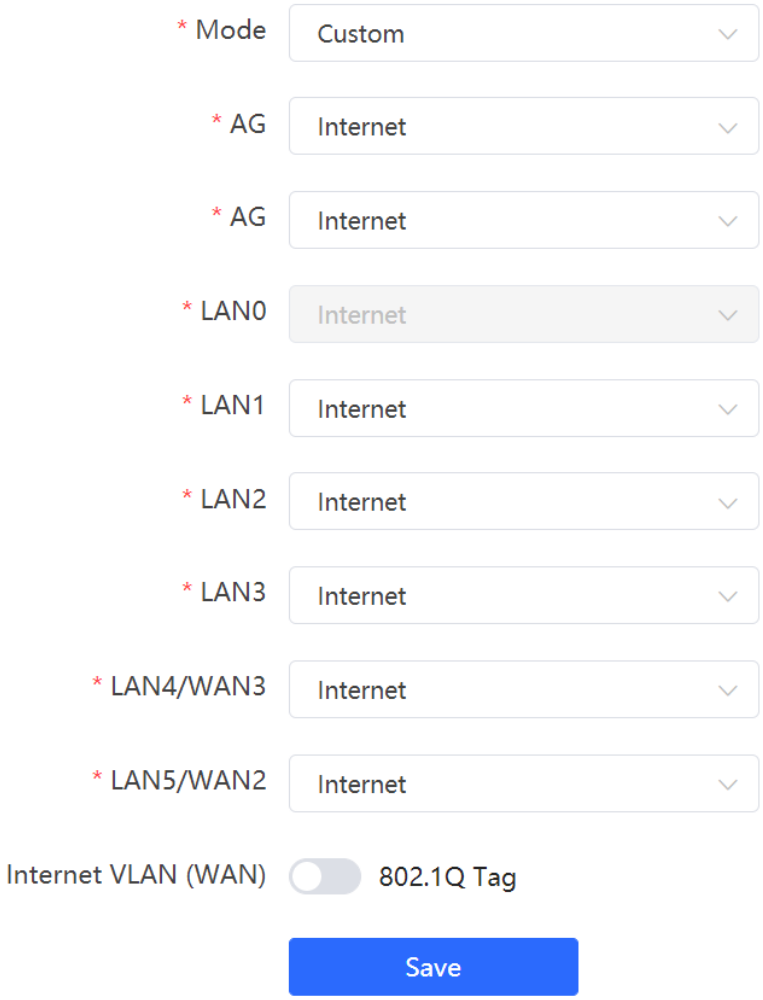
Select a proper mode based on your region, click the drop-down list box next to the interface to connect and select **IPTV**, and enter the VLAN ID provided by the ISP. For example, when you want to connect the IPTV set top box to LAN 3 port of the device and the VLAN ID is 20, the configuration UI is as follows.

Internet VLAN: If you need to set a VLAN ID for the Internet access service, turn on this parameter and enter the VLAN ID. By default, the VLAN tag function is disabled. You are advised to keep the VLAN tag function disabled unless otherwise specified.

After the configuration is completed, confirm that the IPTV set top box is connected to the correct port, for example, LAN 3 in the example.

Caution

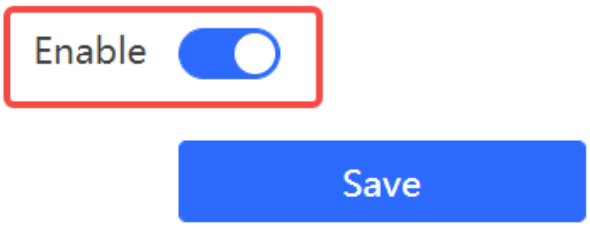
Enabling this function may lead to network disconnection. Exercise caution when performing this operation.



4.17.3 Configuration Steps (IGMP Type)

Choose **One-Device > Gateway > Config > Network > IPTV > IPTV/IGMP**.

The IGMP type is applicable to the ISP FPT. After you enable IPTV connection, connect the IPTV set top box to any LAN port on the router.



4.18 Limiting the Number of Connections

Choose **One-Device > Gateway > Config > Advanced > Session Limit**.

This function is used to control the maximum number of connections per IP address.

Click **Add** to add an IP session limit rule.

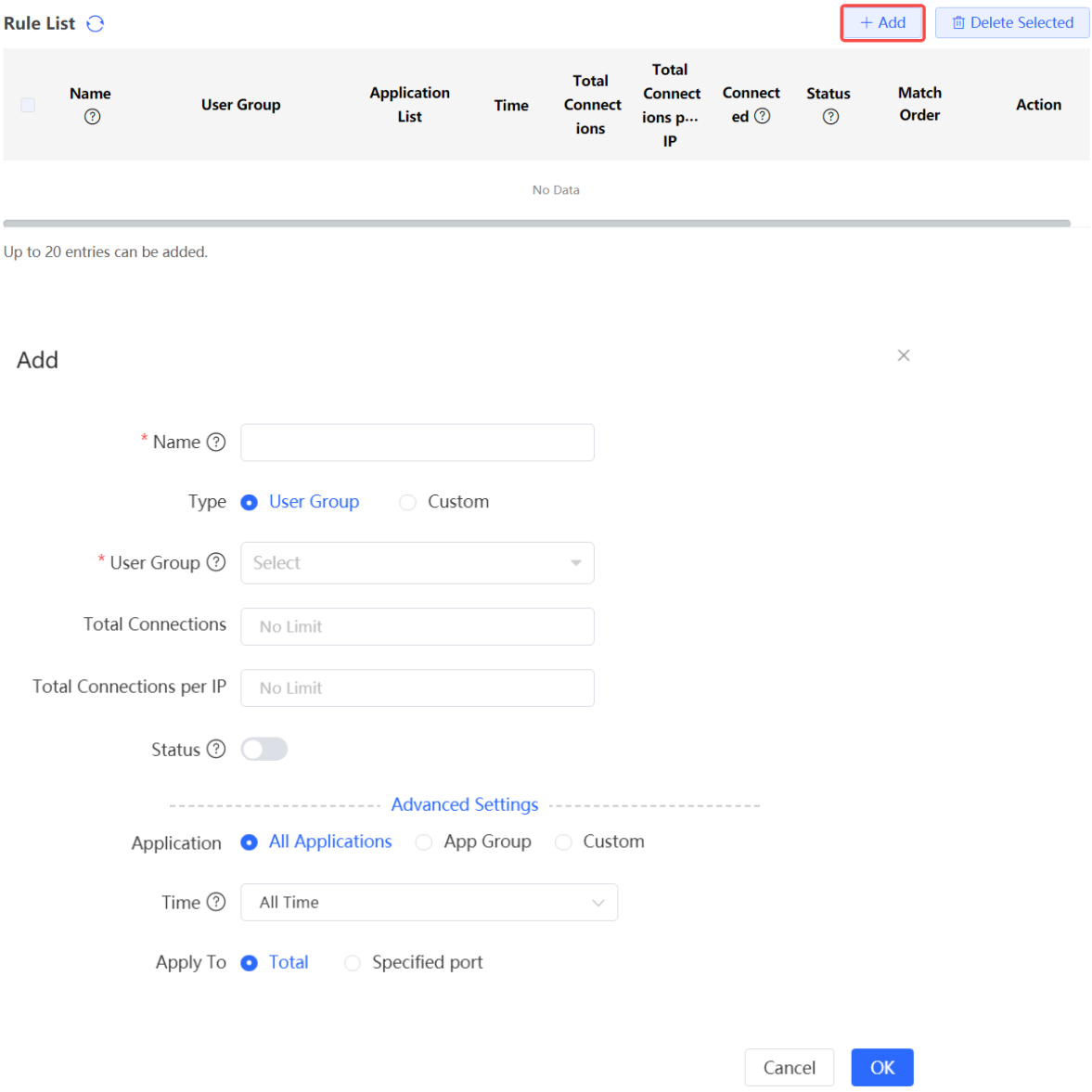


Table 4-40 IP session limit rule information

Parameter	Description
Name	Enter the name of the IP session limit rule.
Type	Select the rule type: ● **User Group**: The rule takes effect on the specified user group. ● **Custom**: The rule takes effect on the custom IP address range.

Parameter	Description
User Group	Select the user group from the list. For details about the user group list, see8.2.2 User Group. If all members of the user group are selected, the rule applies to the entire user group, including future members added to the group. Note: This field is required only when the rule **Type** is set to **User Group**.
Start IP Address	Enter the start IP address for session matching in the rule.
End IP Address	Enter the end IP address for session matching in the rule.
Total Connections	Specify the total number of sessions for all IP addresses matching this rule.
Total Connections per IP	Specify the maximum number of sessions per IP address for all IP addresses matching this rule.
Status	Specify whether the rule is effective. The rule takes effect after you turn on this parameter.
Application	After an application is selected, the rule will take effect on the specified application. ● **All Applications**: The rule takes effect on all applications. ● **App Group**: Select an application group defined in8.4.4 Custom Application Group from the drop-down list box. The rule takes effect on applications in the selected application group. ● **Custom**: The rule takes effect on specified applications in the application list.
Time	The rule is effective in the selected time period. Select a time period from the time periods defined in 8.3 Time Management from the drop-down list, or select **Custom** to manually configure a time period.
Apply To	Set the application scope of the rule: ● **Total**: The rule applies to the entire device. ● **Specified port**: Select the interfaces to which the session count limit will be applied. The rule will be applied to the selected interfaces only.

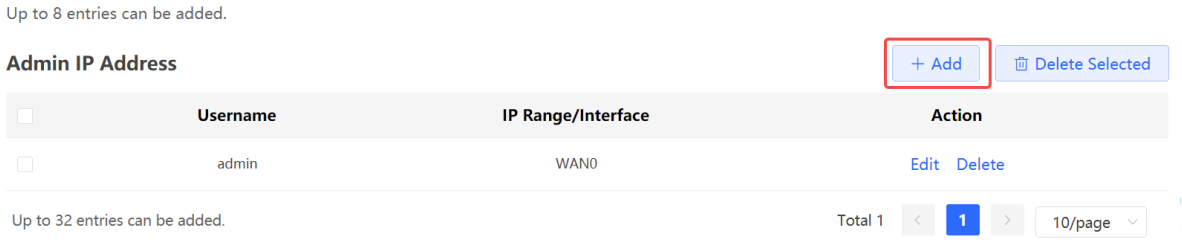
4.19 Configuring Local Security

4.19.1 Configuring an Admin IP Address

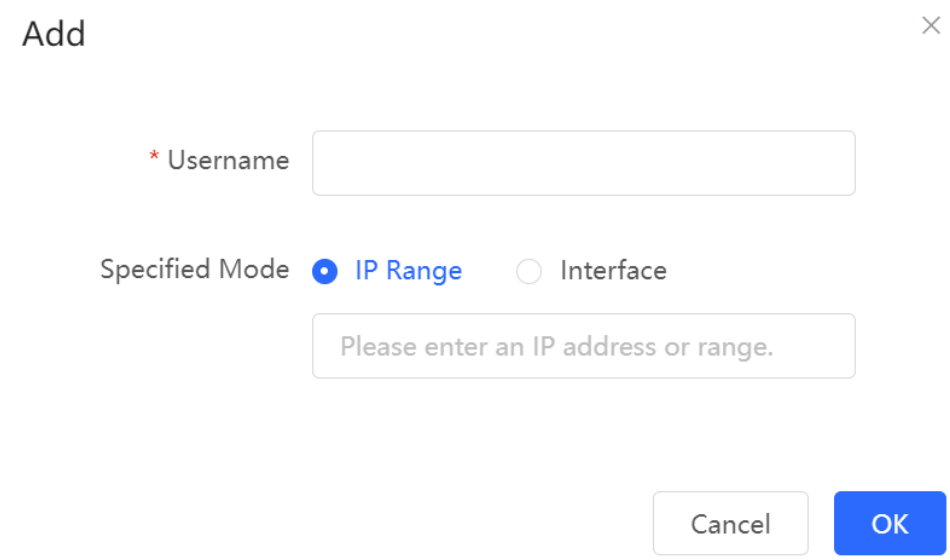
Admin IP addresses are exempt from the ping prohibition function. Packets sent from admin IP addresses can pass through and will not be discarded.

Choose **One-Device > Gateway > Config > Security > Local Security > Security Zone.**

Click **Add**. Then, you can configure admin IP address information.



1. Configuring an Admin IP Address (Based on an IP Address)



(1) Configure a name for the admin IP address.

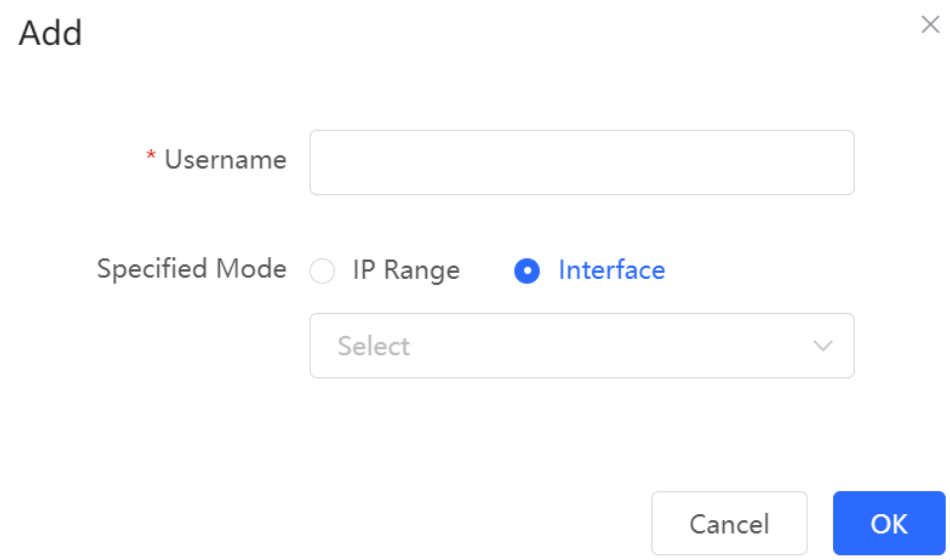
The name is a string of 1–32 characters.

(2) Set **Specific Mode** to **IP Range**.

(3) Configure an IP address.

You can specify a single IP address or an IP address range.

2. Configuring an Admin IP Address (Based on a Port)



(1) Configure a name for the admin IP address.

The name is a string of 1–32 characters.

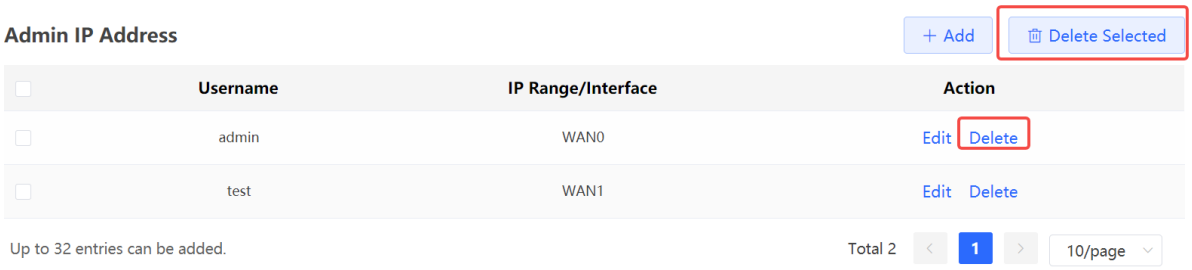
(2) Set **Specific Mode** to **Interface**.

(3) Specify the port.

You can select a LAN port or WAN interface as the interface.

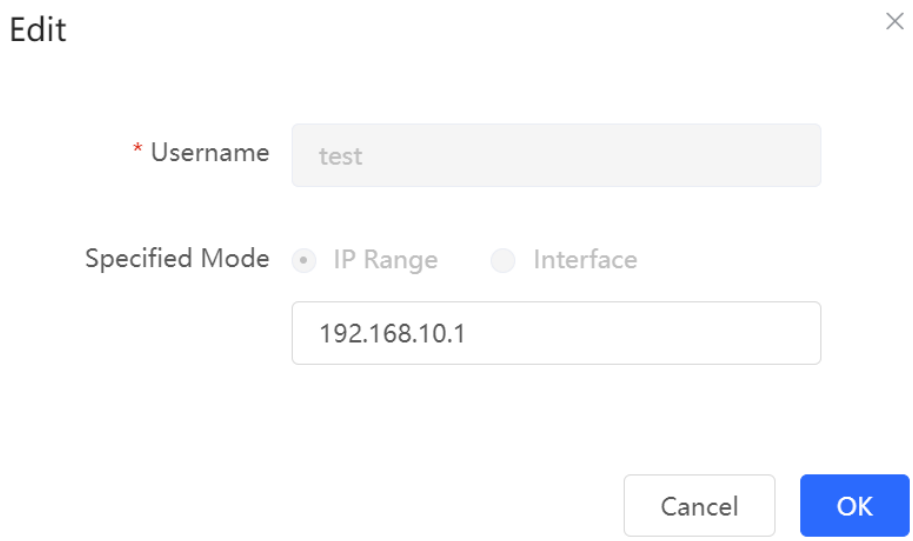
3. Deleting an Admin IP Address

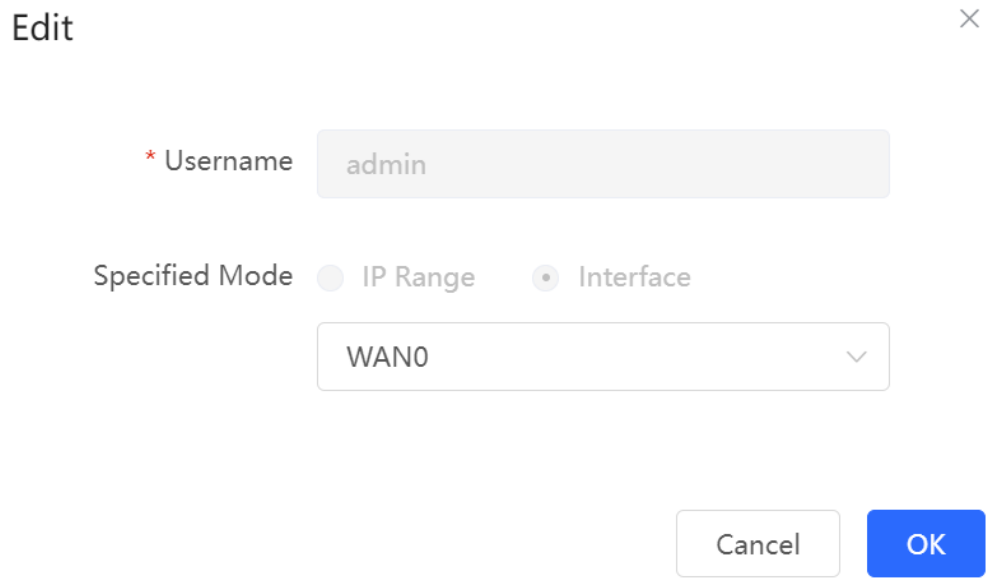
- Select an entry and click **Delete** to delete information about the admin IP address.
- Select multiple entries and click **Delete Selected** to bulk delete selected entries.



4. Editing Information About an Admin IP Address

You cannot modify the name and specified mode of an admin IP address but modify the IP address range or port in the specified mode.





4.19.2 Configuring Security Zones

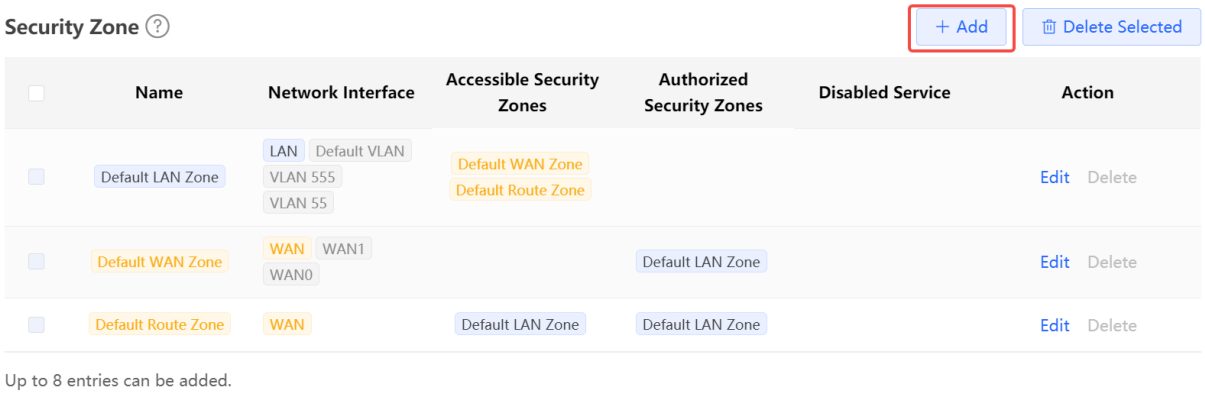
Note

For devices that do not support SNMP, the SNMP service cannot be disabled in a LAN zone.

A security zone is a logical zone consisting of a group of systems that trust each other and share the same security protection requirements. Generally, a security zone consists of a group of interfaces. Networks formed by interfaces in the same security zone share the same security attributes. Each interface can only belong to one security zone.

- Up to eight security zones can be added.
- Pre-defined security zones include:
  - Pre-defined LAN zone: By default, all VLANs are mapped to the pre-defined LAN zone.
  - Pre-defined WAN zone: By default, all WAN interfaces are mapped to the pre-defined WAN zone.

Choose **One-Device > Gateway > Config > Security > Local Security > Security Zone.**



(1) Click **Add**.

(2) Configure parameters for the security zone.

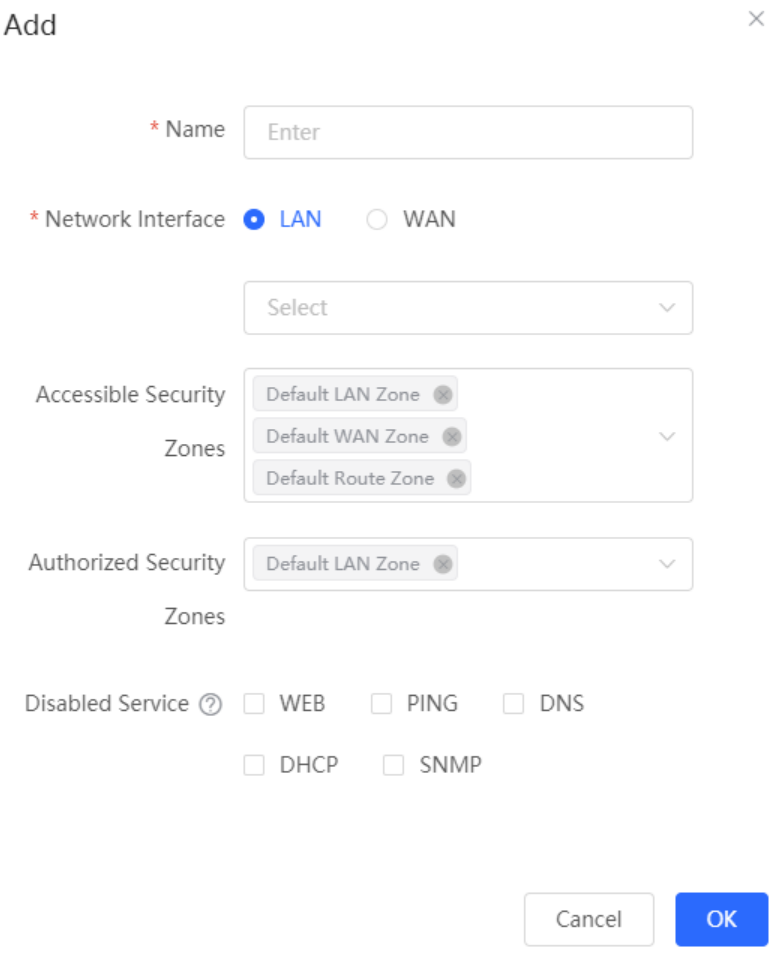


Table 4-41 Description of Security Zone Configuration Parameters

Parameter	Description
Name	Name of the security zone.
Network Interface	Interfaces mapped to the security zone, including LAN and WAN. LAN refers to VLAN, and WAN refers to WAN interfaces. Note: After a new security zone is created and VLANs or WAN interfaces are mapped to this new security zone, the VLANs or WAN interfaces will be removed from the pre-defined LAN zone or pre-defined WAN zone.
Accessible Security Zones	Other security zones to which this security zone can access.
Authorized Security Zones	Other security zones that can access this security zone.
Disabled Service	Services prohibited in this security zone: ● If PING is selected, clients in the security zone cannot ping the local device. ● If Web is selected: clients in the security zone cannot access the local web page. ● If DNS is selected, the address of the DNS server used by clients in the security zone is the local IP address, and web pages cannot be accessed normally. ● If DHCP is selected, clients in the security zone cannot obtain IP addresses. ● If SNMP is selected, clients in the security zone cannot use the SNMP service of the device.

(3) Click **OK**.

4.19.3 Configuring Session Attack Prevention

1. Overview

- Session Attack Prevention

In a session attack, an attacker sends heavy traffic to the device. In this case, the device has to consume many resources when creating connections. To reduce the impact of the attack, you can limit the rate of creating sessions.

- DDoS Attack Prevention

In a DDoS Attack, an attacker sends tremendous abnormal packets to a device. As a result, the device uses a large amount of resources to handle the packets. This causes the device performance to deteriorate or the system to break down.

If the value of TCP SYN and other TCP Flood parameters is too small, the authentication function and access to local web pages will be affected.

If the value of UDP Flood parameter is too small, the DHCP address allocation, DNS domain name resolution, and VPN functionalities will be affected.

You are advised to set the value to be greater than the load capacity of the local device.

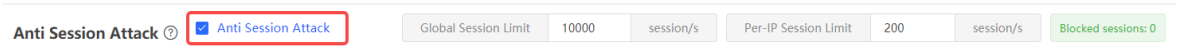
- Suspicious Packet Attack Prevention

In a suspicious packet attack, an attacker sends tremendous error packets to the device. When the host or server handles the error packets, its system will crash.

2. Configuring Session Attack Prevention

Choose **One-Device** > **Gateway** > **Config** > **Security** > **Local Security** > **Attack Defense**.

(1) Enable **Anti Session Attack**.



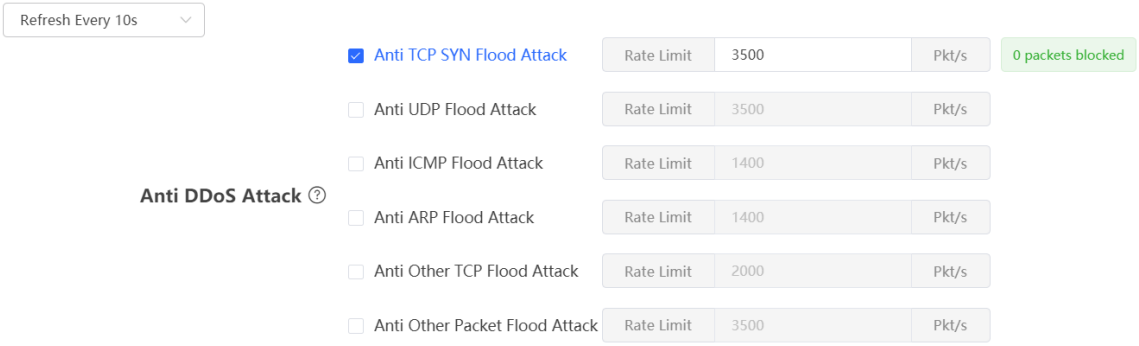
(2) Configure the session creation rate limit, including global and per-IP values.

(3) Click **Save**.

3. Configuring DDoS Attack Prevention

Choose **One-Device** > **Gateway** > **Config** > **Security** > **Local Security** > **Attack Defense**.

(1) Select required attack prevention types and enable this feature.



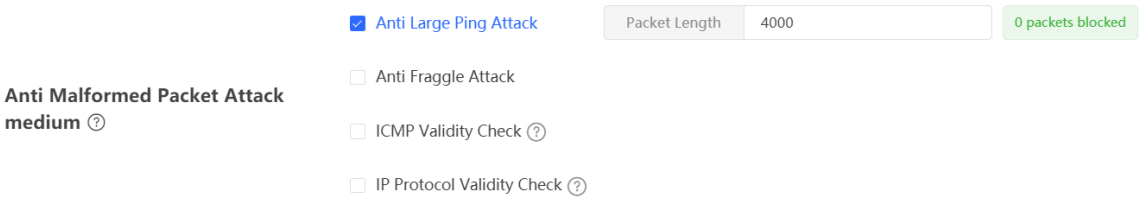
(2) Configure rate limiting.

(3) Click **Save**.

4. Configuring Suspicious Packet Attack Prevention

Choose **One-Device** > **Gateway** > **Config** > **Security** > **Local Security** > **Attack Defense**.

(1) Select required attack prevention types and validity check types to enable this feature.



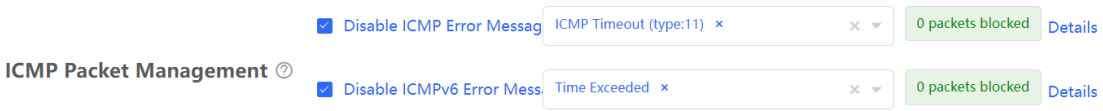
(2) To enable large ping attack prevention, enter the packet length.

(3) Click **Save**.

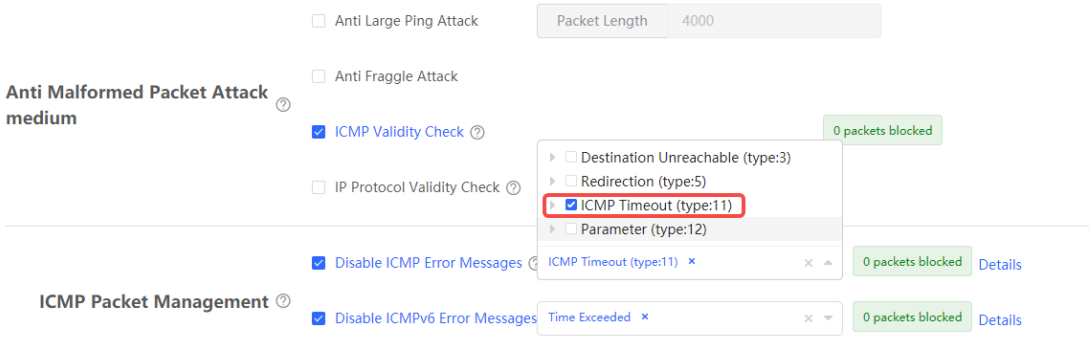
5. Configuring Packet Receiving and Sending Control

Choose **One-Device** > **Gateway** > **Config** > **Security** > **Local Security** > **Attack Defense**.

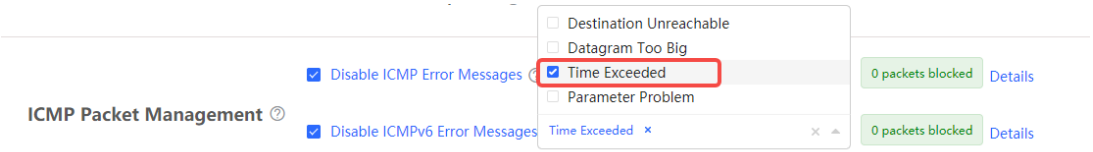
(1) Select the packet types that are prohibited from being sent by the device. Select at least one packet type.



- Enable **Disable ICMP Error Messages**. You can select **ICMP Timeout**, **Destination Unreachable**, **Redirection**, and **Parameter**.



- Enable **Disable ICMPv6 Error Message**. You can select **Destination Unreachable**, **Datagram too Big**, **Time Exceeded**, and **Parameter Problem**.

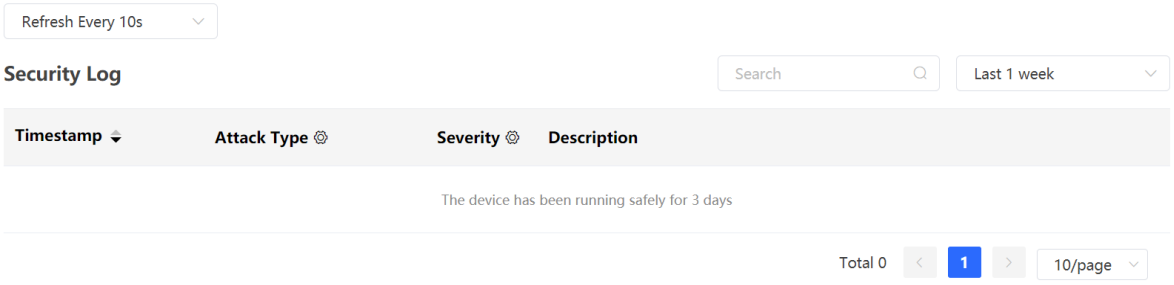


(2) Click **Save**.

4.19.4 Checking the Security Log

Choose **One-Device** > **Gateway** > **Config** > **Security** > **Local Security** >**Security Log**.

Check defense results of the device against various attacks on the **Security Log** page.



4.20 Configuring TTL Rules

4.20.1 Overview

Time to live (TTL) aims to prevent unauthorized connections. It limits the number of devices that can transmit data packets in the network by limiting the existence time of the data packets in the computer network, so as to prevent infinite transmission of data packets in the network and the waste of resources.

When TTL is set to 1 and is valid for LANs, packets are directly discarded when passing through the next router. If a user connects a router to Ruijie device without permission and connects a client to the router, packets cannot pass through the client, either. This restriction prevents users from connecting routers without permission.

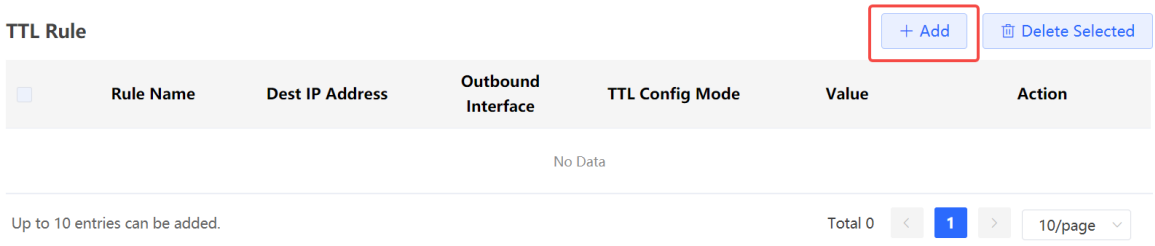
Note

- Changing the TTL affects packet forwarding on the network.
- The following data packets are not affected by this function: data packets forwarded by the express forwarding function of the device, data packets used by Wi-Fi cracking software (Cheetah Wi-Fi) to implement hotspot sharing, data packets forwarded at L2, and data packets passing through devices with TTL changed.

4.20.2 Configuring TTL Rules

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **TTL Rule**.

This operation allows you to change the TTL value in packets forwarded to a specified IP address range or a specified port.



1. Configuring a TTL Rule

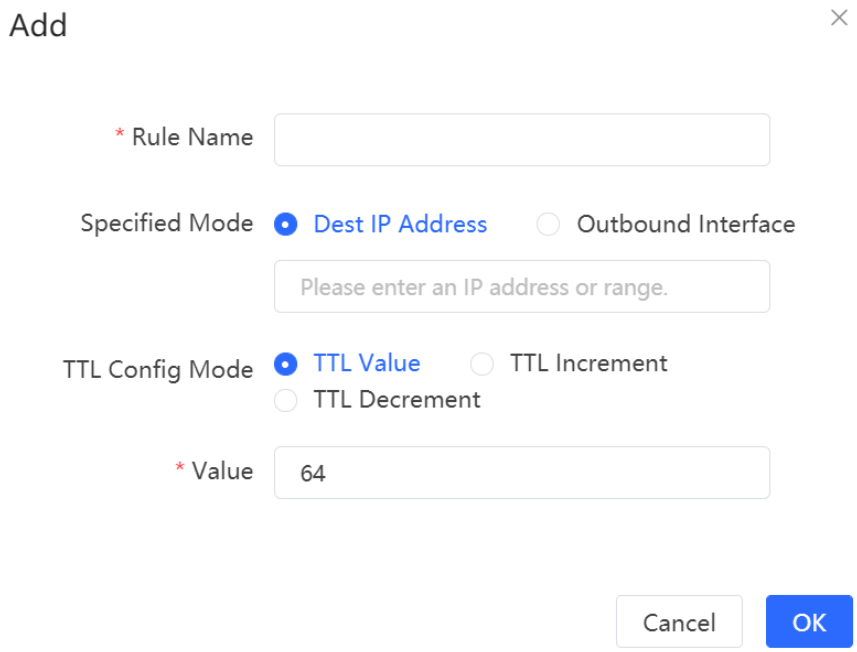
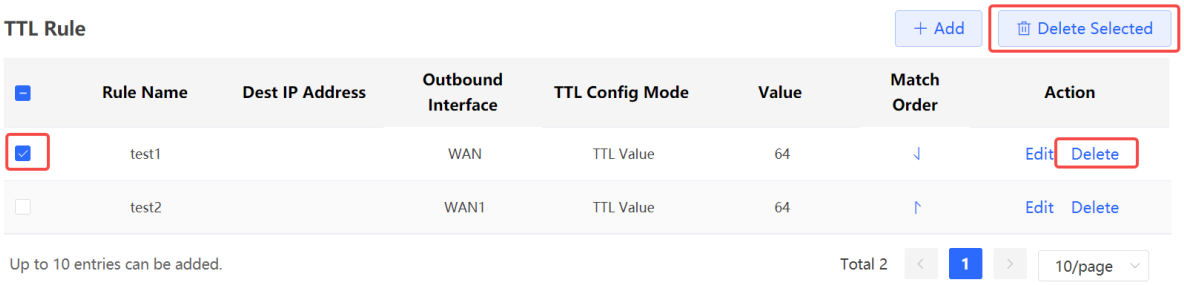


Table 4-42 Description of TTL Rule Configuration

Parameter	Description
Rule Name	Specify the name of a TTL rule.
Specified Mode	Specify the range for the rule to take effect: ● **Dest IP Address**: Indicates that the TTL rule takes effect on a specified IP address or range. ● **Outbound Interface**: Indicates that the TTL rule takes effect on a specified outbound interface.
TTL Config Mode	Configure a rule for TTL values in packets. ● **TTL Value**: Specifies the value, to which the TTL value is changed, after a data packet passes through the device. ● **TTL Increment**: Specifies the increment of the TTL value on the basis of the original value after a data packet passes through the device. ● **TTL Decrement**: Specifies the decrement of the TTL value on the basis of the original value after a data packet passes through the device.
Value	Configure the TTL value in packets. The value range is from 1 to 255.

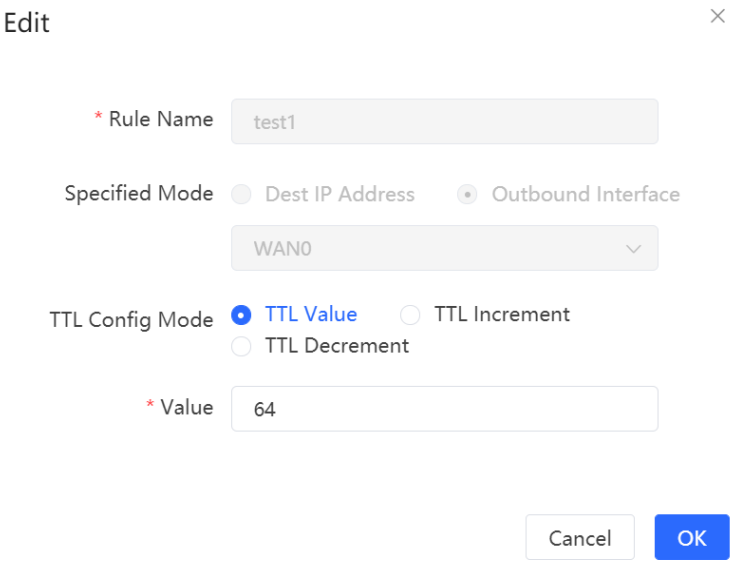
2. Deleting a TTL Rule

- Click **Delete** to delete the configuration of a specified entry.
- Select multiple entries and click **Delete Selected** to bulk delete selected entries.



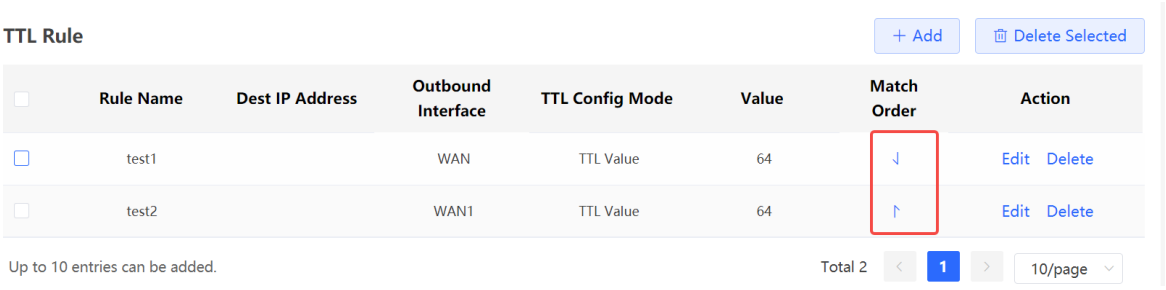
3. Editing a TTL Rule

Click **Edit**. Change the TTL rule configuration mode and TTL value.



4. Adjusting the Sequence of TTL Rules

After configuring multiple TTL rules, you can adjust their sequence to specify the rule matching sequence. TTL rules in front rows are matched first, and those in back rows are matched later. If the ranges of rules overlap, the final effect is the superposition of multiple matching results.



4.21 Disk Management

Note

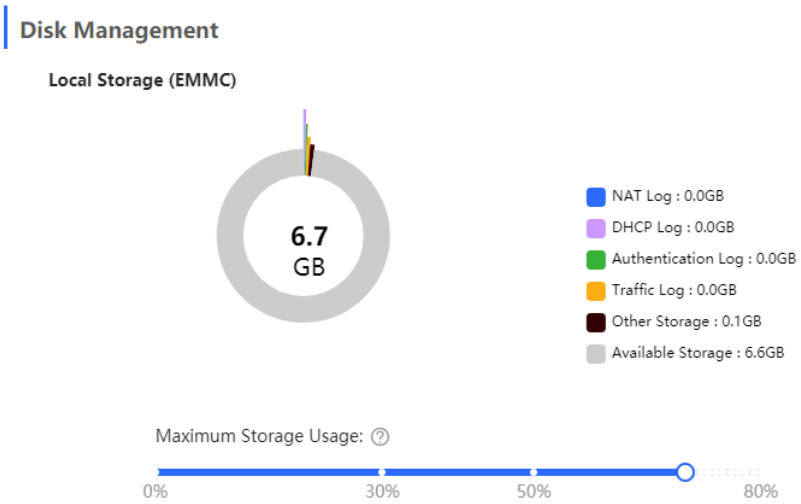
This feature is only supported on RG-EG1510XS.

4.21.1 Configuring Local Storage Settings

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

On the **Local Storage** pane, you can view the usage of the local storage, along with usage details of NAT logs, DHCP logs, authentication logs, traffic logs, other storage space, and available storage space.

To set the maximum storage usage of an eMMC, simply drag the scroll bar and click **Save**.



Caution

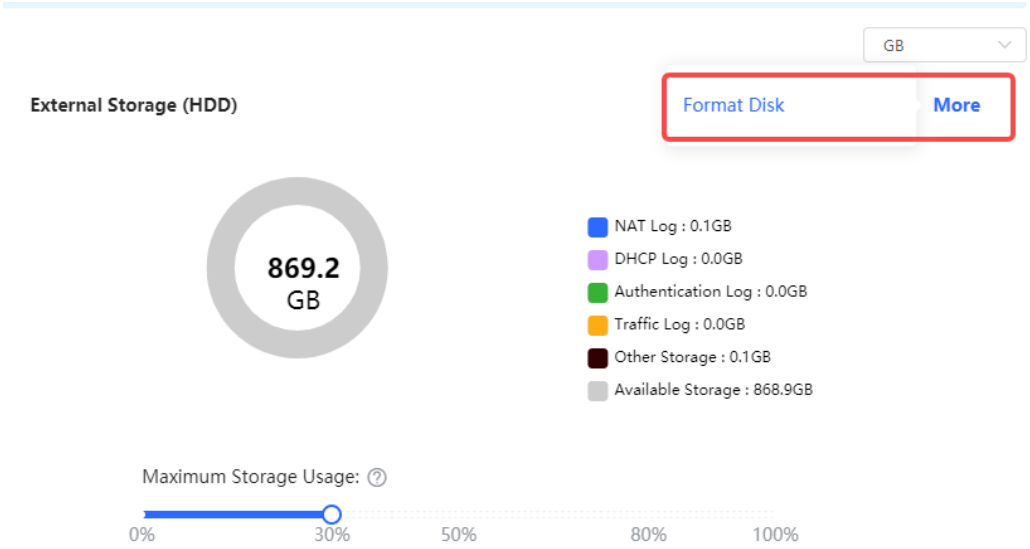
- If the actual space used for log storage exceeds the maximum storage usage limit, the oldest log entries will be overwritten. You are advised to set a proper maximum storage usage to prevent the deletion of critical logs.
- To prolong the service life of the eMMC, you are advised to set the maximum storage usage to 80% or below.

4.21.2 Configuring External Storage Settings

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

On the **External Storage** pane, you can view the usage of the external storage, along with usage details of NAT logs, DHCP logs, authentication logs, traffic logs, other storage space, and available storage space. To set the maximum storage usage of a hard disk drive, simply drag the scroll bar and click **Save**.

Click **More** to find the **Format Disk** option. You can format the hard disk drive using this option.



Caution

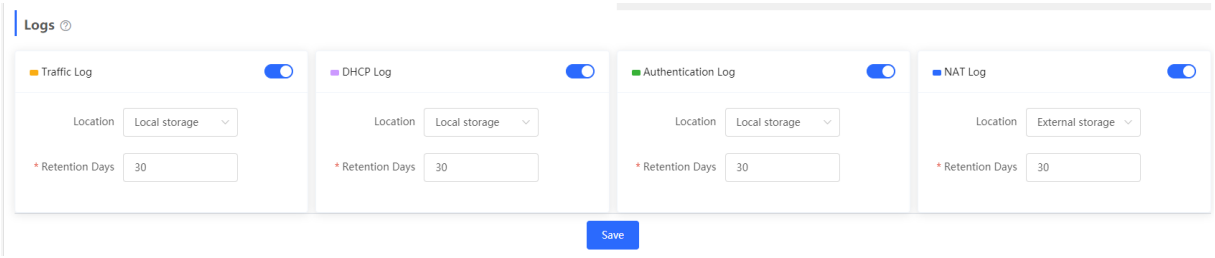
- If the actual space used for log storage exceeds the maximum storage usage limit, some logs will be deleted. You are advised to set a proper maximum storage usage to prevent the deletion of critical logs.
- Formatting the hard disk drive will cause data loss. Exercise caution when performing this operation.

4.21.3 Configuring Log Settings

Choose **Local Device** > **Advanced** > **Disk Management** > **Logs**.

The **Logs** feature enables you to manage the storage of various logs, including traffic logs, DHCP logs, authentication logs, and NAT logs. You can choose the specific types of logs to store, set the storage location, and define the log retention days. Then, click **Save** to apply the settings.

After the configuration is complete, you can access and query NAT logs, DHCP logs, and authentication logs stored on the device by going to **Local Device** > **Network** > **Audit Log Reports**. For traffic logs, you can query them under **Local Device** > **Device Overview** > **Traffic History**.



Caution

Exercise caution when setting the log retention period, as logs older than the specified duration will be overwritten.

4.22 Audit Log Reports

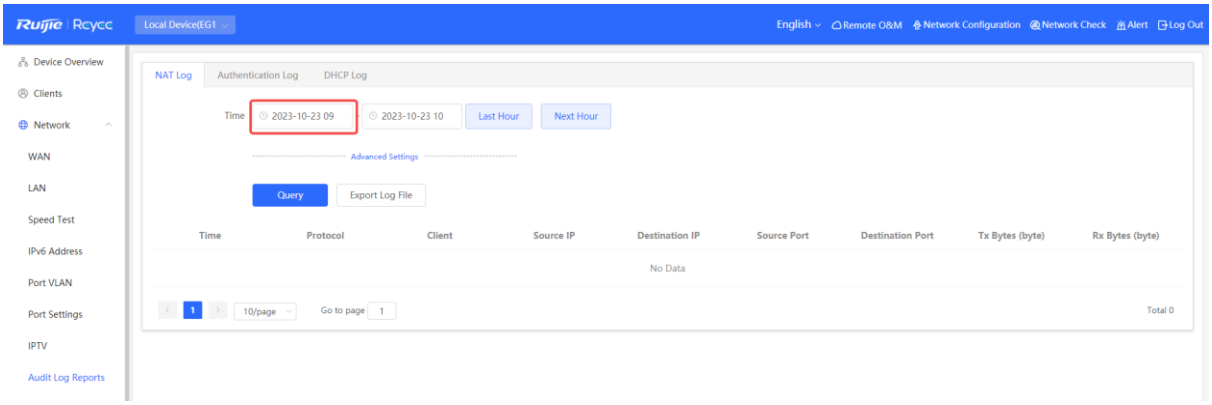
Note

This feature is only supported on RG-EG1510XS.

4.22.1 NAT Log

Choose **Local Device** > **Network** > **Audit Log Reports** > **NAT Log**.

- View log details
  - Select the date and time range to view NAT logs within that period. The logs will include information such as time, protocol, client, source IP, destination IP, source port, destination port, Tx bytes, and Rx bytes.
  - Click **Last Hour** or **Next Hour** to quickly retrieve NAT information from the hour before or after the current time.

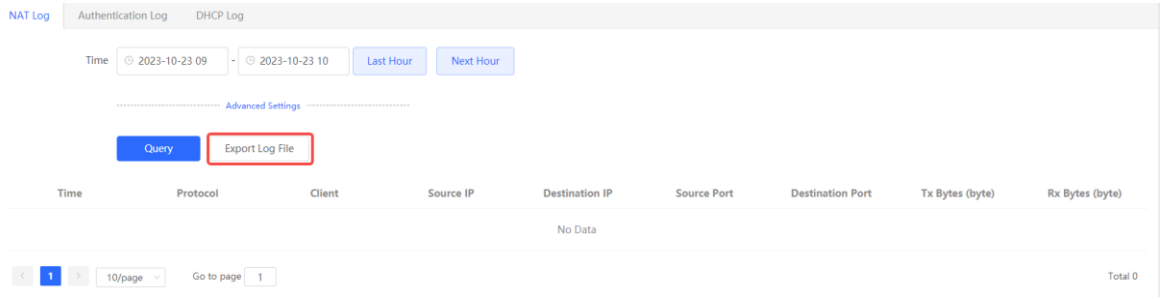


Note

The maximum log query interval is 12 hours.

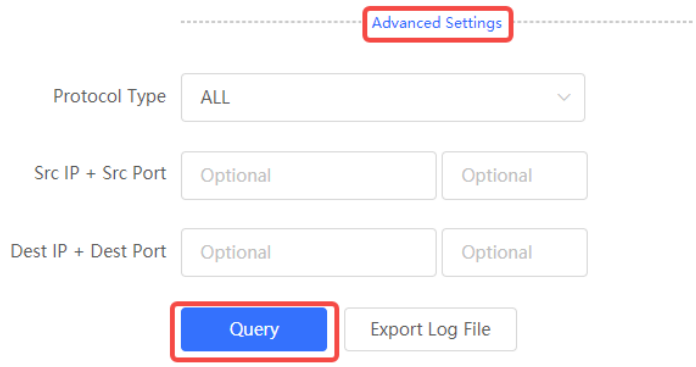
- Export log file

  Click **Export Log File** to export NAT logs within the selected period.



- Query NAT logs

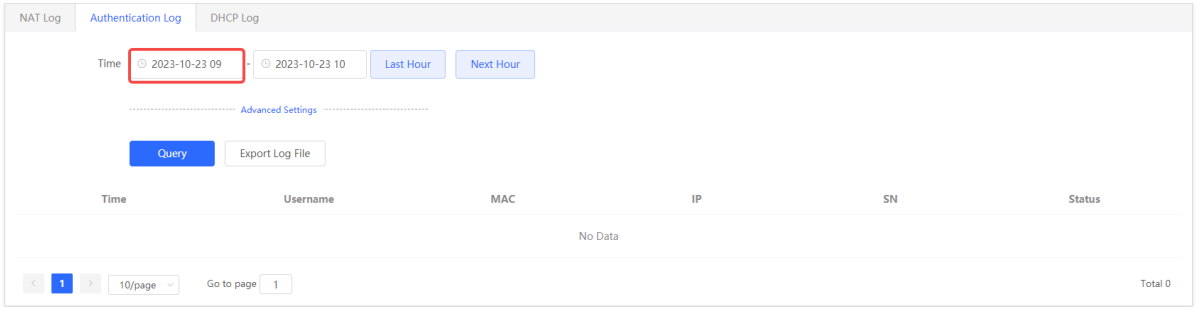
  Click **Advanced Settings** to query NAT logs based on protocol type, source IP + source port, or destination IP + destination port.



4.22.2 Authentication Log

Choose **Local Device** > **Network** > **Audit Log Reports** > **Authentication Log**.

- View log details
  - Select the date and time range to view authentication logs within that period. The logs will include information such as time, username, MAC address, IP address, device SN and status.
  - Click **Last Hour** or **Next Hour** to quickly retrieve authentication information from the hour before or after the current time.

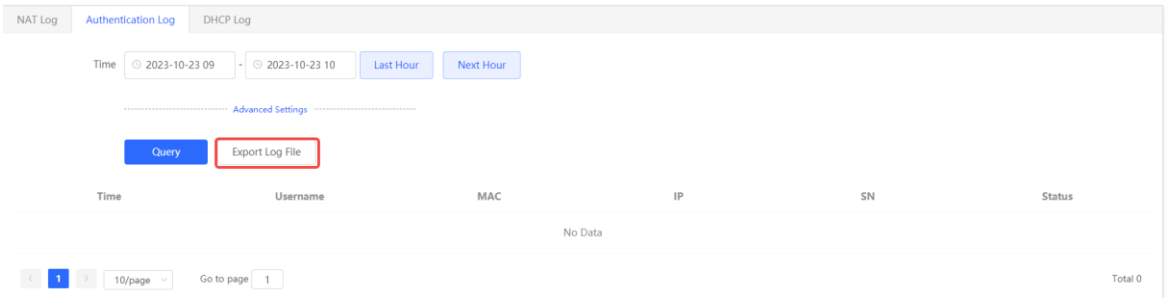


Note

The maximum log query interval is 12 hours.

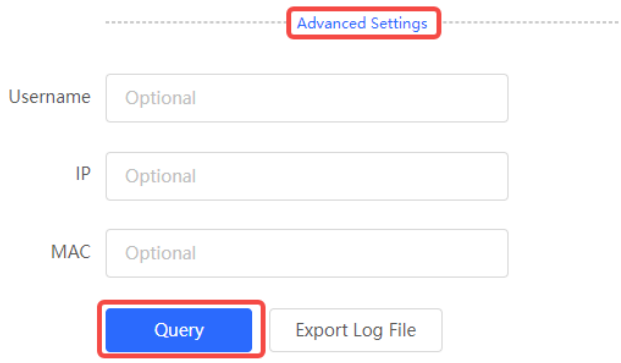
- Export log file

  Click **Export Log File** to export authentication logs within the selected period.



- Query authentication logs

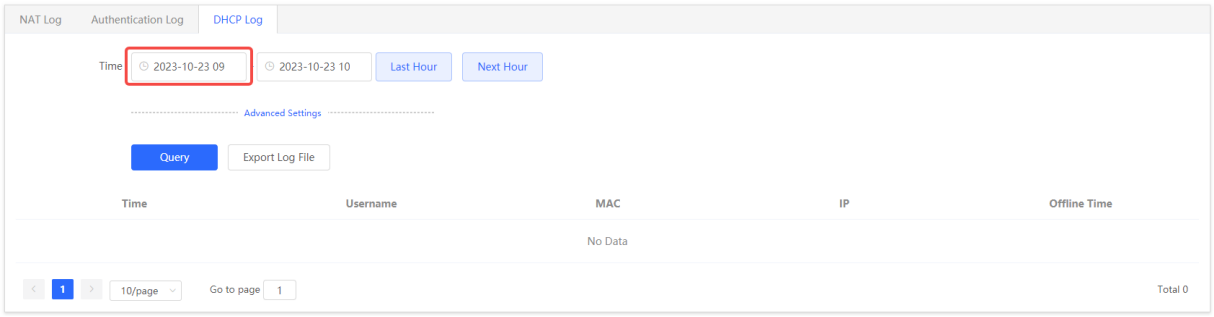
  Click **Advanced Settings** to query authentication logs based on username, IP address, or MAC address.



4.22.3 DHCP Log

Choose **Local Device** > **Network** > **Audit Log Reports** > **DHCP Log**.

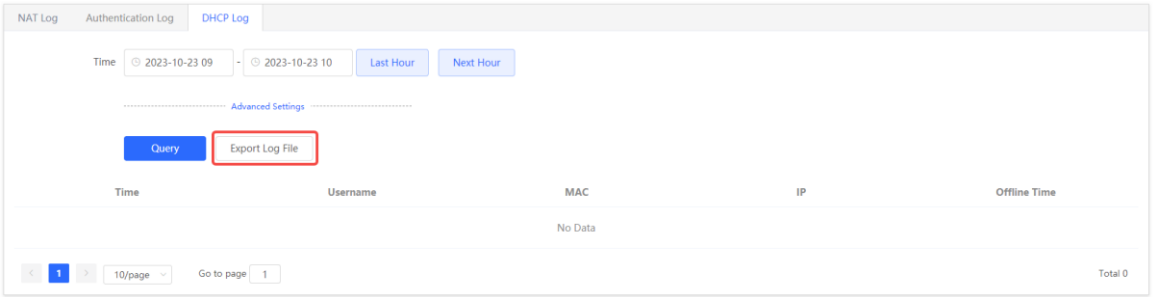
- View log details
  - Select the date and time range to view DHCP logs within that period. The logs will include information such as time, username, MAC address, IP address, and offline time.
  - Click **Last Hour** or **Next Hour** to quickly retrieve DHCP information from the hour before or after the current time.



Note

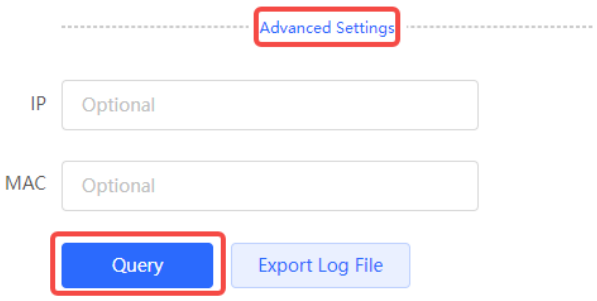
The maximum log query interval is 12 hours.

- Export log file
  Click **Export Log File** to export DHCP logs within the selected period.



- Query DHCP logs

  Click **Advanced Settings** to query DHCP logs based on IP address or MAC address.

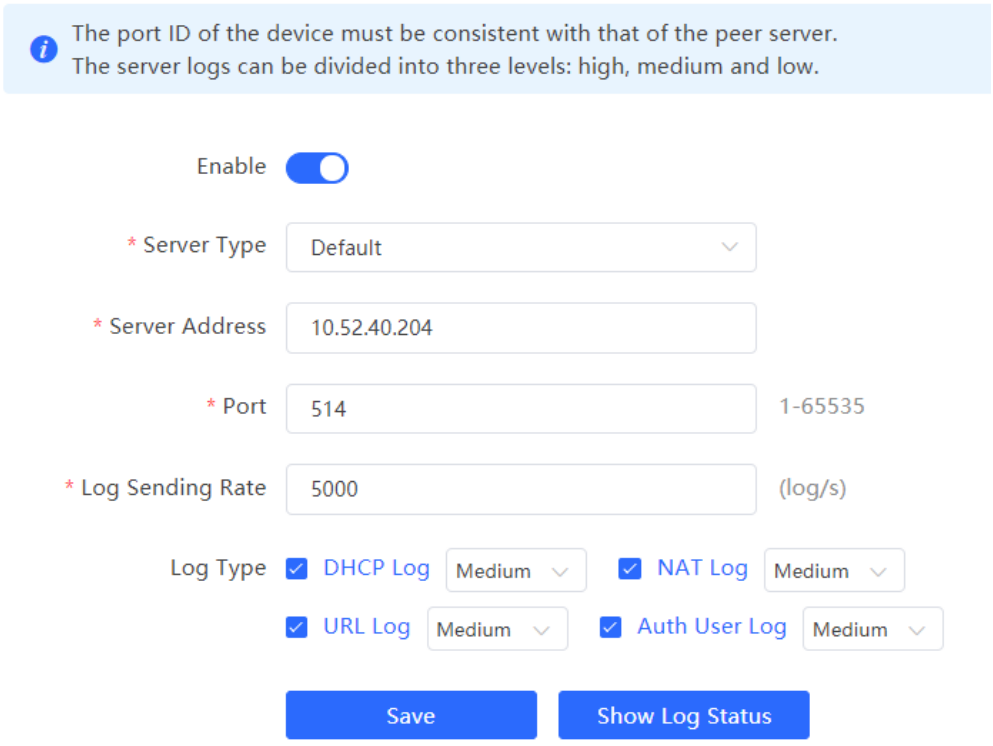


4.23 Configuring Audit Log

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Audit Log**.

After the **Audit Log** function is enabled and configured, the system uploads audit logs of the selected log type to the specified server.

(1) Toggle on **Enable** to enable the **Audit Log** function.



(2) Configure parameters of the **Audit Log** function.

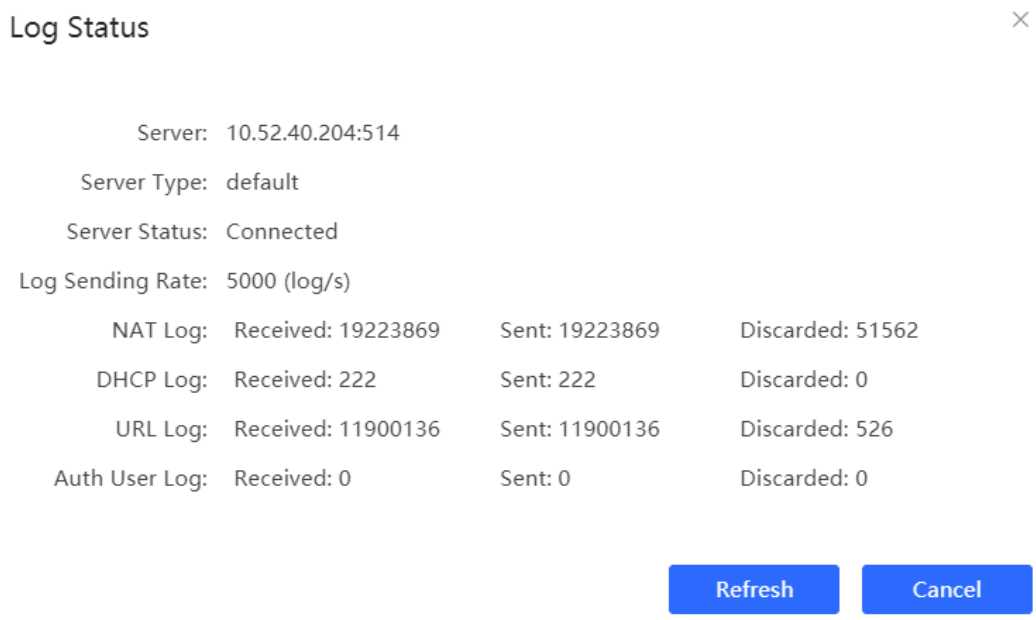
Table 4-43 Audit Log Configuration Parameters

Parameter	Description
Server Type	Server type. The device supports the following three server types: ● Default: Default server type. ● turkiye-5651: Local server in Türkiye. ● Thailand: Local server in Thailand.

Parameter	Description
Server Address	Address of the log server. It can be a domain name and an IPv4 address.
Port	Port number of the server, which can be a custom port number. The default port number is 514.
Log Sending Rate	Rate at which the device sends audit logs to the server. The default rate is 5000 logs per second. The value ranges from 1 log per second to 10000 logs per second.
Log Type	Types of logs to be sent to the server, including DHCP logs, NAT logs, URL logs, and authentication user logs. Priority of sending audit logs: **High**, **Medium**, and **Low**. When the device resources are limited, audit logs with higher priority are sent to the server first.

(3) Click **Save**.

Click **Show Log Status** to view the status of the **Audit Log** function, including the server address, server connection status, and the sending history of each log type (including received, sent, and discarded logs).



4.24 Configuring High-Speed Mode

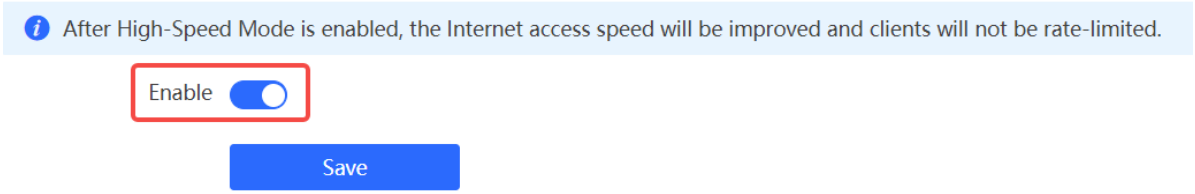
Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **High-Speed Mode**.

After the Audit Log function is enabled and configured, the system uploads audit logs of the selected log type to the specified server.

Note

- When the high-speed mode is enabled, the traffic audit and intelligent traffic control functions will be disabled, and the accuracy of the application control and website control functions will be affected.

- The function is supported by RG-EG210G, RG-EG105G-V2, RG-EG210G-P-V3, RG-EG105G-V3, RG-EG105G-P-V3 and RG-EG209GS



(1) Toggle on the Enable switch.

(2) Click **Save**. The system will prompt that the intelligent traffic control feature will be disabled.

(3) Click **OK**.

4.25 Other Settings

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Other Settings**.

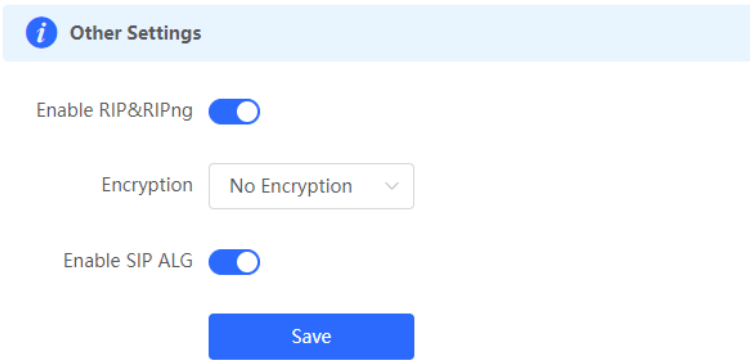
You can set some functions not frequently used on the Other Settings page. By default, all the functions on this page are disabled.

Note

Enable RIP&RIPng is only available on devices that do not support the OSPF protocol. The actual product version prevails.

Enable RIP&RIPng: After this function is enabled, LAN and WAN interfaces support dynamic routing protocols Routing Information Protocol (RIP) and RIP next generation (RIPng) and can automatically synchronize route information from other RIP-enabled routers in the network.

Enable SIP ALG: Some voice communication uses the Session Initiation Protocol (SIP) protocol. If the server is connected to a WAN interface, SIP packets may become unavailable after NAT. After you enable this function, SIP packets are converted by the application-level gateway (ALG). You can enable or disable this function based on actual needs.



5 AP Management

Note

- To manage the downlink AP, please enable self-organizing network discovery (See Section 4.1 Switching the Work Mode for details.). 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 5.1 Configuring AP Groups.
- The device does not emit the Wi-Fi signals. Deliver the wireless settings to the downlink AP to take effect.

5.1 Configuring AP Groups

5.1.1 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.

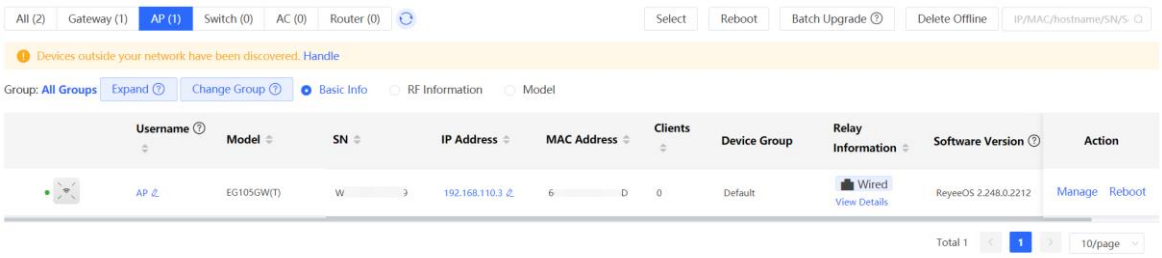
Note

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

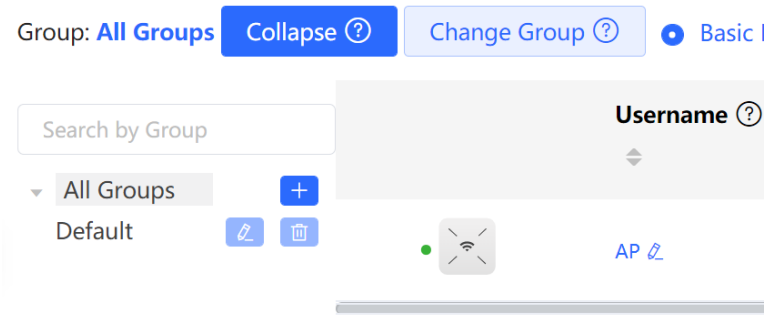
5.1.2 Configuration Steps

Choose **Network-Wide > Devices > AP**.

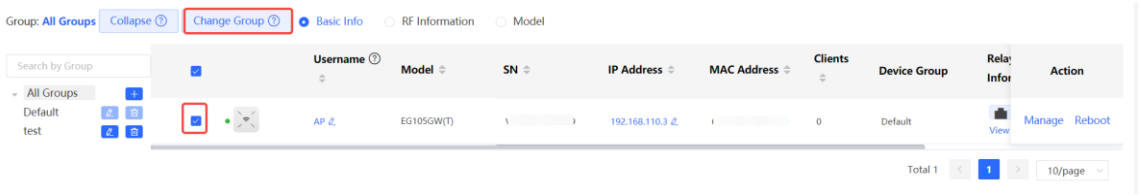
(1) View the information of all APs in the current network, including the basic information, RF information, and model. Click the SN of an AP to configure the AP separately.

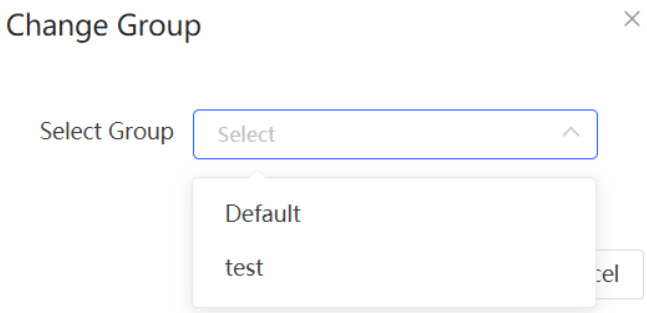


(2) Click **Expand**. Information of all the current groups is displayed to the left of the list. Click + to create a group. You can create a maximum of eight groups. Select the target group and click to modify the group name or click to delete the group. You cannot modify the name of the default group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



(3) Click a group name in the left. All devices in the group are displayed. One device can belong to only one group. By default, all devices 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.

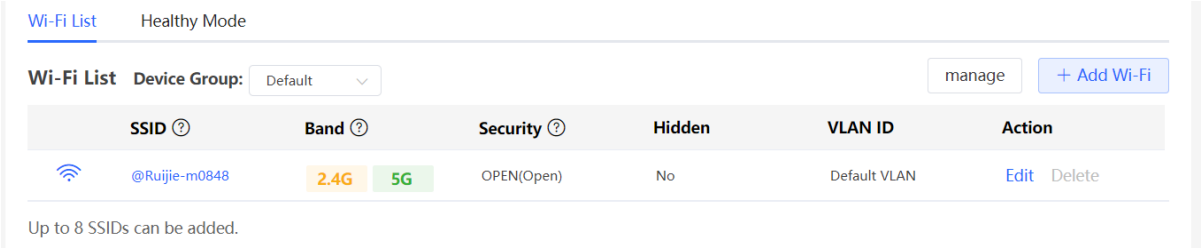




5.2 Configuring Wi-Fi

5.2.1 Adding a Wi-Fi Network

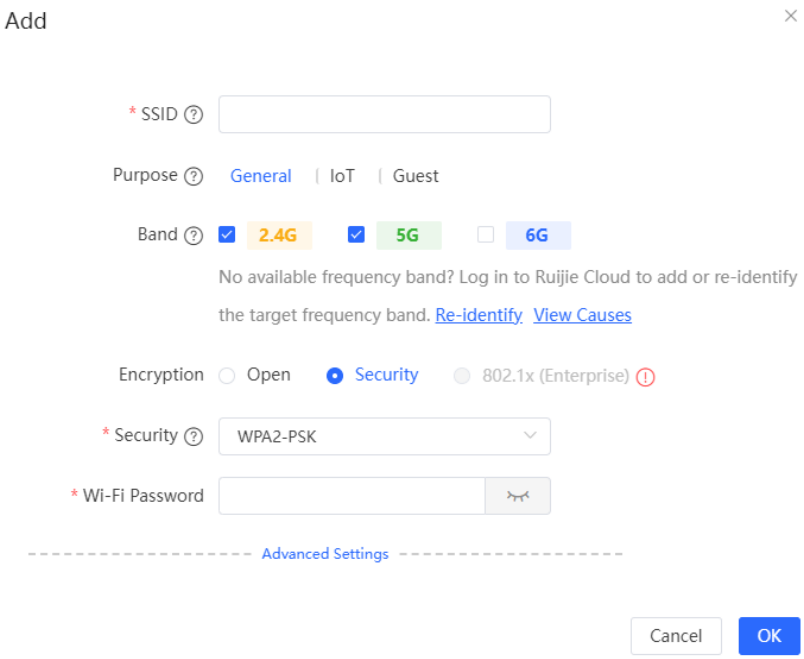
Choose **Network-Wide** > **Workspace** > **Wireless** > **Wi-Fi** > **Wi-Fi List**.



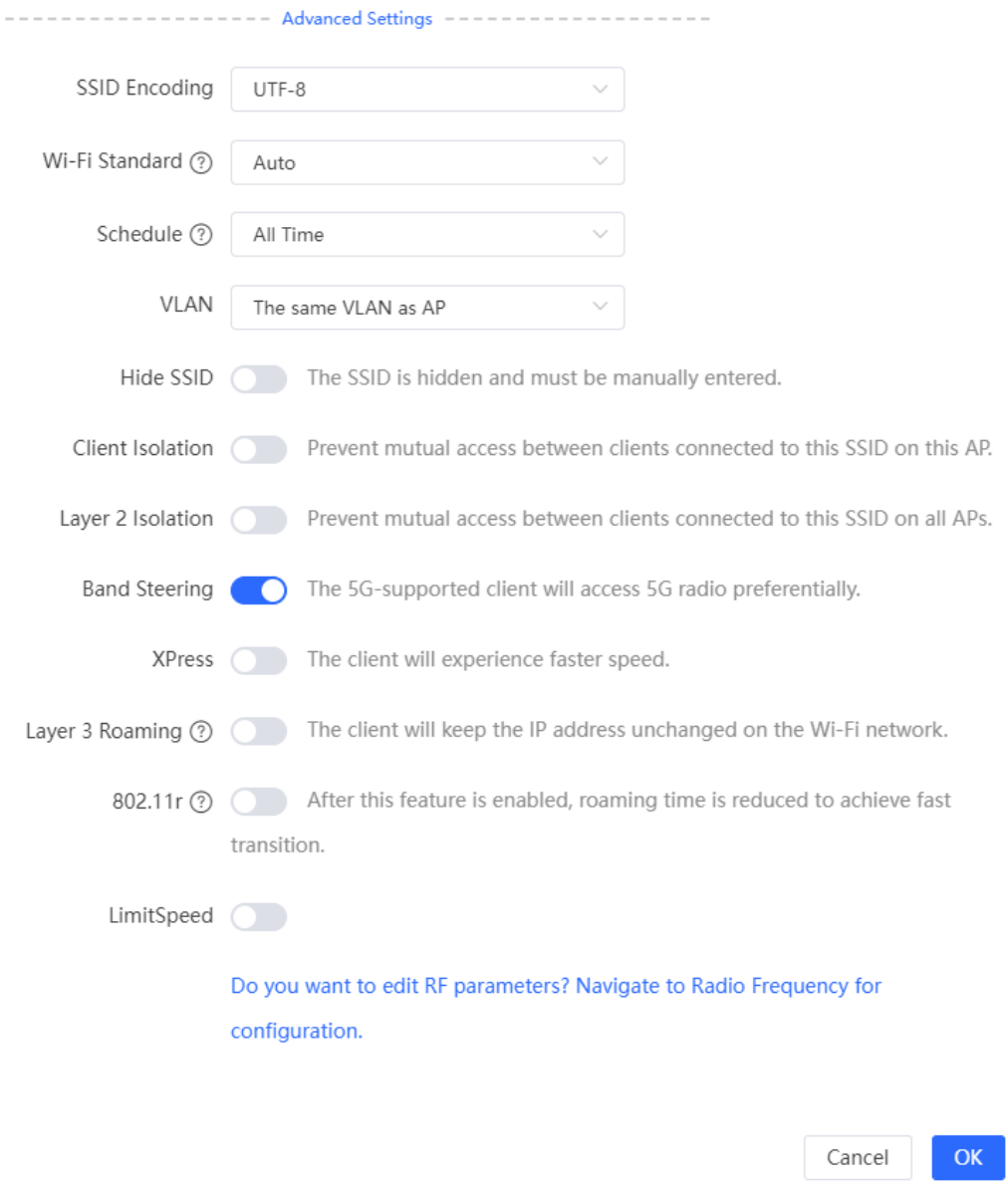
Caution

Modification will cause restart of the wireless configuration, resulting in logout of connected clients. Exercise caution when performing this operation.

(1) Click **Add Wi-Fi**, enter the SSID and Wi-Fi password, select purpose and a frequency band.



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



(3) Click **OK**.

Table 5-1 Wireless network configuration

Parameter	Description
SSID	Enter the name displayed when a wireless client searches for a wireless network.
Purpose	Set the Wi-Fi usage scenario. The options include **General**, **IoT**, and **Guest**. The system will recommend different Wi-Fi parameter combinations based on the selected purpose.

Parameter	Description
Band	Set the band used by the Wi-Fi signal. The options are 2.4 GHz, 5 GHz and 6 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. The 6 GHz band has a higher network transmission rate and less interference compared to the 2.4 GHz and 5 GHz bands, but it is usually not as good as the 2.4 GHz and 5 GHz frequency bands in terms of signal coverage and wall penetration. 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. **Note** In networks with APs supporting the 6 GHz frequency band, you'll see an additional '6G' option in the frequency settings. The 6 GHz-band provides faster data transmission rates, but it's worth noting that-not all access devices may fully support this band. The RG-RAP73(HD) supports 6 GHz band.
Encryption	The encryption options for a Wi-Fi network include **Open**, **Security**, and **802.1x (Enterprise)**.
Wi-Fi Password	When the **Encryption** is set to **Security**, you need to set the password for connecting to the wireless network. The password is a string of 8 to 63 characters.
Select server group	When the **Encryption** is set to **802. 1x (Enterprise)**, you need to configure a remote server set for authentication and authorization.
SSID Encoding	The SSID encoding standard is set to "UTF-8" by default when Chinese characters are included in the SSID. If the Chinese characters are garbled, you can choose GB2312 as the SSID encoding standard.
Wi-Fi Standard	The Wi-Fi standards include **802.11be (Wi-Fi 7)**, **802.11ax (Wi-Fi 6)**, **Compatibility Mode**, or **Auto**. The final effective Wi-Fi standard depends on the support of Wi-Fi standards on each device. The latest standard is recommended. If there is a compatibility issue, try use an older standard. However, an old standard setting will affect the bandwidth.
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.

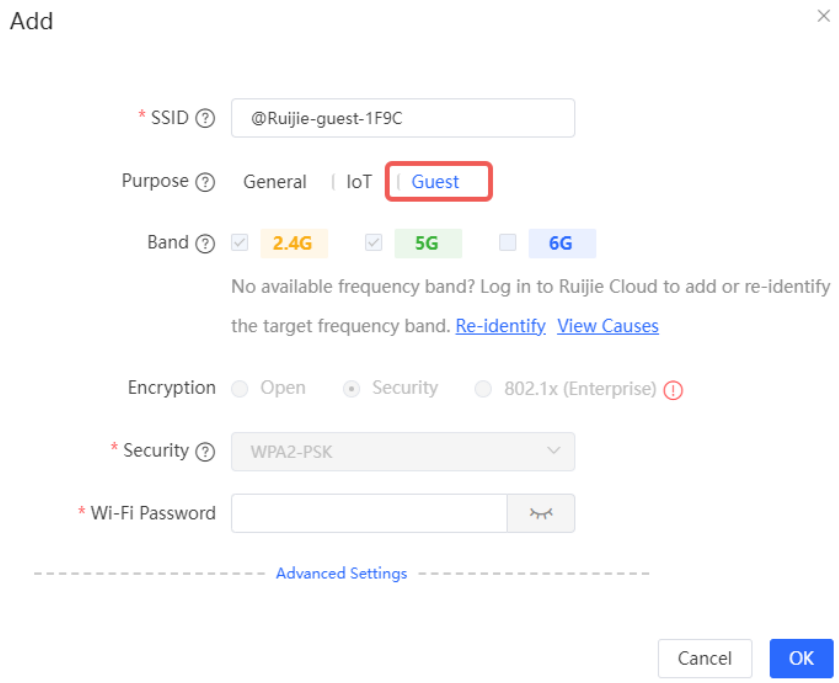
Parameter	Description
VLAN	Set the VLAN to which the Wi-Fi signal belongs. You can choose from the available VLANs or click **Add New VLAN**, and go to the **LAN Settings** page to add a VLAN.
Hide SSID	Enabling the hide SSID function can prevent unauthorized user access to Wi-Fi, improving security. However, mobile phones or computers cannot find the SSID after this function is enabled. You must manually enter the correct name and password to connect to Wi-Fi. Record the current SSID before you enable this function.
Client Isolation	When enabled, devices connected to this Wi-Fi network under the same access point (AP) will be isolated from each other. This prevents end users from accessing other users on the same subnet, thereby enhancing security.
Layer 2 Isolation	When enabled, clients connected to this SSID are isolated from each other, and cannot access other clients connected to this SSID on all APs on Layer 2, thereby improving 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.
802.11r	Enabling the 802. 11r function can shorten the roaming handover time. The 802. 11r function is supported only when **Encryption** is set to **Security** or **802. 1x (Enterprise)**. Once 802. 11r is enabled, the encryption type can only be WPA2-PSK or WPA2-802. 1X. **Note** Only in networks with Wi-Fi 7 Products, Wi-Fi 6 Products and 16M Wi-Fi 5 Products supporting the 802.11r.
LimitSpeed	After enabling Wi-Fi rate limiting, you can set the uplink and downlink rate limits for users. ● Rate Limit Per User: The rate limit applies to all clients connected to the SSID. ● Rate Limit All Users: All clients connected to the SSID share the configured rate limit equally. The rate limit of each client changes dynamically with the number of clients connected to the SSID.

5.2.2 Configuring Guest Wi-Fi

Guest Wi-Fi, the Wi-Fi service provided for guests, is disabled by default. By default, user isolation is enabled for the guest Wi-Fi. That is, users connected to the guest Wi-Fi are isolated from each other and can only access the Internet through the Wi-Fi network, which improves security. Guest Wi-Fi can be disabled at a scheduled time. When the scheduled time arrives, the guest Wi-Fi is automatically disabled.

Choose **Network-Wide** > **Workspace** > **Wireless** > **Wi-Fi** > **Wi-Fi List.**

Click **Add Wi-Fi**, set the **Purpose** to **Guest**, and configure the Wi-Fi name and password. Click **Advanced Settings** to configure the effective time of the guest Wi-Fi and other Wi-Fi parameters. After the settings are saved, guests can connect to the Internet through the SSID and password. For details, see 5.2.1 Adding a Wi-Fi Network.



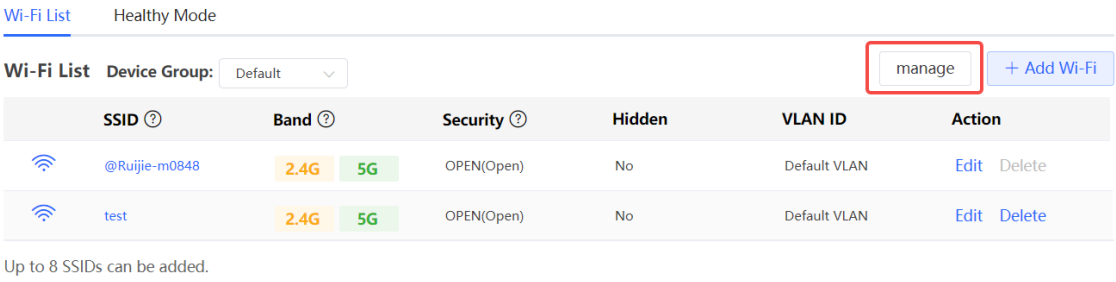
Note

In networks with APs supporting the 6 GHz frequency band, you'll see an additional '6G' option in the frequency settings. The RG-RAP73(HD) supports 6 GHz band.

5.2.3 Managing Wi-Fi Networks

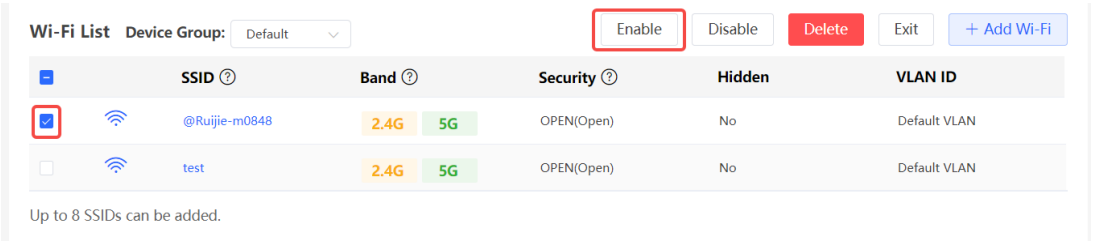
Choose **Network-Wide** > **Workspace** > **Wireless** > **Wi-Fi** > **Wi-Fi List.**

(1) Click **manage** to batch manage Wi-Fi networks.

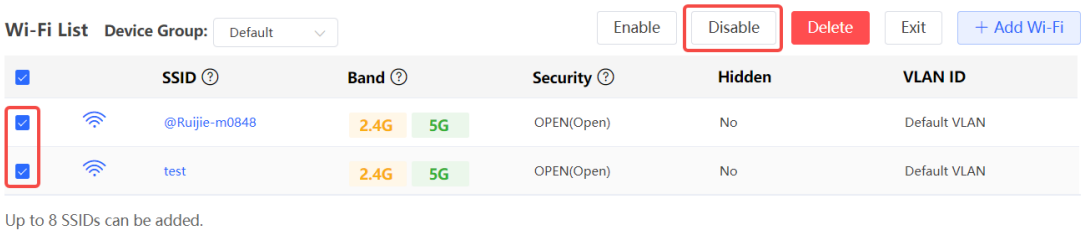


(2) Batch manage Wi-Fi networks.

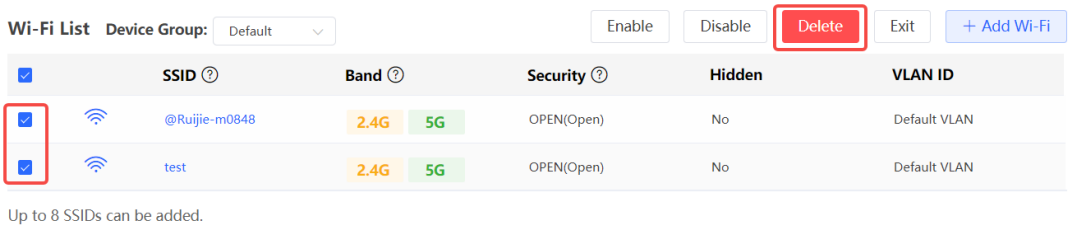
- Batch enable Wi-Fi networks: Select the desired Wi-Fi networks, and click **Enable**.



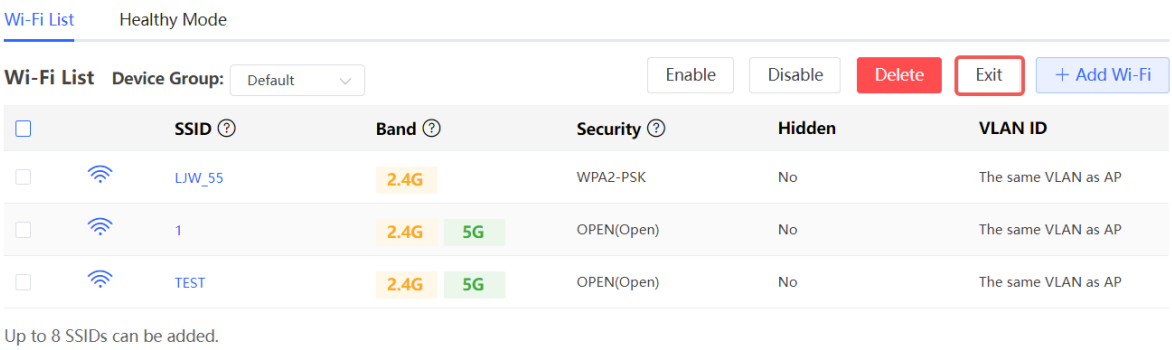
- Batch disable Wi-Fi networks: Select the desired Wi-Fi networks, and click **Disable**.



- Batch delete Wi-Fi networks: Select the desired Wi-Fi networks, and click **Delete**.



(3) Click **Exit** to exit Wi-Fi network batch management.

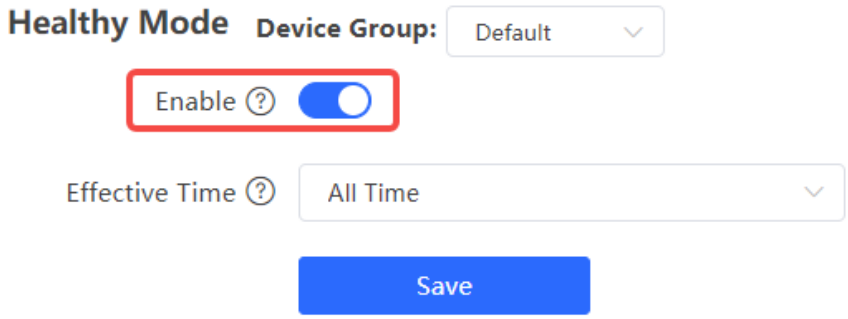


5.3 Healthy Mode

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



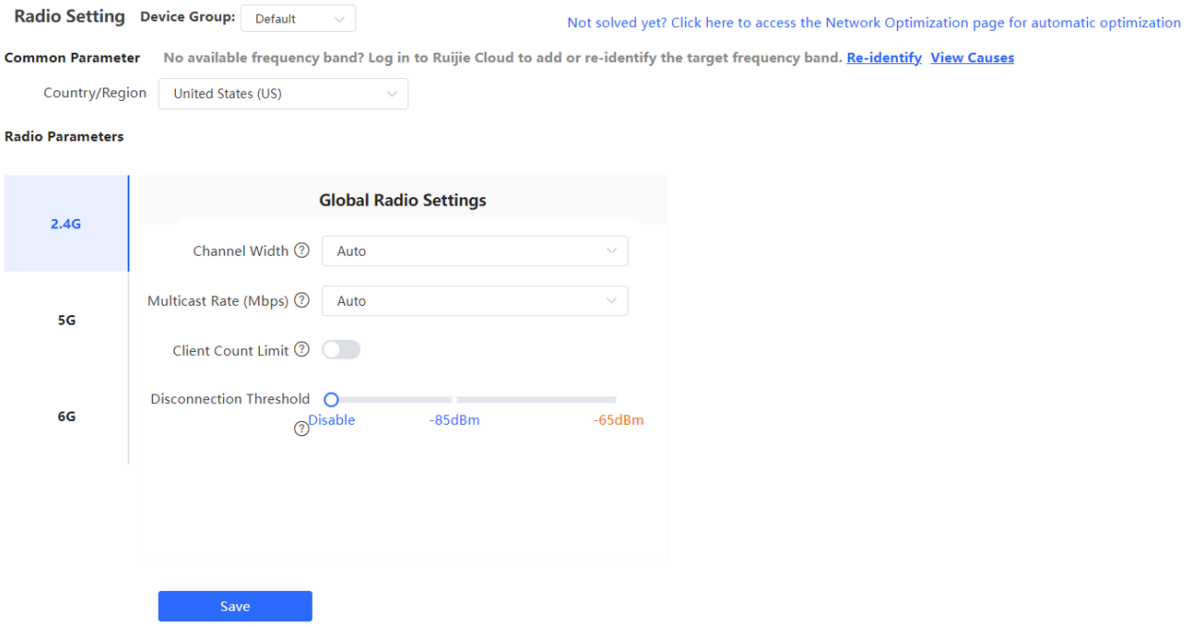
5.4 RF Settings

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

The 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.



Note

In networks with APs supporting the 6 GHz frequency band, you'll see an additional '6G' option in the frequency settings. The RG-RAP73(HD) supports 6 GHz band.

Table 5-2 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/6G 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, 80 MHz and 160 MHz bandwidths. The 6 GHz band supports the 20 MHz, 40 MHz, 80 MHz, 160 MHz and 320 MHz bandwidths. By default, the value is **Auto**, indicating that the bandwidth is selected automatically based on the environment.
Multicast Rate (Mbps)	Select the data rate of broadcast and multicast packets. ● Tip: A higher multicast rate may lead to a higher multicast packet loss rate. A lower multicast rate may cause heavier traffic on the wireless air interface. ● Suggestion: Use a high rate in the case of severe network congestion and a medium rate in the case of mild network lag.

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. You can toggle on the **Client Count Limit** toggle switch to set a client limit. 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.
Disconnection 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/region code. Select the country/region code based on the country or region of your device.
- Channel, transmit power, and roaming sensitivity cannot be set globally. Please perform the configurations on the devices separately.

5.5 Configuring Wi-Fi Blocklist or Allowlist

5.5.1 Overview

You can configure the global or SSID-based blocklist and allowlist. The MAC address supports full match and OUI match.

Wi-Fi blocklist: Clients in the Wi-Fi blocklist are prevented from accessing the Internet. Clients that are not added to the Wi-Fi blocklist are free to access the Internet.

Wi-Fi allowlist: Only clients in the Wi-Fi allowlist can access the Internet. Clients that are not added to the Wi-Fi allowlist are prevented from accessing the Internet.

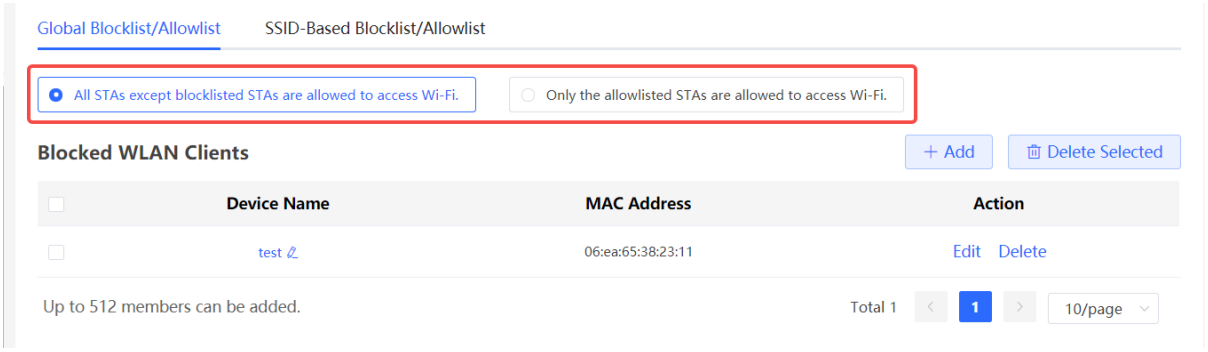
Caution

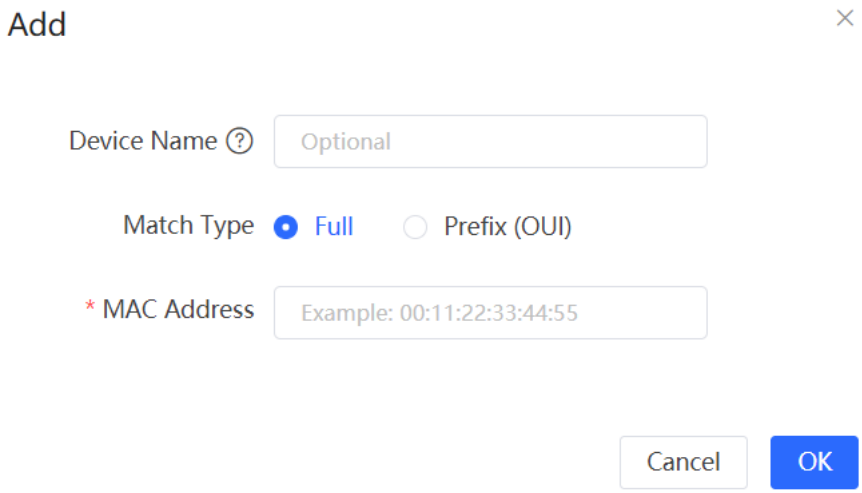
If the allowlist is empty, the allowlist does not take effect. In this case, all clients are allowed to access the Internet.

5.5.2 Configuring a Global Blocklist/Allowlist

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

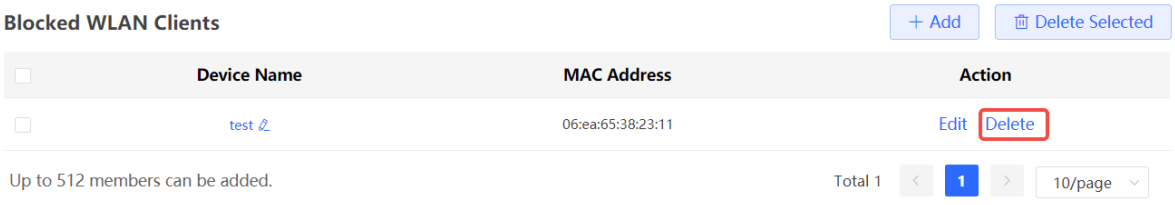
Select the blocklist or allowlist mode and click **Add** to configure a blocklist or allowlist client. In the **Add** dialog box, enter the **Device Name**, **Match Type** and **MAC Address** of the target client and click **OK**. If a client is already associated with the router, its MAC address will pop up automatically. Click the MAC address directly for automatic input. All clients in the blocklist will be forced offline and not allowed to access the Wi-Fi network. The global blocklist and allowlist settings take effect on all Wi-Fi networks of the router.





If you delete a client from the blocklist, the client will be allowed to connect to the Wi-Fi network.

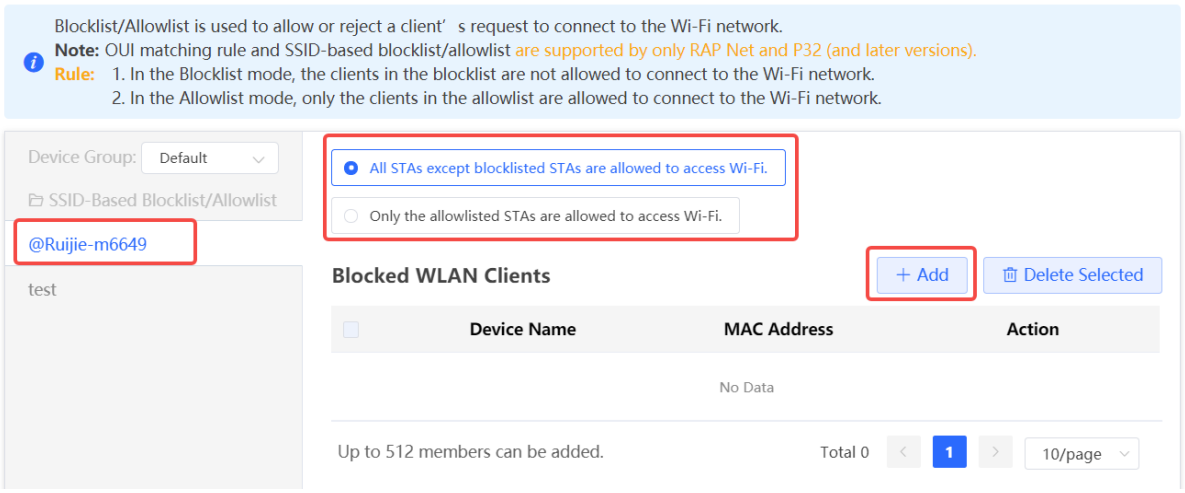
If you delete a client from the allowlist, the client will be forced offline and denied access to the Wi-Fi network.



5.5.3 Configuring an SSID-based Blocklist/Allowlist

Choose **Network-Wide** > **Workspace** > **Wireless** > **Blocklist and Allowlist** > **SSID-Based Blocklist/ Allowlist**.

Select a target Wi-Fi network from the left column, select the blocklist or allowlist mode, and click **Add** to configure a blocklist or allowlist client. The SSID-based blocklist and allowlist will restrict the client access to the specified Wi-Fi.



5.6 Configuring AP Load Balancing

5.6.1 Overview

The AP load balancing function is used to balance the load of APs in the wireless network. When APs are added to a load balancing group, clients will automatically associate with the APs with light load when the APs in the group are not load balanced. AP load balancing supports two modes:

- **Client Load Balancing**: The load is balanced according to the number of associated clients. When a large number of clients have been associated with an AP and the count difference to the AP with the lightest load has reached the specified value, the client can only associate with another AP in the group.
- **Traffic Load Balancing**: The load is balanced according to the traffic on the APs. When the traffic on an AP is large and the traffic difference to the AP with the lightest load has reached the specified value, the client can only associate with another AP in the group.

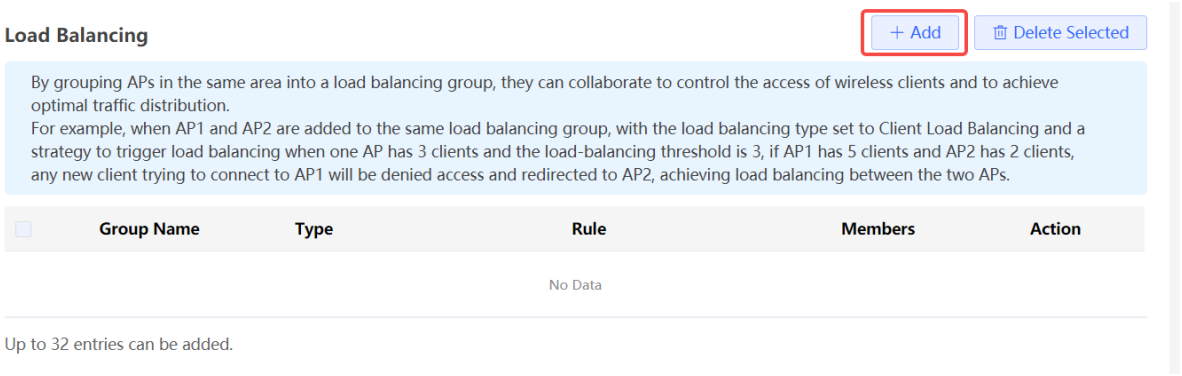
Example: Add AP1 and AP2 into a group and select client load balancing. Set both the client count threshold and difference to 3. AP1 is associated with 5 clients and AP2 is associated with 2 clients, triggering load balancing. New clients' attempt to associate to AP1 will be denied, and therefore they can associate only with AP2.

After a client request is denied by an AP and it fails to associate with another AP in the group, the client will keep trying to associate with this AP. If the client attempts reach the specified value, the AP will permit connection of this client, ensuring that the user can normally access the Internet.

5.6.2 Configuring Client Load Balancing

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

Click **Add**. In the dialog box that appears, set **Type** to **Client Load Balancing**, and configure **Group Name**, **Members**, and **Rule**.



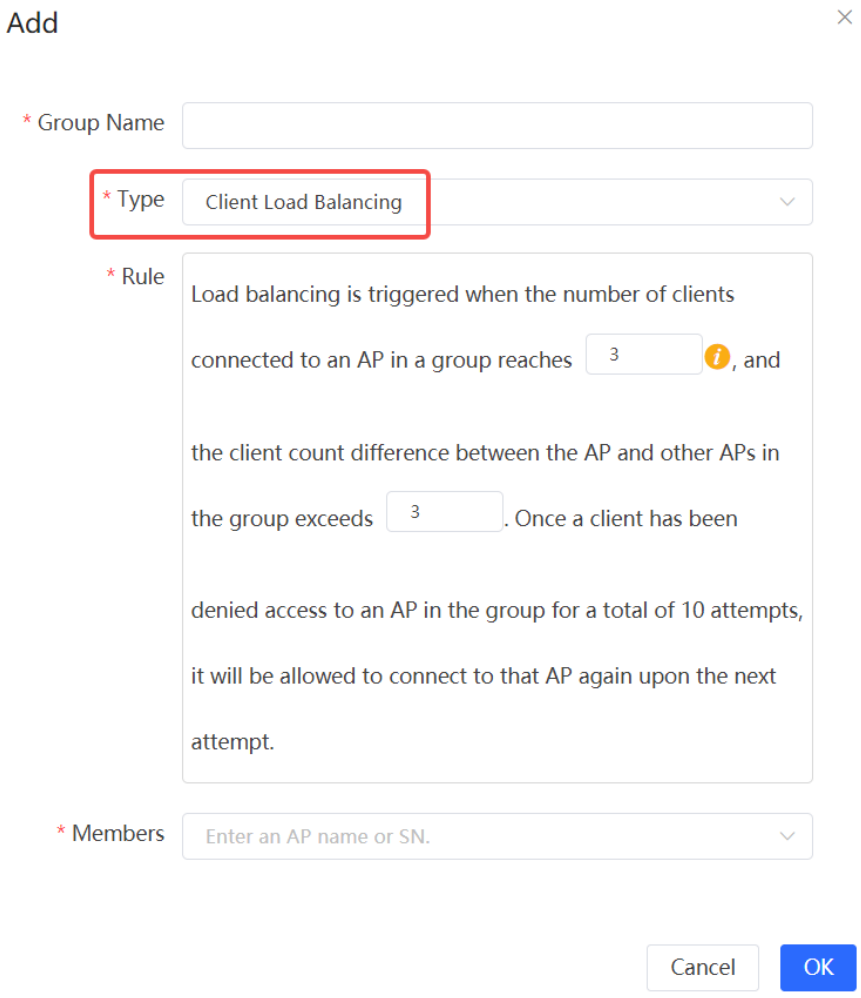


Table 5-3 Client load balancing configuration

Parameter	Description
Group Name	Enter the name of the AP load balancing group.
Type	Select **Client Load Balancing**.

Parameter	Description
Rule	Configure a detailed load balancing rule, including the maximum number of clients allowed to associate with an AP, the difference between the currently associated client count and client count on the AP with the lightest load, and the number of attempts to the AP with full load. By default, when an AP is associated with 3 clients and the difference between the currently associated client count and client count on the AP with the lightest load reaches 3, clients can associate only to another AP in the group. After a client association is denied by an AP for 10 times, the client will be allowed to associate to the AP upon the next attempt.
Members	Specify the APs to be added to the AP load balancing group.

5.6.3 Configuring Traffic Load Balancing

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

Click **Add**. In the dialog box that appears, set **Type** to **Traffic Load Balancing**, and configure **Group Name**, **Members**, and **Rule**.

Table 5-4 Traffic load balancing configuration

Parameter	Description
Group Name	Enter the name of the AP load balancing group.
Type	Select **Traffic Load Balancing**.
Rule	Configure a detailed load balancing rule, including the maximum traffic allowed on an AP, the difference between the current traffic and the traffic on the AP with the lightest load, and the number of attempts to the AP with full load. By default, when the traffic load on an AP reaches 500 Kbit/s and the difference between the current traffic and the traffic on the AP with the lightest load reaches 500 Kbps, clients can associate only to another AP in the group. After a client association is denied by an AP for 10 times, the client will be allowed to associate to the AP upon the next attempt.
Members	Specify the APs to be added to the AP load balancing group.

5.7 Configuring Wireless Rate Limiting

5.7.1 Overview

The device supports four rate limiting modes: client-based rate limiting, SSID-based rate limiting, AP-based rate limiting, and packet-based rate limiting. For the same client, if multiple rate limiting modes are configured, the priority order is as follows: client-based rate limiting > SSID-based rate limiting > AP-based rate limiting.

- Client-based rate limiting: This function allows you to limit the rate based on the MAC address of the client, so as to limit or guarantee the bandwidth required by specific clients.
- SSID-based rate limiting: This function provides two rate limiting modes for a specified SSID: Rate Limit Per User and Rate Limit All Users. Rate Limit Per User means that all clients connected to the SSID use the same rate limit. Rate Limit All Users means that the configured rate limit value is evenly allocated to all clients connected to the SSID. The rate limit value of each client dynamically changes with the number of clients connected to the SSID.
- AP-based rate limiting: This function limits the client rates based on the whole network. All clients connected to the network will work according to the configured rate limit value.
- Packet-based rate limiting: This function limits the client rates based on the downlink broadcast and multicast packets. The device supports rate limiting for specific broadcast packets (such as ARP and DHCP), multicast packets (such as MDNS and SSDP), or all types of broadcast and multicast packets. If network stalling remains during network access and there is no client with large traffic, you are advised to adjust the rate between 1 Kbps and 512 Kbps.

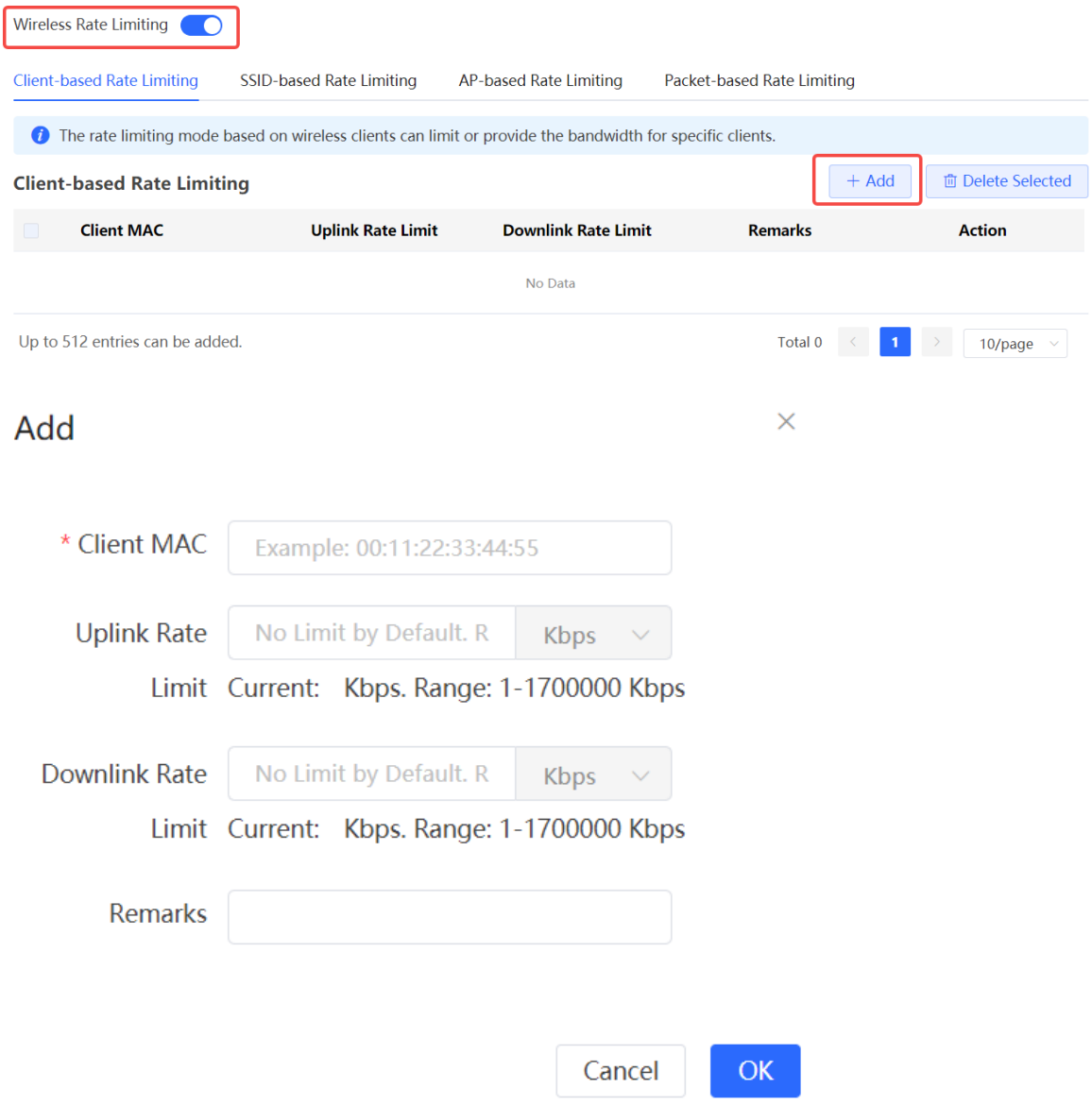
5.7.2 Configuration Steps

1. Configuring Client-based Rate Limiting

Choose **Network-Wide** > **Workspace** > **Wireless** > **Rate Limiting** > **Client-based Rate Limiting**.

(1) Enable Wireless Rate Limiting.

(2) Click **Add**. In the dialog box that appears, set the MAC address and uplink and downlink rate limit values of the client, and click **OK**.

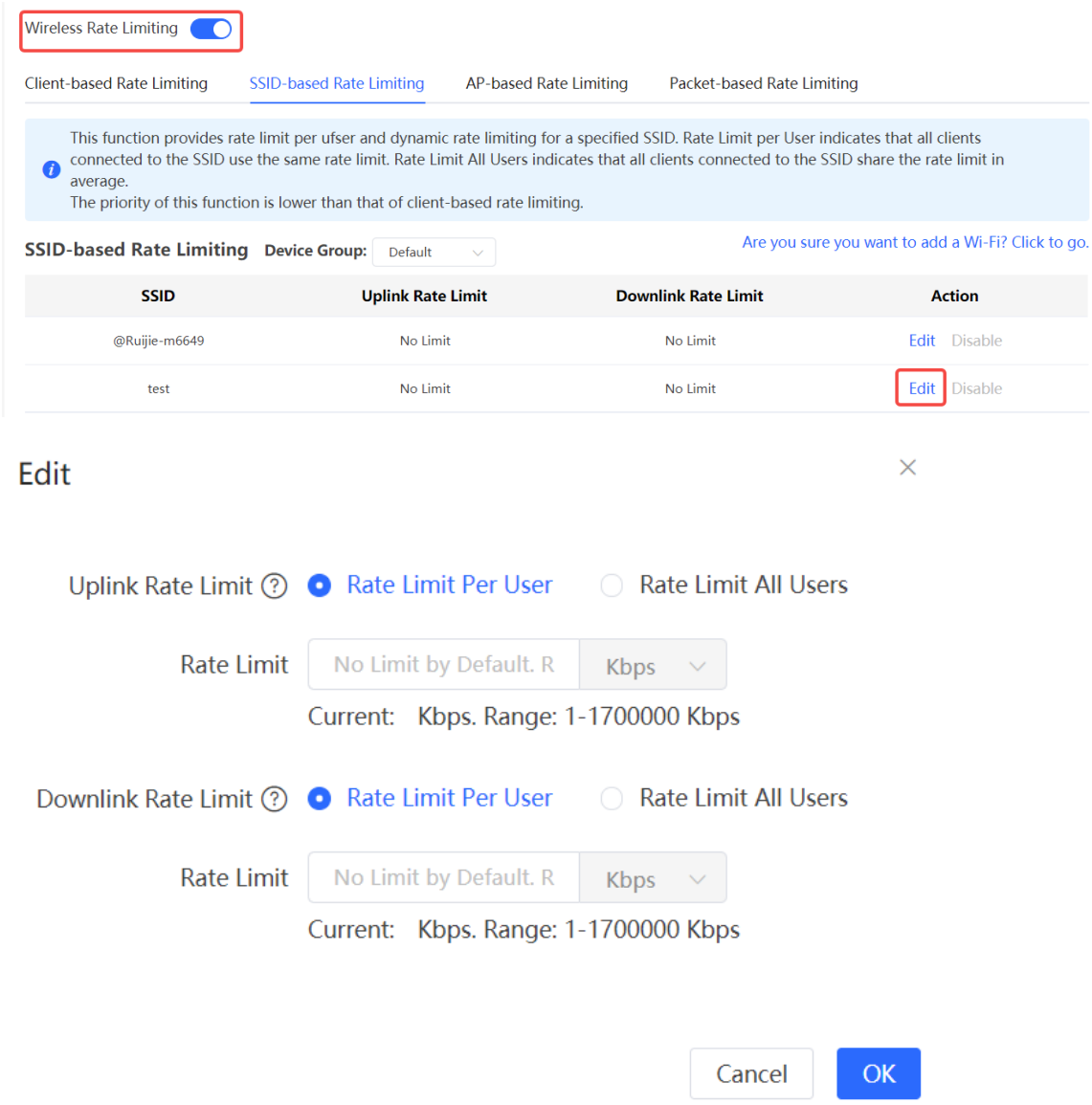


2. Configuring SSID-based Rate Limiting

Choose **Network-Wide** > **Workspace** > **Wireless** > **Rate Limiting** > **SSID-based Rate Limiting**.

(1) Enable Wireless Rate Limiting.

(2) Click **Edit** in the **Action** column of the target SSID. In the dialog box that appears, set the uplink and downlink rate limit modes and values, and click **OK**.

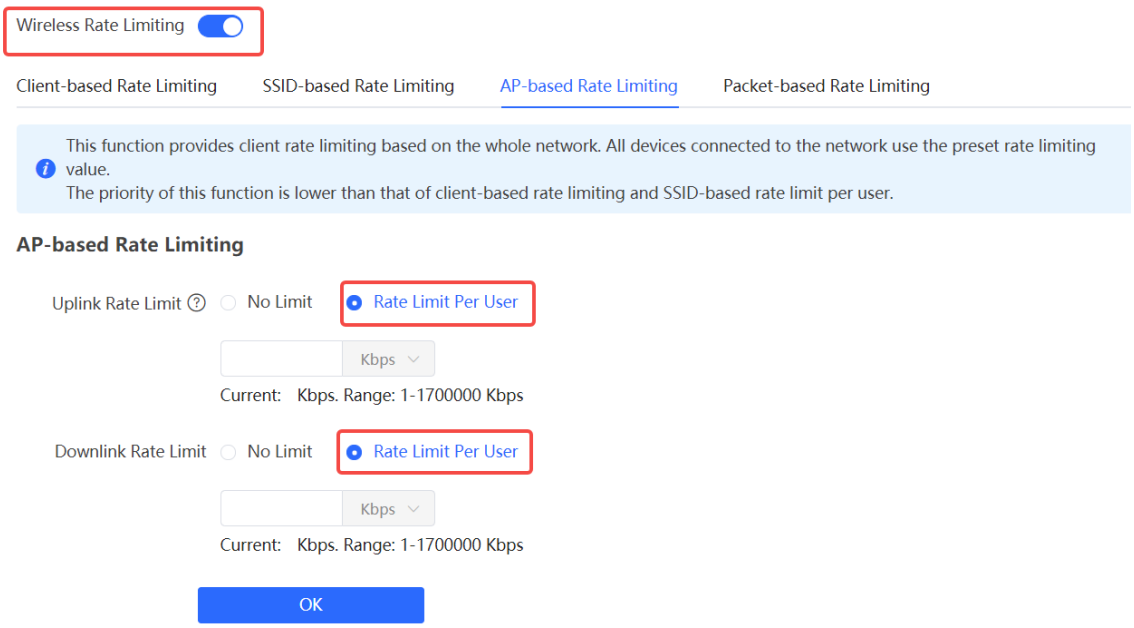


3. Configuring AP-based Rate Limiting

Choose **Network-Wide** > **Workspace** > **Wireless** > **Rate Limiting** > **AP-based Rate Limiting**.

(1) Enable Wireless Rate Limiting.

(2) Set the uplink and downlink rate limit modes to **Rate Limit Per User**, configure the rate limit values, and click **OK**.

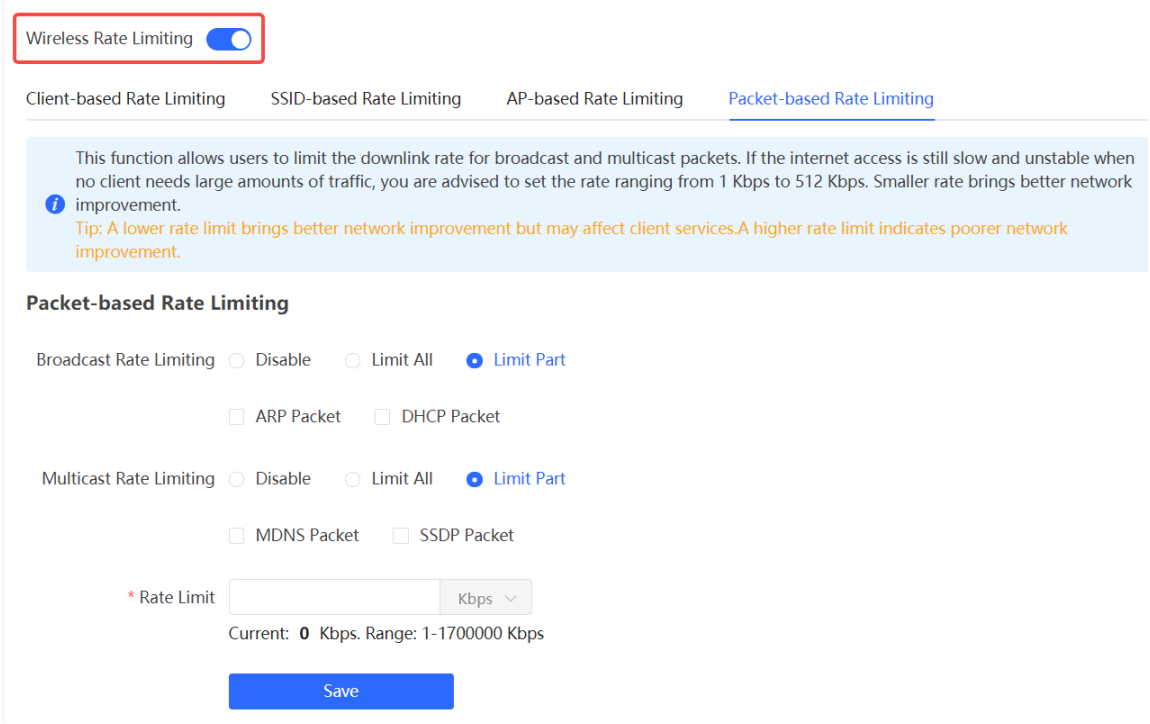


4. Configuring Packet-based Rate Limiting

Choose **Network-Wide** > **Workspace** > **Wireless** > **Rate Limiting** > **Packet-based Rate Limiting**.

(1) Enable Wireless Rate Limiting.

(2) Select the specific type of packets for rate limiting, configure the rate limit value, and click **Save**.



5.8 Wireless Network Optimization

5.8.1 One-Click Wireless Optimization

Select the optimization mode, the system automatically optimize the wireless network.

Caution

- WIO is supported only in the self-organizing network mode.
- The client may be offline during the optimization process. The configuration cannot be rolled back once optimization starts. Therefore, exercise caution when performing this operation.

Choose **Network-Wide** > **Workspace** > **WLAN Optimization** > **Network Optimization**.

(1) Select the optimization mode. Then, click **OK** to optimize the wireless network.

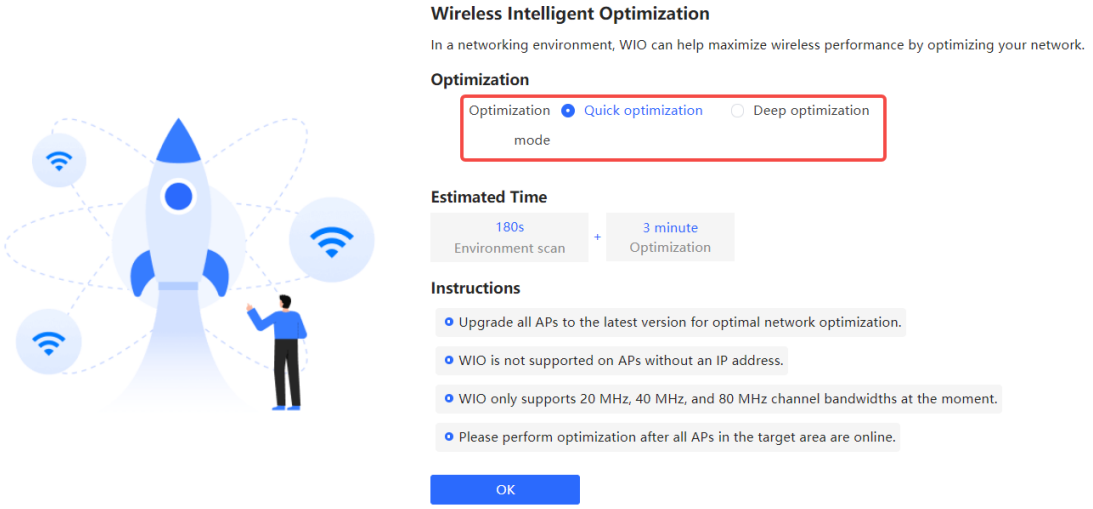
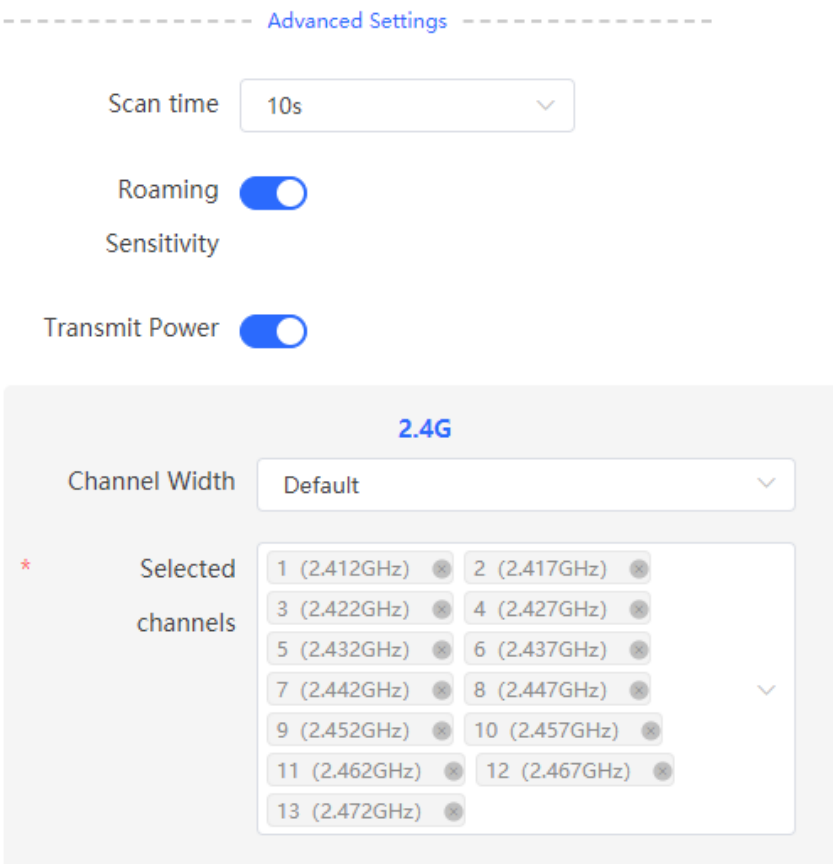


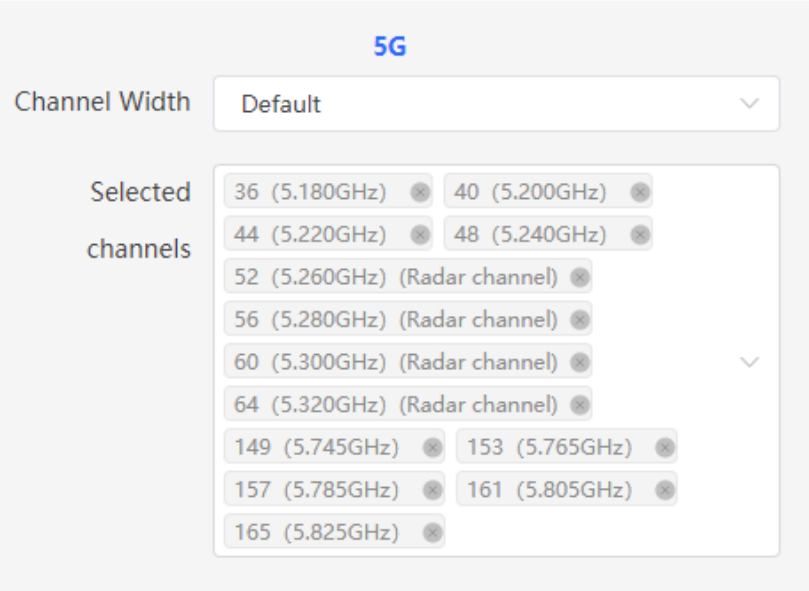
Table 5-5 Description of Tuning Mode

Parameter	Description
Quick tuning	In this mode, external interference and bandwidth are not considered. A quick optimization is performed to optimize channel, power, and management frame power.

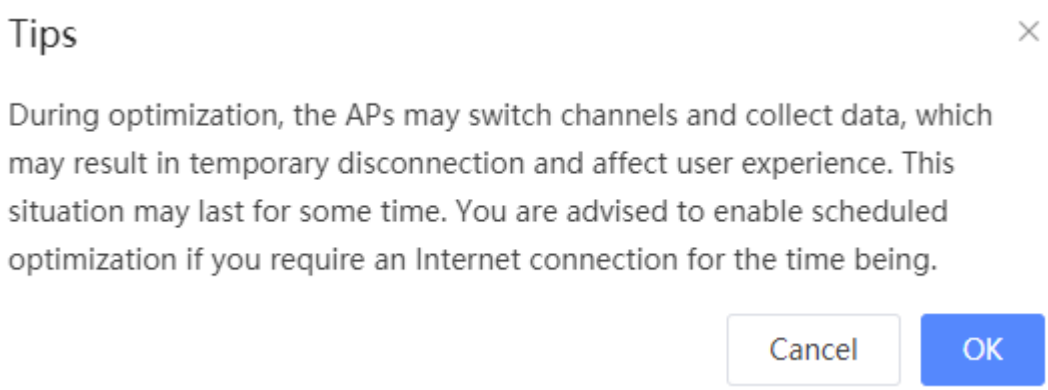
Parameter	Description
Deep tuning	In this mode, external interference and bandwidth are considered. A deep optimization is performed to optimize channel, power, and management frame power. Click to expand **Advanced Settings** to configure the **Scan Time**, **Roaming Sensitivity**, **Transmit Power**, **Channel Width** and **channels**. ● Scan Time: Indicates the time for scanning channels during the optimization. ● Roaming Sensitivity: You can adjust the roaming sensitivity to balance the roaming performance and connection stability of the device during roaming. ● Transmit Power: You can adjust the transmit power of wireless devices to optimize the performance and coverage of the Wi-Fi network. ● 2.4G ○ Channel Width: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. ○ Selected channels: Indicates the channels to be optimized. ● 5G ○ Channel Width: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. ○ Selected channels: Indicates the channels to be optimized.

(2) (Optional) When the **Optimization Mode** is configured as **Deep optimization**, expand the **Advanced Settings** to set the scan time, roaming sensitivity, transmit power, channel width and channels.



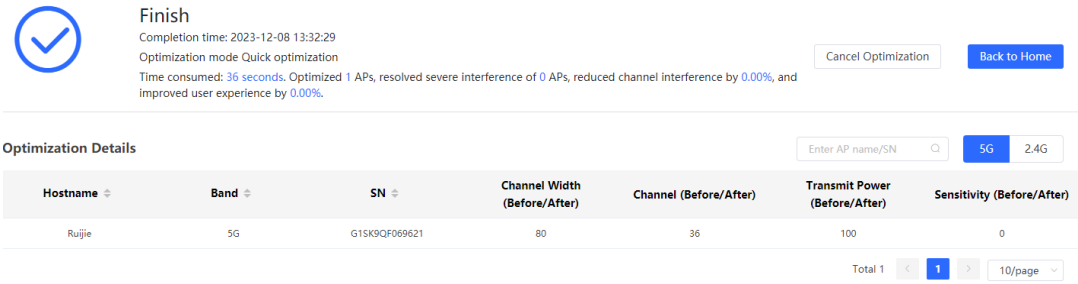


(3) Confirm the tips, and Click **OK**.



(4) After optimization starts, please wait patiently until optimization is complete. After optimization is complete, you can click **Cancel Optimization** to restore the radio parameters to the default values.

The **Channel Width**, **Channel**, and **Transmit Power** columns in the **Optmization Details** section show the changes in the bandwidth, channel, and transmit power of the AP before and after optimization.



(5) Click **Optimization Record** Tab to view details of the latest optimization.

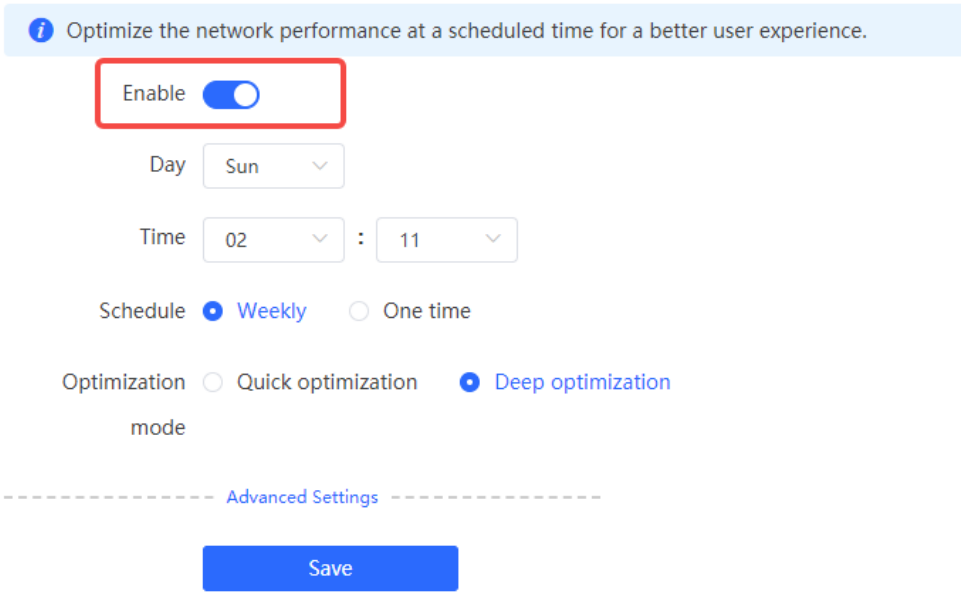
5.8.2 Scheduled Wireless Optimization

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.

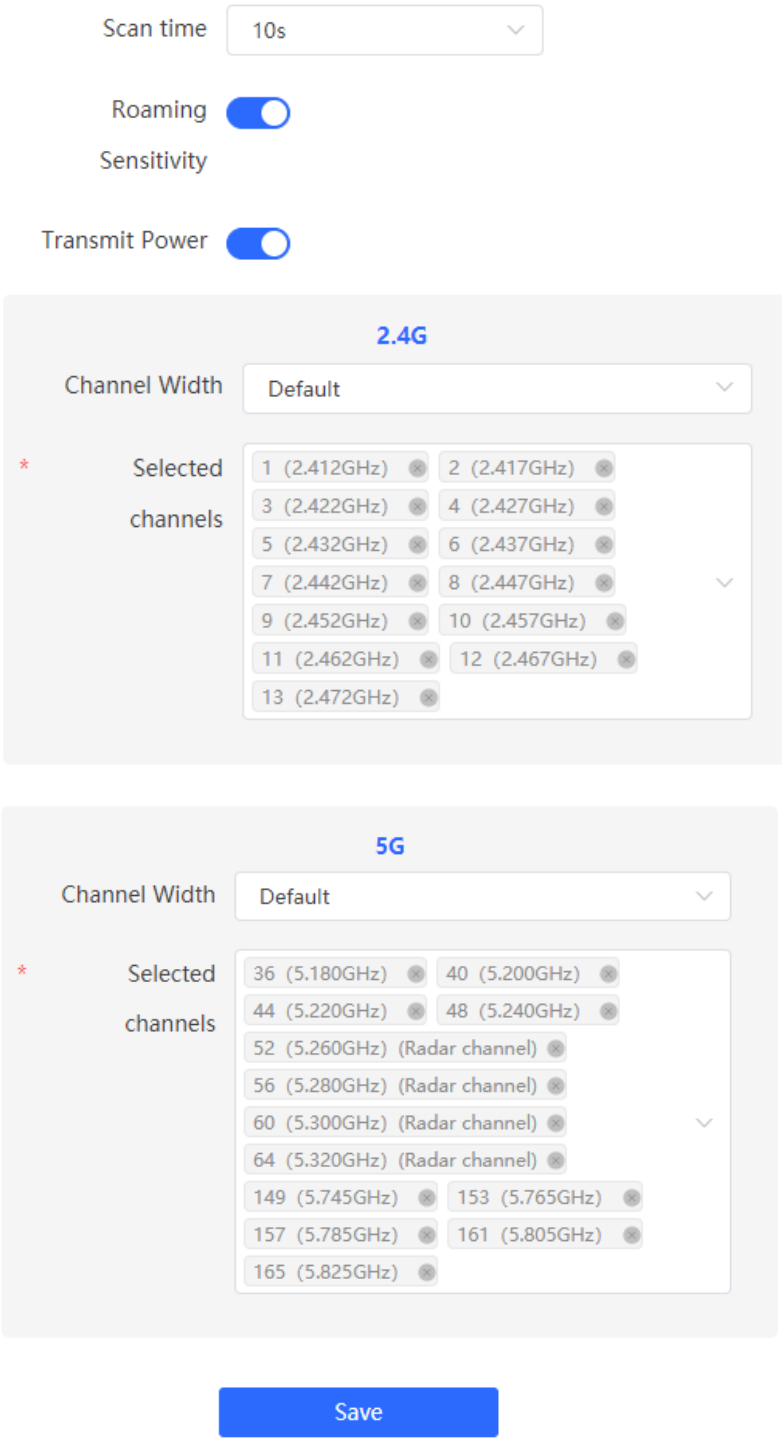
Choose **Network-Wide** > **Workspace** > **WLAN Optimization** > **Scheduled Optimization**.



(1) Configure the scheduled time.

(2) Select the Optimization mode.

(3) (Optional) When the **Optimization Mode** is configured as **Deep optimization**, expand the **Advanced Settings** to set the scan time, roaming sensitivity, transmit power, channel bandwidth and selected channels.



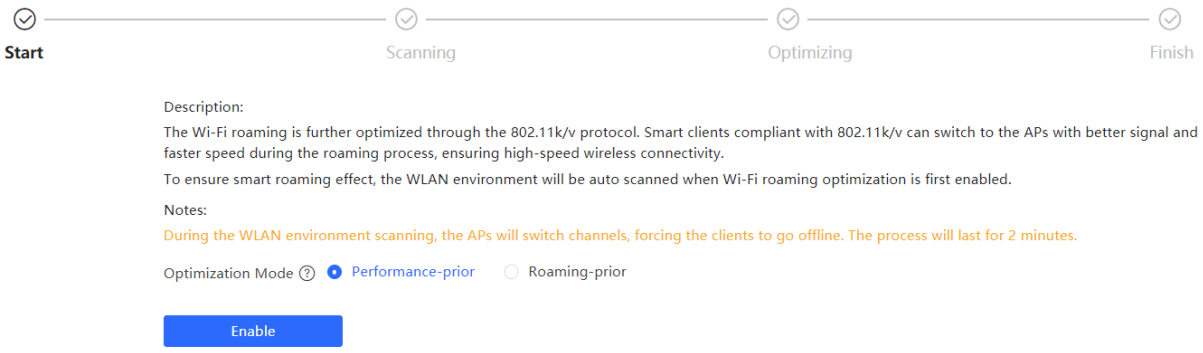
(4) Click **Save**.

5.8.3 Wi-Fi Roaming Optimization (802.11k/v)

Wi-Fi roaming is further optimized through the 802.11k/802.11v protocol. Smart endpoints compliant with IEEE 802.11k/v can switch association to the access points with better signal and faster speed, thereby ensuring high-speed wireless connectivity.

To ensure high quality of smart roaming service, the WLAN environment will be automatically scanned when Wi-Fi roaming optimization is first enabled.

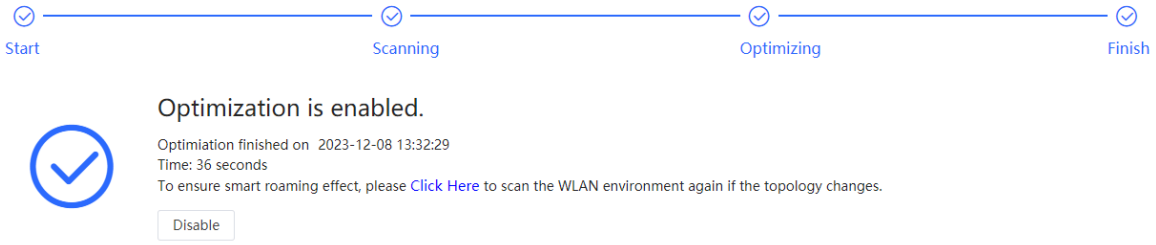
Choose **Network-Wide** > **Workspace** > **WLAN Optimization** > **802.11k/v Roaming Optimization**.



Caution

During the optimization, the clients may be forced offline. Please proceed with caution.

Select **Optimization Mode** and click **Enable**, then the optimization starts.



5.9 Wi-Fi Authentication

5.9.1 Overview

With the popularity of wireless networks, Wi-Fi has become one of the marketing means for merchants. Customers can connect to the Wi-Fi provided by the merchants to surf the Internet after watching advertisements. In addition, to defend against security vulnerabilities, the wireless office network usually allows only employees to associate with Wi-Fi, so the identity of the clients needs to be verified.

The Wi-Fi authentication function of the device uses the Portal authentication technology to implement information display and user management. After users connect to Wi-Fi, the traffic will not be directly routed to the Internet. Wi-Fi users must pass authentication on the Portal authentication website, and only authenticated users are allowed to use network resources. Merchants or enterprises can customize Portal pages for identity authentication and advertisement display.

5.9.2 Getting Started

(1) Before you enable Wi-Fi authentication, ensure that the wireless signal is stable and users can connect to Wi-Fi and surf the Internet normally. The wireless SSID used for authentication in the network should be set to the open state.

(2) If the IP address of an AP in the network is within the authentication scope, add the AP as the authentication-free user. For details, see Section 5.9.8 Authentication-Free.

- In a Layer 2 network, add the MAC address of the AP to the authentication-free MAC address allowlist.
- In a Layer 3 network, add the IP address of the AP to the authentication-free IP address Allowlist.

5.9.3 WiFiDog Authentication

1. Overview

The EG device is connected to the MACC authentication server on the cloud. After Wi-Fi users connect to Wi-Fi, a Portal page pops up. The users need to enter the account and password to pass authentication before they can access the Internet. According to the authentication configuration on the MACC authentication server, you can set the authentication mode to SMS authentication, fixed account authentication, or account-free one-click login.

2. Getting Started

(1) WiFiDog is a Layer 2 protocol. Ensure that the authentication device can obtain the MAC addresses of the wireless users.

- The gateway address of the wireless users to be authenticated is deployed on the authentication device.
- If the gateway address is not deployed on the authentication device, the device functions as a DHCP server to allocate IP addresses to the wireless users and obtain MAC addresses of the wireless users. In this scenario, you need to set Network Type to Layer-3 Network.

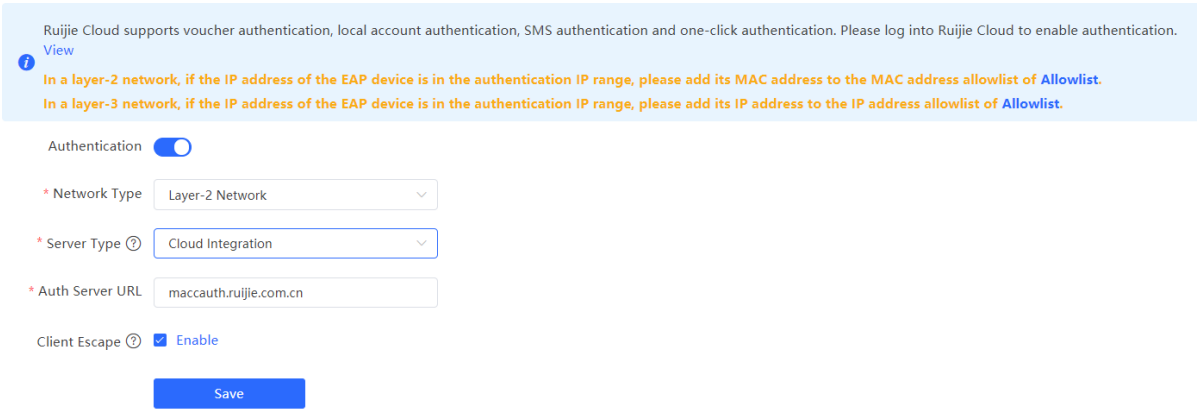
(2) Complete the corresponding configuration on the Ruijie Cloud platform before you enable the authentication function on the device. If SMS authentication is used, you also need to configure the SMS gateway.

3. Configuration Steps

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Authentication** > **Cloud Auth**.

(1) Turn on **Authentication**.

(2) Set **Server Type** to **Cloud Integration**, configure **Network Type**, **Auth Server URL**, and **Client Escape**, and click **Save**.



(3) In the **Net List** area, click **Add**. In the displayed dialog box, enter the **VLAN** name and the **Auth IP / IP Range** to be authenticated and click **OK**.

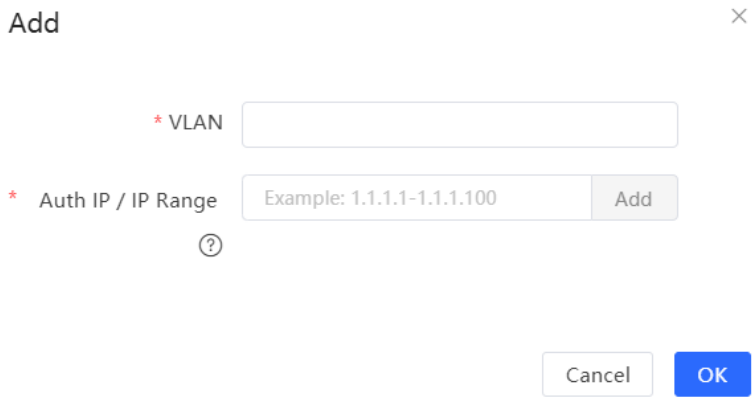


Table 5-6 Description of WiFiDog Authentication Configuration

Parameter	Description
Network Type	The default value is **Layer-2 Network**. Set the parameter based on the actual network environment.
Server Type	Select **Cloud Integration** from the drop-down list.
Auth Server URL	After completing the configuration at the server end, the Ruijie Cloud authentication server returns a URL. The device sends authentication requests to the URL during authentication.
Client Escape	After the client escape function is enabled, if an exception occurs on the authentication server, the device disables authentication to allow all clients to directly access the Internet. After the server recovers, the device automatically enables authentication.
VLAN	Specify the name of a Wi-Fi network, to which clients connect. A maximum of eight VLAN names can be configured.
Auth IP / IP Range	Specify the IP address range to be authenticated. You can enter a single IP address (such as 192.168.112.2) or an IP address range (such as 192.168.112.2–192.168.112.254). A maximum of five IP address ranges can be configured.

4. Verifying Configuration

After a mobile phone connects to a specific Wi-Fi, the Portal authentication page pops up automatically.

If the authentication mode configured on the Ruijie Cloud authentication server is SMS authentication, the user needs to enter the mobile number to obtain an Internet access password and enter the password to complete authentication.

If the authentication mode configured on the Ruijie Cloud authentication server is account-free one-click authentication, the user can directly access the Internet after clicking the corresponding button on the page.

If the authentication mode configured on the Ruijie Cloud authentication server is fixed account login, the user can access the Internet after entering the account and password configured on the cloud.

After successful connection, you can choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Authentication** > **Online Clients** to view information about this authenticated user. For details, see Section 5.9.9 Online Authenticated User Management.

5.9.4 Configuring Third-Party Authentication

Note

This feature is supported on RG-EG105G-V3, RG-EG105G-P-V3, RG-EG209GS, RG-EG210G-P-V3, RG-EG310GH-E, RG-EG305GH-P-E, RG-EG310GH-P-E and RG-EG1510XS running ReyeeOS 2.237 or later.

1. Overview

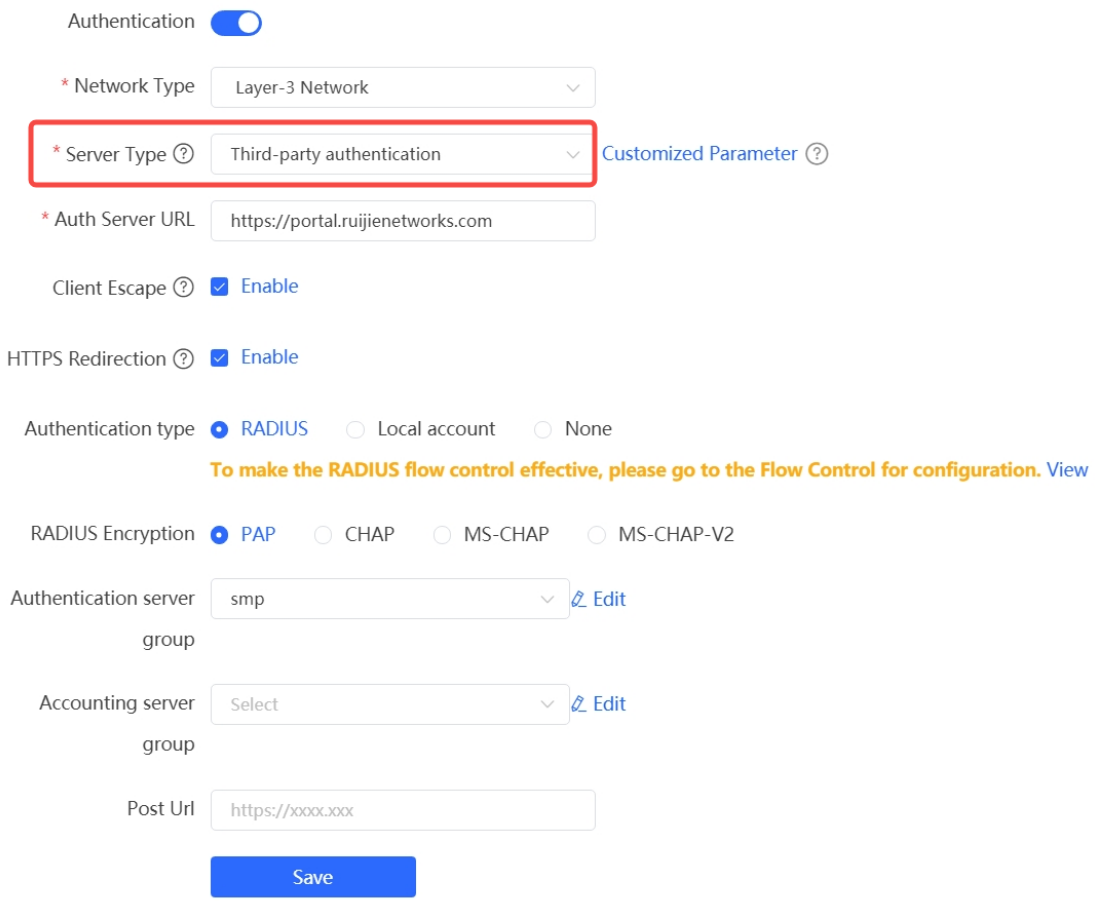
Reyee EG series gateway devices can interwork with WISPr-compliant external authentication servers. After a wireless client is connected to the Wi-Fi network, a Portal page pops up. The wireless client needs to be authenticated before it can access the Internet. Based on the services provided by different authentication servers, you can choose RADIUS authentication, local account authentication, or no authentication for third-party authentication.

2. Getting Started

- Ensure that the authentication server can obtain the MAC address of the wireless client:
  - The gateway address of the wireless client to be authenticated is deployed on the authentication server.
  - If the gateway address of the wireless client to be authenticated is not deployed on the authentication server, then the device must act as a DHCP server to assign an IP address to the wireless client in order to obtain its MAC address. In this scenario, the **Network Type** must be set to **Layer 3 Network**.
- Complete relevant configurations on the third-party authentication platform, and then enable the Wi-Fi authentication feature on the device. For specific configurations, see the configuration manual of relevant third-party authentication platforms.

3. Configuration Steps

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Authentication** > **Cloud Auth**.

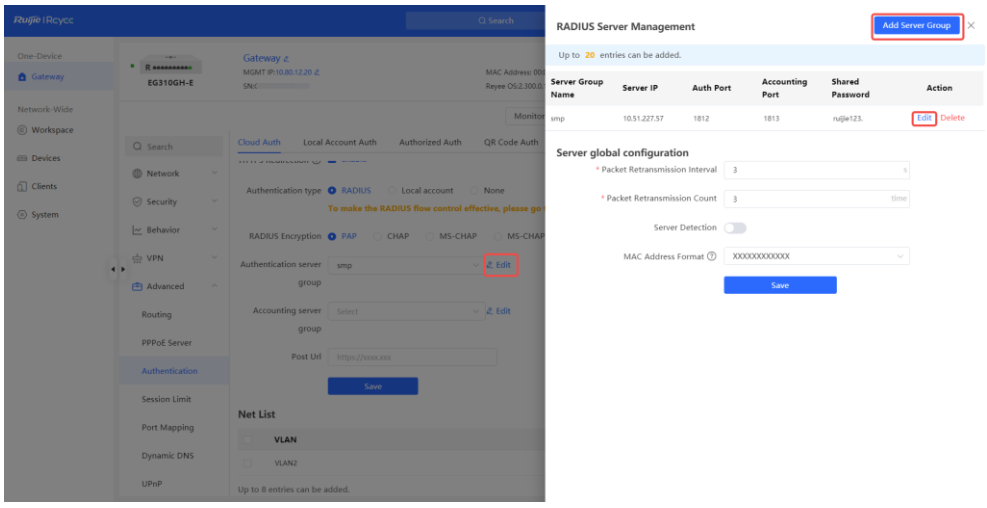


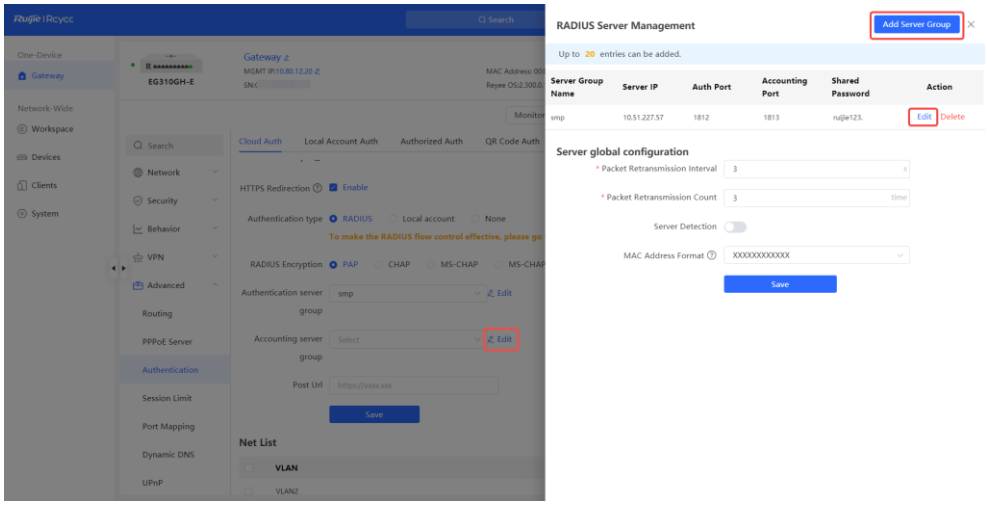
(1) Toggle on **Authentication**.

(2) Set **Server Type** to **Third-party Authentication**, configure third-party authentication parameters, and click **Save**.

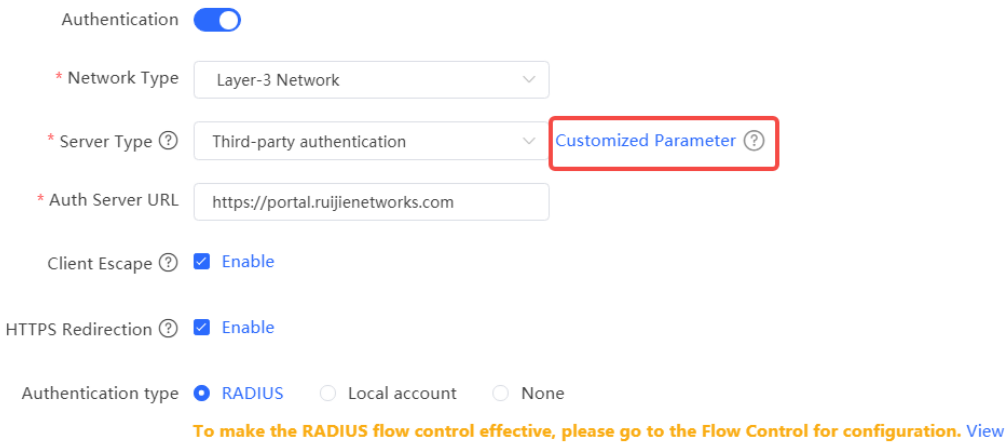
Table 5-7 Description of Third-Party Authentication Configuration Parameters

Parameter	Description
Network Type	The default value is **Layer-2 Network**. Set the parameter based on the actual network environment.
Server Type	Select **Third-party authentication** from the drop-down list.
Auth Server URL	After completing the configuration on the third-party authentication server, the third-party authentication server returns a URL. The device sends authentication requests to the URL during authentication.
Client Escape	After the client escape function is enabled, if an exception occurs on the authentication server or the RADIUS server, the device disables authentication to allow all clients to directly access the Internet. After the server recovers, the device automatically enables authentication.

Parameter	Description
HTTPS Redirection	Enabling **HTTPS Redirection** ensures that data is encrypted during user authentication, thus improving the security of the authentication process. When **HTTPS Redirection** is disabled, you will be redirected to HTTP pages only.
Authentication type	Types of third-party authentication, which include: ● **RADIUS**: The wireless client is authenticated by the RADIUS server. ● **Local account**: The wireless client is authenticated based on local username and password. ● **None**: No authentication is required for the wireless client.
RADIUS Encryption	When **Authentication Type** is set to **RADIUS**, you need to configure the encryption mode for RADIUS authentication: ● **RAP**: This mode has low security. Passwords are transmitted in plain text, posing a risk of interception. ● **CHAP**: The server sends a random CHAP challenge to the client, and the client uses the password to calculate and returns a response. ● **MS-CHAP**: Functions such as password change and failed attempt count are supported. This mode is more secure and flexible than CHAP. ● **MS-CHAPv2**: As an improved version of MS-CHAP, this mode provides higher security and better encryption.
Authentication server group	Select a RADIUS authentication server group from the drop-down list box. This parameter is mandatory when the **Authentication Type** is set to **RADIUS**. You can click **Edit** next to the input box to create or modify a RADIUS authentication server group in the pop-up box. For details, see12.5.3 Configuring the RADIUS Server. 

Parameter	Description
Accounting server group	Select a RADIUS accounting server group from the drop-down list box. This parameter is mandatory when the **Authentication Type** is set to **RADIUS**. You can click **Edit** next to the input box to create or modify a RADIUS accounting server group in the pop-up box. For details, see12.5.3 Configuring the RADIUS Server 
Post URL	The URL to which the user will be redirected after authentication.

(3) (Optional) Considering the different HTTP parameters and request methods required by different third-party authentication platforms. To configure custom third-party authentication parameters, you can click **Customized Parameter** next to **Server Type** and set **Parameter template** to **Custom**.



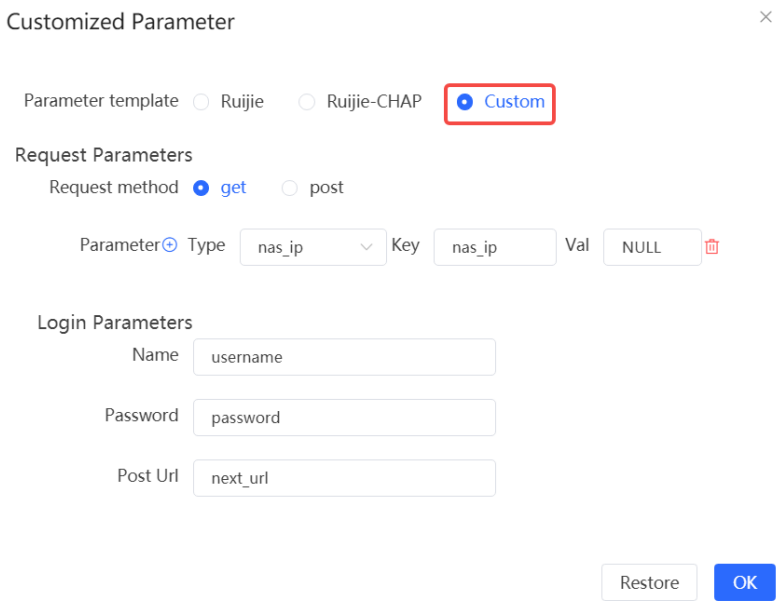


Table 5-8 Description of Custom Third-Party Authentication Parameters

Parameter	Description
Parameter template	The built-in parameter template. Default parameters are used when the **Parameter Template** is set to **Ruijie** or **Ruijie-CHAP**. When the **Parameter Template** is set to **Custom**, the parameters can be customized.
Request method	The HTTP request methods used for requesting the portal page.

Parameter	Description
Parameter	Parameters in the parameter template for requesting the portal page: ● When the parameter type is not **other**, the **Val** field is invalid, and the default value **NULL** can be used. The Reyee EG gateway device will automatically populate the value of this parameter. ● When the parameter type is **other**, you need to enter a value in the **Val** field. Parameters include: ● nas_ip: IP address of the Reyee EG series gateway device. Example: 10.52.48.7. ● nas_mac: MAC address of the Reyee EG series gateway device. Example: 11:22:33:44:55:66. ● client_ip: IP address of the wireless client to be authenticated. Example: 192.168.110.5. ● client_mac: MAC address of the wireless client to be authenticated. Example: 11:22:33:44:55:66. ● orig_url: Original URL accessed by the wireless client to be authenticated. Example: https://www.baidu.com. ● login_url: Login interface received by the Reyee EG series gateway device from the third-party authentication platform. Example: http://192.168.110.1:2060/ext_login. ● logout_url: Logout interface received by the Reyee EG series gateway device from the third-party authentication platform. Example: http://192.168.110.1:2060/ext_logout. ● ssid: SSID or VLAN name associated with the wireless client to be authenticated. Example: VLAN233. ● sn: SN of the gateway. ● identity: ID of the gateway. ● chap_id: Identifier or session ID stored during CHAP authentication. ● chap_challenge: The challenge string used in the CHAP authentication process. ● interface_name: Name of the interface through which the wireless client accesses the network. ● login_host: IP address of the login interface on the Reyee EG series gateway device. Example: 192.168.110.1:2060. ● other: other custom field. Multiple custom fields are supported.
Login Parameters	Custom fields of the login interface received by the Reyee EG series gateway devices from the third-party authentication platform, including: ● **Name**: username. ● **Password**: password. ● **Post Url**: URL to which the wireless client is redirected after successful authentication.

4. Verifying Configuration

Connect your smartphone to the specific Wi-Fi network to verify that the portal page pops up automatically.

Connect to different authentication platforms to view services provided by these authentication platforms.

After the connection is successful, view the details of the wireless client by going to **Advanced** > **Authentication** > **Online Clients**. For details, see 5.9.9 Online Authenticated User Management.

5.9.5 Local Account Authentication

1. Overview

The device is connected to the local authentication server, and user identity is verified based on the account and password. Local account authentication is applicable to the wireless office network environment.

2. Getting Started

Ensure that the device with the authentication function enabled has been connected to the Internet. Otherwise, the authentication page does not pop up when a client associates with Wi-Fi.

3. Configuration Steps

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Authentication** > **Local Account Auth**.

(1) Enable account authentication.

Turn on **Local Account Auth**, enter the IP address range of clients to be authenticated, and click **Save**. After account authentication is enabled, clients in the specified IP address range can access the Internet only after passing authentication.

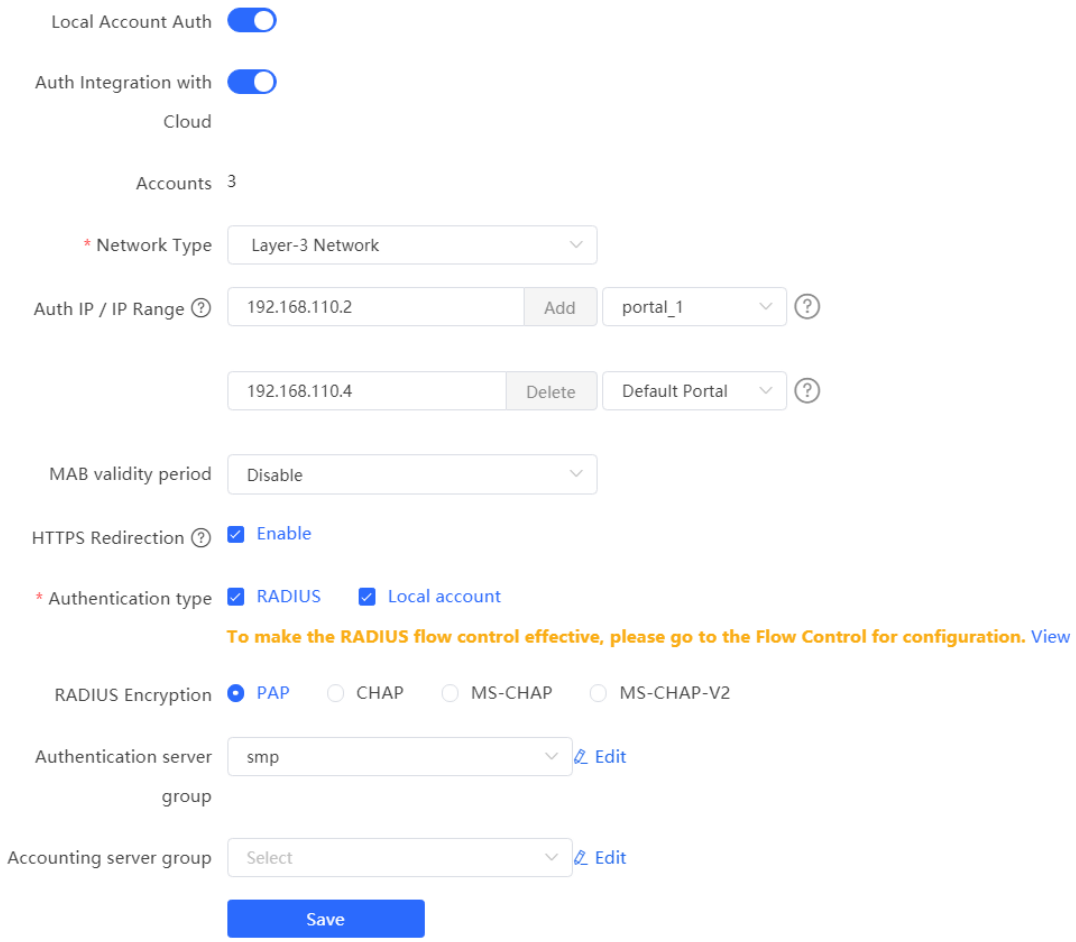
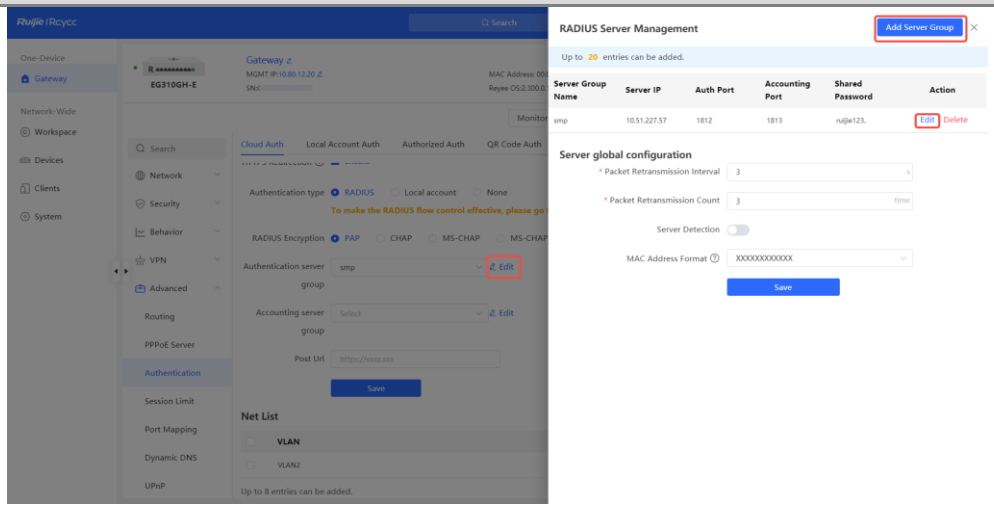
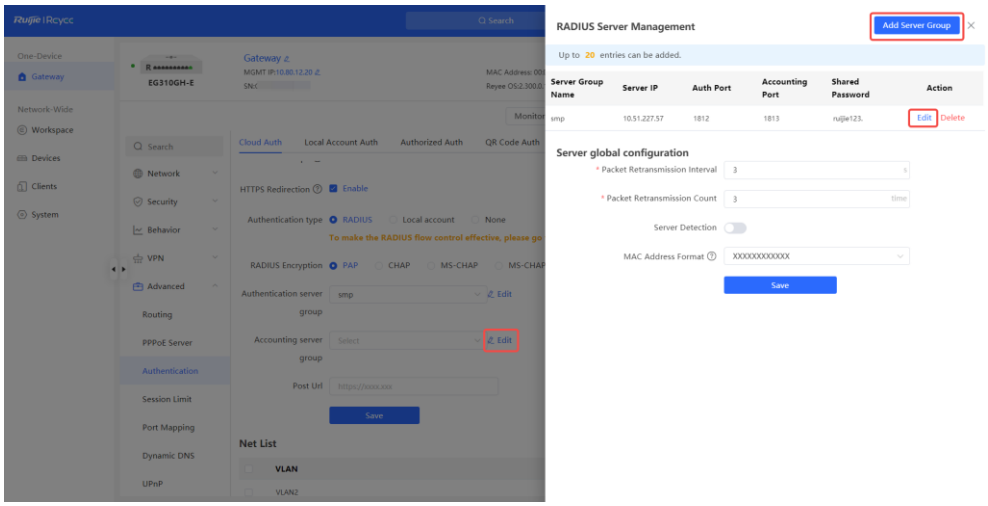


Table 5-9 Description of Local Account Authentication Configuration Parameters

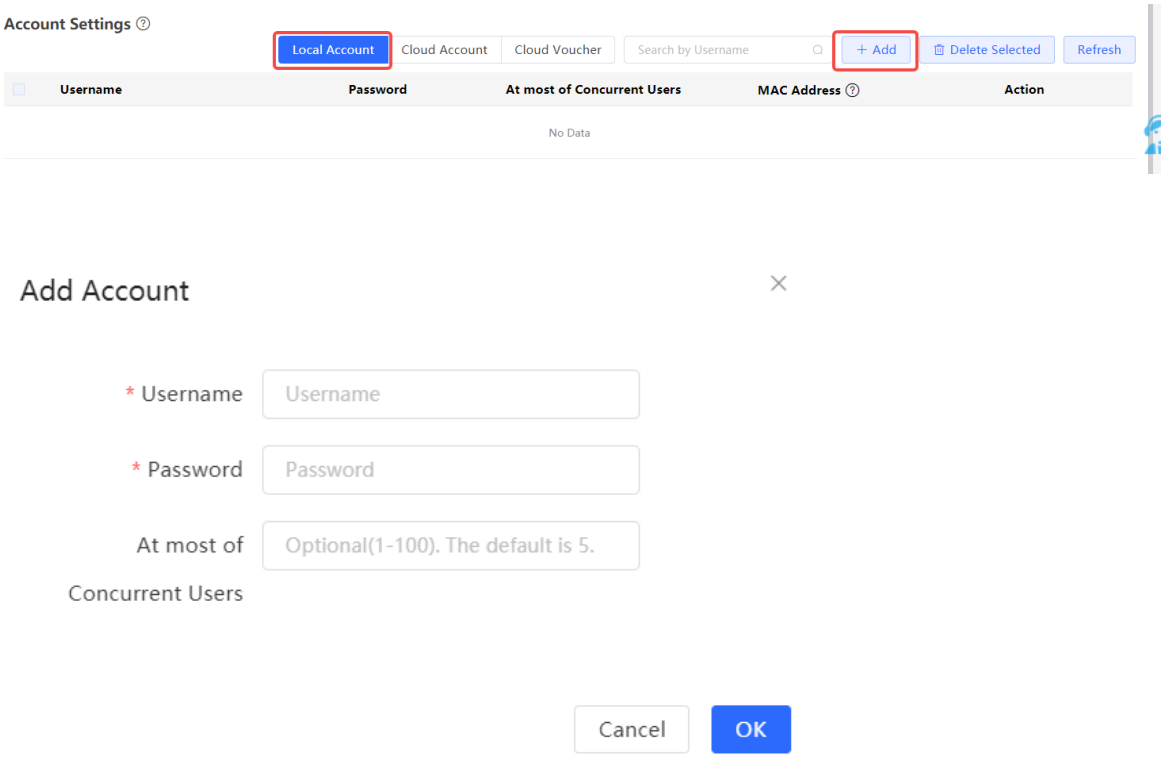
Parameter	Description
Auth Integration with Cloud	Use the authentication service integrated in Ruijie Cloud.
Accounts	The number of created authentication accounts.
Network Type	The default value is **Layer-2 Network**. Set the parameter based on the actual network environment.
Auth IP / IP Range	Specify the IP address range to be authenticated. You can enter a single IP address (such as 192.168.112.2) or an IP address range (such as 192.168.112.2–192.168.112.254). A maximum of five IP address ranges can be configured. After setting the IP address or IP address range, select the portal page for this IP address or IP address range from the drop-down list box on the right. For details about the configuration of the portal page, see 5.9.10 Custom Portal Page.
MAB validity period	Set the validity period of MAB authentication. After a user is authenticated successfully for the first time, the user will be automatically authenticated when connecting to the Wi-Fi network within the validity period.
HTTPS Redirection	Enabling **HTTPS Redirection** ensures that data is encrypted during user authentication, thus improving the security of the authentication process. When **HTTPS Redirection** is disabled, you will be redirected to HTTP pages only.
Authentication type	Types of local account authentication, which include: ● RADIUS: The wireless client is authenticated by the RADIUS server. ● Local account: The wireless client is authenticated based on local username and password.
RADIUS Encryption	When **Authentication Type** is set to **RADIUS**, you need to configure the encryption mode for RADIUS authentication: ● **RAP**: This mode has low security. Passwords are transmitted in plain text, posing a risk of interception. ● **CHAP**: The server sends a random CHAP challenge to the client, and the client uses the password to calculate and returns a response. ● **MS-CHAP**: Functions such as password change and failed attempt count are supported. This mode is more secure and flexible than CHAP. ● **MS-CHAP-V2**: As an improved version of MS-CHAP, this mode provides higher security and better encryption.
Authentication server group	Select a RADIUS authentication server group from the drop-down list box. This parameter is mandatory when the **Authentication Type** is set to **RADIUS**. You can click **Edit** next to the input box to create or modify a RADIUS authentication server group in the pop-up box. For details, see12.5.3 Configuring the RADIUS Server

Parameter	Description
	
Authentication server group	Select a RADIUS accounting server group from the drop-down list box. This parameter is mandatory when the **Authentication Type** is set to **RADIUS**. You can click **Edit** next to the input box to create or modify a RADIUS accounting server group in the pop-up box. For details, see12.5.3 Configuring the RADIUS Server 

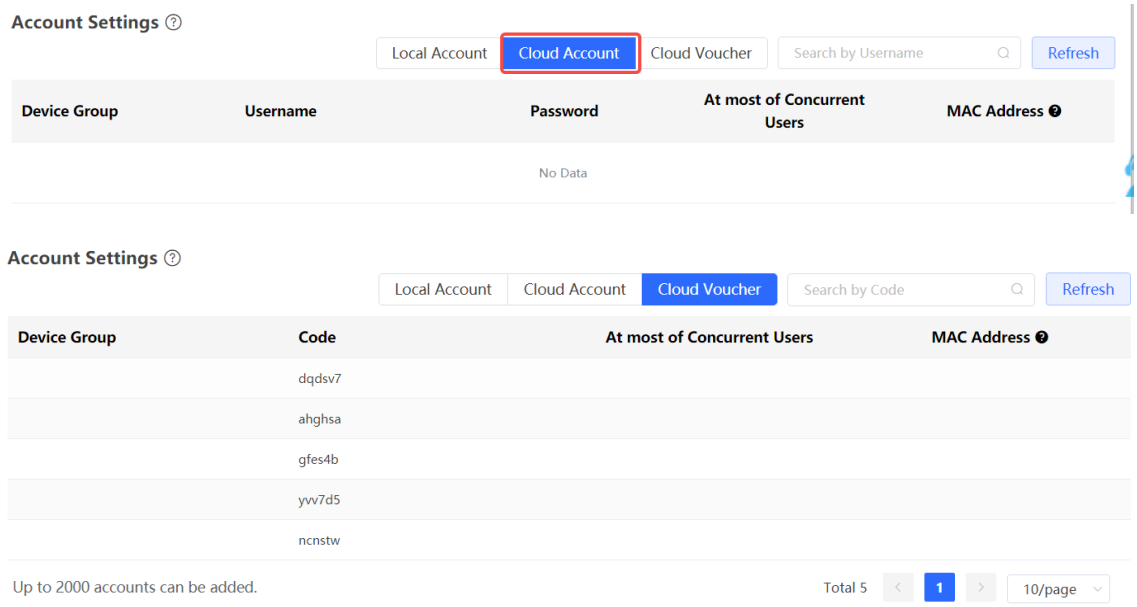
(2) Configure an authentication account.

Choose the **Local Account** tab, and click **Add** to configure an authentication account for Internet access. Multiple clients can access the Internet using the same account and password. The **At most of Concurrent Users** parameter specifies the maximum number of users allowed to access the Internet using the same account.

After a **Wi-Fi user** passes authentication using an account, the IP address of the authenticated user is displayed in the **MAC Address** column next to the account. The account list records a maximum of five latest device IP addresses using the same account.

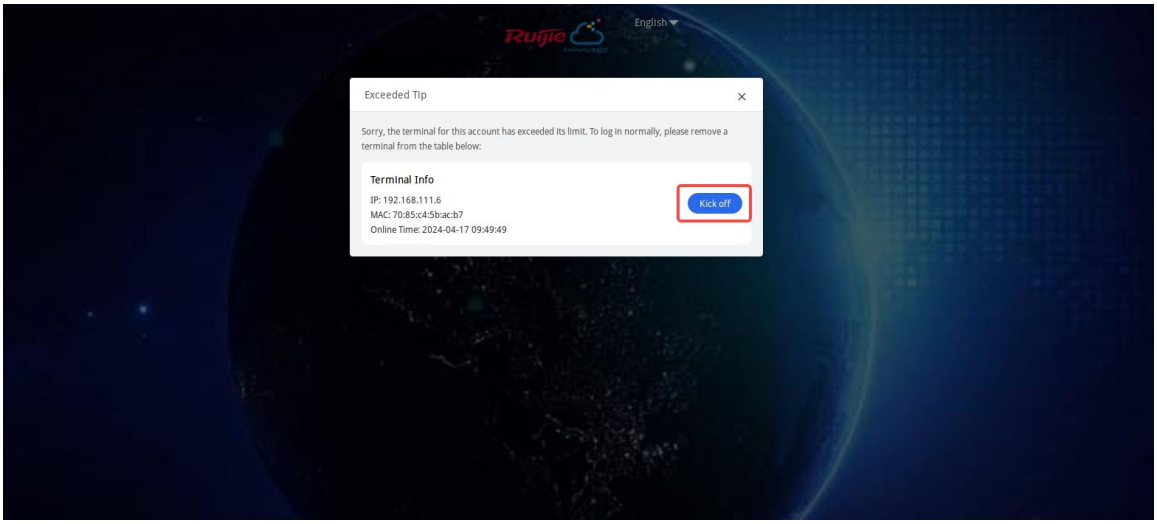


Click **Cloud Account** or **Cloud Voucher** to view the account and voucher information synchronized from Ruijie Cloud.



(3) Disconnect an online user.

When the number of concurrent users in a single account exceeds the limit, a prompt will appear when a new user attempts to connect. You can then choose to disconnect a specific user by clicking the Kick off button. After re-logging in, the user can access the network.



4. Verifying Configuration

After a client connects to the specific Wi-Fi, the authentication page pops up automatically. The user can normally access the Internet only after entering the account and password configured on the local server on the authentication page. You can choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Authentication** > **Online Clients** to view information about the successfully connected user. For details, see Section 5.9.9 Online Authenticated User Management.

5.9.6 Authorized Guest Authentication

1. Overview

The device is connected to the local authentication server. After a guest connects to Wi-Fi, the guest can access the Internet after the specified authorization IP user or account and password authentication user scans the QR code that pops up for guest authentication. For example, in the wireless office network, users in the employee network segment are authorized to scan the guest authentication QR code for users in the guest network segment.

2. Getting Started

Ensure that the device with the authentication function enabled has been connected to the Internet. Otherwise, the authentication page does not pop up when a client associates with Wi-Fi.

3. Configuration Steps

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Authentication** > **Authorized Auth**.

Turn on **Authorized Auth**, configure **Popup Message**, **Auth IP / IP Range**, **Authorization IP/IP Range**, and **Limit Online Duration**, and click **Save**.

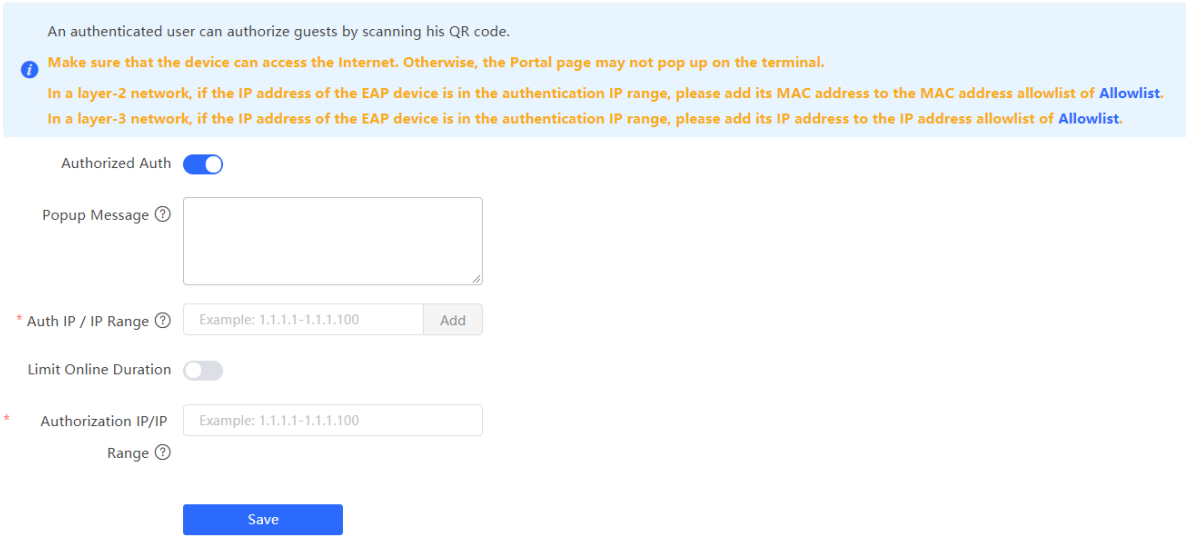


Table 5-10 Authorized guest authentication configuration

Parameter	Description
Popup Message	Specify the text to be displayed on the pop-up QR code page.
Auth IP / IP Range	Specify the IP address range for users to be authenticated. The value can be a single IP address (such as 192.168.110.2) or an IP address range (such as 192.168.110.2-192.168.110.254). Users in the specified IP address range can access the Internet only after passing authentication.
Limit Online Duration	Specify whether to limit the online duration of guests. After you enable this function, you need to configure **Duration Limit**. If the online duration of a guest exceeds the specified value, the guest can continue Internet access only after re-authorization. By default, this function is disabled, indicating that guests can use Wi-Fi without limit on the online duration.
Duration Limit	Specify the maximum online duration of authorized guests. If the online duration of an authorized guest exceeds the specified value, the guest goes offline automatically and needs to be re-authorized for login again.
Authorization IP/IP Range	Specify the IP address range of authorization users. Users in this range can scan the QR code to authorize guests.

4. Verifying Configuration

After a guest connects to Wi-Fi, the QR code authentication page pops up. The guest can access the Internet after the specified authorization user scans this QR code. You can choose **One-Device** > **Gateway** > **Config** >

Advanced > **Authentication** > **Online Clients** to view information about the successfully connected user. For details, see Section 5.9.9 Online Authenticated User Management.

5.9.7 Guest Authentication through QR Code Scanning

1. Overview

Guests scan the specified QR code to access the Internet. For example, in the wireless office network, guests scan the pasted QR code to access the Internet after they connect to Wi-Fi.

2. Getting Started

Ensure that the device with the authentication function enabled has been connected to the Internet. Otherwise, the authentication page does not pop up when a client associates with Wi-Fi.

3. Configuration Steps

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Authentication** > **QR Code Auth**.

Turn on **QR Code Auth**, configure **Auth IP / IP Range**, **Limit Online Duration**, and **QR Code Generator**, and click **Save**.

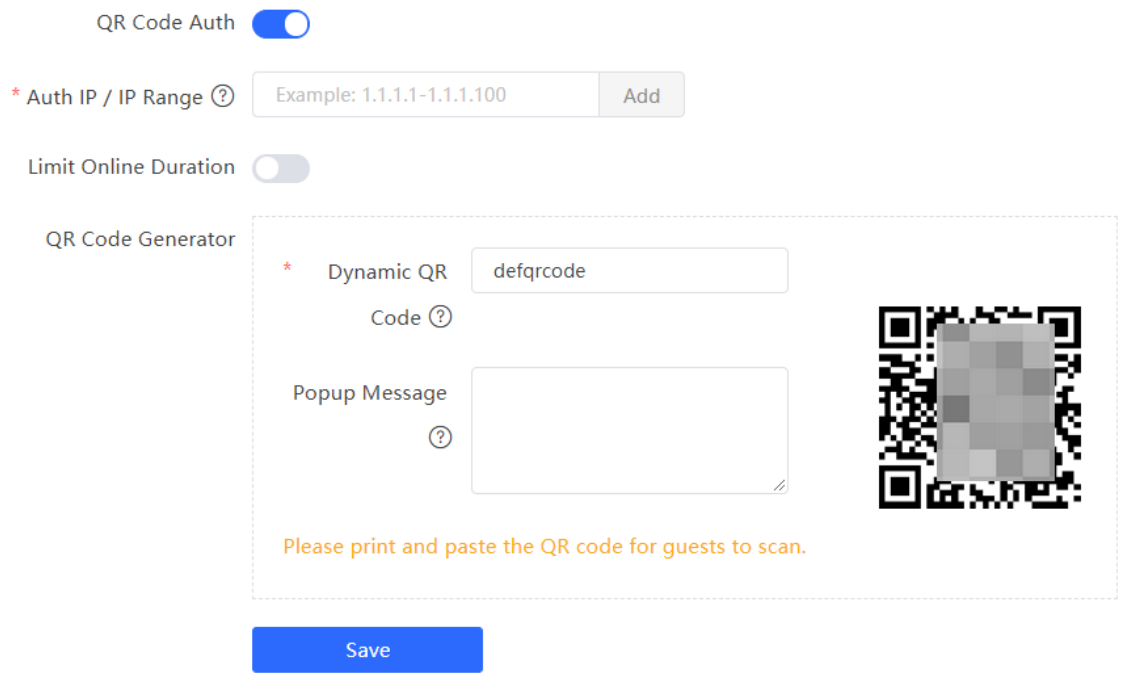


Table 5-11 Guest authentication through QR code scanning configuration

Parameter	Description
Auth IP / IP Range	Specify the IP address range for users to be authenticated. The value can be a single IP address (such as 192.168.110.2) or an IP address range (such as 192.168.110.2-192.168.110.254). Users in the specified IP address range can access the Internet only after passing authentication.

Parameter	Description
Limit Online Duration	Specify whether to limit the online duration of guests. After you enable this function, you need to configure **Duration Limit**. If the online duration of a guest exceeds the specified value, the guest needs to scan the QR code again before continuing Internet access. By default, this function is disabled, indicating that guests can use Wi-Fi without limit on the online duration.
Duration Limit	Specify the maximum online duration of authorized guests. If the online duration of an authorized guest exceeds the specified value, the guest goes offline automatically and needs to be re-authenticated.
Dynamic QR Code	The dynamic QR code is used to generate a QR code image. After the dynamic QR code is updated, the QR code image changes and the previous image becomes invalid. You can print and paste the generated QR code image, which can be scanned by guests to access the Internet.
Popup Message	Specify the QR code prompt message displayed on the page after a guest scans the QR code.

4. Verifying Configuration

After a client connects to Wi-Fi, the guest can scan the QR code to pass authentication and access the Internet. You can choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Authentication** > **Online Clients** to view information about the successfully connected user. For details, see Section 5.9.9 Online Authenticated User Management.

5.9.8 Authentication-Free

1. Overview

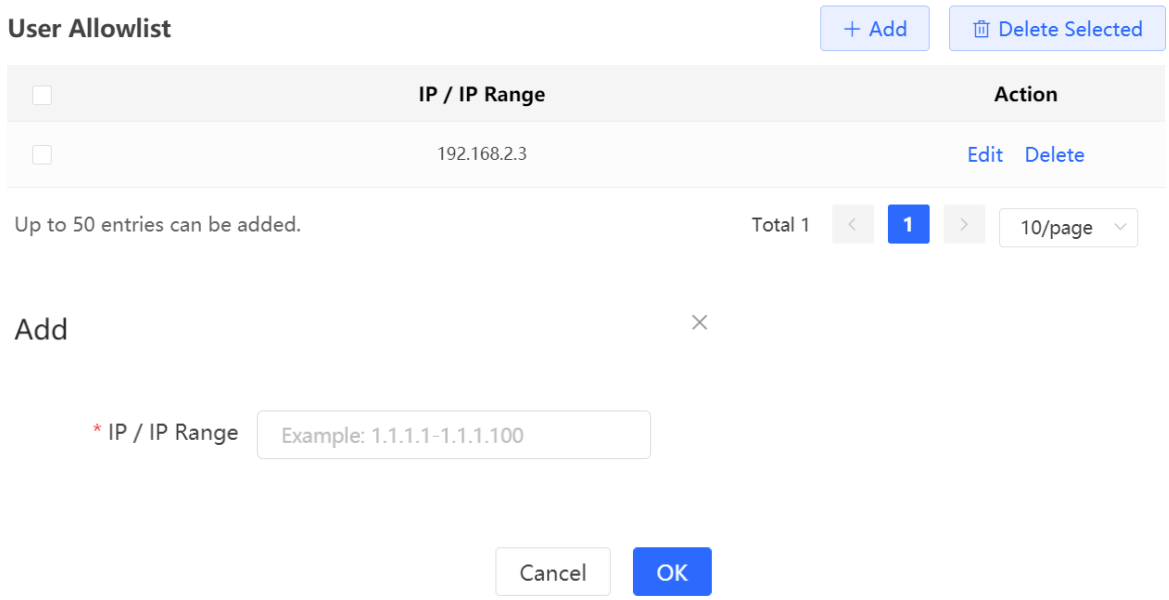
After IP addresses or MAC addresses are configured for authentication-free users, they can directly access the Internet without passing authentication. Traffic from all the users in the blocklist is blocked.

2. Configuring an Authentication-Free User

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Authentication** > **Allowlist** > **User Allowlist**.

Authentication-free user: Users in the specified IP address range can directly access the Internet without passing authentication.

Click **Add** to configure the IP address range for authentication-free users. The value can be a single IP address (such as 192.168.110.2) or an IP address range (such as 192.168.110.2-192.168.110.254). A maximum of 50 entries are supported.

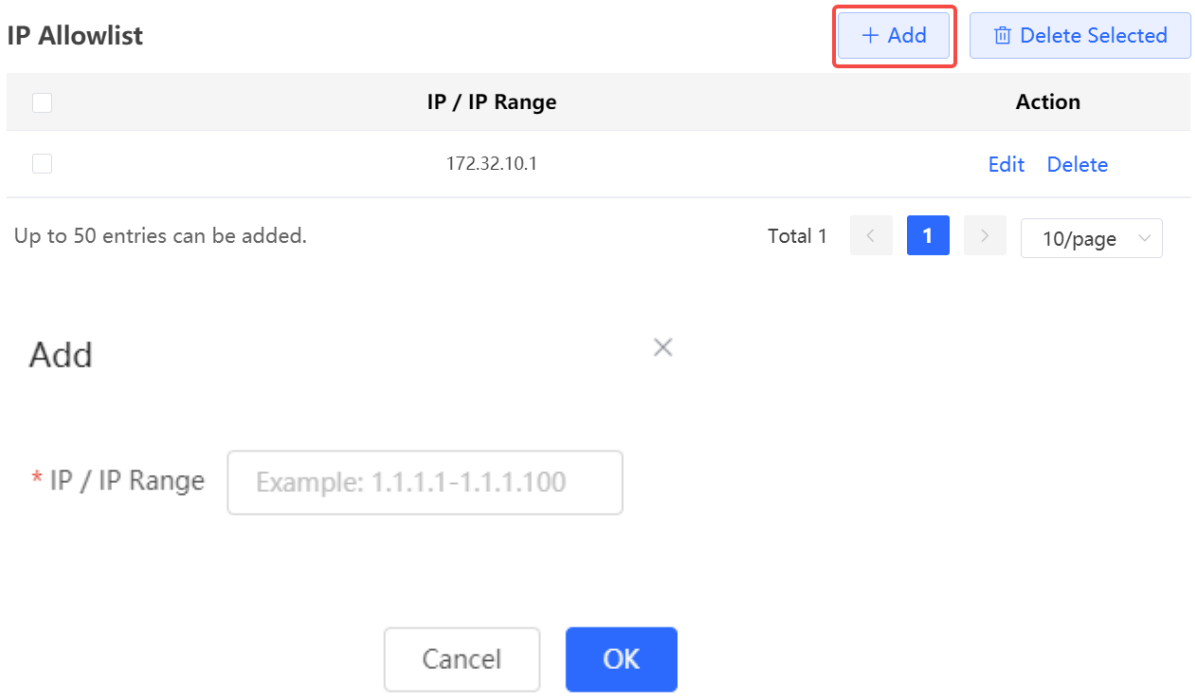


3. Configuring Extranet IP Addresses for Authentication-Free

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Authentication** > **Allowlist** > **IP Allowlist.**

Extranet IP address for authentication-free: Specify the IP addresses that can be assessed by all users including unauthenticated users.

Click **Add** to configure extranet IP addresses that can be assessed by users without authentication. A maximum of 50 entries are supported.

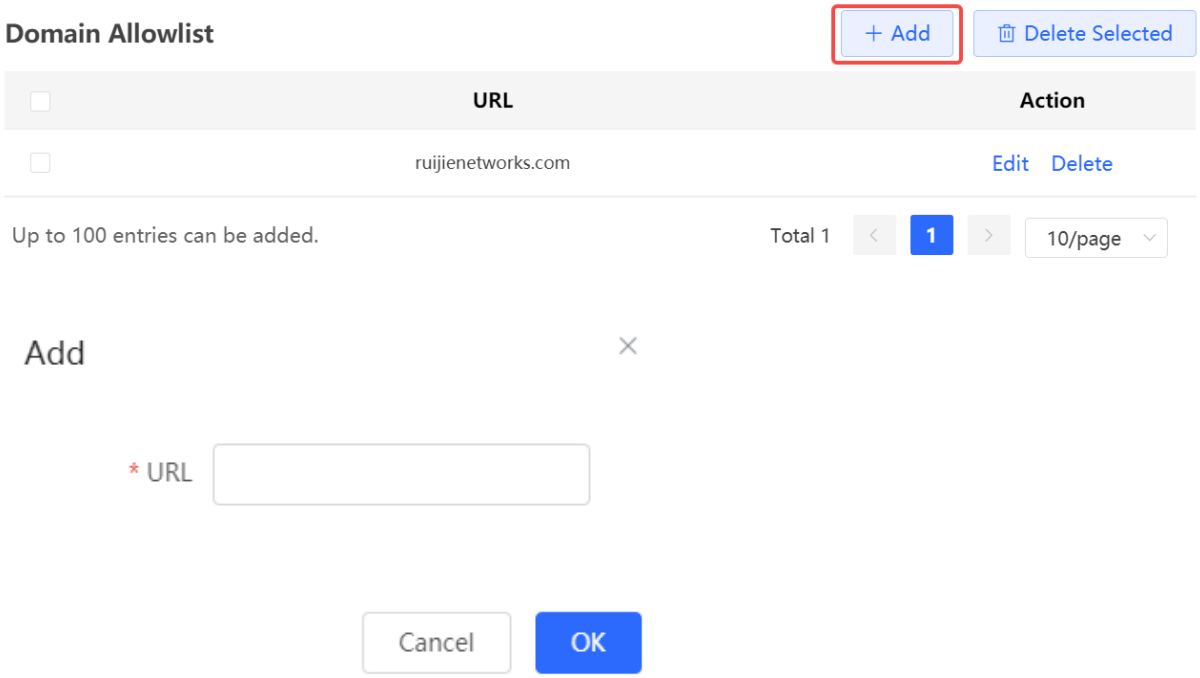


4. Configuring a Domain Allowlist

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Authentication** > **Allowlist** > **Domain Allowlist**.

Domain Allowlist: Specify the URLs that can be accessed without authentication.

Click **Add**. In the dialog box that appears, enter the authentication-free URLs, and then click OK. When the destination URL of the user is in the **Domain Allowlist** traffic from the user will be permitted directly, regardless of whether the user passes authentication. A maximum of 100 entries are supported.

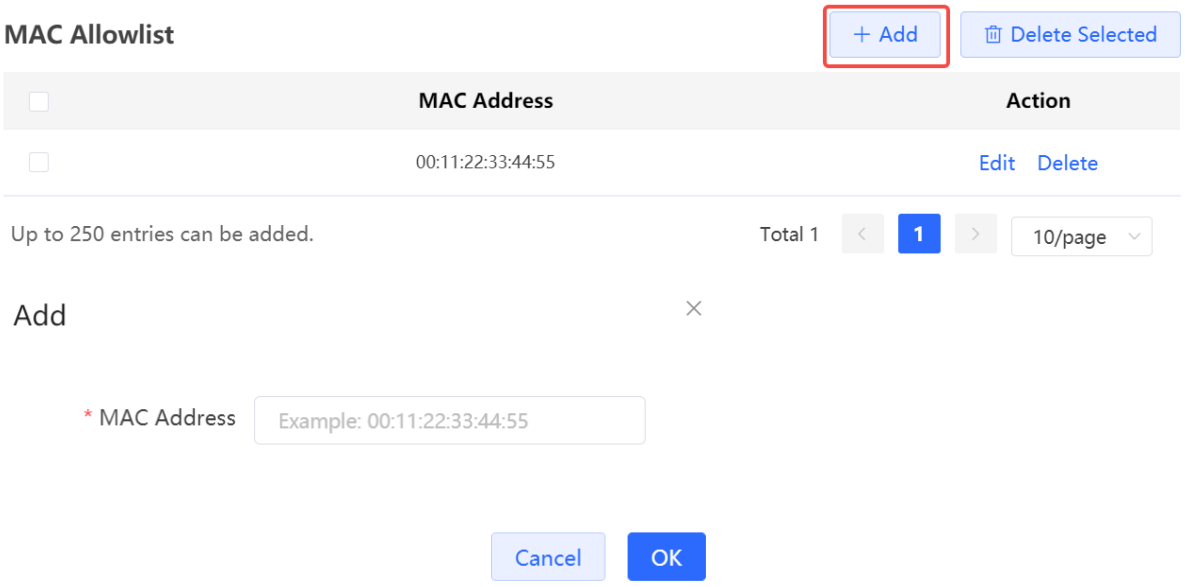


5. Configuring a User MAC Allowlist

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Authentication** > **Allowlist > MAC Allowlist.**

MAC **Allowlist**: Clients whose MAC addresses are in the **Allowlist** can access the Internet through Wi-Fi without the need for authentication.

Click **Add**. In the dialog box that appears, enter the MAC addresses of authentication-free users, and then click **OK**. A maximum of 250 entries are supported.

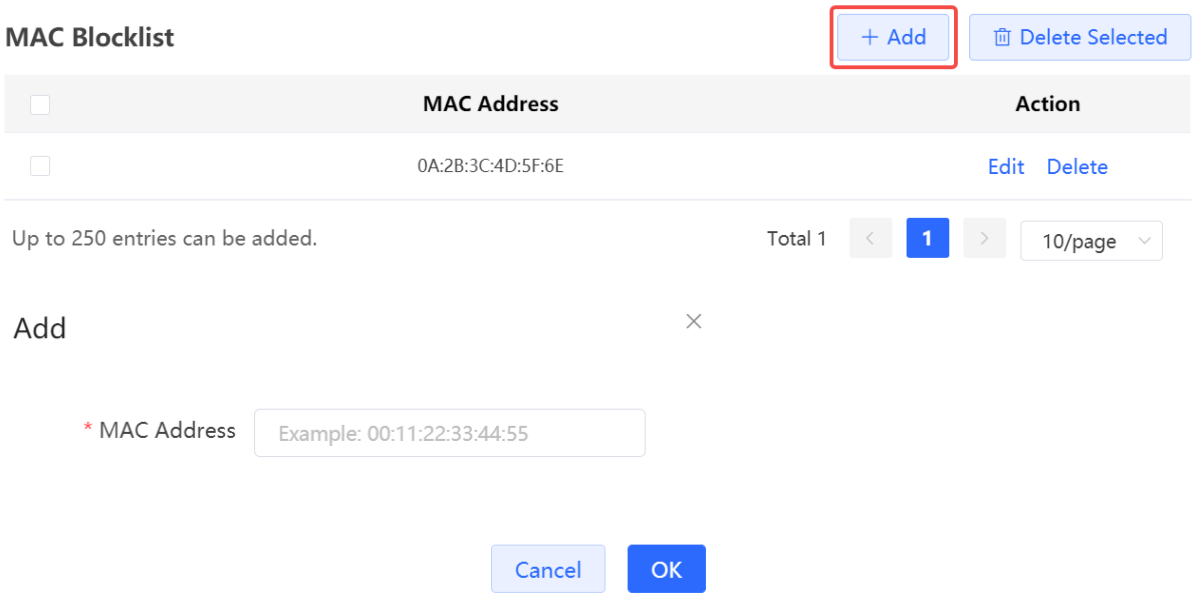


6. Configuring a User MAC Blocklist

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Authentication** > **Allowlist > MAC Blocklist**.

User MAC Blocklist Clients whose MAC addresses are in the blocklist are prohibited from accessing the Internet.

Click **Add**. In the dialog box that appears, enter the MAC addresses of users in the blocklist, and then click **OK**. A maximum of 250 entries are supported.

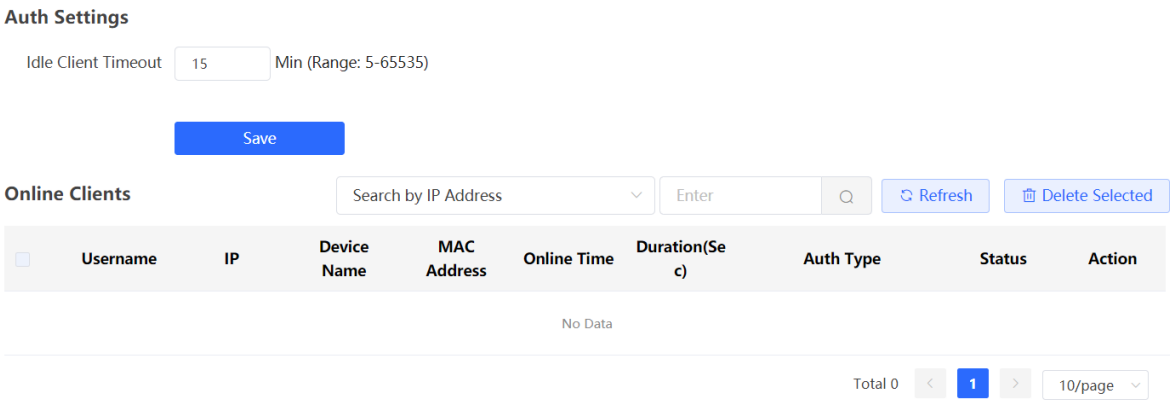


5.9.9 Online Authenticated User Management

1. Configuring the Idle Client Timeout Period

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Authentication** > **Online Clients**.

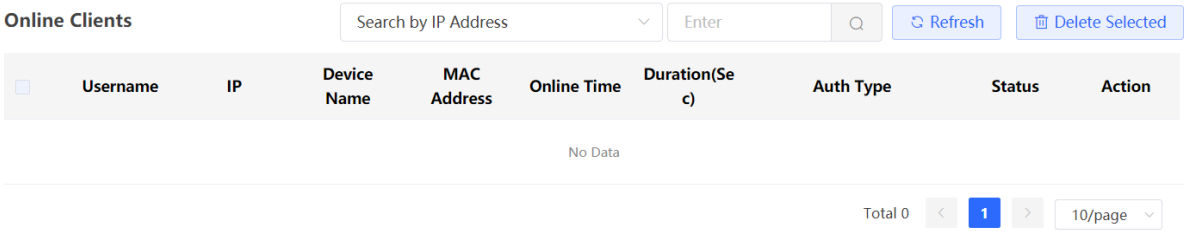
You can configure the idle client timeout period. The default value is 15 minutes. If no traffic from an online user passes through the device within the specified period, the device will force the user offline. The user can continue Internet access only after re-authentication.



2. Kicking a User Offline

The online client list displays information about all the current online clients, including the client IP address, client MAC address, login time, and authentication mode. You can find the client information based on the IP address,

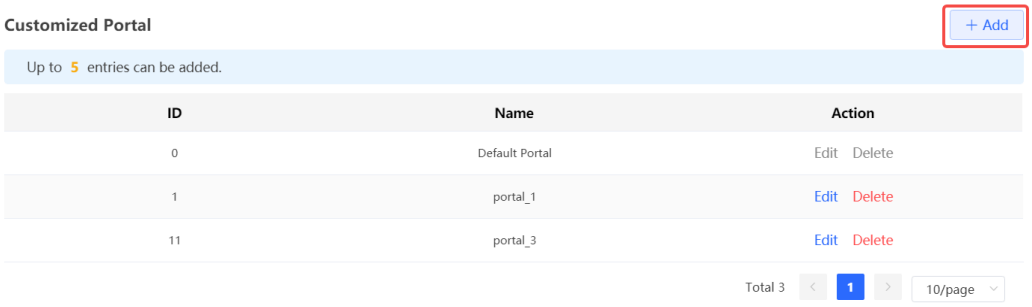
MAC address, or username. Find the target client in the online client list and click **Delete** in the **Action** column to kick the client off and disconnect the Wi-Fi connection of the client.



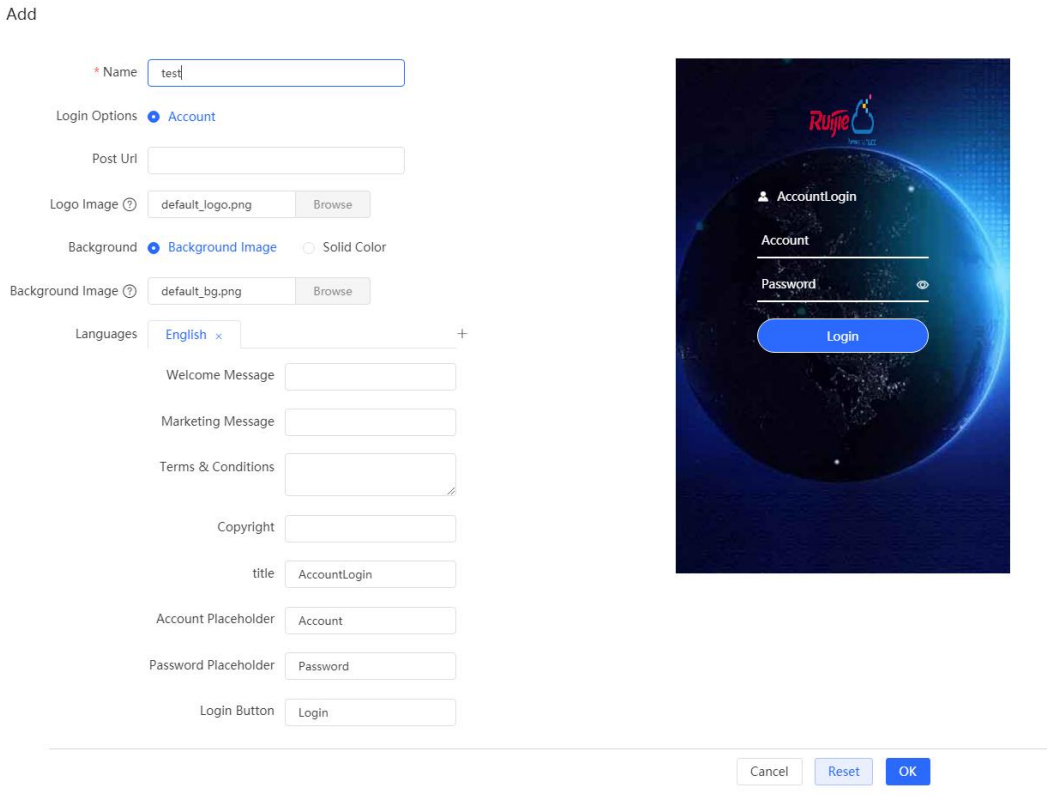
5.9.10 Custom Portal Page

1. Customized Portal

(1) On the **Customized Portal** page, click **Add**.



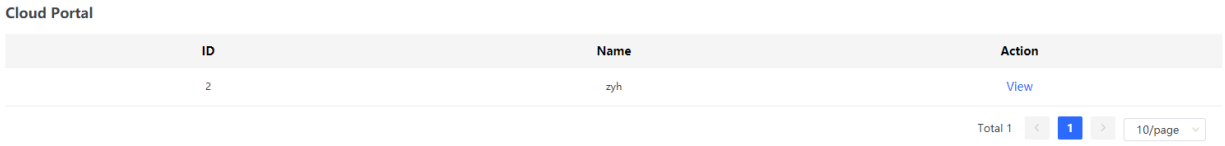
(2) Enter the portal page name and customize its content. The preview page will update in real-time as you enter the values.



(3) Click **OK**.

2. Cloud Portal

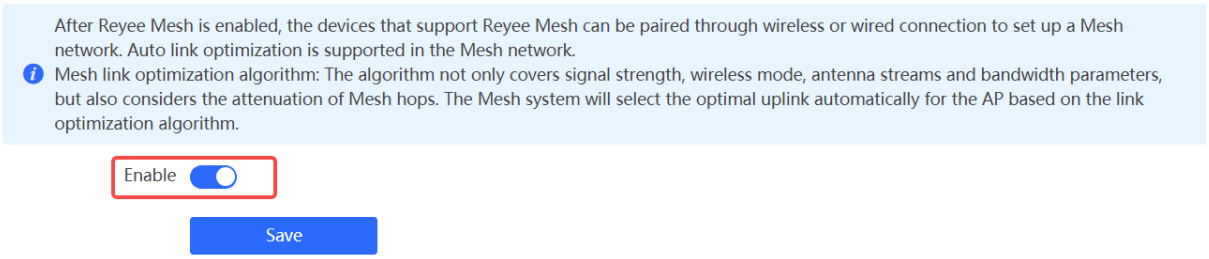
In the **Cloud Portal** pane, the portal page configured in Ruijie Cloud is displayed. Click **View** to preview the page content.



5.10 Enabling Reyee Mesh

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

After Reyee Mesh is enabled, you can set up a Mesh network through Mesh pairing between the devices that support Reyee Mesh. You can press the **Mesh** button on the device to automatically discover a new device for Mesh pairing or log in to the management page to select a new device for Mesh pairing. Reyee Mesh is enabled on the device by default.



5.11 Configuring the LAN Port of Downlink Access Point

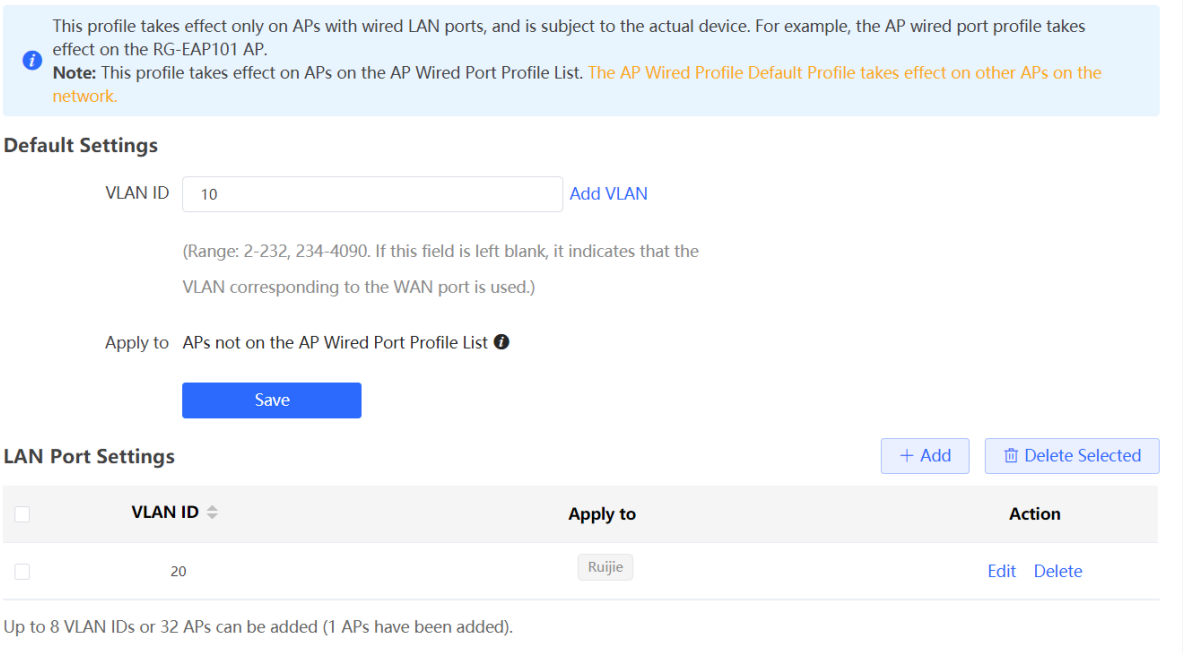
Caution

The configuration takes effect only for a downlink access point with a wired LAN port.

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



5.12 Wireless Authentication

Note

This feature is supported on RG-EG105G-V3, RG-EG105G-P-V3, RG-EG209GS, RG-EG210G-P-V3, RG-EG310GH-E, RG-EG305GH-P-E, RG-EG310GH-P-E and RG-EG1510XS.

5.12.1 Overview

Use the wireless authentication function to perform authentication configuration for the AP connected to the gateway. After users connect to the Wi-Fi signals released by the AP, the traffic will not be directly routed to the Internet. Wi-Fi users must pass authentication before accessing network resources.

Note

- The EG series router supports egress authentication. When an EG router is used independently, you are advised to use the authentication function of the router. Log in to the web interface of the EG router. Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Authentication**. For details, see 5.9 Wi-Fi Authentication.s
- When the EG router connects to the AP, the **Wireless Auth** action entry point appears on the **Network** page but not on the **Local Device** page.

5.12.2 Configuring Captive Portal on Ruijie Cloud

1. Prerequisites

If you want to configure **SMS Authentication** on Ruijie Cloud, please add a Twilio account first.

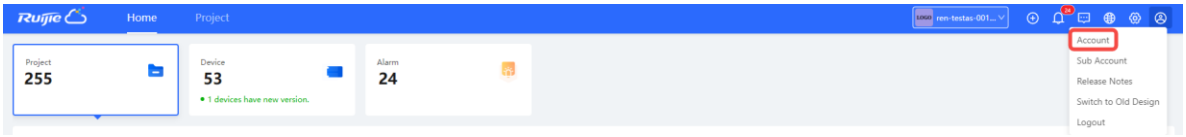
A Twilio account has been applied for from the Twilio official website (https://www.twilio.com/login).

Note

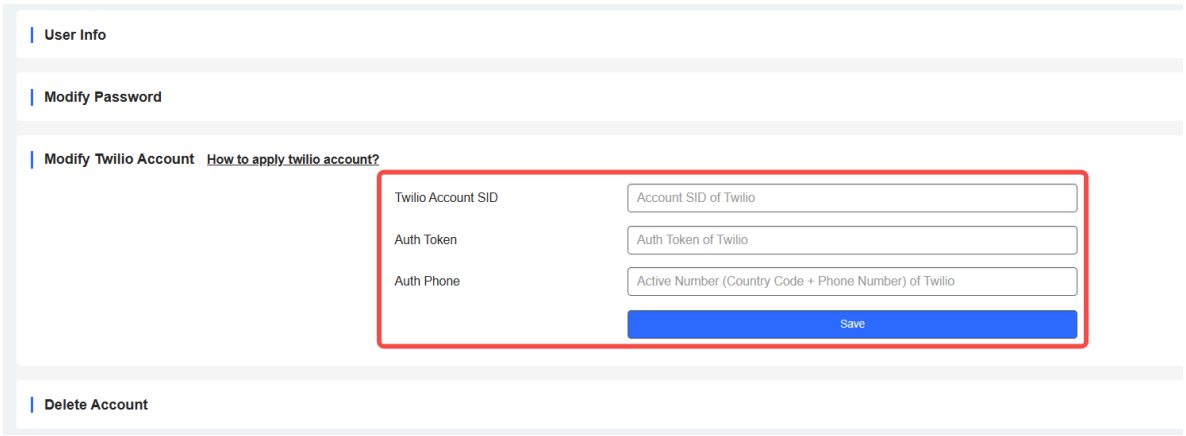
A Twilio account is used to send the SMS verification code.

Configuration Steps

(1) Log in to Ruijie Cloud and choose > **Account**

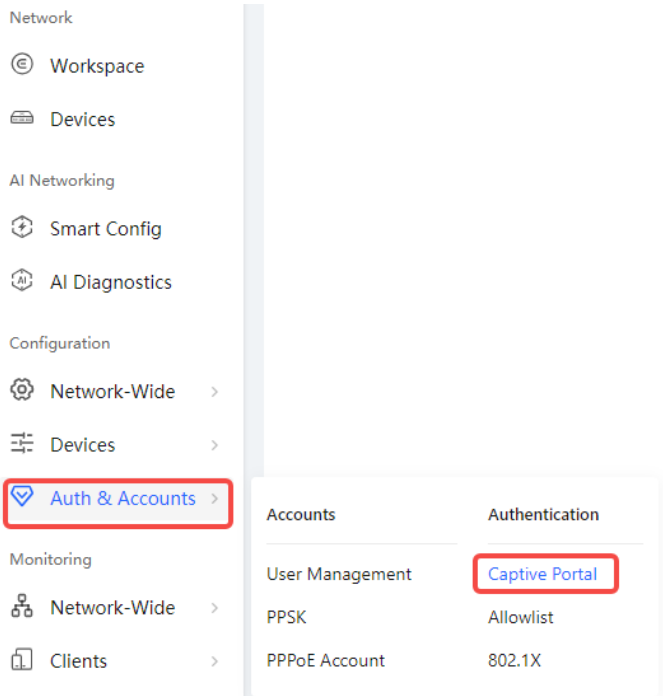


(2) Add Twilio account information and click **Save**

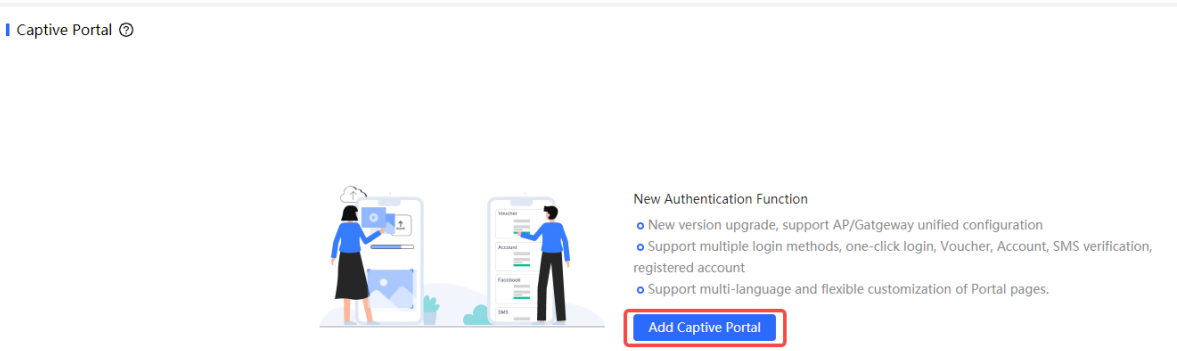


2. Configuring a Portal Page

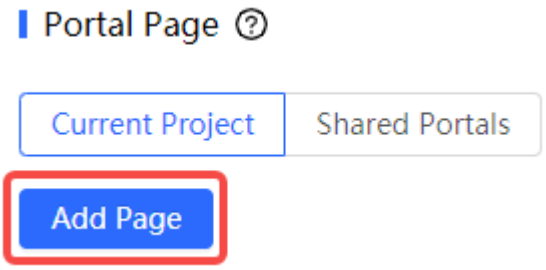
(1) Log in to Ruijie Cloud, choose **Project** > **Configuration > Auth&Account > Authentication** > **Captive Portal**, and select a network that needs to configure wireless authentication.



(2) Click **Add Captive Portal** to open the portal template configuration page.



(3) Click **Add Page** to customize a portal page.



(4) Configure basic information of the portal template.

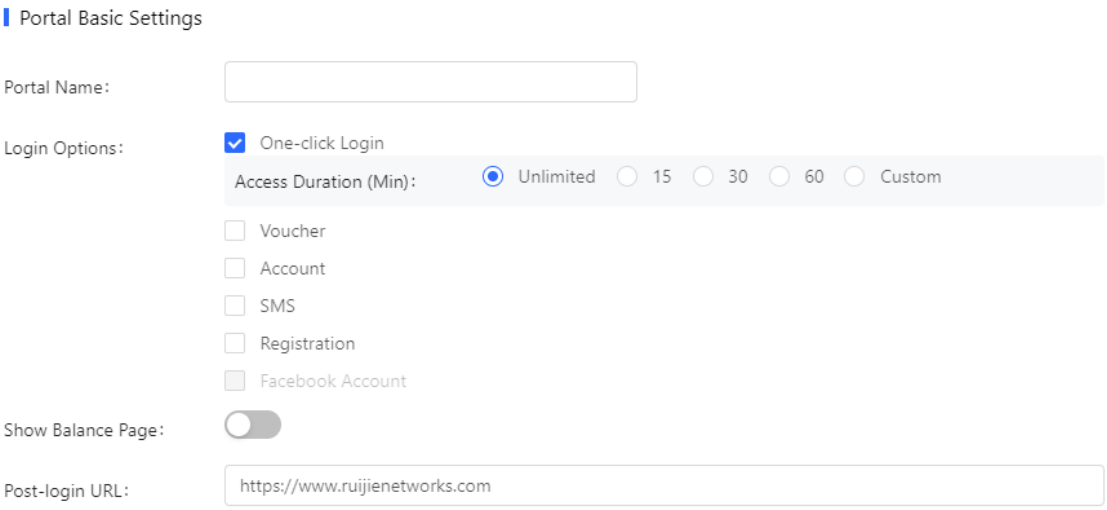
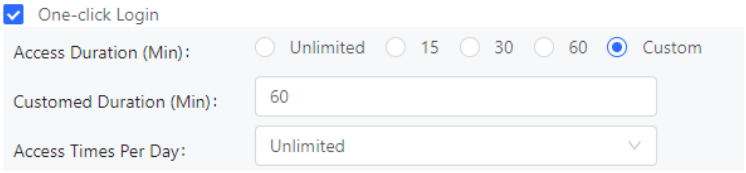
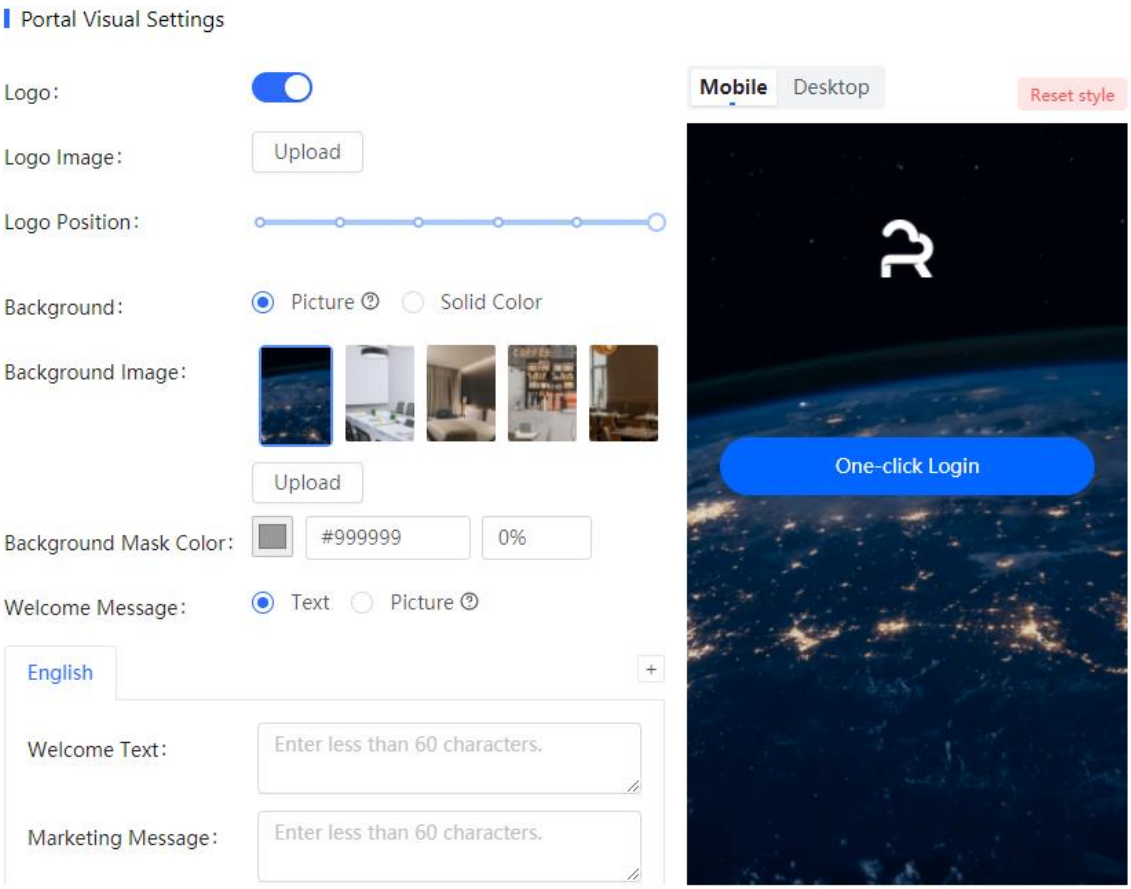


Table 5-12 Basic Information of the Portal Settings

Parameter	Description
Portal Name	Indicates the name of a captive portal template.

Parameter	Description
Login Options	Indicates the option to perform the desired action. ● One-click Login: indicates login without the username and password. You can set Access Duration and Access Times Per Day.  ● Voucher: indicates login with a random eight-digit password. ● Account: indicates login with the account and password. ● SMS: indicates login with the phone number and code. ● Registration: indicate that new account registration is supported.
Show Balance Page	Indicates the available duration, time, or data after portal authentication.
Post-login URL	Indicates the URL that is displayed after portal authentication.

(5) Configure visual settings of the portal template.



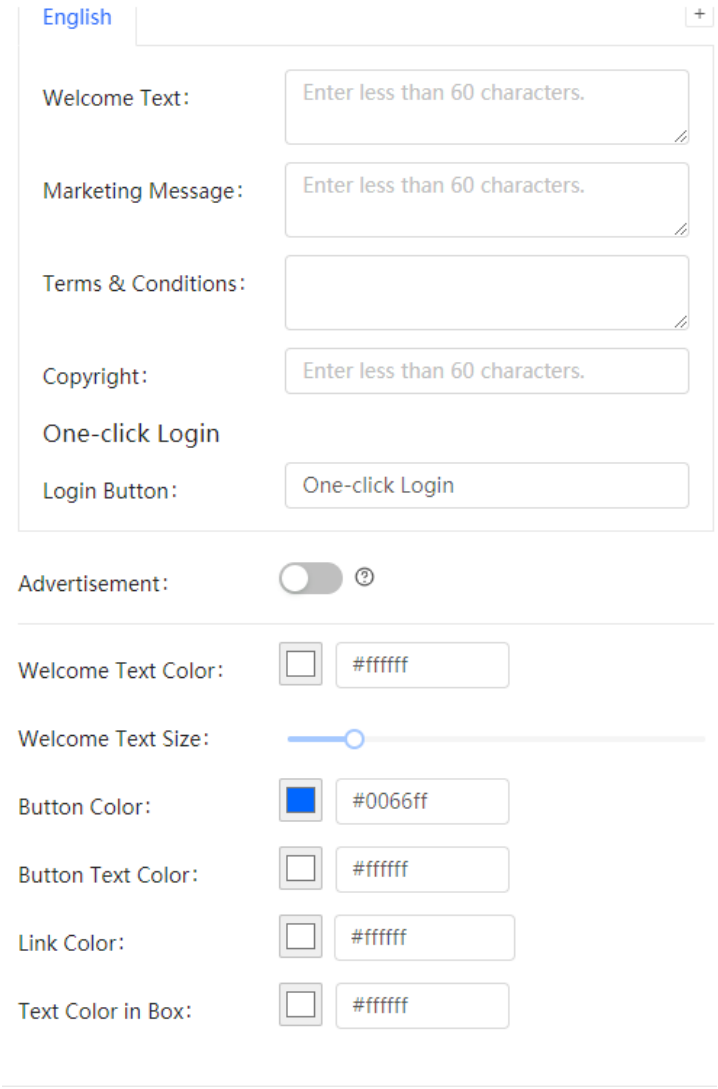
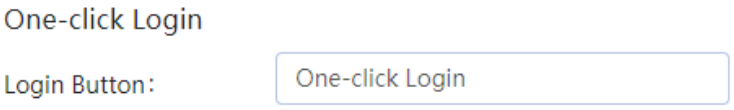
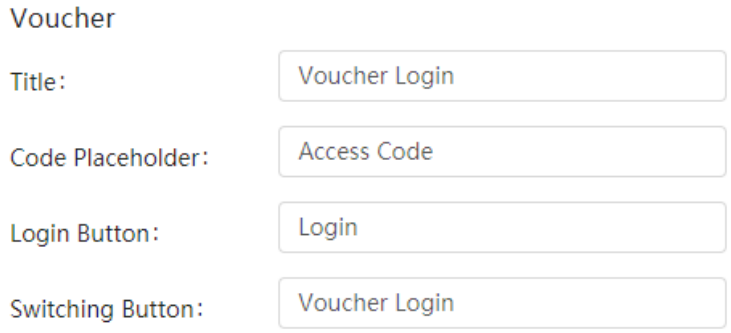
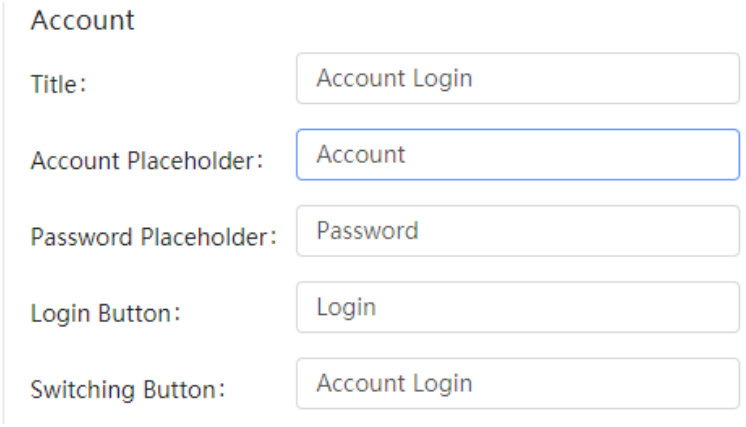


Table 5-13 Visual Settings of the Portal Page

Parameter	Description
Logo	Select whether to display the logo image.
Logo Image	When Logo is set to Image, upload the logo picture or select the default logo.
Logo Position	Select the logo position (Upper, Middle, or Lower).
Background	Select the background with the image or the solid color.
Background Image	When Background is set to Image, upload the background image or select the default image.
Background Mask Color	When Background is set to Solid Color, configure the background color. The default value is #ffffff.
Welcome Message	Select the welcome message with the image or text.

Language	Select the language of the portal page and configure the content displayed on the portal page as required. You can click + to add portal pages in other languages. ● Welcome Text: Select the welcome message with the image or text. ● Marketing message: Enter the marketing message. ● Terms & Conditions: Enter terms and conditions. ● Copyright: Enter the copyright. ● One-click Login: After One-click Login is enabled, you can customize the button name displayed on the portal page, which is set to One-click Login by default.  ● Voucher Login: After Voucher Login is enabled, you can customize the names of controls related to voucher authentication.  ● Account Login: After Account Login is enabled, you can customize the names of the controls related to account authentication.  ● SMS Login: After SMS Login is enabled, you can customize the names of the controls related to SMS authentication.

Parameter	Description
	SMS Title: SMS Login Phone Placeholder: Phone Code Placeholder: Verification Code Code Button: Get Code Login Button: Login Switching Button: SMS Login ● Registration: After Registration is enabled, you can customize the names of the controls related to register new account. Registration Title: Login Email: Email Phone number: Phone User: Your Name Registration Button: Login Switching Button: Register New Account
Advertisement	Select whether to display the advertisement.
Welcome Text Color	Select the welcome message text color. The default value is #ffffff.
Welcome Text Size	Select the welcome text size.
Button Color	Select the button color. The default value is #0066ff.
Button Text Color	Select the button text color. The default value is #ffffff.
Link Color	Select the link color. The default value is #ffffff.
Text Color in Box	Select the text color in the box. The default value is #ffffff.

(6) After the configuration, click **OK** to save the portal template configurations.

3. Configuring Policy Info

Configure basic information of the policy info to add captive portal. After the configuration, click **OK** for the configurations to take effect.

Note

When Encryption Mode is set to a value other than WPA2-Enterprise(802.1x), Auth is available and you can select whether to perform wireless authentication.

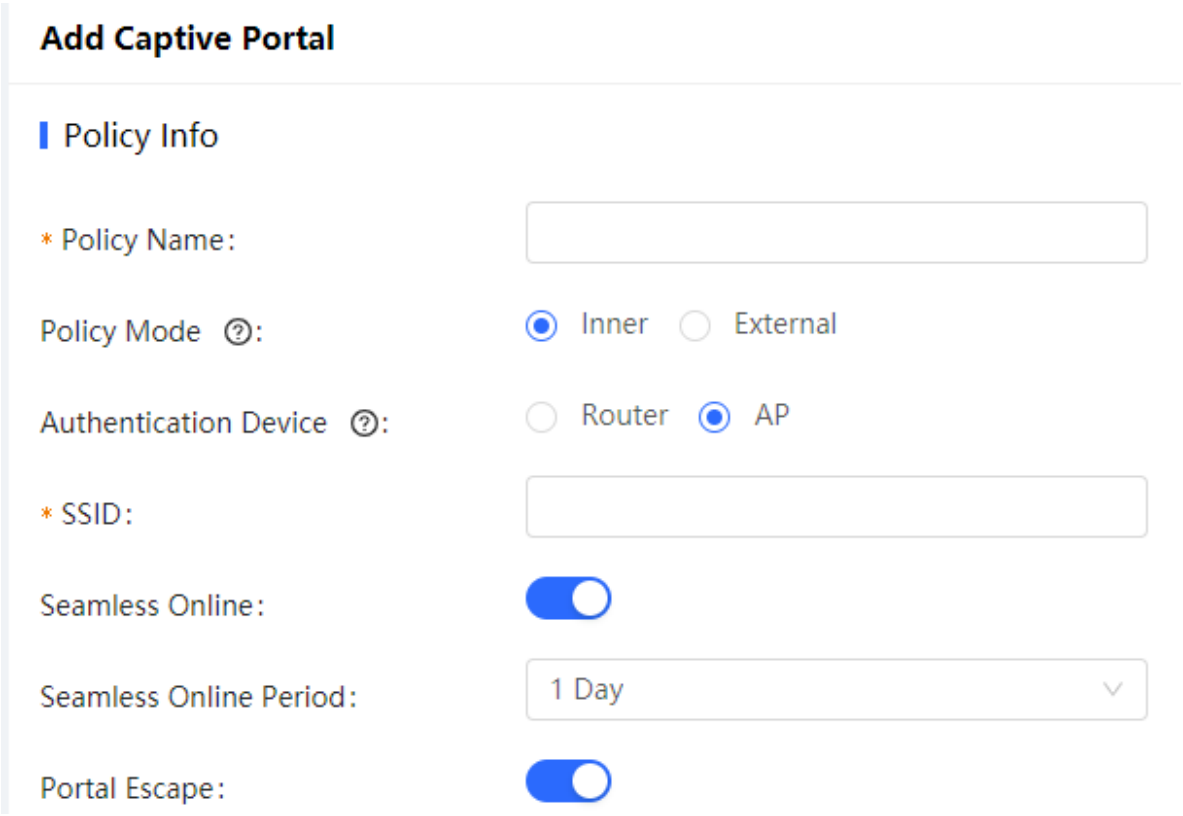


Table 5-14 Basic Information of the Captive Portal

Parameter	Description
Policy Name	Indicates the name of a captive portal template.
Policy Mode	Indicates the authentication mode to which the captive portal applies: Inner: Cloud-based authentication. The built-in authentication server in the public cloud is used for authentication. Local: Device-based local authentication and acceleration. Portal pages and accounts in the cloud are synchronized with the device for local authentication and acceleration. External: Third-party authentication, facilitating integration between the device and a third-party authentication server for authentication.

Parameter	Description
Authentication Device	Indicates the device that performs the authentication. When there is a router on the network, you are advised to enable authentication on the router. You can perform authentication on either an access point (AP) or a router. AP: An AP acts as the NAS. Router: A router or gateway acts as the NAS responsible for performing authentication at the gateway exit. Reyee AP Authentication: RAP/EWR, ReyeeOS 1.219 or later version. Reyee EG WiFiDog Authentication: EG/EGW, ReyeeOS 1.202 or later version. Reyee EG Local Authentication: EG210G-E, EG210G-P-E, EG310GH-E, EG310GH-P-E, EG305GH-E, EG305GH-P-E, ReyeeOS 1.230 or later version. This parameter is not required if the policy mode is Local.
Network	Indicates the wired network that requires authentication. Enter the network segment in this field. Users connecting to the wired network corresponding to this network segment must be authenticated. This parameter is required if the Authentication Device is Router.
SSID	Indicates the network name of the Wi-Fi network that requires authentication. Users connecting to this wireless network must be authenticated. This parameter is required if the Authentication Device is AP.
Seamless Online	After this function is enabled, if the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within a certain period of time.
Seamless Online Period	Indicates the time period for seamless online. If the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within this period of time.
Portal Page	Indicates the portal page that is displayed after portal authentication. Click Current Project to select the portal page for an existing project. Click Shared Portals to select an existing portal page. Click Add Page to customize a portal page.

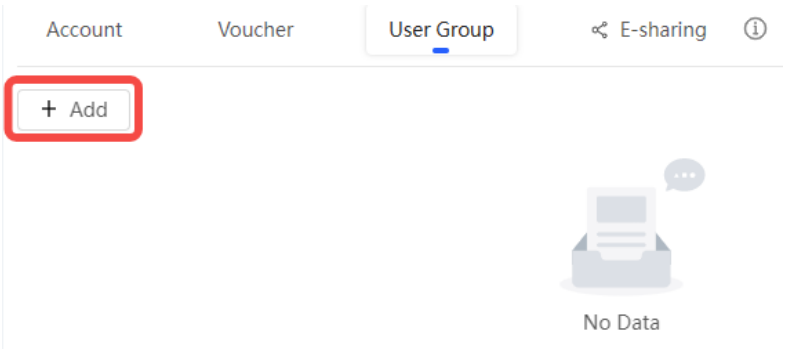
4. (Optional) Adding a Voucher

If the **Login Options** is **Voucher**, you should configure a voucher as the following steps.

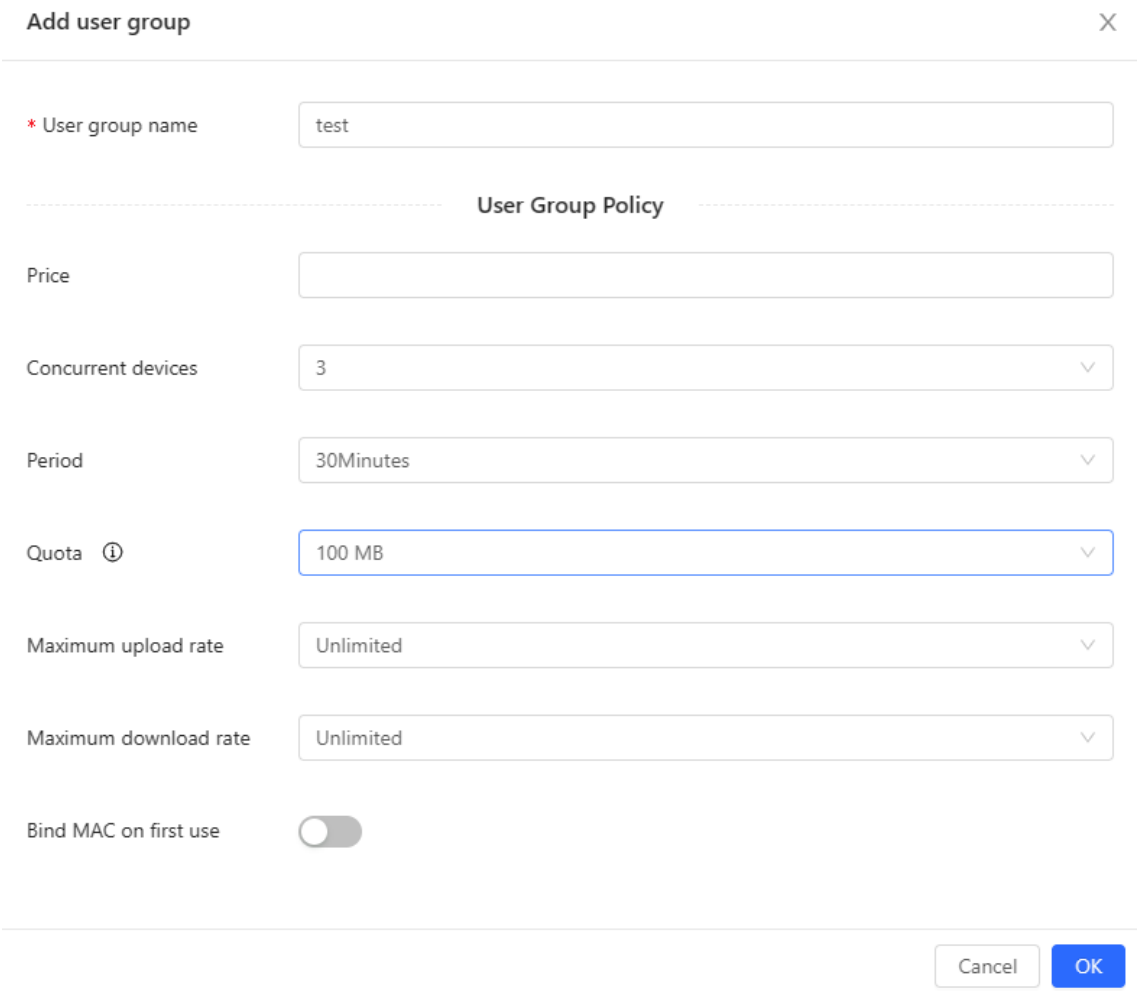
(1) Log in to Ruijie Cloud, choose **Project** > **Authentication** > **User Management**, **and** select a network in this account**.**

(2) Configure a user group.

On the **User Group** tab, click **Add**.



Configure user group parameters. After the configuration, click OK.

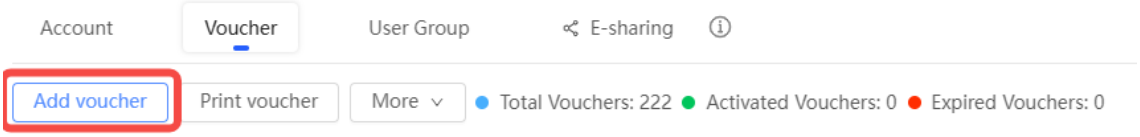


- **User Group Name**: indicates the user group name.
- **Price**: indicates the price of the user group. Mark user groups by numeral. The current version has no impact on network usage.

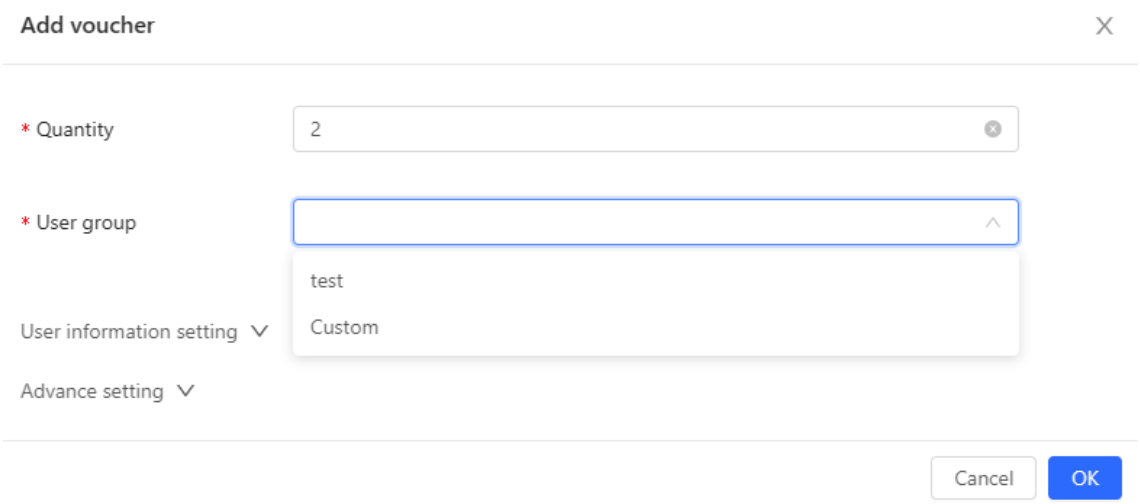
- **Concurrent Devices**: indicates the number of concurrent devices for one account.
- **Period**: indicates the maximum validity time of an account. The maximum value is counted after the client passes authentication and successfully accesses the Internet.
- **Quota**: indicates the maximum amount of data transfer.
- **Maximum upload rate**: indicates the maximum upload rate.
- **Maximum download rate**: indicates the maximum download rate.
- **Bind MAC on first use**: indicates that the MAC address of the first device used will be bound and other devices used by the same user will be prohibited from accessing the Internet.

(3) Configure a voucher.

On the **Voucher** tab, click **Add voucher**.

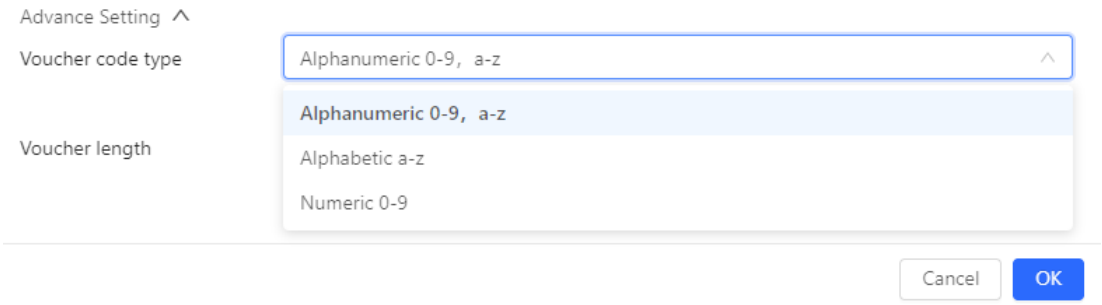


Configure voucher parameters. After the configuration, click OK.

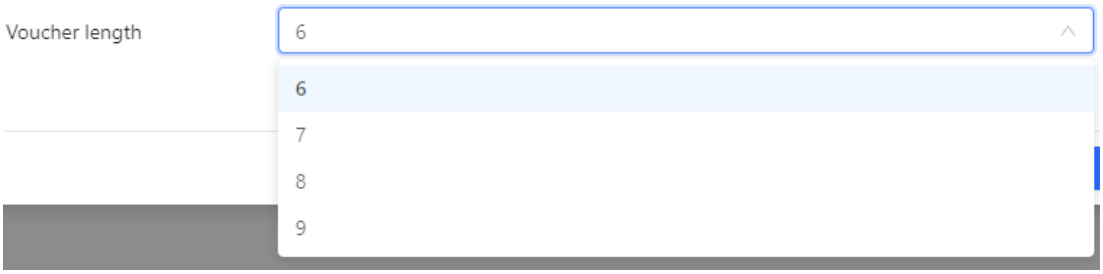


- **Quantity**: Enter the quantity of the voucher to print. When the value is set to 1, you can add a voucher and configure the name and the email address. When the value is greater than 1, you can add vouchers in batches. In this case, you can only configure the name and email address separately after the vouchers are added.
- **User group**: Select a created user group from the drop-down list. If the created user group does not meet the requirements, click **Custom** to create a user group.
- **User information setting**: Configure user information, which is optional.
- **Advance setting**:

  Voucher code type: Set the value to Alphanumeric 0-9, a-z, Alphabetic a-z, or Numeric 0-9.



Voucher length: Select the voucher length. The value ranges from 6 to 9.



(4) Obtain the voucher code from the voucher list.

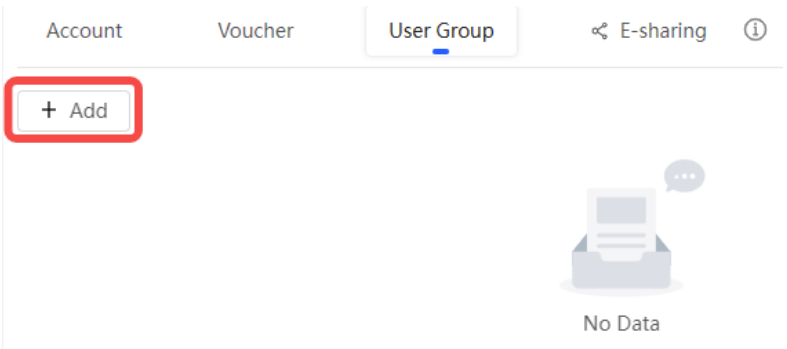
5. (Optional) Adding an Account

If the **Login Options** is set to **Account**, you should add accounts through the following steps.

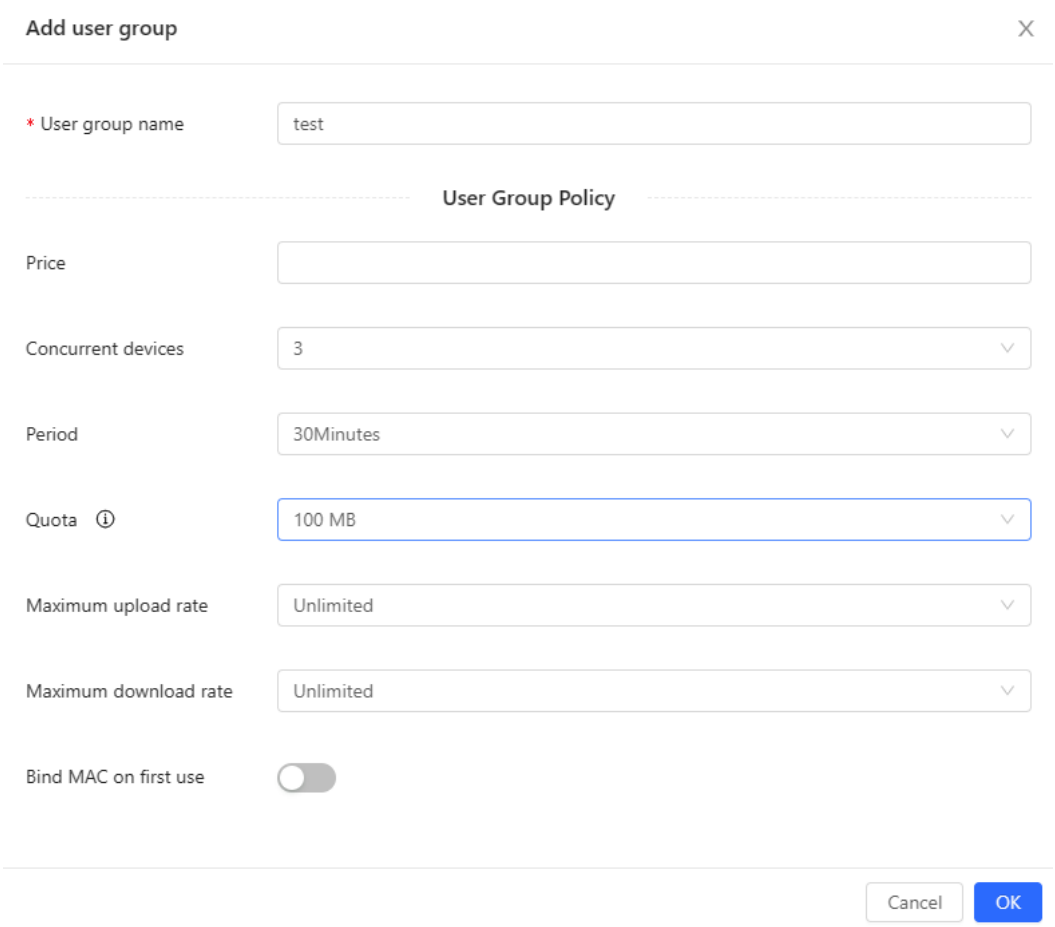
(1) Log in to Ruijie Cloud, choose **Project** > **Authentication** > **User Management**, **and** select a network in this account**.**

(2) Configure a user group.

On the **User Group** tab, click **Add**.



Configure user group parameters. After the configuration, click **OK**.

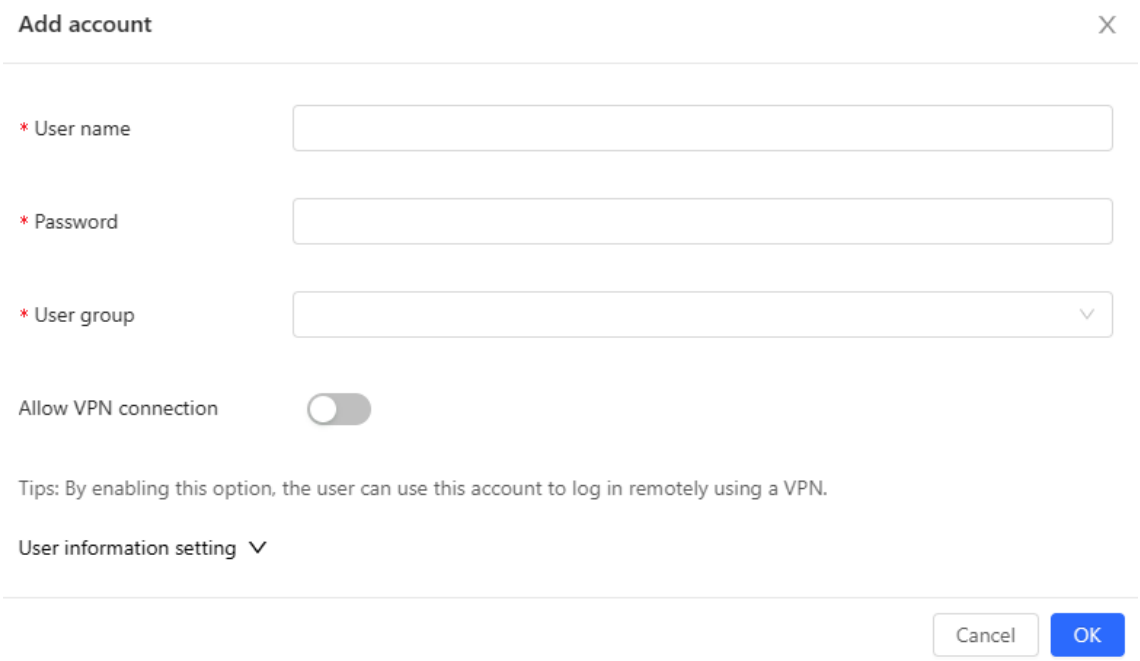


- User **Group Name**: indicates the user group name.
- **Price**: indicates the price of the user group. Mark user groups by numeral. The current version has no impact on network usage.
- **Concurrent Devices**: indicates the number of concurrent devices for one account.
- **Period**: indicates the maximum validity time of an account. The maximum value is counted after the client passes authentication and successfully accesses the Internet.
- **Quota**: indicates the maximum amount of data transfer.
- **Maximum upload rate**: indicates the maximum upload rate.
- **Maximum download rate**: indicates the maximum download rate.
- **Bind MAC on first use**: indicates that the MAC address of the first device used will be bound and other devices used by the same user will be prohibited from accessing the Internet.

(3) On the **Account** tab, add an account. Accounts can be added manually or through batch import.

- Adding an account manually

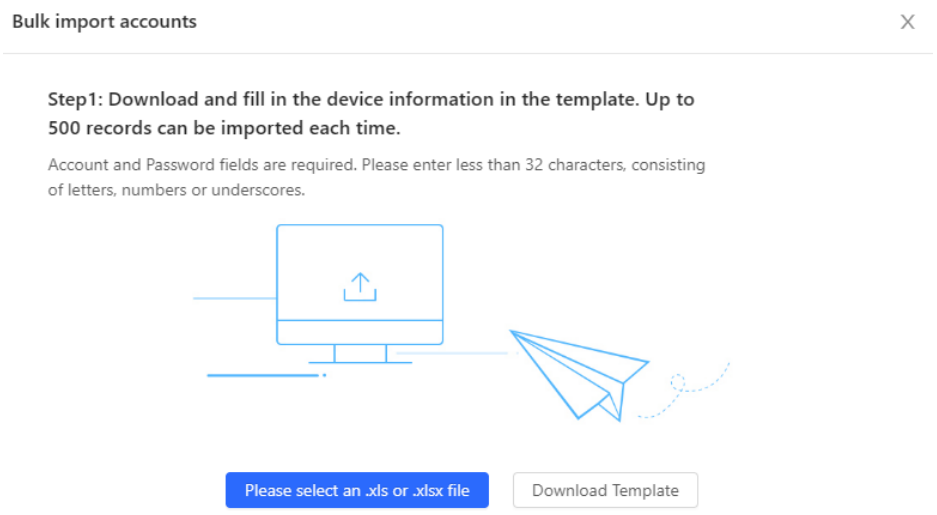
  Click **Add an Account**, set parameters about the account, and click **OK**.



- **User name**: The value is a string of less than 32 characters, consisting of letters, numerals, and underscores.
- **Password:** The value is a string of less than 32 characters, consisting of letters, numerals, and underscores.
- **User group**: **Select a created user group from the drop-down list. If the created user group does not meet the requirements, click Custom to create a user group.**
- **Allow VPN connection:** By enabling this option, the user can use this account to log in remotely using a VPN.
- **User information setting:** You can expand it to have more user information displayed, including the first name, last name, email, phone number, and alias.

- Adding accounts through batch import

  Click **Bulk import**.



  Click **Download Template** to download the template.

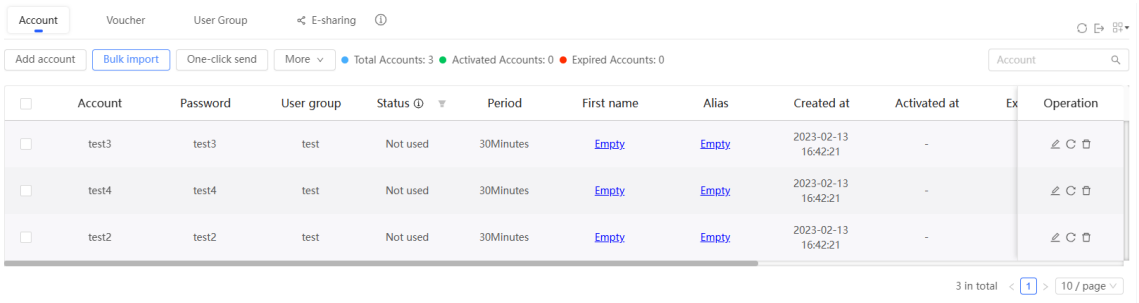
Edit the template and save it.

Note

- **Account**, **Password**, and **User Group** are mandatory.
- Check that the user group already exists and the added accounts are not duplicate with existing accounts.

Account	Password	First name	Last name	Alias	User group	Email
test2	test2				test	
test3	test3				test	
test4	test4				test	

Click **Please select an .xls or .xlsx file** to upload the file. After uploading, users are automatically created.



5.12.3 Configuring an Authentication-Free Account on the Web Interface

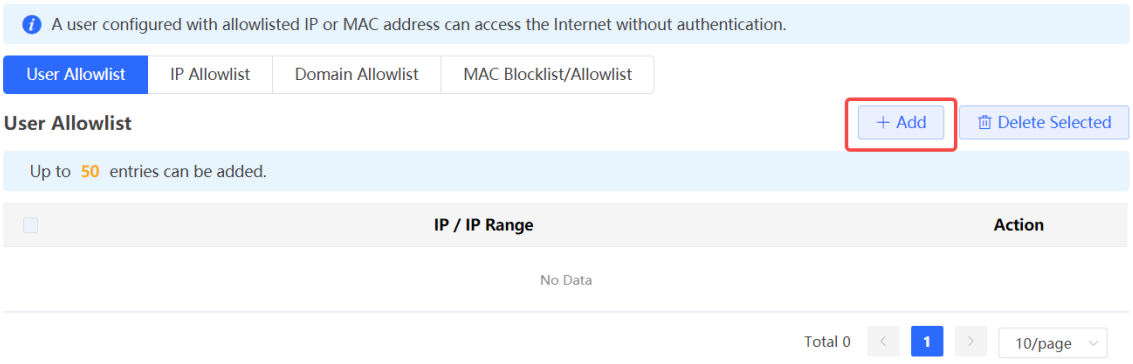
1. Configuring an Authentication-Free Account

The authentication-free user can access the Internet without authentication.

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

(1) Click **User Allowlist**.

(2) Click **Add**.



(3) Configure the IP address or IP address range for authentication-free users.

(4) Click **OK**.

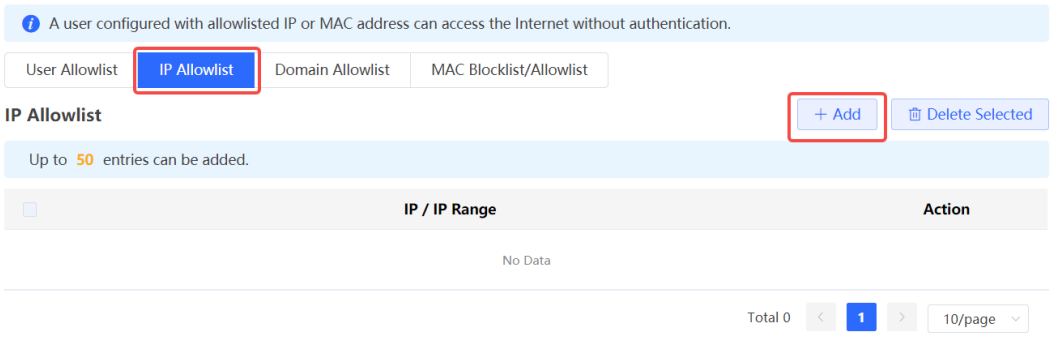
2. Configuring Authentication-Free External IP Addresses

After configuration, the user can access the authentication-free external IP address without authentication.

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

(1) Click **IP Allowlist**.

(2) Click **Add**.



(3) Configure authentication-free external IP address or IP address range.

(4) Click **OK**.

3. Configuring a Domain Allowlist

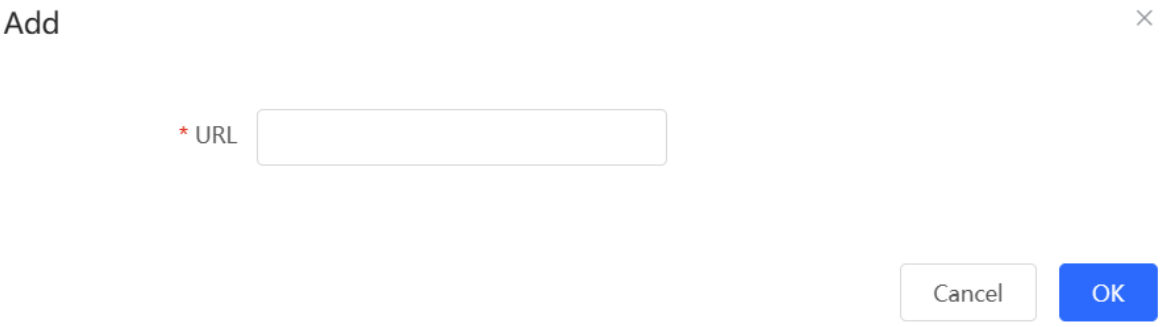
The user can access the URL in the domain allowlist without authentication.

(1) Choose **Network-Wide** > **Workspace** > **Wireless** > **Wireless Auth** > **Allowlist**.

(2) Click **Domain Allowlist**.

(3) Click **Add**.

(4) Configure authentication-free domains.



(5) Click **OK**.

4. Configuring a MAC Address Blocklist and Allowlist

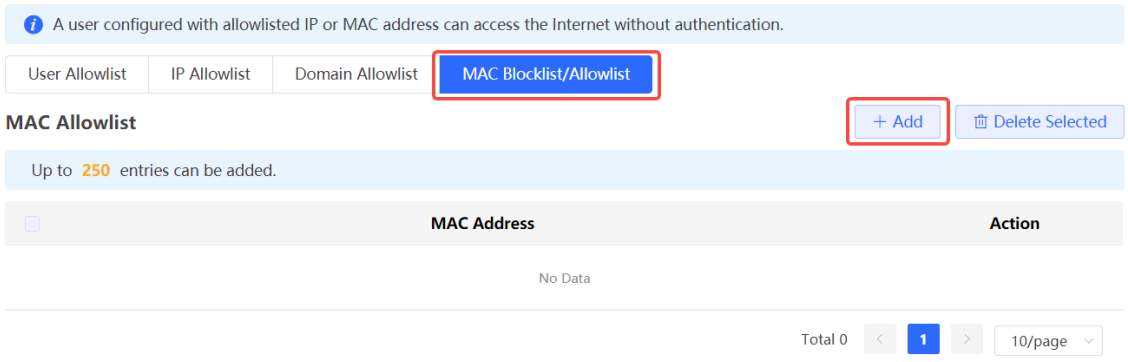
After configuration, the STA with an Allowlist MAC address can access the Internet without authentication while the STA with a blocklist MAC address is forbidden to access the Internet.

(1) Choose **Network-Wide** > **Workspace** > **Wireless** > **Wireless Auth** > **Allowlist**.

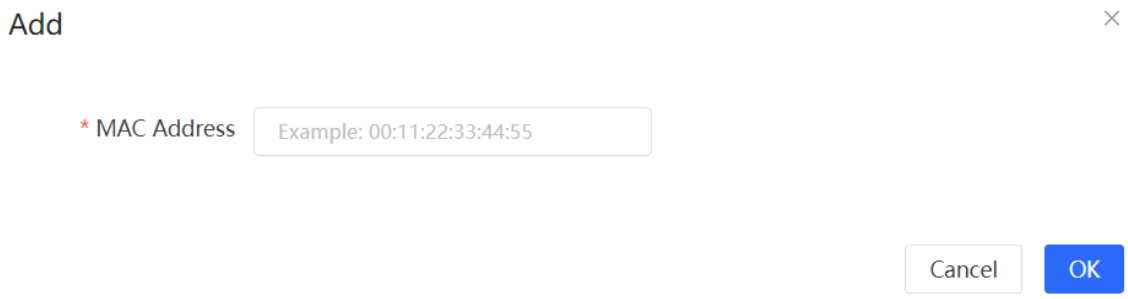
(2) Click **MAC Blocklist/Allowlist**.

(3) Configure a MAC address allowlist.

Click **Add** on the **MAC Allowlist** page.

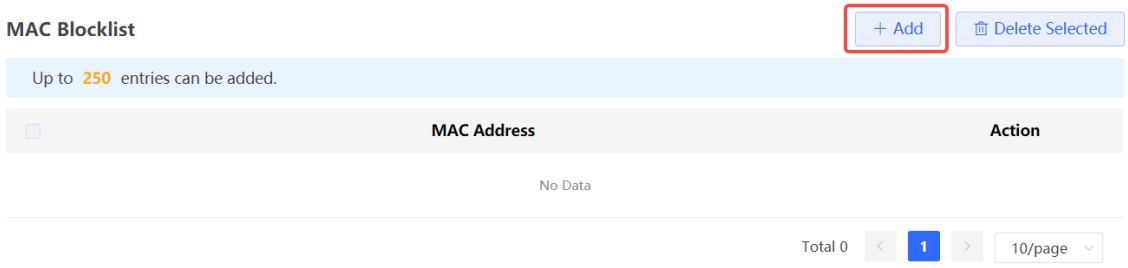


Add the MAC address to the allowlist.

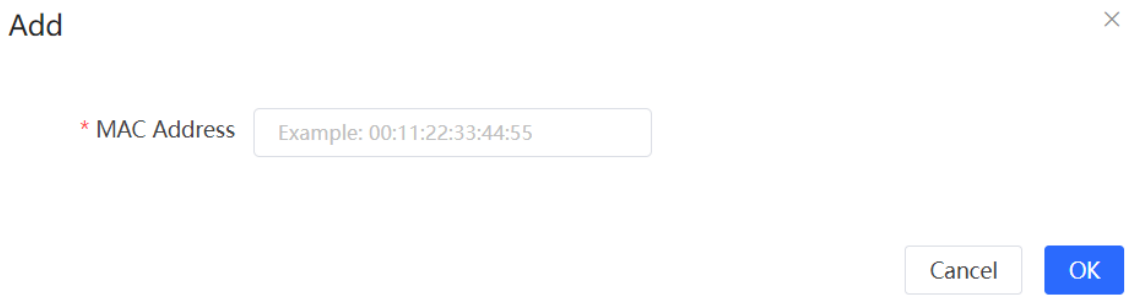


(4) Configure a MAC address blocklist.

Click **Add** on the **MAC Blocklist** page.



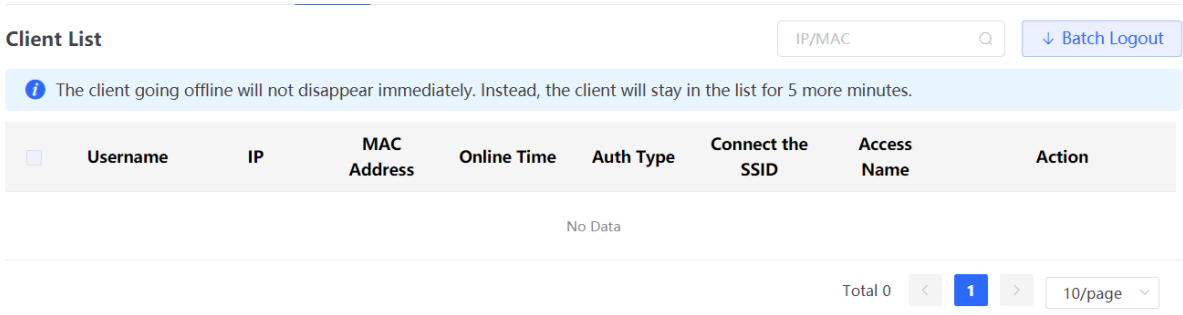
Add the MAC address to the blocklist.



5.12.4 Checking Authentication Client List

Check authentication users in the list view.

Choose **Network-Wide** > **Workspace** > **Wireless** > **Wireless Auth** > **Client List**.



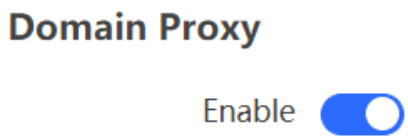
Click **Offline** in the **Action** column to disconnect users to release network resources.

5.13 Configuring Domain Proxy

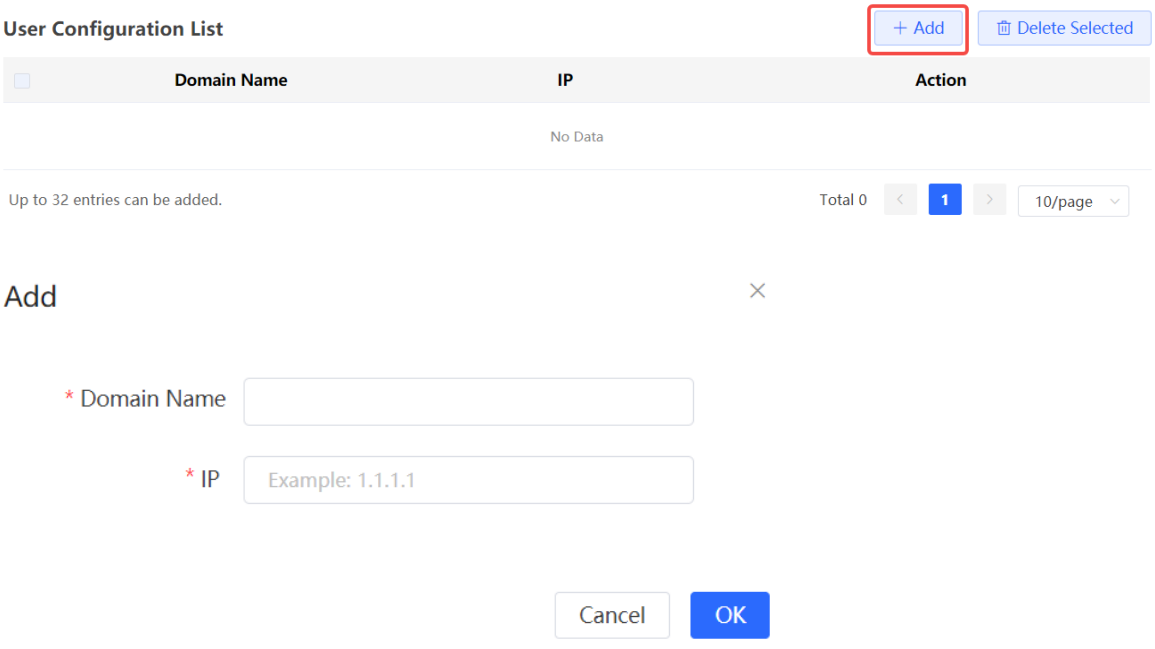
Choose **Network-Wide** > **Workspace** > **Wireless** > **Domain Proxy**.

When a client accesses a Wi-Fi network, the message "No Internet connection" or "The Wi-Fi is not connected to the Internet" may be displayed. The possible cause is that the client's operating system introduces an Internet detection mechanism. Generally, the detection mechanism sends a probe packet to a specified domain name and evaluates whether the wireless network can access the Internet based on the detection result. If the DNS server takes a long time to parse a domain name or returns a probe node with a long delay, the probe may be deemed unreachable, causing a false network unavailability.

After the **Domain Proxy** function is enabled, the device returns the preset domain name node to the client, reducing the misjudgment of network unavailability of the client.



Click **+Add**, enter the preset domain name and IP address, and click **OK**.



5.14 Client Association

5.14.1 Configuring Intelligent Association

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

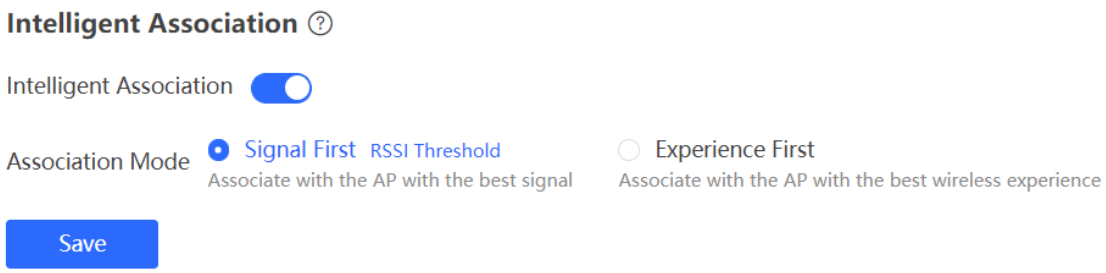
Note

Intelligent association is not supported by Wi-Fi 5 APs. Enabling it on Wi-Fi 5 APs may lead to suboptimal performance.

After certain smart home devices are associated with a remote AP, they are unable to re-associate with a nearby AP, resulting in poor user experience and significant delays.

With the Intelligent Association feature enabled, clients can dynamically select the access point for association, eliminating issues related to poor user experience caused by remote associations.

Toggle on the **Intelligent Association** switch, select the association mode, and click **Save**.



- Signal First

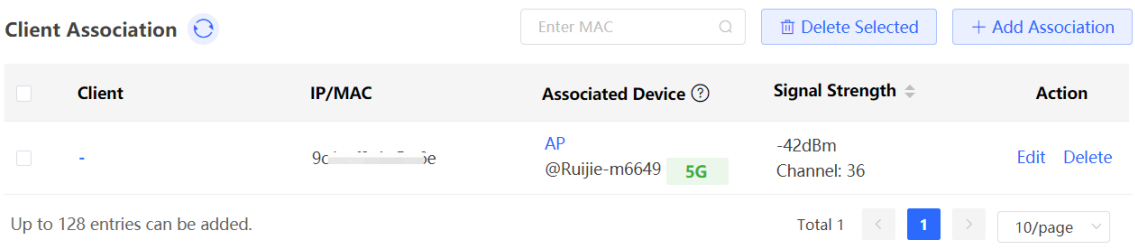
  Associate with the AP with the best signal.

- Experience First

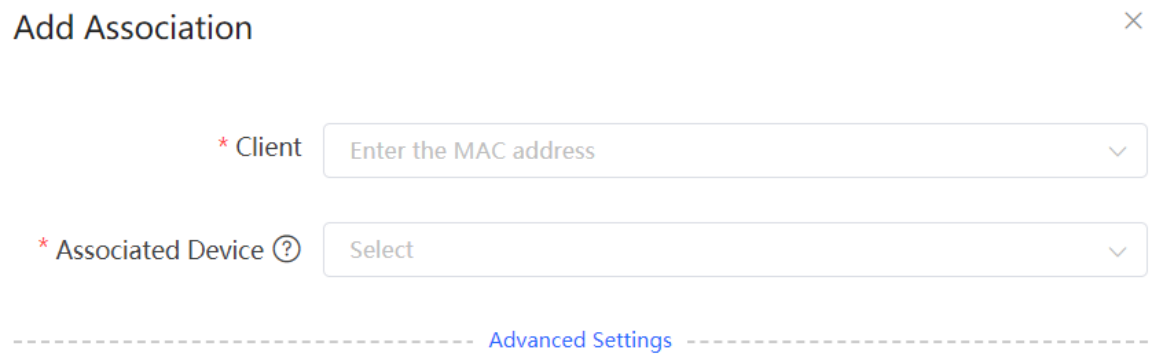
  Associate with the AP with the best wireless experience.

5.14.2 Configuring Client Association

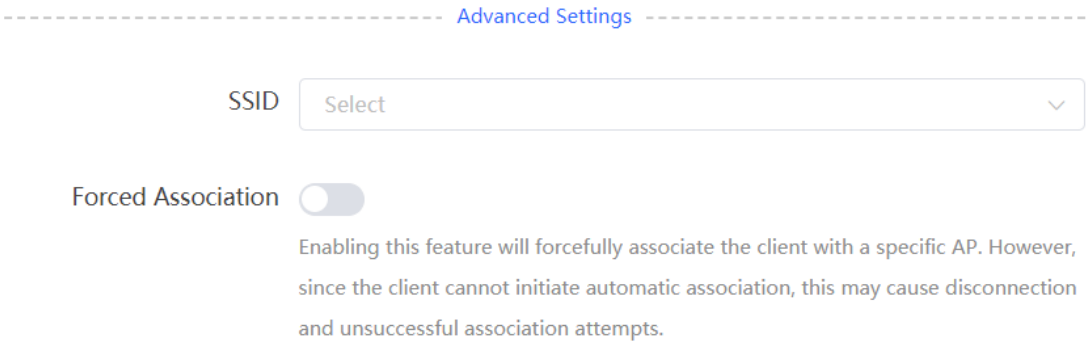
Choose **Network-Wide** > **Workspace** > **Wireless** > **Client Association**.



Click **Add Association**. Select the client and the associated device. You can associate the client with a specified AP on the network to reduce remote association and improve the wireless experience.



Click **Advanced Settings** to configure the SSID for client association and to enable **Forced Association**.



Caution

The **Forced Association** feature may cause the client to go offline or fail to associate with the AP. Therefore, exercise caution when performing this configuration.

6 Switch Management

6.1 Configuring RLDP

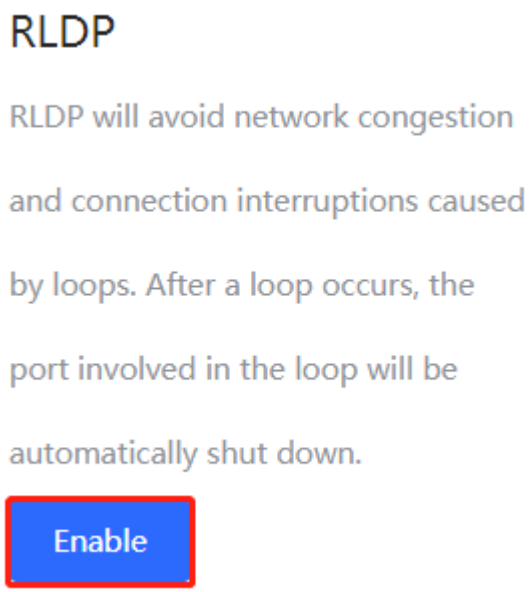
6.1.1 Overview

Rapid Link Detection Protocol (RLDP) is an Ethernet link fault detection protocol used to quickly detect link faults and downlink loop faults. RLDP can prevent network congestion and connection interruptions caused by loops. After a loop occurs, the port on the access switch involved in the loop will shut down automatically.

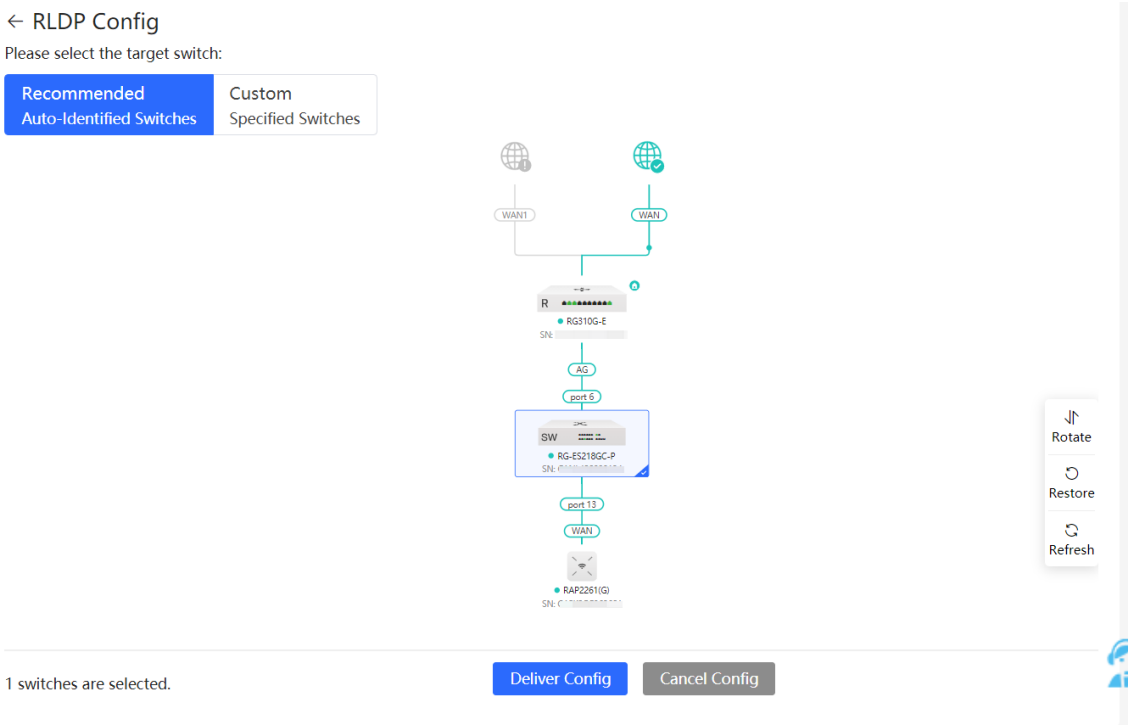
6.1.2 Configuration Steps

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

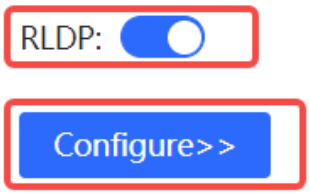
(1) Click **Enable** to access the **RLDP Config** page.



(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.



6.2 Configuring DHCP Snooping

6.2.1 Overview

DHCP Snooping implements recording and monitoring the usage of client IP addresses through exchange of DHCP packets between the server and client. In addition, this function can filter invalid DHCP packets to ensure that clients can obtain network configuration parameters only from the DHCP server in the controlled range. DHCP Snooping will prevent rogue DHCP servers offering IP addresses to DHCP clients to ensure the stability of the network.

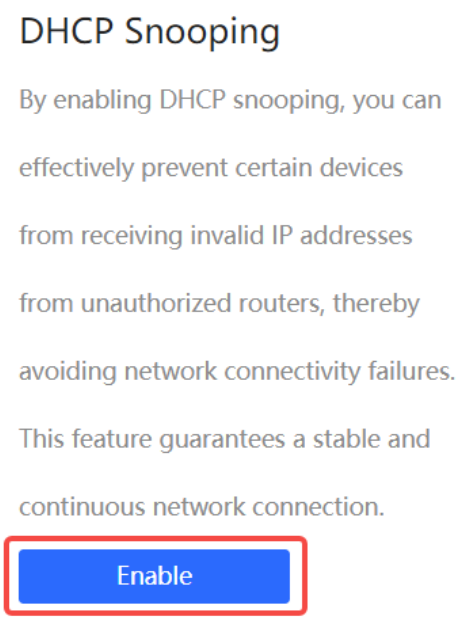
Caution

After DHCP Snooping is enabled on the switch, the switch does not forward invalid DHCP packets. However, if a client directly connects to a rogue DHCP server, it cannot access the Internet as the obtained IP address is incorrect. In this case, you need to find the rogue router and disable DHCP on it, or use the WAN interface for uplink connection.

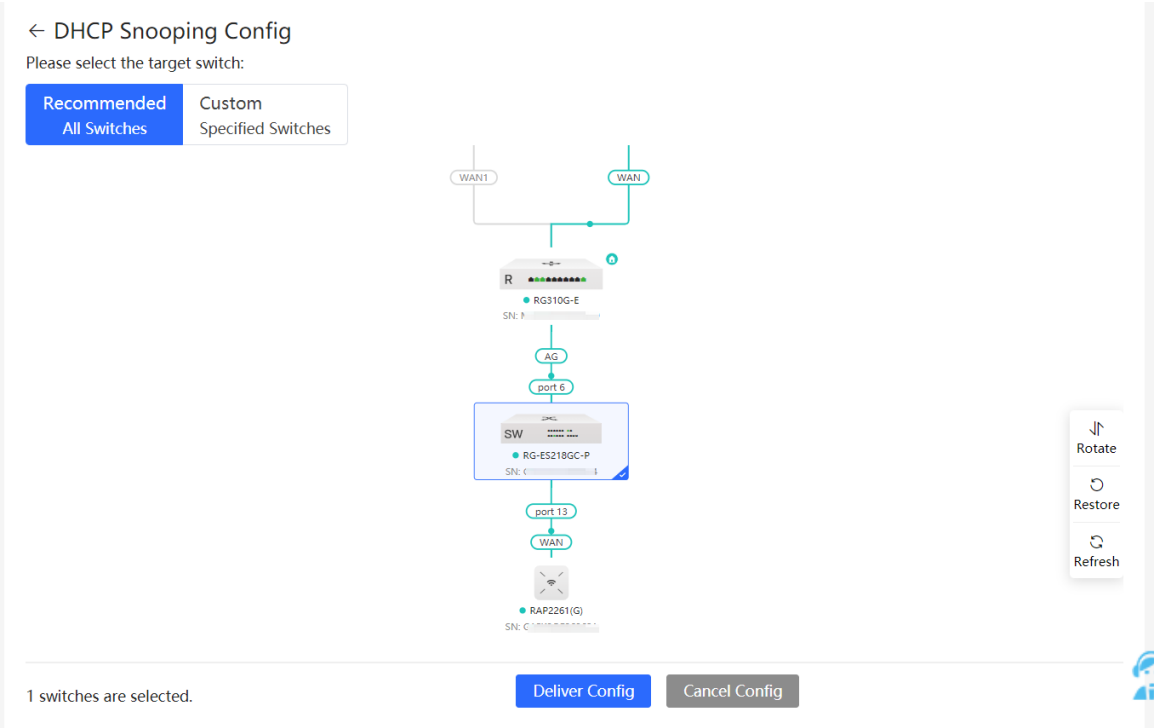
6.2.2 Configuration Steps

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

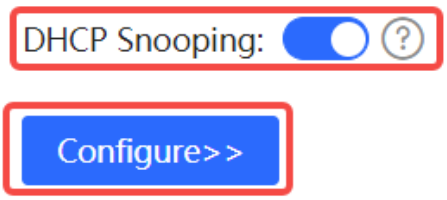
(1) Click **Enable** to access the **DHCP Snooping Config** page.



(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 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.



6.3 Batch Configuring Switches

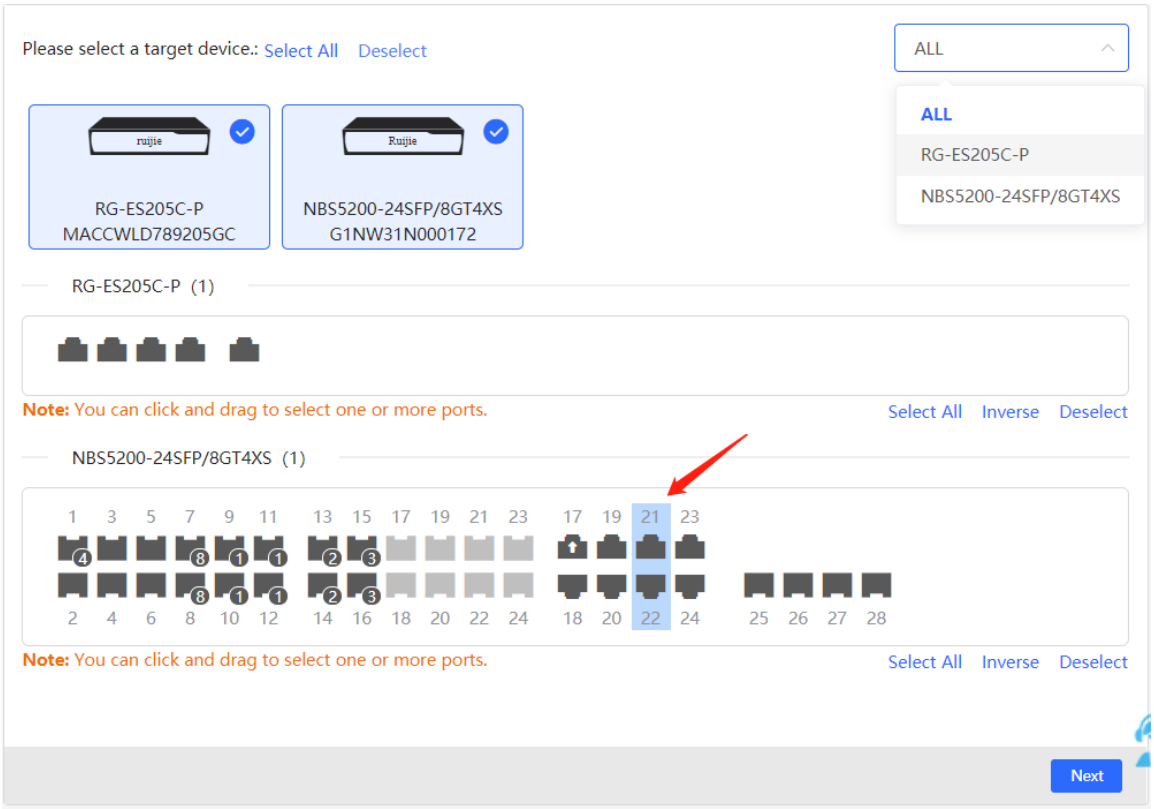
6.3.1 Overview

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

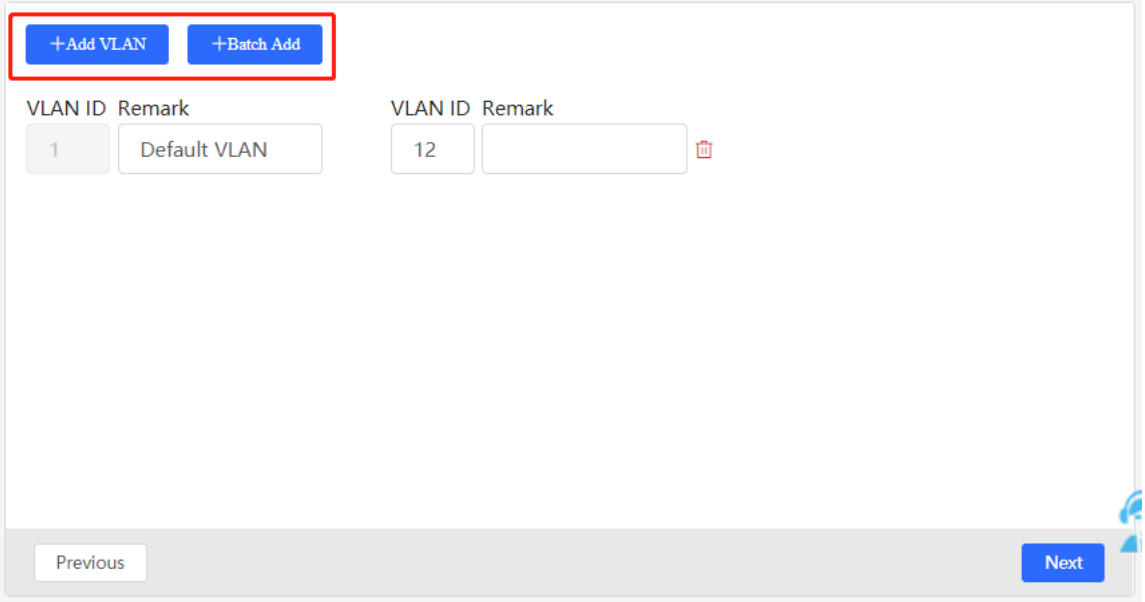
6.3.2 Configuration Steps

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

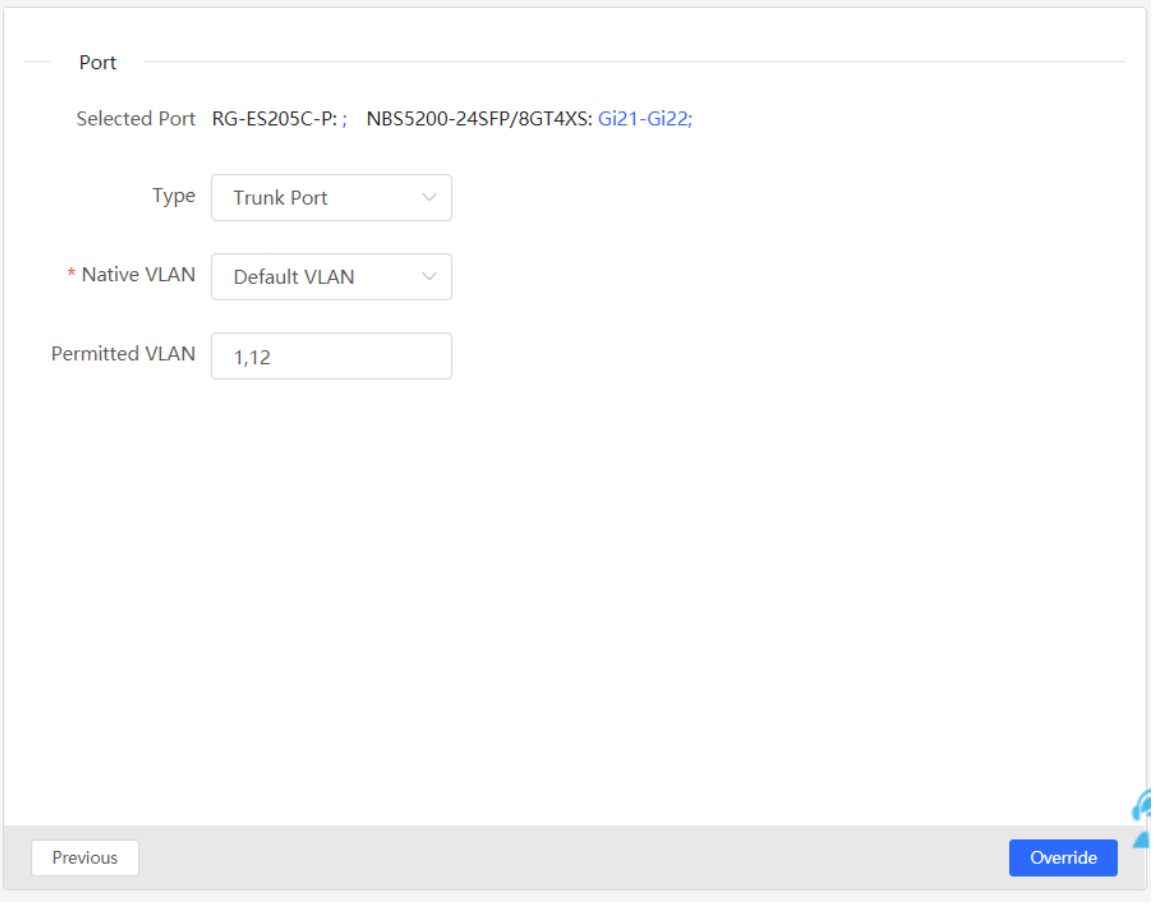
(1) The page displays all switches in the current network. Select the switches to configure, and then select the desired ports in the device port view that appears below. If there are a large number of devices in the current network, select a product model from the drop-down list box to filter the devices.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



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

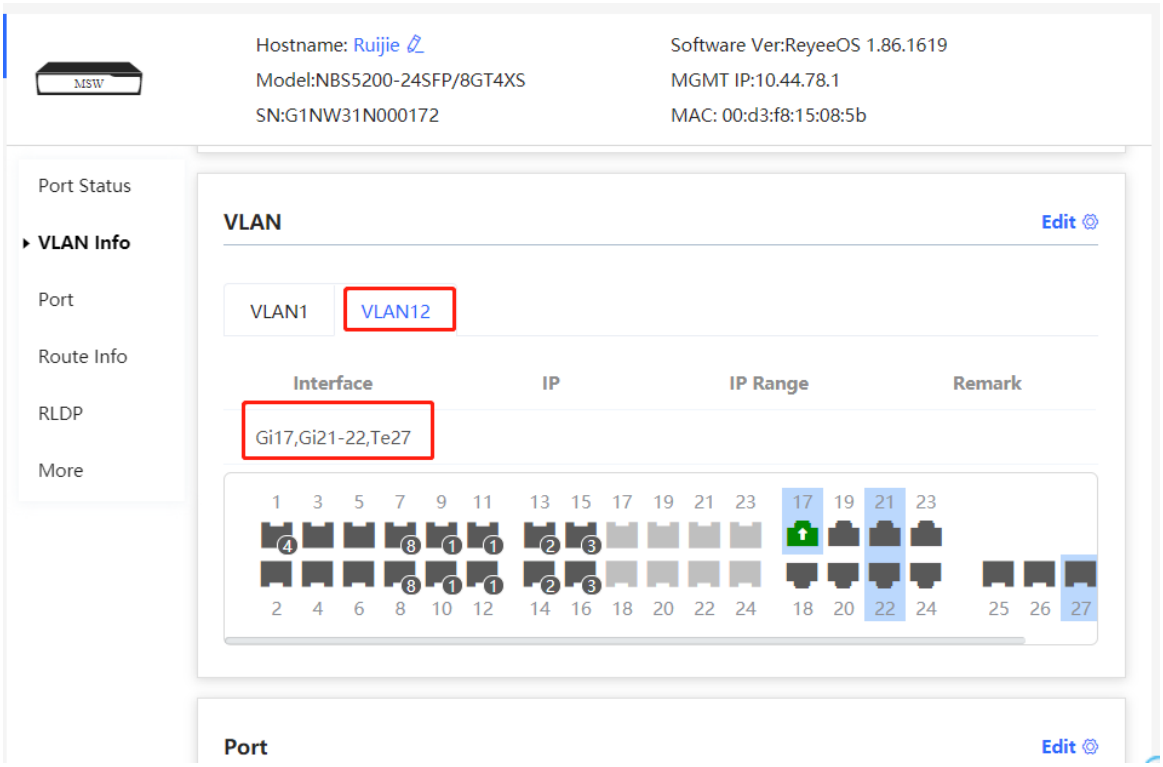


(3) Configure port attributes for the ports selected in Step 1 in a batch. Select a port type. If you set **Type** to **Access Port**, you need to configure **VLAN ID**. If you set **Type** to **Trunk Port**, you need to configure **Native VLAN** and **Permitted VLAN**. After setting the port attributes,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



6.3.3 Verifying Configuration

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



7 Firewall Management

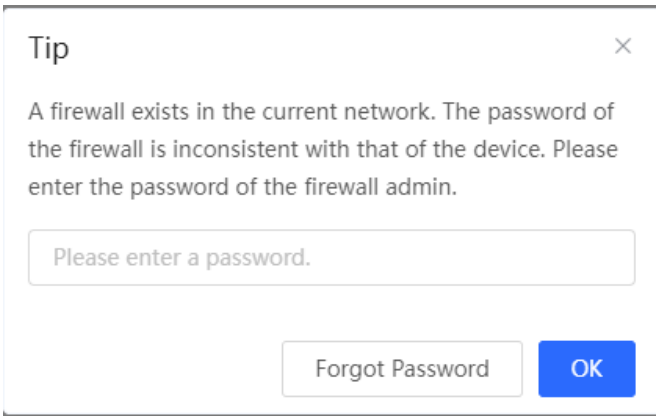
After a firewall is added to the network, you can manage and configure the firewall on the Web management system.

7.1 Viewing Firewall Information

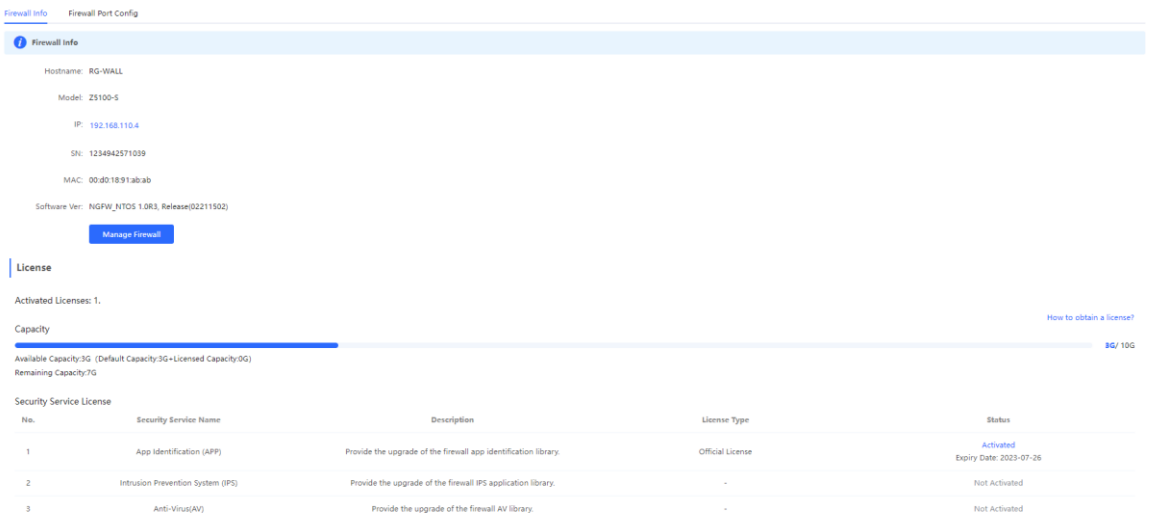
You can view the basic information and license of the firewall on the Web management system.

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**.



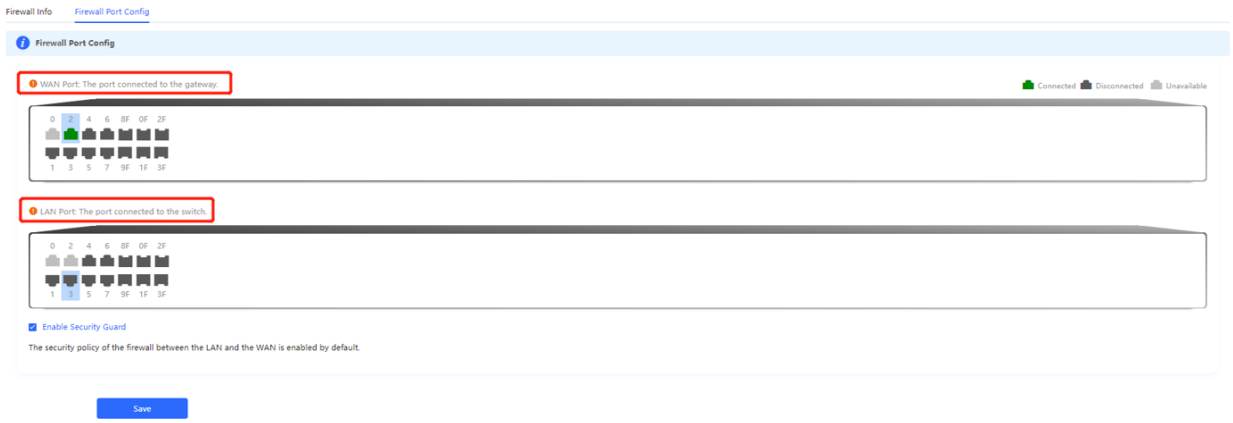
(2) The basic information, capacity, and security service license of the firewall are displayed on the Web management system.



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.

7.2 Configuring Firewall Port

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



8 Online Behavior Management

8.1 Overview

Online behavior management aims to block or prohibit specific Internet access behaviors of LAN users. Online behavior management functions are classified into five categories: app control, website filtering, QQ management, flow control, and access control. The effective range of each behavior management policy is flexibly controlled by the specified client IP address and effective time.

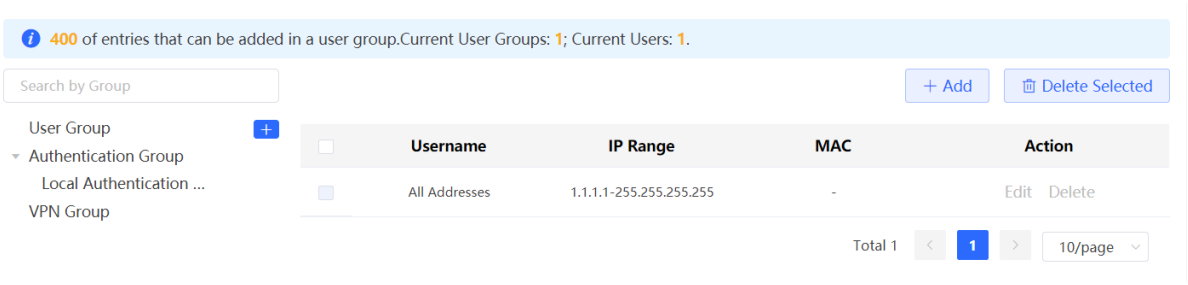
8.2 User Management

8.2.1 Overview

The management policy of online behavior needs to flexibly match with specific user groups. Please manage and classify users before the behavior management policy is configured, ensuring efficient configuration and management. User management is used to maintain user information based on IP addresses. When managing online behaviors, you can limit the effective scope of application blocking, traffic auditing, flow control and other services by specifying created or authenticated users.

A user group contains three default root user groups: user group, authentication group, and VPN user group.

You can create and configure users and user groups in a user group.



Note

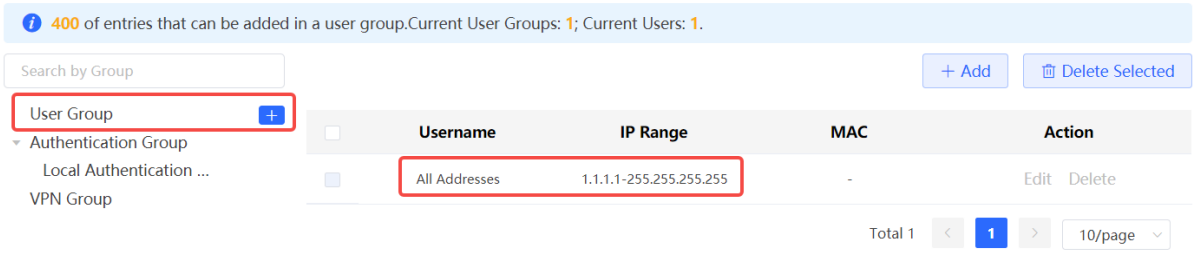
- The system creates a VPN user group by default. The VPN accounts added in the system are automatically added to a VPN user group. You can select a VPN user group to control VPN accounts when you create a policy of application control, network management or flow control.
- RG-EG3XX series devices (such as RG-EG310GH-E) and RG-EG1510XS contain four default root user groups: user group, authentication group, client group, and VPN user group.

8.2.2 User Group

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **User Management**.

You can add new user groups or users below the first-level user group. Up to three levels of grouping is supported. If a user is a leaf node, no users or user groups can be created below this leaf node. A created user group can be used as a configuration item in a behavior management policy and is directly referenced by the user group name.

All Addresses client exists in the user group list by default. The IP range is from 1.1.1.1 to 255.255.255.255. This client cannot be edited or deleted.



1. Creating a User Group

Click + near **User Group** or click **Add** at the upper right of the page. Select the type of **User Group** and enter the group name, and click **OK**. You can create a sub-user group below this user group.

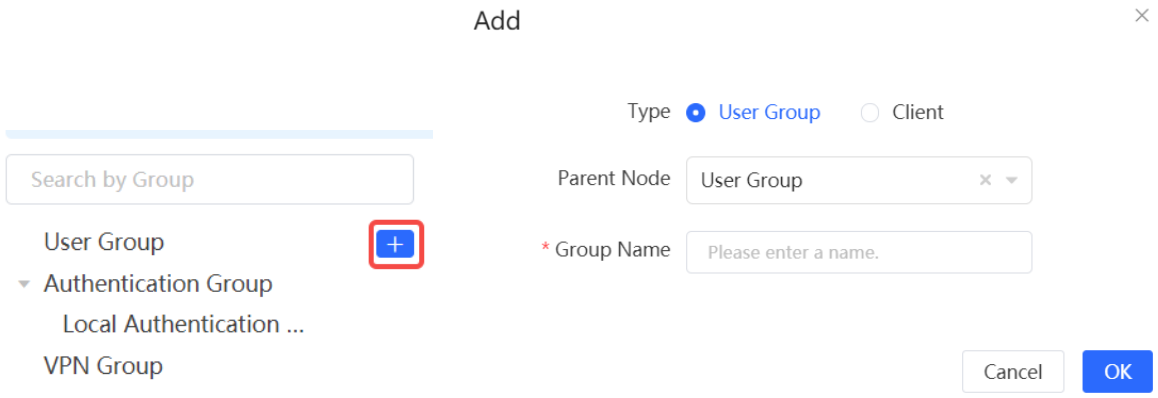


Table 8-1 Parameter Descriptions of User Group

Parameter	Description
Parent Node	Configure the parent group to which the created user group belongs. Up to three levels of groups are allowed below a user group currently (such as Root Node/R&D Center/R&D Section 1). No user groups are allowed below the third-level group.
Group Name	Configure the name of the user group.

2. Creating a User

Click **User Group** to display the users in the current group. Click + or click **Add** at the upper right of the page. Select the type of **Client** and enter the user name and IP range, and click **OK**. You can create a user under the user group.

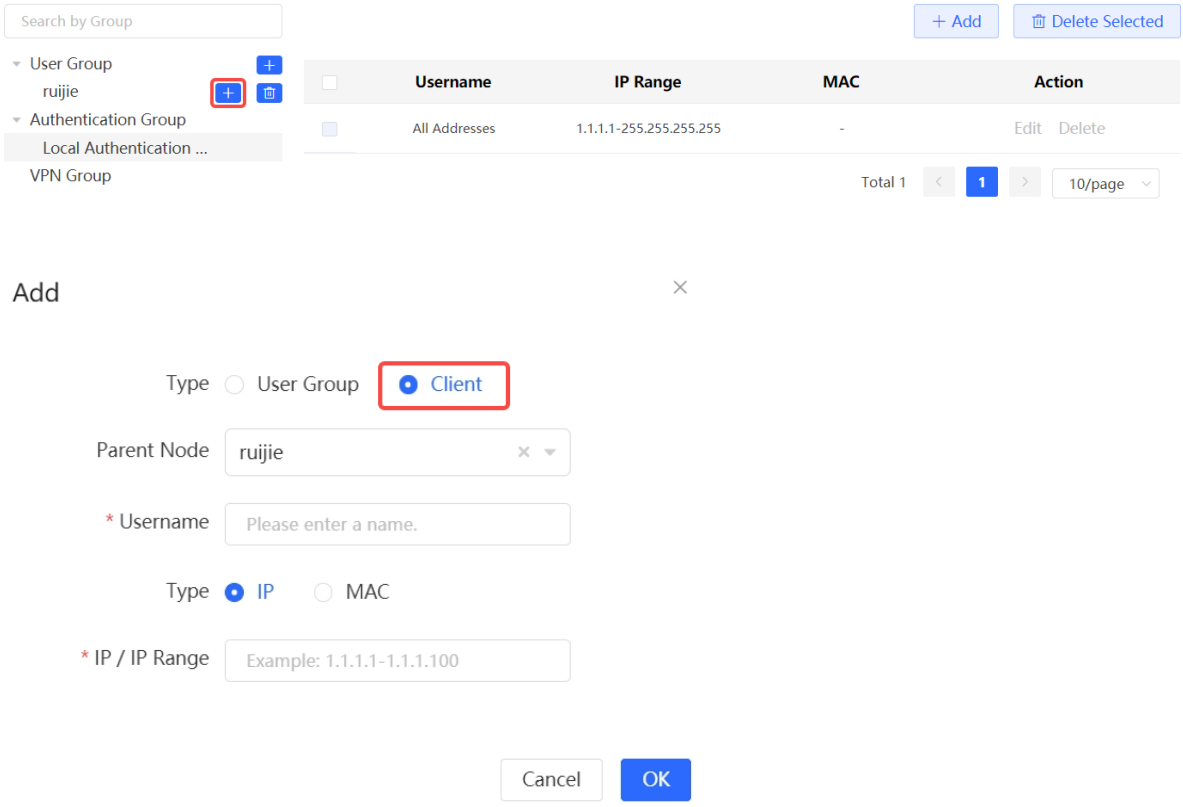
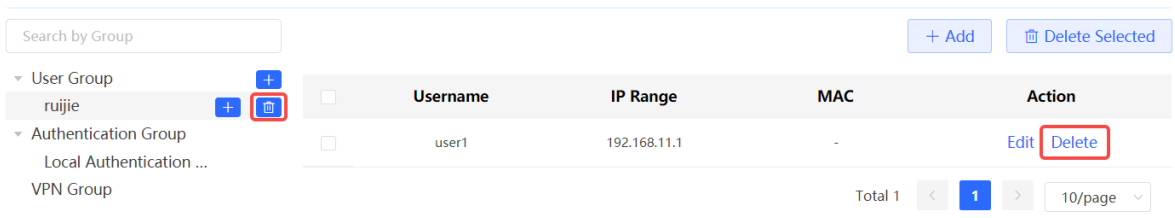


Table 8-2 Parameter Descriptions of User

Parameter	Description
Parent Node	Configure the group to which the created user belongs, Click the drop-down list box to display all the currently created user groups and click to select one group.
Username	Configure the name of the user.
IP /IP Range	Configure the IP address of the user. You can enter an IP address or IP range. If a rule is valid to this user, the rule takes effect in this IP range.

3. Deleting a User Group or a User

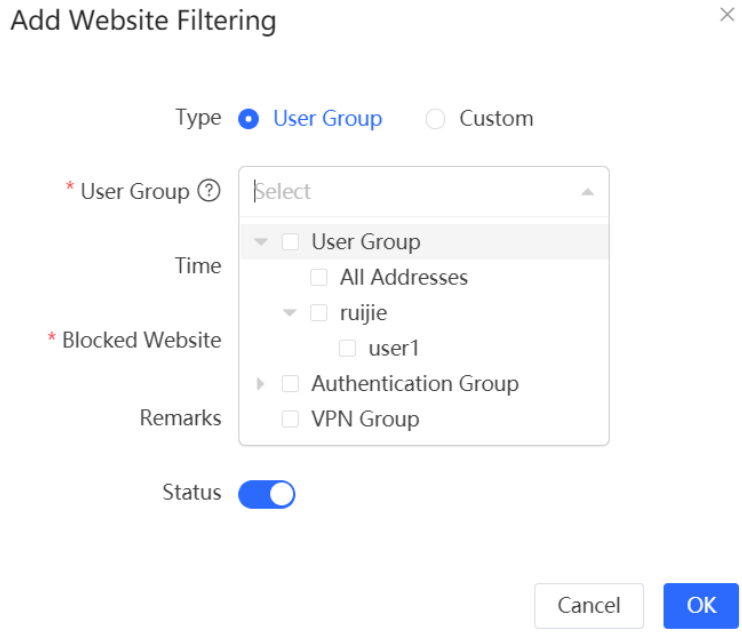
Click  near **User Group** to delete the user group and its members. Click **Delete** in the **Action** bar in the user list to delete the specified user.



4. Verifying Configuration

(1) You can view the created user groups on the left part of the page after user groups and users are configured. Click **User Group** to view user details in this group.

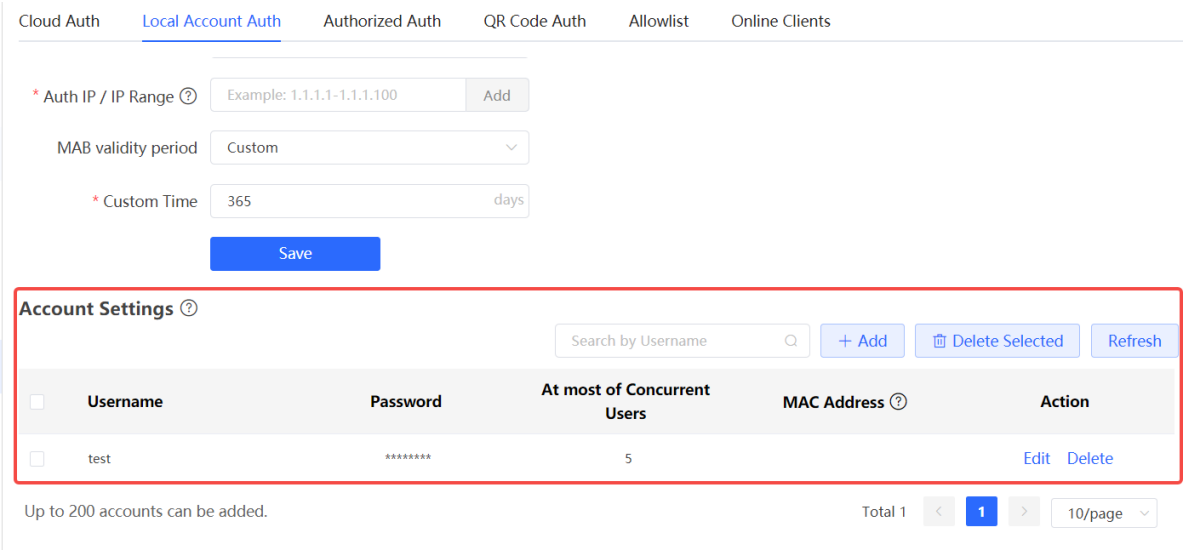
(2) When configuring the behavior management policy (such as adding an application control rule), you can view and select the created user groups and the members.

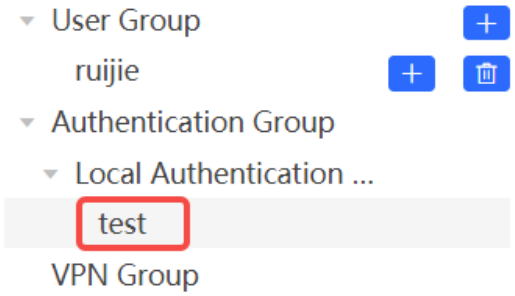


8.2.3 Authentication Group

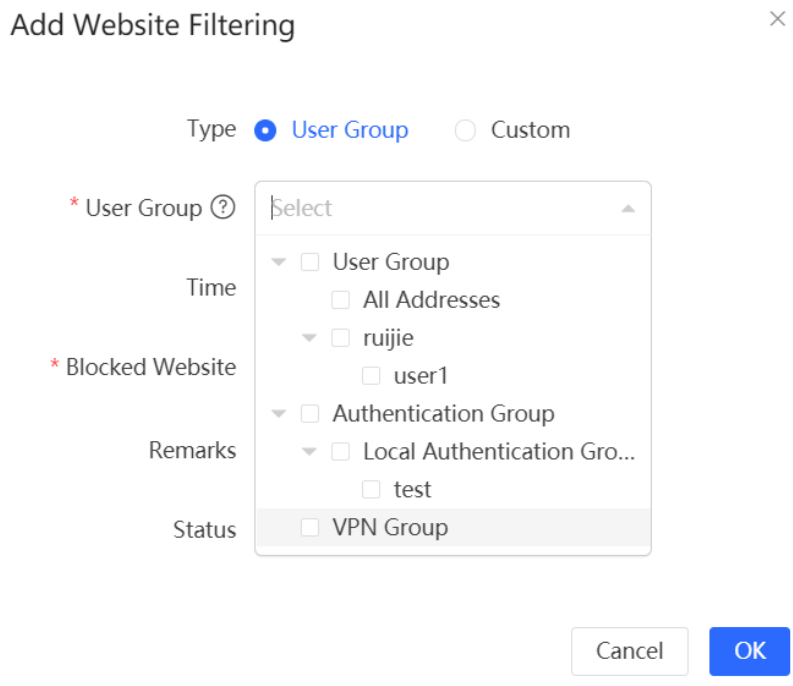
Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **User Management**.

The users in the **Authentication Group** are synchronized from the authentication server to the **Authentication Group**. The local authentication account set by the device (See Section 5.9.5 Local Account Authentication for details.) is automatically synchronized to the **Local Authentication Group**.





When configuring the behavior management policy (such as adding an application control rule), you can configure a policy to take effect in the specified authentication group. After an authenticated user goes online, the user automatically matches with the authentication group and then associates with the behavior management policy, enabling online behavior control over the authenticated user.



8.3 Time Management

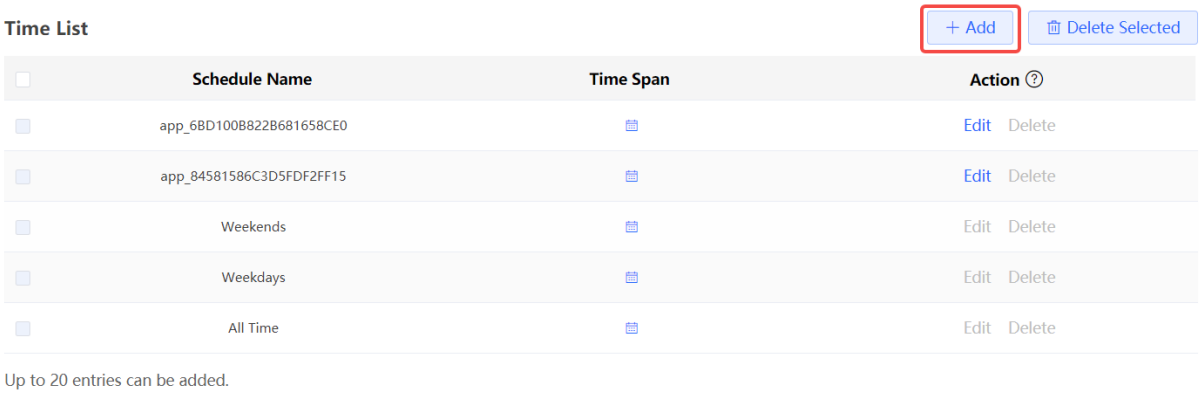
Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Time Management**.

You can create time entries to classify time information. A created time entry can be used as a configuration item in a behavior management policy and is directly referenced by the time entry name.

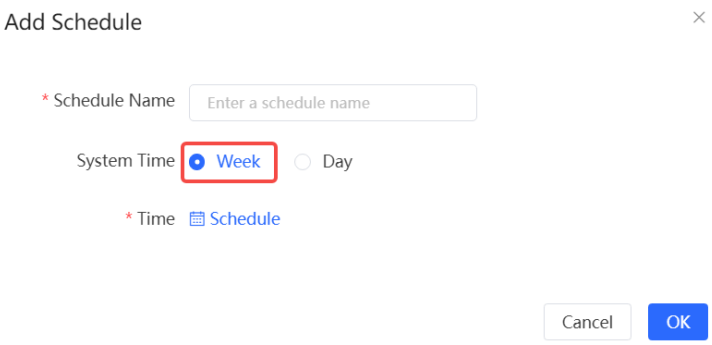
All the created time entries are displayed in the time entry list. In the list, find the target time entry and click **Edit** to modify the time span. Find the target time entry and click **Delete** to delete it. By default, the time entries named **All Time**, **Weekdays**, and **Weekends** are available and they cannot be modified or deleted.

Caution

If a time entry is referenced in any policy, it cannot be deleted on the **Time Management** page. To delete the time entry, remove the reference relationship first.



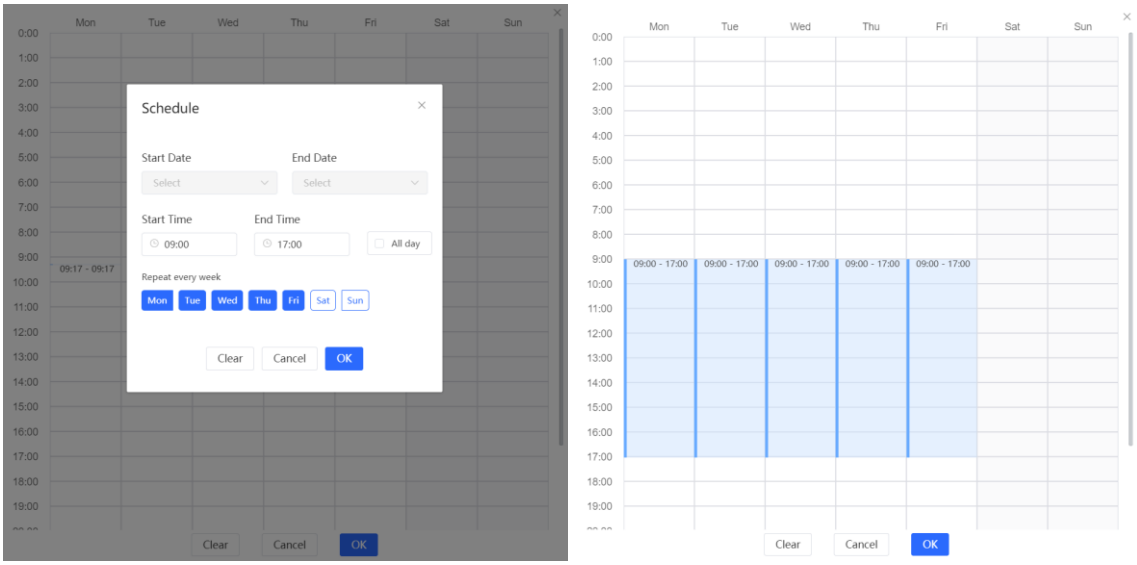
8.3.1 Configuring a Schedule by Week



(1) Click **+Add**. On the **Add Schedule** page that is displayed, enter the name of the schedule.

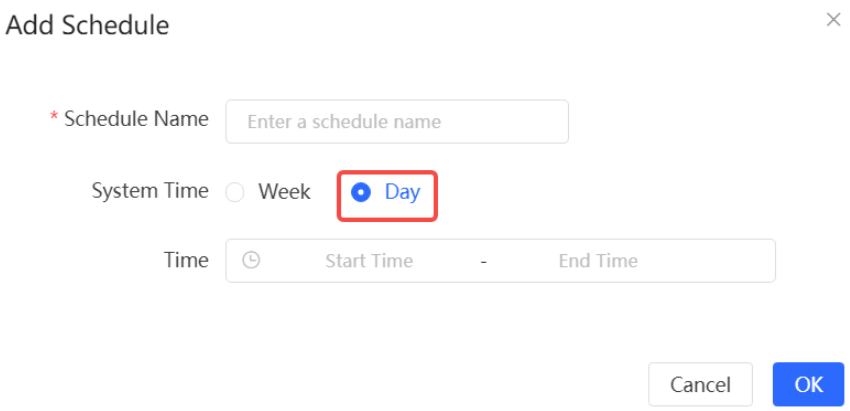
(2) Set **System Time** to **Week**.

(3) Click **Wireless Schedule** to set the time period. On the **Schedule** pop-up box, set the time period to be repeated every week and click **OK**.



(4) Click **OK**.

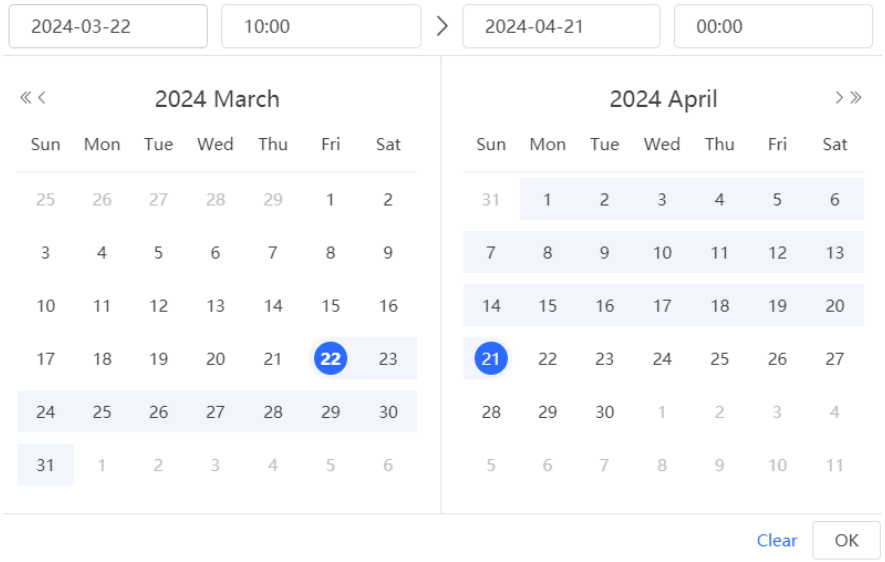
8.3.2 Configuring a Schedule by Date



(1) Click **+Add**. On the **Add Schedule** page that is displayed, enter the name of the schedule.

(2) Set **System Time** to **Day**.

(3) Choose the start and end dates, and click **OK**.



(4) Click **OK**.

8.4 App Control

8.4.1 Overview

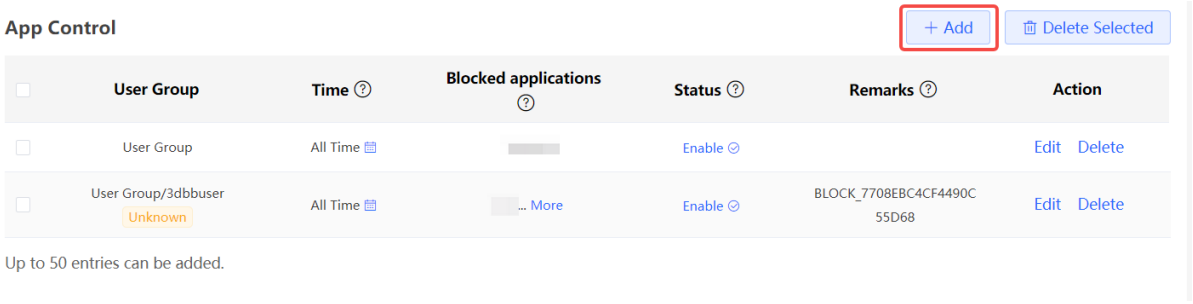
App control aims at controlling the range of specific apps that can be accessed by users. By default, users can access any app. After an app control policy is configured, users in the current network cannot access prohibited apps. App access can be prohibited based on the specified user group and time range. For example, employees in the office network are prohibited from accessing entertainment and game software during work periods to improve network security.

8.4.2 Configuring App Control

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **App Block > App Control**.

1. Configuring App Control

Click **Add** to create an App control policy.



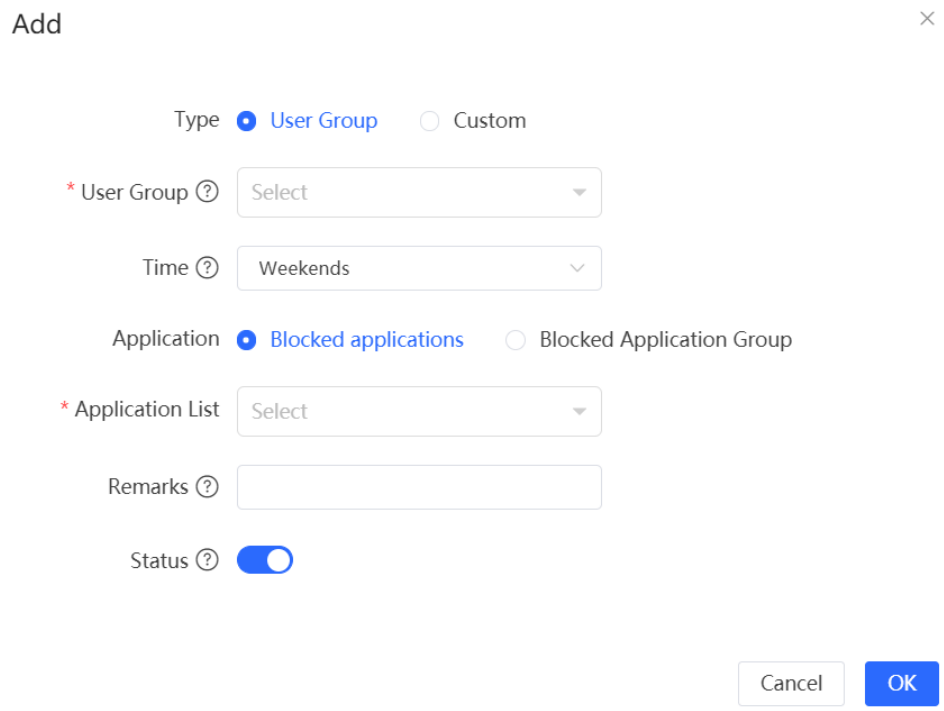


Table 8-3 App control policy configuration

Parameter	Description
Type	● **User Group**: The policy is applicable to users in the specified user group. Please select the target user group. ● **Custom**: The policy is applicable to users in the specified IP range. Please manually enter the managed IP range.
User Group	Select the users managed by the policy from the list of user groups. For the configuration of the user group list, see Section 8.2 User Management. If all members in the user group are selected, the policy takes effect on the user group and is also valid for new members added to this group.
IP Address Group	If the IP range is restricted by the APP control policy and the type of the policy is set to **Custom**, please enter the IP range manually.
Time	Specify the time range under app control. In the specified time range, managed clients cannot access the selected apps in the list of prohibited apps. You can select a time range defined in Section 8.3 Time Management from the drop-down list box, or select **Custom** and manually enter the specific time range.
Application	Specify the applications or application groups to block.
Application List	When **Blocked applications** is selected, you can select the applications that need to be blocked.

Parameter	Description
App Group	When **Blocked Application Group** is selected, you can select the application groups that need to be blocked.
Remarks	Enter the policy description.
Status	Specify whether to enable the app control policy.

8.4.3 Custom App

1. Overview

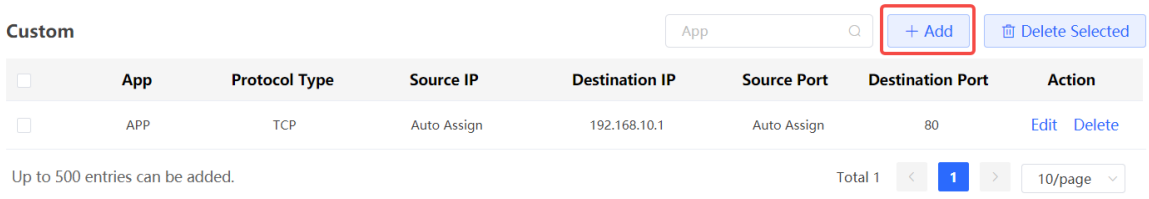
Based on traffic packets of certain websites or apps that are captured by the device, users can analyze and extract 5-tuple information characteristics (protocol, source IP address, source port, destination IP address, and destination port) of the packets. You can define apps that are not in the default application list.

After custom apps are configured successfully, you can configure control policies for custom apps on the app control page to block users from accessing the custom apps on the current network.

2. Procedure

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **App Block** > **Custom**.

(1) Click **Add**. Enter information about a custom app.



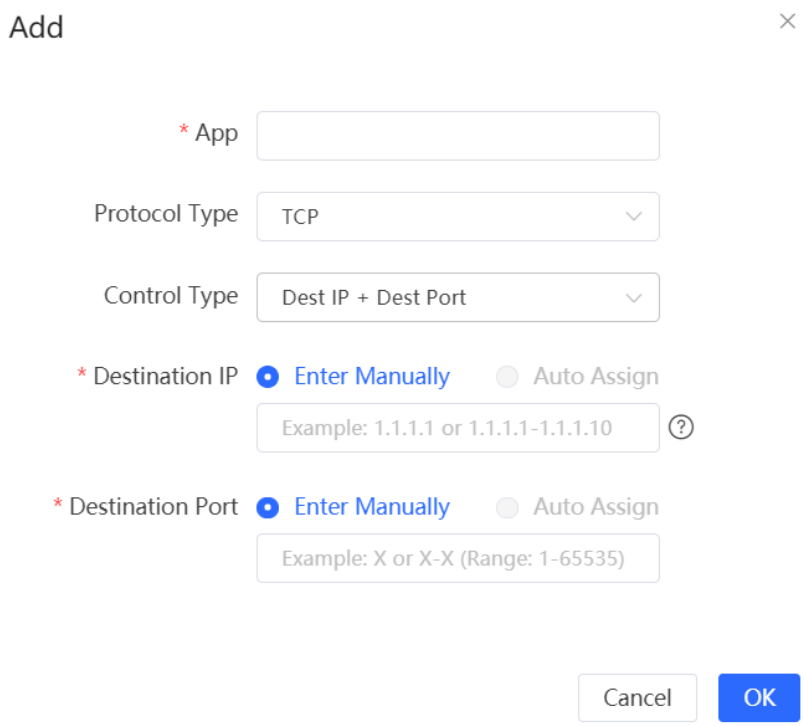


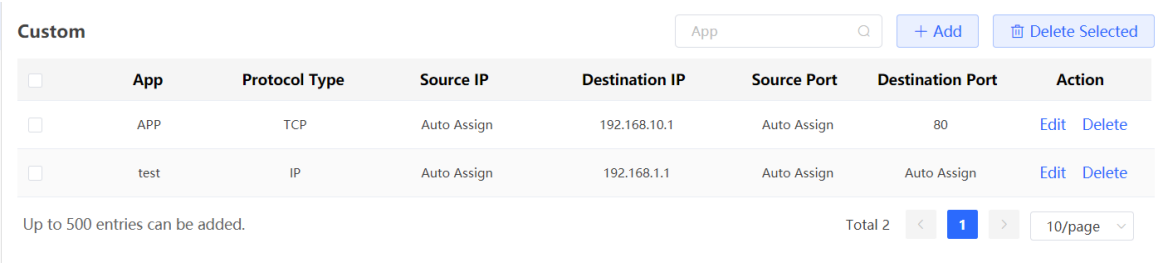
Table 8-4 Description of Custom App Configuration

Parameter	Description
App	Configure the app name (the name cannot be duplicated with a name in the app list).
Protocol Type	Select a protocol type based on the protocol used by captured packets. It can be set to **TCP**, **UDP**, or **IP**.
Control Type	Select a rule type based on 5-tuple information characteristics of extracted packets. It can be set to the following: ● Src IP + Src Port ● Dest IP + Dest Port ● Src IP+ Dest IP
Source/Destination IP	Enter a characteristic IP address.
Source/Destination Port	Enter a characteristic port number.

Note

- If **Control Type** is set to **Src IP + Src Port**, you need to set the source IP address and source port.
- If **Control Type** is set to **Dest IP + Dest Port**, you need to set the destination IP address and destination port.
- If **Control Type** is set to **Src IP + Dest IP**, you need to set the source and destination IP addresses. The source IP address can be also to **Auto Assign**.

(2) Click **OK**.



8.4.4 Custom Application Group

1. Overview

You can add multiple applications with the same features into a customer application group, which is a logical group. The custom application group can be used for policy.

The system has a default blocking group to block applications. (The blocking group is associated with relevant applications by default.) The applications added to the blocking group are directly blocked.

2. Procedure

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **App Block** > **Custom Application Group**.

(1) Click **Add** to configure the parameters for an application group.

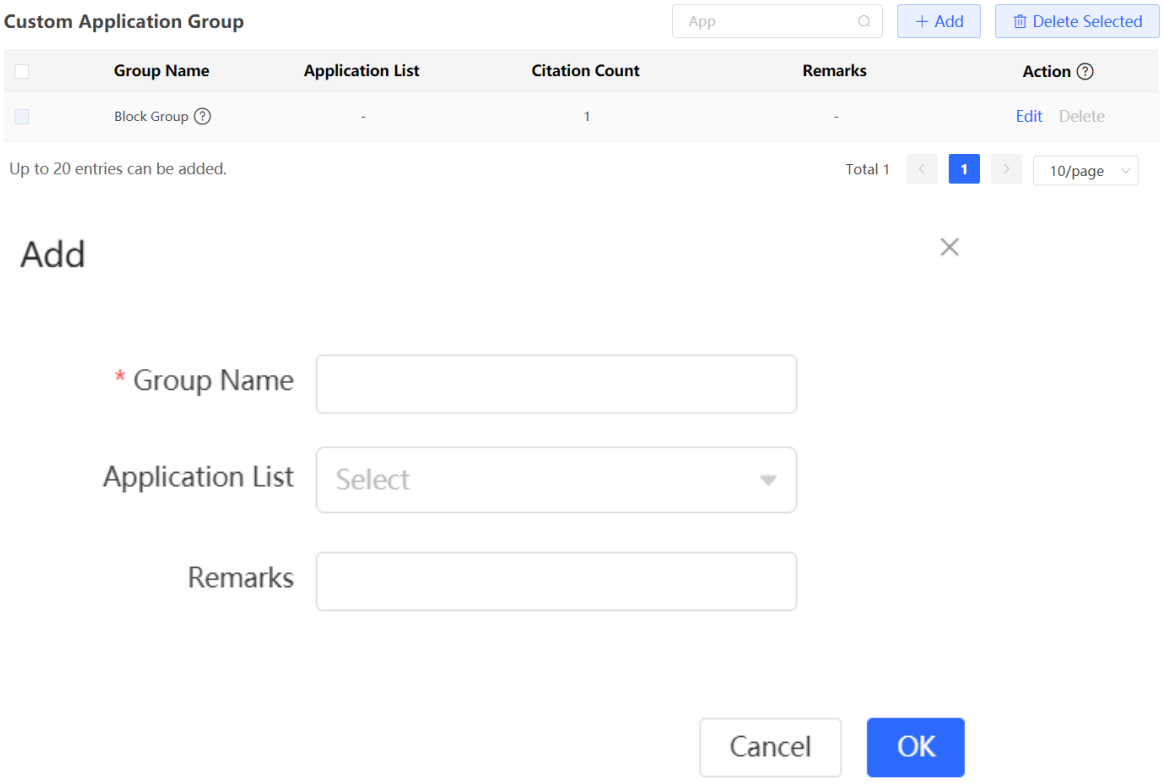


Table 8-5 Custom Application Group

Parameter	Description
Group Name	The application group name customized by a user. (The group name must differ from the application names in the group list.)

Parameter	Description
Application List	Multiple applications involved in an application group.
Remark	Description of an application group.

(2) Click **OK**.

8.5 Website Management

8.5.1 Overview

Website management consists of website grouping and website filtering. Website grouping refers to the classification of website URLs. You can modify existing website groups or create new website groups. Website filtering refers to access control to existing website groups to prohibit user access to websites in specific groups. Website filtering can be applied based on the specified user group and time range. For example, employees in the office network are prohibited from accessing game websites during work periods to improve network security.

8.5.2 Configuration Steps

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Website Management**.

1. Configuring Website Groups

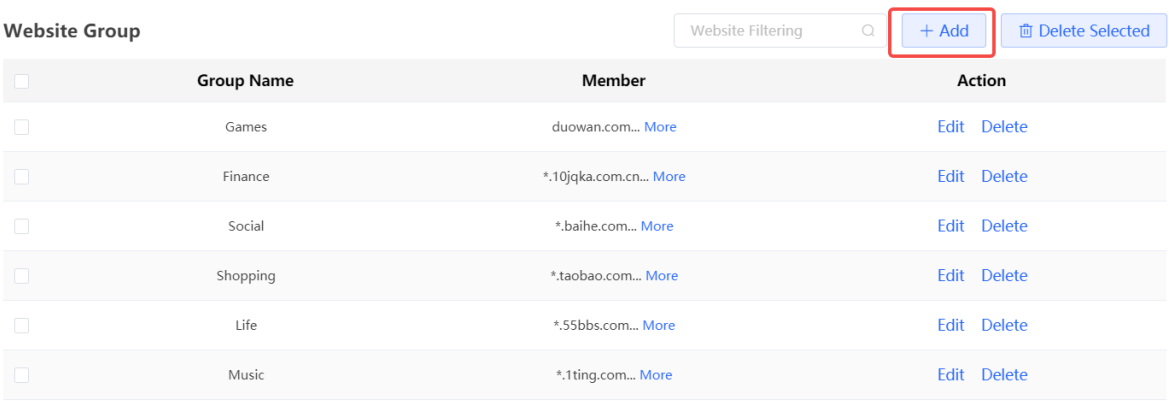
Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Website Management** > **Website Group**.

Click the **Website Group** tab. On the page that appears, all the created website groups are displayed in the list. Find the target group and click **More** in the **Member** column to view all the website URLs in the group. Find the target group and click **Edit** in the **Action** column to modify the member website URLs in the group. Find the target group and click **Delete** in the **Action** column to delete the group.

Click **Add** to create a new website group.

Caution

If a website filtering rule in a website group is being referenced, the group cannot be deleted from the website group list. To delete this group, modify the website filtering configuration to remove the reference relationship first.



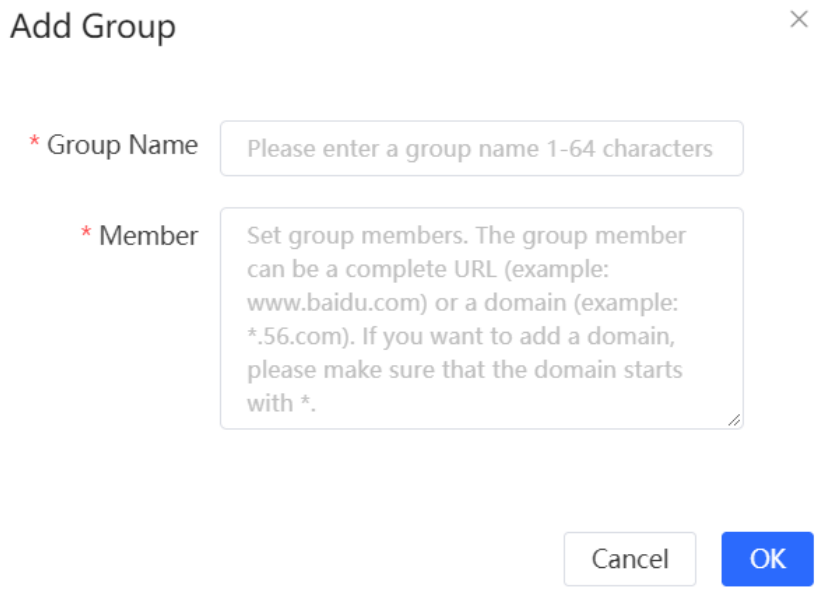


Table 8-6 Website group configuration

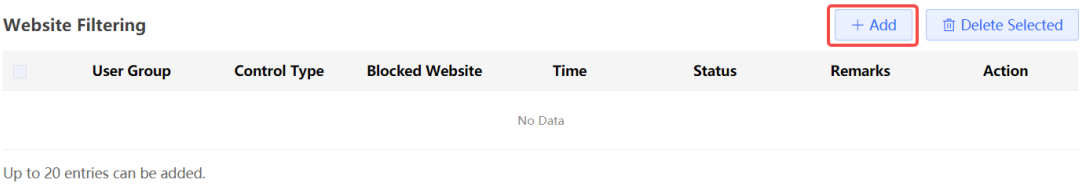
Parameter	Description
Group Name	Configure a unique name for the website group. The name can be a string of 1 to 64 characters.
Member	Specify members in the website group. You can enter multiple websites in a batch. The group member can be complete URL (such as www.baidu.com) or keywords in the URL (domain name with a wildcard in front, such as *.baidu.com). The wildcard can only appear at the beginning of a URL, and it cannot be in the middle or end of the domain name.

2. Configuring Website Filtering

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Website Management** > **Website Filtering**.

(1) Click the **Website Filtering** tab. On the page that appears, all the created website filtering rules are displayed in the list.

(2) Click **Add** to create a website filtering rule.



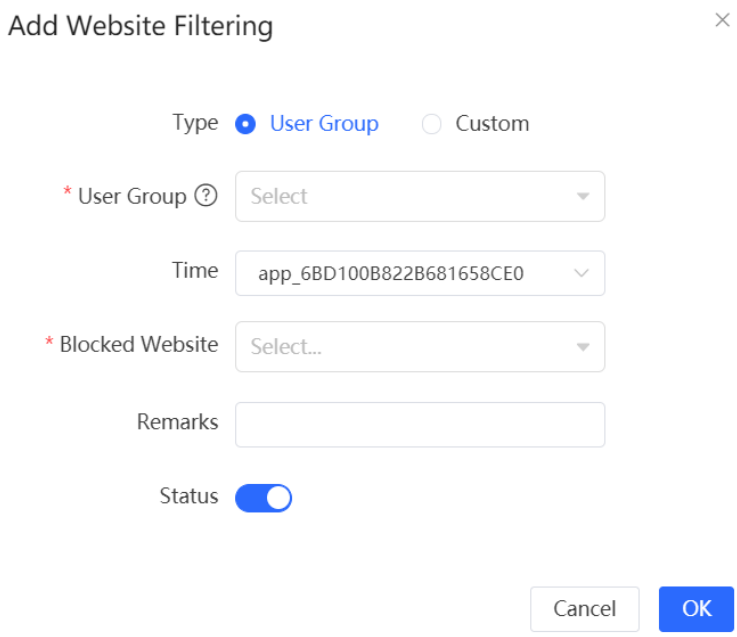


Table 8-7 Website filtering rule configuration

Parameter	Description
Type	● **User Group**: The policy is applicable to users in the specified user group. Please select the target user group. ● **Custom**: The policy is applicable to users in the specified IP range. Please manually enter the managed IP range.
User Group	Select the users managed by the policy from the list of user groups. For the configuration of the user group list, see Section 8.2.2 User Group. If all members in the user group are selected, the policy takes effect on the user group and is also valid for new members added to this group.
IP Address Group	If the IP range is restricted by the APP control policy and the type of the policy is set to **Custom**, please enter the IP range manually.
Time	Specify the time range under website filtering control. In the specified time range, managed clients cannot access the prohibited websites. You can select a time range defined in Section 8.3 Time Management from the drop-down list box, or select **Custom** and manually enter the specific time range.
Blocked Website	Configure the type of websites to block. You can select an existing website group. After a website group is selected, users are prohibited from accessing all websites in this group. For details on how to create or modify a website group, see Configuring Website Groups.
Remarks	Enter the rule description.

Parameter	Description
Status	Specify whether to enable the website filtering rule.

After the website filtering rules are configured, click **Edit** to modify the rule information. Click **Delete** to delete the specific filtering rule.

8.6 Flow Control

8.6.1 Overview

Flow control is a mechanism that classifies flows based on certain rules and processes flows using different policies based on their categories. You can configure flow control to guarantee key flows and suppress malicious flows. You can enable flow control when the bandwidth is insufficient or flows need to be distributed properly.

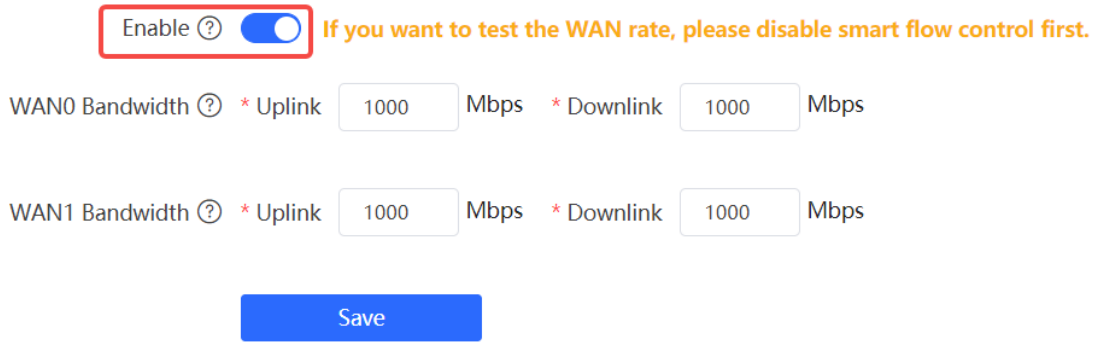
8.6.2 Smart Flow Control

1. Overview

When you need to limit the uplink traffic and downlink traffic bandwidth of the device ports (such as WAN and WAN 1), you can enable the smart flow control function. After the line bandwidth is configured for a port, the uplink and downlink traffic of the port will be limited within the specified range. In addition, the per user bandwidth should be intelligently adjusted according to the number of users to ensure that users fairly share the bandwidth.

2. Configuration Steps

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Flow Control** > **Smart Flow Control**.



Turn on **Enable** on the **Smart Flow Control** tab and set the line bandwidth based on the bandwidth actually allocated by the ISP. If the device has multiple lines, you can set the bandwidth for these WAN interfaces separately. For details on the multi-line configuration, see 4.2 Port Settings.

Click **Save** to make the configuration take effect.

Caution

Enabling flow control will affect network speed testing. If you want to test the network speed, disable flow control first.

Table 8-8 Smart flow control configuration

Parameter	Description
Enable	Specify whether to enable the smart flow control function. By default, smart flow control is disabled.
WAN Bandwidth	Set the uplink and downlink bandwidth limits for the WAN interfaces, in Mbit/s.

Note

Smart flow control can be used to control the line traffic in different networking modes, including bandwidth-based, static IP address, and dynamic IP address.

8.6.3 Custom Policies

1. Overview

Custom policies are used to restrict the traffic with specific IP addresses based on the smart flow control function, thereby meeting the bandwidth requirements of specific users or servers. When you create a custom flow control policy, you can flexibly configure the limited user range, the bandwidth limit, the limited application traffic, and the rate limit mode. When a custom policy is enabled, it takes precedence over the smart flow control configuration.

Custom policies fall into common policies and VPN policies.

Common policies include the custom policies configured on the web interface or Ruijie Cloud and the flow control policies configured on Ruijie Cloud for authentication accounts. Common policies manage common traffic.

Common policies and VPN policies are used to manage common traffic and VPN traffic, respectively.

2. Getting Started

Before you configure a custom policy, enable smart flow control first. For details, see Section 8.6.2 Smart Flow Control.

3. Configuring a Normal Policy

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Flow Control** > **Custom Policy**.

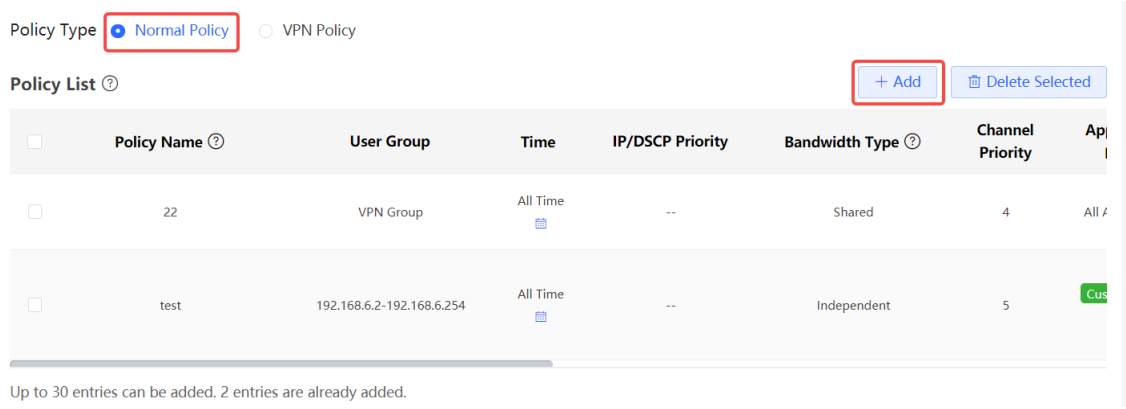
Note

The flow control policies configured on Ruijie Cloud and the web interface are displayed in the **Normal Policy** list. The flow control policies for authentication accounts configured on Ruijie Cloud cannot be edited or deleted on the web interface. You can only enable or disable these policies and change the priority of them.

(1) Set **Policy Type** to **Normal Policy** and click **Add** to create a custom flow control policy.

You can set up to 30 custom common policies, including the custom policies configured on the web interface and Ruijie Cloud.

You can set up to 20 flow control policies for authentication accounts on Ruijie Cloud. The web interface only displays these policies.



(2) Configure items related to a common policy.

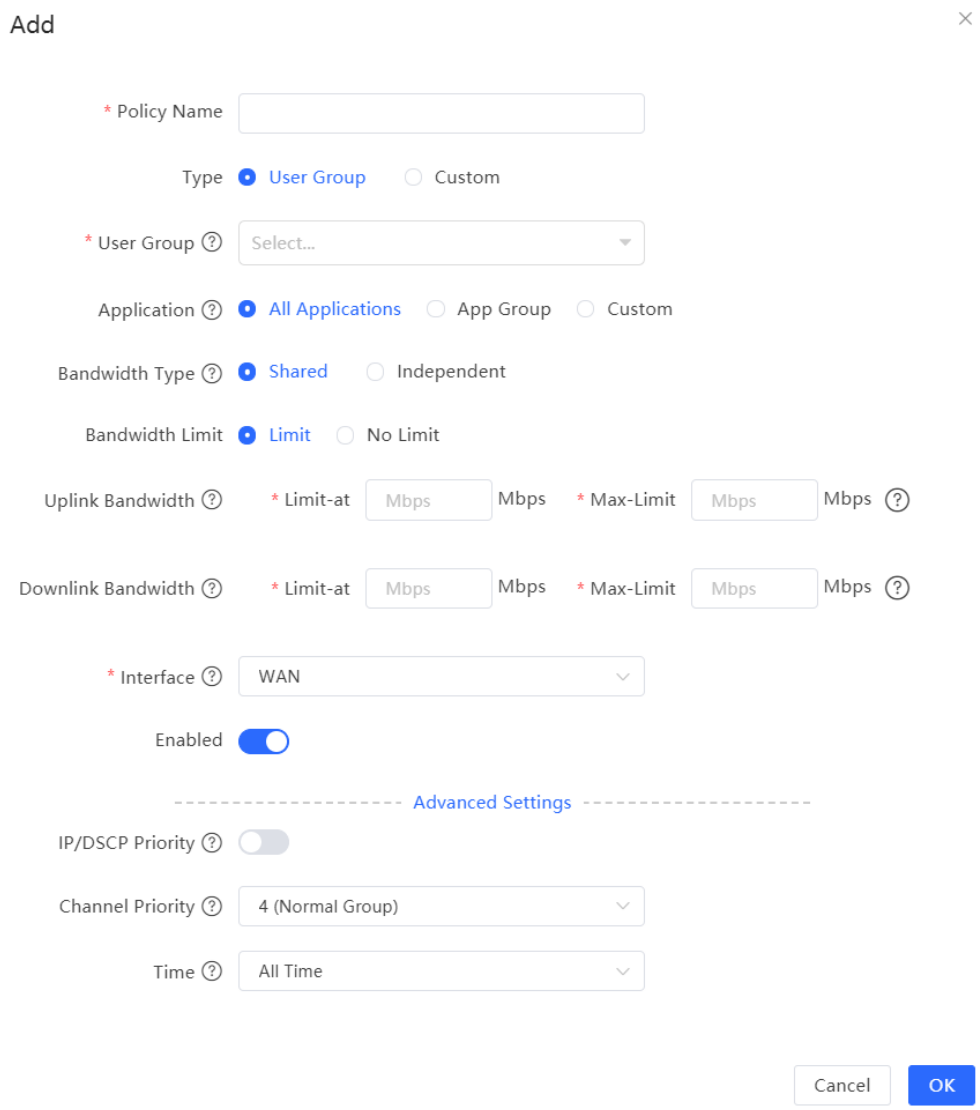


Table 8-9 Configuration of a Custom Policy

Parameter	Description
Policy Name	A policy name uniquely identifies a custom flow control policy. It cannot be modified.
Type	The type of a flow control policy can be set to the following: ● **User Group**: Indicates that the policy is applied to users in a specified user group. You need to select a user group to be managed. ● **Custom**: Indicates that the policy is applied to users in a specified IP address segment. You need to manually enter the IP address range to be managed.
User Group	Select a user to be managed by the policy from the user group list. For details about how to set the user group list, see 8.2 User Management. If you select all members of a user group, the policy takes effect on the entire user group (it also takes effect on members added to the user group later). This parameter is required when **Type** is set to **User Group**.
IP/IP Range	Specify the IP address range for the flow control policy to take effect. When **Type** is set to **Custom**, enter the IP address manually. You can enter a single IP address or an IP address segment. This parameter is required when **Type** is set to **Client**. The IP address range must be within a LAN segment. You can choose **One-Device** > **Gateway > Monitor** > **Ethernet status** to check the network segment of the current LAN port. For example, the network segment of the LAN port shown in the figure below is 192.168.2.0/24. 
Application	When **Bandwidth Type** is set to **Shared**, the flow control policy can be configured to take effect only on specified applications. ● **All Applications**: Indicates that the flow control policy takes effect on all applications in the current application library. ● **Custom**: Indicates that the flow control policy takes effect only on specified applications in the application list. ● **Application Group**: Indicates that the flow control policy takes effect only on specified applications in the application list. For details about how to set the application group list, see 8.4.4 Custom Application Group. When **Bandwidth Type** is set to **Independent**, some models do not support application selection and the flow control policy takes effect on all applications in the current application library by default. For the models, contact technical support engineers.
Application List	When **Application** is set to **Custom**, it specifies the applications, on which the policy takes effect. The traffic of the selected applications is subject to the policy.

Parameter	Description
Application Group	When **Application** is set to **Application Group**, it specifies the application groups, on which the policy takes effect. The traffic of the selected application group is subject to the policy.
Bandwidth Type	● **Shared**: Indicates that all users in a user group (all IP addresses in an address range) share the configured uplink and downlink bandwidths, and the bandwidth of a single user is not limited. ● **Independent**: Indicates that all users in a user group (all IP addresses in an address range) share the configured uplink and downlink bandwidths, and the maximum bandwidth of a single user can be limited.
Bandwidth Limit	Configure whether to limit the bandwidth. ● **Limit**: You can set the uplink and downlink bandwidth limits as needed. ● **No Limit**: When the bandwidth is sufficient, the maximum bandwidth is not limited. When the bandwidth is insufficient, the minimum bandwidth cannot be guaranteed.
Uplink/ Downlink Bandwidth	Configure the data transmission rate in uploading and downloading, in Mbps. It includes Limit-at, Max-Limit, and Max-Limit per User. ● **Limit-at**: Specifies the minimum bandwidth that can be shared by all users when the bandwidth is insufficient. ● **Max-Limit**: Specifies the total maximum bandwidth that can be occupied by all users when the bandwidth is sufficient. ● **Max-Limit per User**: Specifies the maximum bandwidth that can be occupied by each user when multiple users share the bandwidth. It is optional and can be configured only when **Bandwidth Type** is set to **Independent**. The rate is not limited by default.
Interface	Specify the WAN interface, on which the policy takes effect. When it is set to **All WAN Ports**, the policy will be applied to all WAN interfaces.
Enabled	Set whether to enable the flow control policy. If it is disabled, the policy does not take effect.
IP/DSCP Priority	Specifies the priority of packets to differentiate various types of traffic and allocate different levels of service quality. Flow control policies are applied based on the IP/DSCP field in the packet.
Channel Priority	Specify the traffic guarantee level. The value range is from 0 to 7. A smaller value indicates a higher priority and the value **0** indicates the highest priority. Different traffic priority values correspond to different application groups in an application template. **2** indicates the key group, **4** indicates the normal group, and **6** indicates the suppression group. For the description of application groups in a priority template, see 8.6.4 Application Priority.
Time	Specifies the time period during which the rule takes effect. You can choose from existing time rules or create custom ones.

(3) Click **OK**.

4. Configuring a VPN policy.

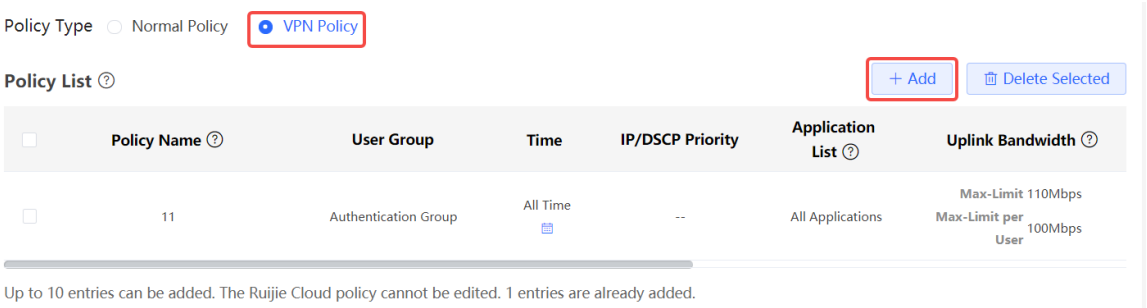
Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Flow Control** > **Custom Policy**.

Note

The flow control policies configured on Ruijie Cloud and the web interface are displayed in the **Normal Policy** list. The flow control policies for authentication accounts configured on Ruijie Cloud cannot be edited or deleted on the web interface. You can only enable or disable these policies and change the priority of them.

(1) Set **Policy Type** to **VPN Policy** and click **Add** to create a custom VPN flow control policy.

A maximum of 10 VPN policies can be configured.



(2) Configure items related to a VPN policy.

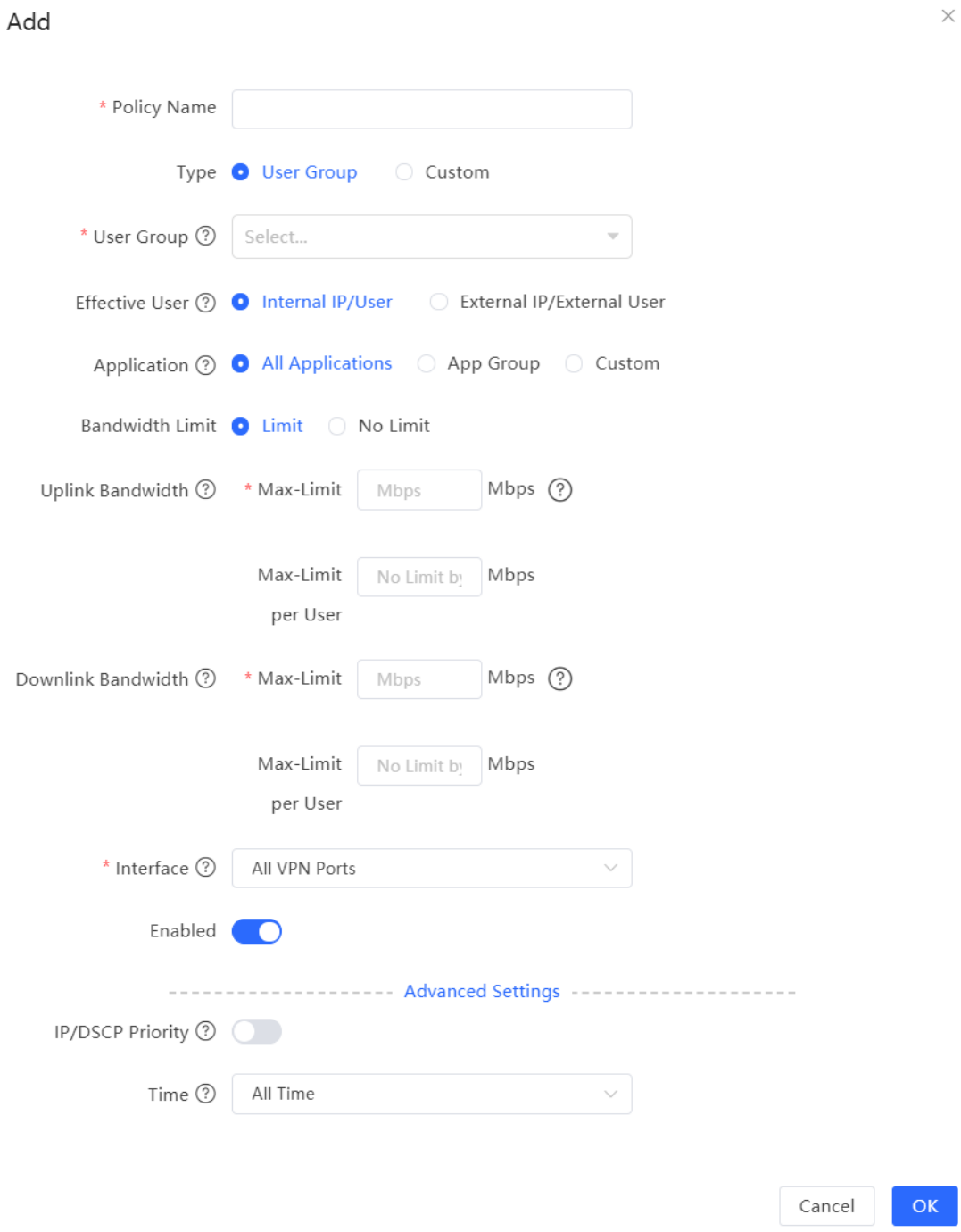


Table 8-10 Configuration of a Custom VPN Policy

Parameter	Description
Policy Name	A policy name uniquely identifies a custom flow control policy. It cannot be modified.
Type	The type of a flow control policy can be set to the following: ● **User Group**: Indicates that the policy is applied to users in a specified user group. You need to select a user group to be managed. ● **Custom**: Indicates that the policy is applied to users in a specified IP address segment. You need to manually enter the IP address range to be managed.

Parameter	Description
User Group	Select a user to be managed by the policy from the user group list. For details about how to set the user group list, see 8.2 User Management. If you select all members of a user group, the policy takes effect on the entire user group (it also takes effect on members added to the user group later). This parameter is required when **Type** is set to **User Group**.
IP/IP Range	Enter an IP address or IP range manually. This parameter is required when **Type** is set to **Client**.
Effective User	Specify the type of effective users. It can be set to the following: ● **Internal IP/User**: For a gateway, IP addresses of clients connected to the gateway are internal IP addresses. ● **External IP/External User**: For a gateway, non-gateway internal IP addresses are external IP addresses. The configuration suggestions are as follows: ● When clients are configured to control VPN traffic, select **Internal IP/ User** to control the traffic of internal network users. When the VPN server is configured to control the VPN traffic, select **External IP/External User** to control the traffic of external network users. ● For the VPN of the NAT model, the external IP address of the server must be in the IP address segment of the VPN address pool. ● For the VPN in router mode, the IP address segment must be set to IP addresses of restricted users. For the VPN in router mode, to configure flow control on internal IP addresses of clients, set internal IP addresses to the IP addresses of the flow control objects. Note: The external IP address configured by the Open VPN server is the IP address of the address pool. The internal IP address configured by the client is the actual IP address of the client.
Application	● **All Applications**: Indicates that the flow control policy takes effect on all applications in the current application library. ● **Custom**: Indicates that the flow control policy takes effect only on specified applications in the application list. ● **Application Group:** Indicates that the flow control policy takes effect only on specified application groups. The traffic of applications involved in the application group is subject to the policy. For details about how to set the application group list, see 8.4.4 Custom Application Group.
Application List	When **Application** is set to **Custom**, it specifies the applications, on which the policy takes effect. The traffic of the selected applications is subject to the policy.
Application Group	When **Application** is set to **Application Group**, it specifies the application group, on which the policy takes effect. The traffic of the selected application group is subject to the policy.
Bandwidth Limit	Configure whether to limit the bandwidth. ● **Limit**: You can set uplink and downlink bandwidth limits as needed. ● **No Limit**: When the bandwidth is sufficient, the maximum bandwidth is not limited. When the bandwidth is insufficient, the minimum bandwidth is not guaranteed.

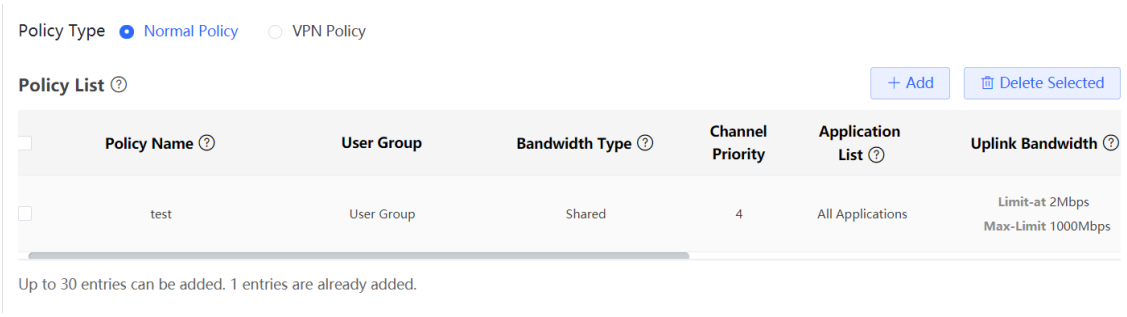
Parameter	Description
Uplink/ Downlink Bandwidth	Configure the maximum uplink/downlink bandwidth shared by VPN users matching the policy in Mbps. When the bandwidth is shared by multiple users, you can also set the maximum uplink/downlink bandwidth per user in Mbps. The uplink/downlink bandwidth is not limited by default. Note: The parameter is valid when **Bandwidth Limit** is set to **Limit**.
Interface	Specify the VPN port, on which the policy takes effect. When it is set to **All VPN Ports**, the policy will be applied to all VPN ports.
Enabled	Set whether to enable the flow control policy. If it is disabled, the policy does not take effect.
IP/DSCP Priority	Specifies the priority of packets to differentiate various types of traffic and allocate different levels of service quality. Flow control policies are applied based on the IP/DSCP field in the packet.
Time	Specifies the time period during which the rule takes effect. You can choose from existing time rules or create custom ones.

(3) Click **OK**.

5. View Custom Policies

The current custom policies are displayed in the **Policy List** section. You can modify and delete a custom policy. To delete multiple custom policies in a batch, select the desired policies and click **Delete Selected**.

- Normal policy list



- VPN policy list

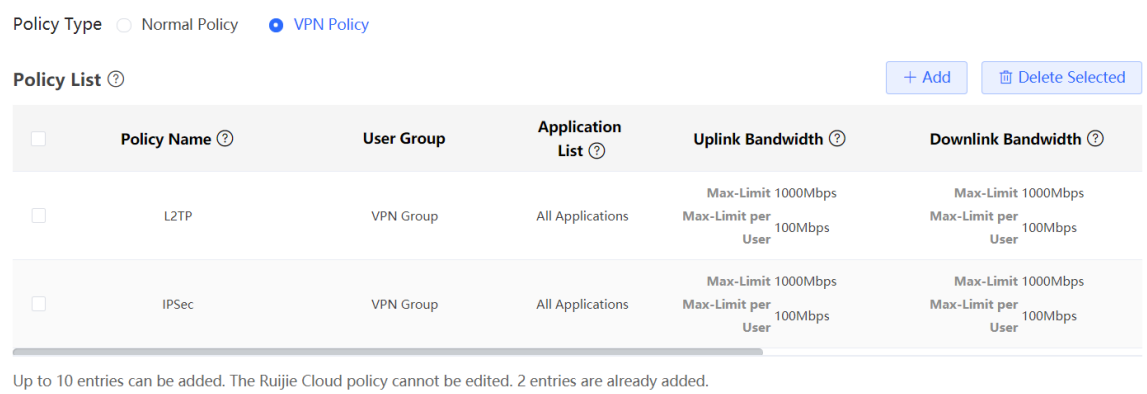


Table 8-11 Policy list information

Parameter	Description
Application List	The **Application List** contains the applications to which the policy is valid. If the **Application Library** matches with the **Application** that is set to **Custom** and supported by the policy, Custom is displayed in the **Application List**. If not, Custom is displayed.
Status	Indicate whether the current policy is enabled. You can click to edit the status. If the **Application Library** does not match with the **Application** that is set to **Custom** and supported by the policy, you cannot edit the **Status** directly. Please click **Edit** in the action bar to edit the policy.
Effective State	Indicate whether the policy is effective in the current system. If **Inactive** is displayed, check whether the policy is enabled, whether the policy-enabled port exists, and whether the **Application Library** matches with the **Application** to which the policy is valid.
Match Order	All the created custom policies are displayed in the policy list, with the latest policy listed on the top. The device matches the policies according to their sorting in the list. You can manually adjust the policy matching sequence by clicking or in the list.
Action	You can modify and delete the custom policy.

8.6.4 Application Priority

1. Overview

After smart flow control is enabled, you can set the application priority to provide guaranteed bandwidth to applications with high priority and suppress the bandwidth for applications with low priority. You can predefine a list of applications whose bandwidth needs to be guaranteed preferentially and a list of applications whose bandwidth needs to be suppressed based on actual needs.

Caution

If one application exists in both the custom policy list and the application priority list, the custom policy prevails.

2. Getting Started

- Before you configure application priority, enable smart flow control first. For details, see Section 8.6.2 Smart Flow Control.
- Confirm that the appropriate application library is selected on the **Custom Policy** page (See Section 8.6.3

Custom Policies for details.).

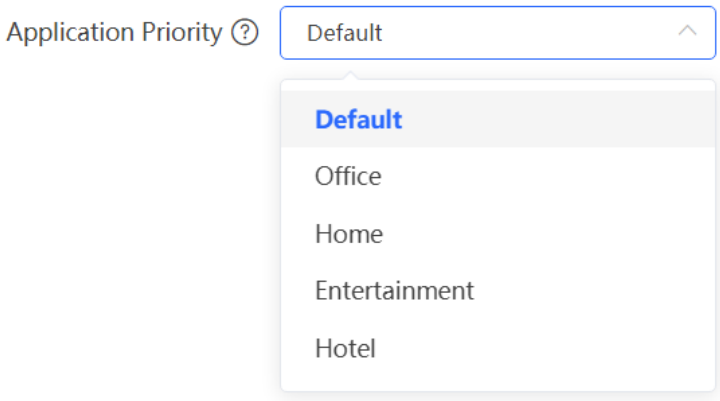
3. Configuration Steps

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Flow Control** > **Application Priority**.

(1) Create an application priority template.

Select a template from the **Application Priority** drop-down list box.

Five application priority templates are predefined to meet the needs in different scenarios. You can switch among the templates based on actual needs.



The application priority templates are as follows:

- **Default**: This template is used during device initialization. The traffic bandwidth is not guaranteed or suppressed for any application.
- **Office**: This template is designed for the office scenario, where the application traffic from the office network is guaranteed preferentially.
- **Home**: This template is designed for the home scenario, where the application traffic from the home network is guaranteed preferentially.
- **Entertainment**: This template is designed for the entertainment scenario, where the application traffic from the entertainment network is guaranteed preferentially.
- **Hotel**: This template is designed for the hotel scenario, where the application traffic from the hotel network is guaranteed preferentially.

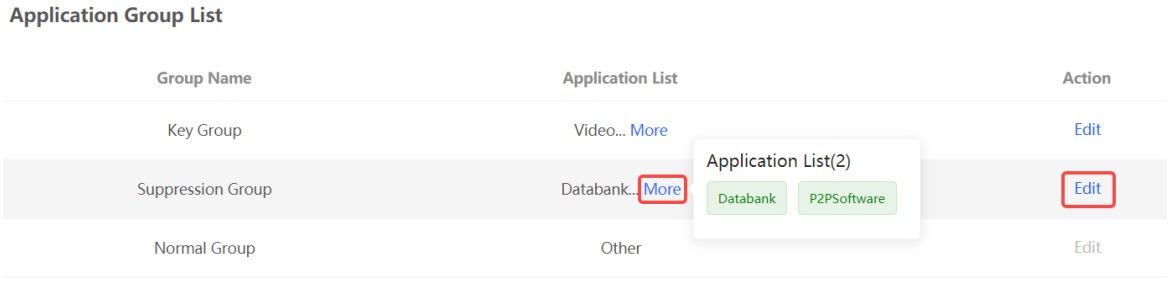
(2) Create an application group list.

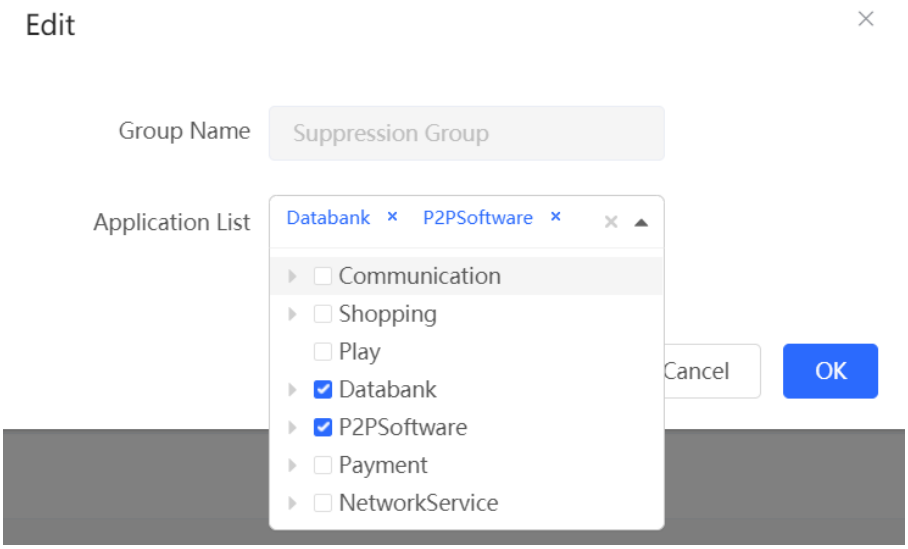
Each default template has three application groups: key group, block group, and normal group. The application priority of the three groups decreases in the following order: key group, normal group, and block group.

- **Key Group**: The traffic from applications in the application list for this group is guaranteed preferentially.
- **Block Group**: The traffic from applications in the application list for this group is suppressed to preferentially guarantee the traffic from applications with higher priority.
- **Normal Group**: All the applications in the application library beyond the key group and block group are in this group. The traffic from applications in this group are guaranteed after that from the key group.

After you select a template, three application groups **Key Group**, **Block Group**, and **Normal Group** and the application list for each group in the current template are displayed. You can click **More** to view the details of each application list.

You can click **Edit** in the **Action** column next to the key group and block group to edit the application list for the groups, allowing the traffic from these applications to be guaranteed or suppressed.





8.7 Access Control

8.7.1 Overview

The access control function matches data packets passing through the device based on specific rules and permits or drops data packets in the specified time range. This function controls whether to permit LAN user access to the Internet and whether to block a specific data flow. The device matches packets based on the MAC address or IP address.

8.7.2 Configuration Steps

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Access Control**.

The access control rule list displays the created access control rules. Click **Add** to add an access control rule.

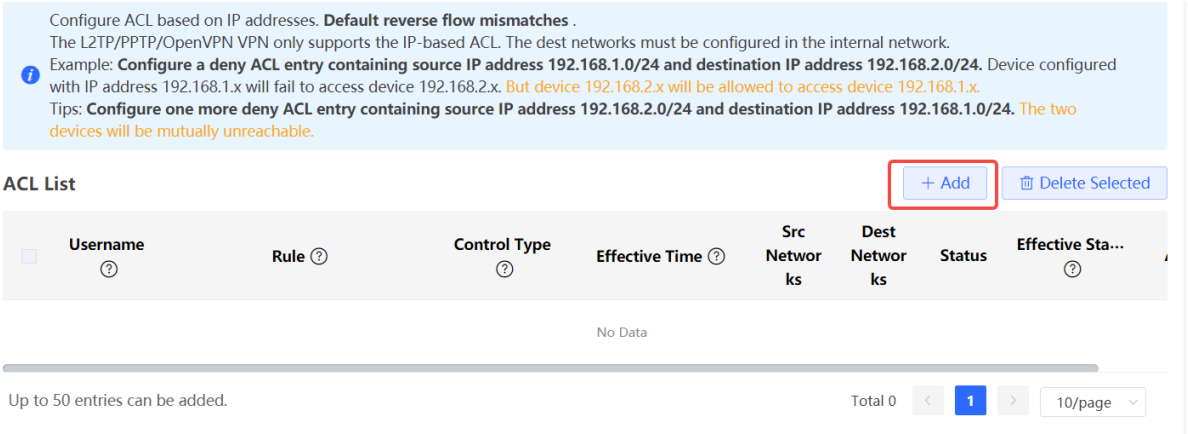


Table 8-12 Access Control Rule Information

Parameter	Description
Username	Identify the purpose of the rule.
Rule	Display a summary of the control information. MAC-based: Display the MAC address matching the rule. IP-based: Display the connection type, source IP address, destination IP address, and protocol type of packets matching the rule.
Control Type	Indicate how packets that match the rule are processed. • Allow: Permit the packets that match the rule. • Block: Discard the packets that match the rule.
Effective Time	Indicate the time period during which the rule takes effect.
Src Networks	Indicate the source interface that matches the rule. If the rule is based on the MAC address, then this field is set to "All Intranets" by default. If the rule is based on IP addresses, then this field can be set to "All Networks", "All Extranets", "All Intranets", or a specific network.
Dest Networks	Indicate the destination interface that matches the rule. If the rule is based on the MAC address, then this field is set to "All Extranets" by default. If the rule is based on IP addresses, then this field can be set to "All Networks", "All Extranets", "All Intranets", or a specific network.
Status	Indicate whether the rule is enabled. You can click to switch the status. When this toggle switch is off, the rule will not take effect.
Effective State	Indicate whether the rule is effective. If **Ineffective** is displayed, it might be because the current system time is not within the designated effective period. You can hover the mouse over to view more details on the cause.

Parameter	Description
Match Order	All the created rules are displayed in the ACL list, with the latest rule listed on the top. The device matches the rules according to their sorting in the list. You can manually adjust the rule matching sequence by clicking or in the list.
Action	You can modify or delete a rule.

1. Configuring a MAC Address-based ACL Rule

MAC address-based ACL rules enable the device to match data packets based on the source MAC address, and are generally used to control Internet access from online users or specific clients.

Set **Based on MAC**, enter the MAC address of the client, select a rule type, set the effective time range, and click **OK**.

Note

MAC address-based ACL rules are valid on WAN interfaces by default.

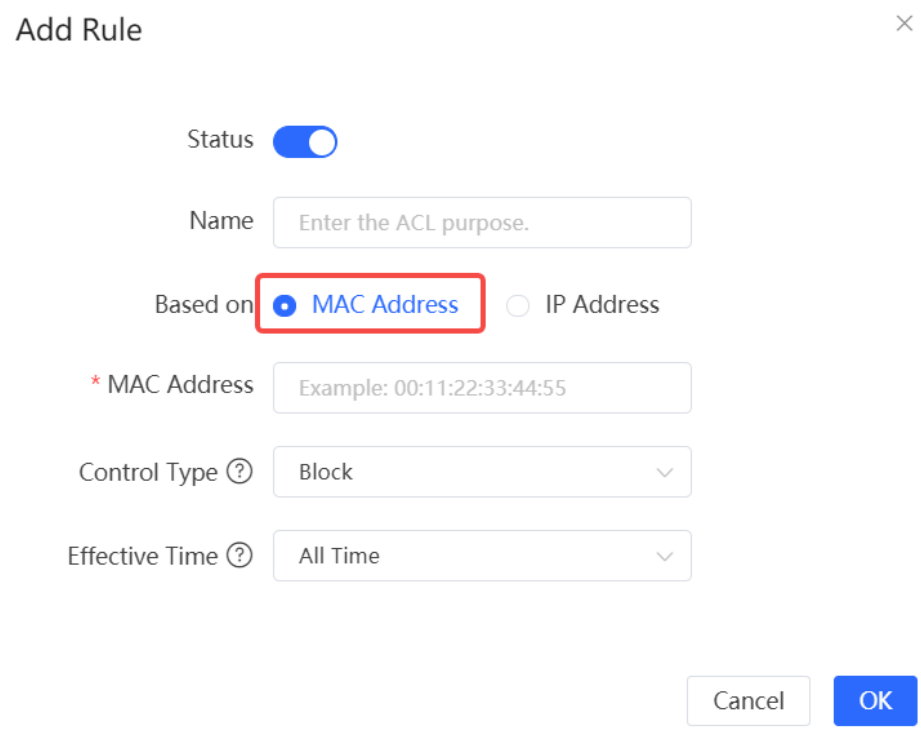


Table 8-13 MAC address-based ACL configuration

Parameter	Description
Status	Indicate whether the rule is enabled. You can click to switch the status. When this toggle switch is off, the rule will not take effect.

Parameter	Description
Name	Identify the rule. This field can be customized by the user.
MAC Address	Enter the target MAC address. When you click on the input box, the information of the user currently online will be displayed. By simply clicking on the displayed information, the corresponding MAC address will be automatically filled in for you.
Control Type	Indicate how packets that match the rule are processed. ● Allow: Permit the packets that match the rule. ● Block: Discard the packets that match the rule.
Effective Time	Indicate the time period during which the rule takes effect. You can select a time range from the drop-down list in 8.3 Time Management, or select **Custom** to manually set a time range.

2. Configuring an IP Address-based ACL Rule

IP address-based ACL rules enable the device to match data flows according to the source IP address, destination IP address, and protocol number.

Set **Based on IP**, click **IPv4** or **IPv6** next to the **Internet** parameter and enter the source IP address and port and destination IP address and port of the data flow, select the protocol type, rule type, effective time range, and effective port, and click **OK**.

Caution

- IP address-based ACL rules are effective in only one direction. For example, in a block rule, the source IP address segment is 192.168.1.0/24 and the destination IP address segment is 192.168.2.0/24. According to this rule, the device with the IP address 192.168.1.x cannot access the device with the IP address 192.168.2.x, but the device with the IP address 192.168.2.x can access the device with the IP address 192.168.1.x. To block bidirectional access in this network segment, you need to configure another block rule with the source IP address segment 192.168.2.0/24 and destination IP address segment 192.168.1.0/24.
- L2TP/PPTP VPN supports only IP address-based access control and the effective ports must be in the LAN.

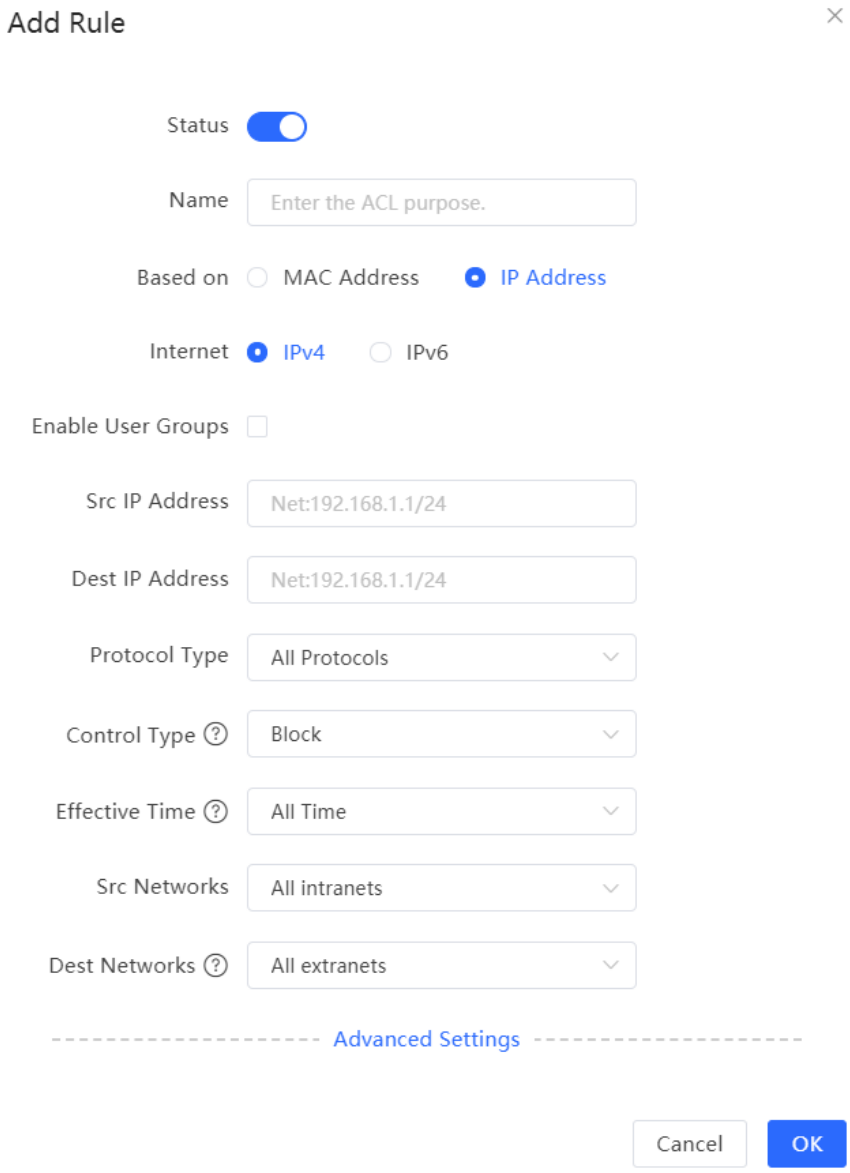


Table 8-14 IP address-based ACL configuration

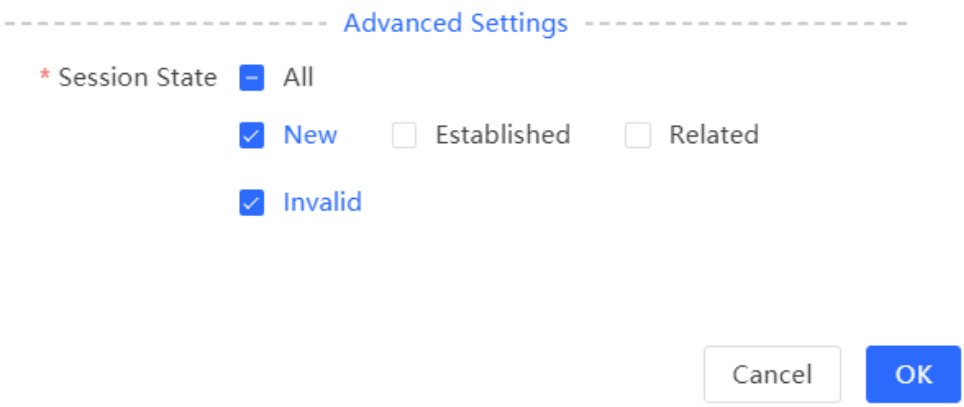
Parameter	Description
Status	Indicate whether the rule is enabled. You can click to switch the status. When this toggle switch is off, the rule will not take effect.
Name	Identify the purpose of the rule, which can be customized by the user.
Internet	Format of the IP address. Both IPv4 and IPv6 address formats are supported.

Parameter	Description
Src IP Address: Port	The source IP address and port of the packet. If this parameter is left empty, it means all IP addresses and ports. If the Internet is set to IPv4, then the format of the IP address is IPv4. Example: 192.168.1.1/24. If the Internet is set to IPv6, then the format of the IP address is IPv6. Example: 2000::1.
Dest IP Address: Port	The destination address and port of the packet. If this parameter is left empty, it means all IP addresses and ports. If the Internet is set to IPv6, then the format of the IP address is IPv6. Example:192.168.1.1/24 If the Internet is set to IPv6, then the format of the IP address is IPv6. Example:2000::1
Protocol Type	Specify the protocol type for data packet matching. The options are TCP, UDP, and ICMP.
Control Type	Specify the method for processing data packets matching the conditions. Allow: Permit the data packets matching the conditions. Block: Drop the data packets matching the conditions. This rule is valid only in one direction, and does not block the reverse flow.
Effective Time	You can select a time range defined in Section 8.3 Time Management from the drop-down list box, or select Custom and manually enter the specific time range.
Interface	Select the port on which the rule applies. LAN: The rule takes effect on a LAN port to control data packets to the LAN. WAN: The rule takes effect on a WAN interface to control data packets received from or sent to the Internet.
Src Networks	Indicate the source interface that matches the rule. If the rule is based on the MAC address, then this field is set to "All Intranets" by default. If the rule is based on IP addresses, then this field can be set to "All Networks", "All Extranets", "All Intranets", or a specific network.
Dest Networks	Indicate the destination interface that matches the rule. If the rule is based on the MAC address, then this field is set to "All Extranets" by default. If the rule is based on IP addresses, then this field can be set to "All Networks", "All Extranets", "All Intranets", or a specific network.

To limit the session state of packets matching the rule, you can click **Advanced Settings** and select one or more session states as required. These session states include New, Established, Related, and Invalid. Then, click **OK**.

Note

If no session state is selected, the rule matches all sessions by default.



8.8 Clients Management

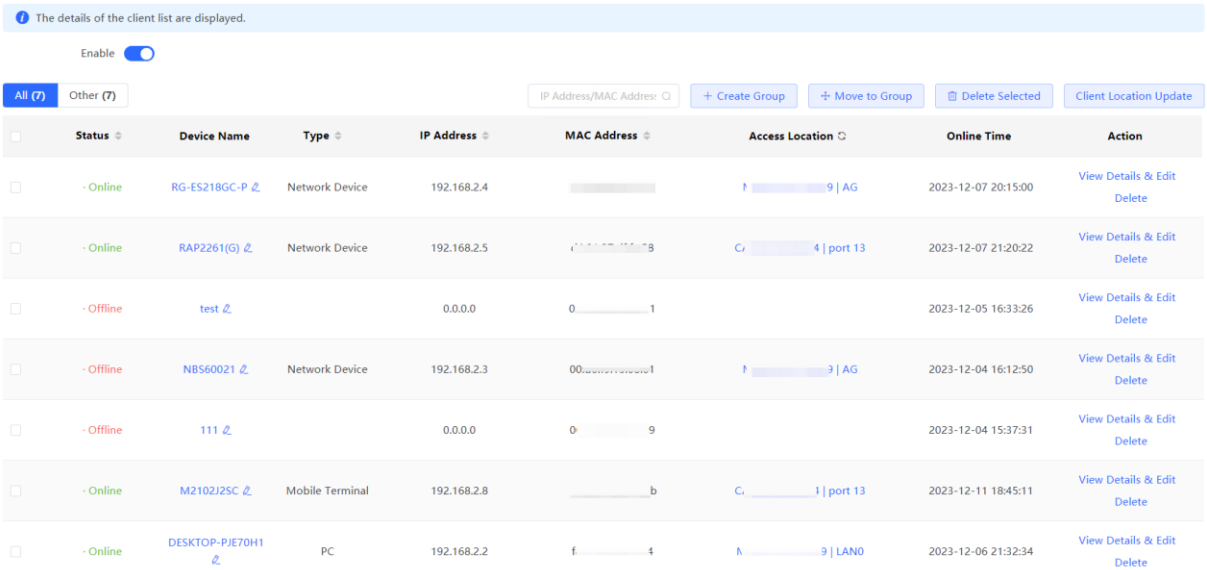
Note

Only RG-EG105G-V3, RG-EG105G-P-V3, RG-EG210G-P-V3, RG-EG209GS, RG-EG3XX series devices (such as RG-EG310GH-E) and RG-EG1510XS support this function.

8.8.1 Managing Online Clients

The **Client List** page displays client information. You can create client groups based on identified client information.

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Clients Management**.

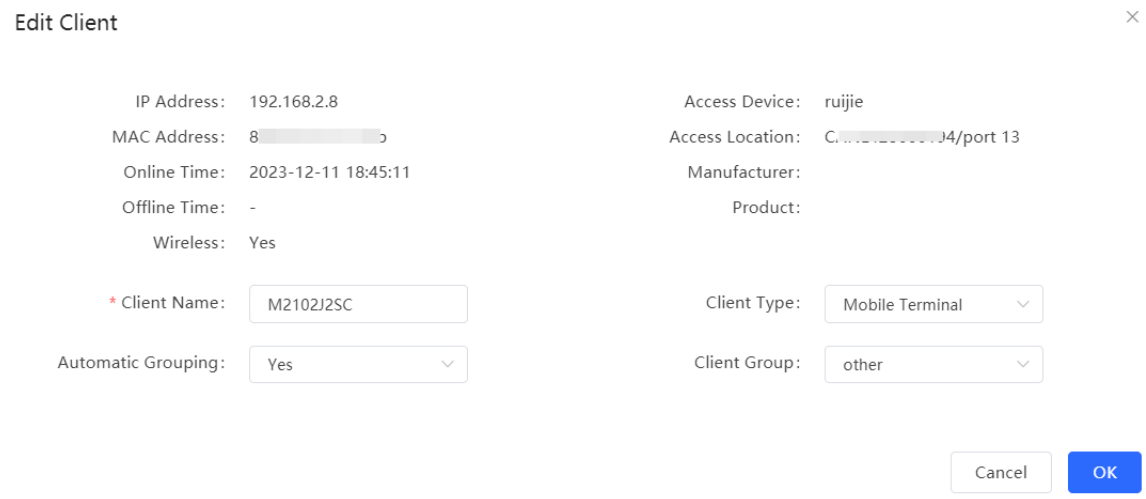


1. Viewing and Editing Client Information

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Clients Management > Client List**.

(1) Select the client to view details on the **Client List** page.

(2) Click **View Details & Edit**. The system displays details of the client.



(3) Edit client information as required.

- **Client Name**: indicates the client name.
- **Client Type**: indicates the client type.
- **Automatic Grouping**: indicates automatic client grouping.
- **Client Group**: indicates the client group.

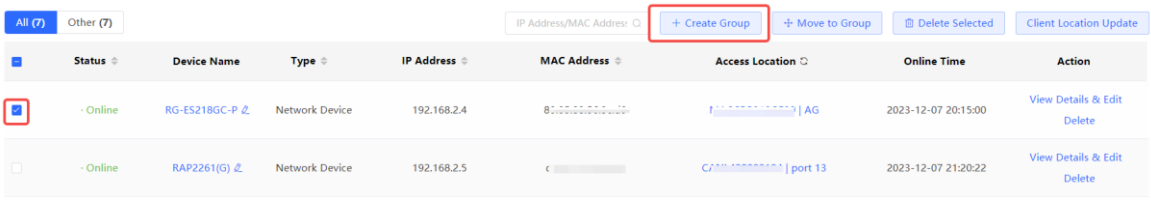
(4) Click **Save**.

2. Creating a Client Group

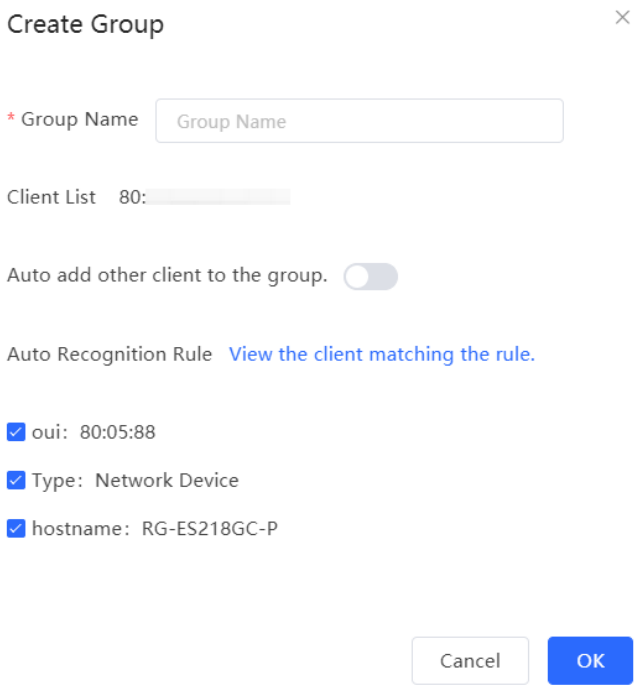
You can create a client group to manage multiple clients uniformly.

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Clients Management** > **Client List**.

(1) Select the clients to be grouped in **Client List** and click **Create Group**.



(2) The system identifies client rules automatically.



(3) Set a group name.

(4) (Optional) Enable **Auto add other client to the group** to add other clients in **Client List** to the group.

(5) (Optional) Click **View the client matching the rule** to view the client list where all clients match the same rule based on **oui**, **type**, or **hostname**

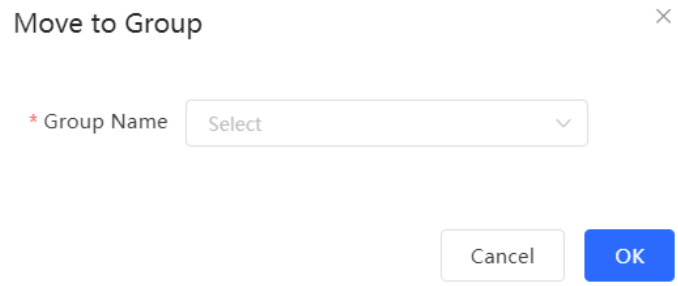
(6) Click **Save** to create a client group.

3. Moving a Client to Another Group

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Clients Management** > **Client List**.

(1) Select the clients to be moved to another group and click **Move to Group**.

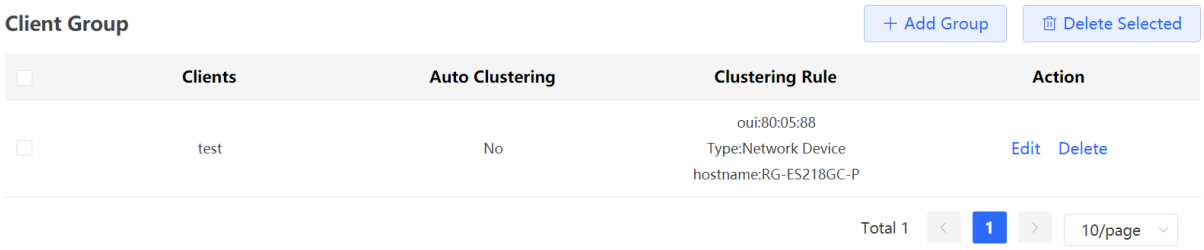
(2) Select a group from the **Group Name** drop-down list box to move the clients to the group.



8.8.2 Managing Client Groups

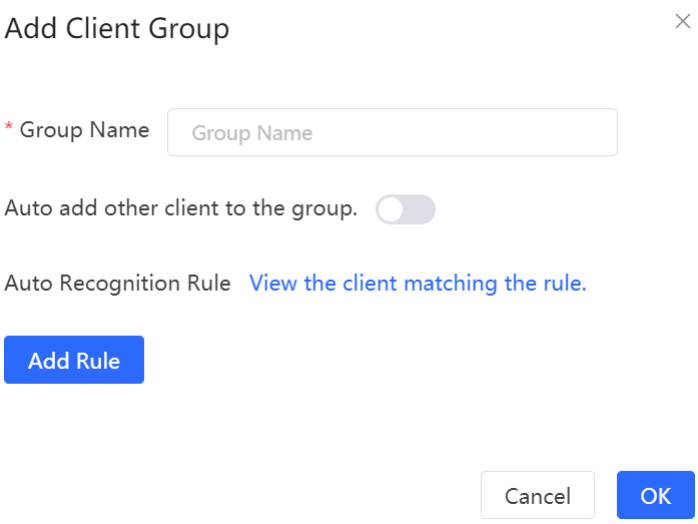
Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Clients Management > Client Group Config**.

You can specify client rules manually to create a client group and modify attributes of the client group.



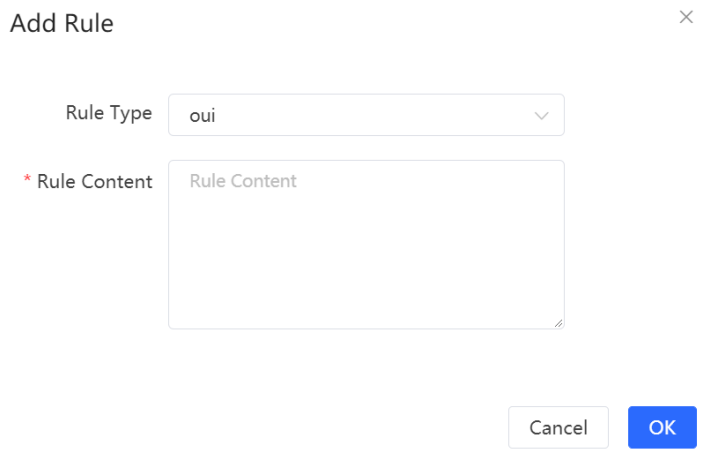
1. Creating a Client Group

(1) Click **Add Group**.



(2) Configure **Group Name**.

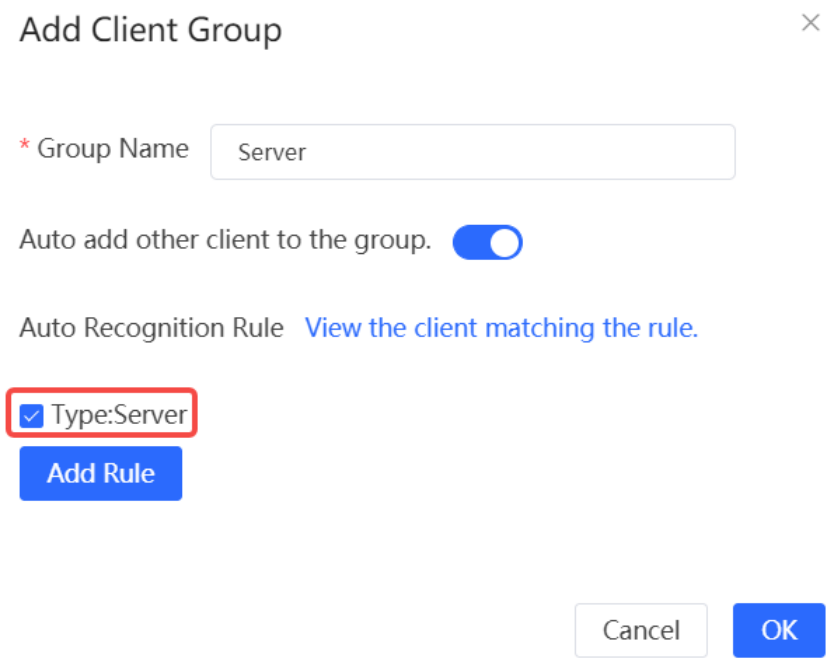
(3) Click **Add Rule** to create a client rule.



The system supports the following three types of rules.

- **oui:** indicates that the first three bytes of a MAC address is used as a grouping rule, such as 70:B5:E8.
- **Type**: indicates that the client type is used as a grouping rule. The client types include computers, mobile terminals, cameras, printers, servers, network devices, and monitors.
- **hostname**: indicates that the hostname of a device is used as a grouping rule, such as DESKTOP-PJE70H1.

(4) Select at least one new rule.



(5) (Optional) Click **View the client matching the rule** to view the client list where all clients match the same rule based on **oui**, **type**, or **hostname**.

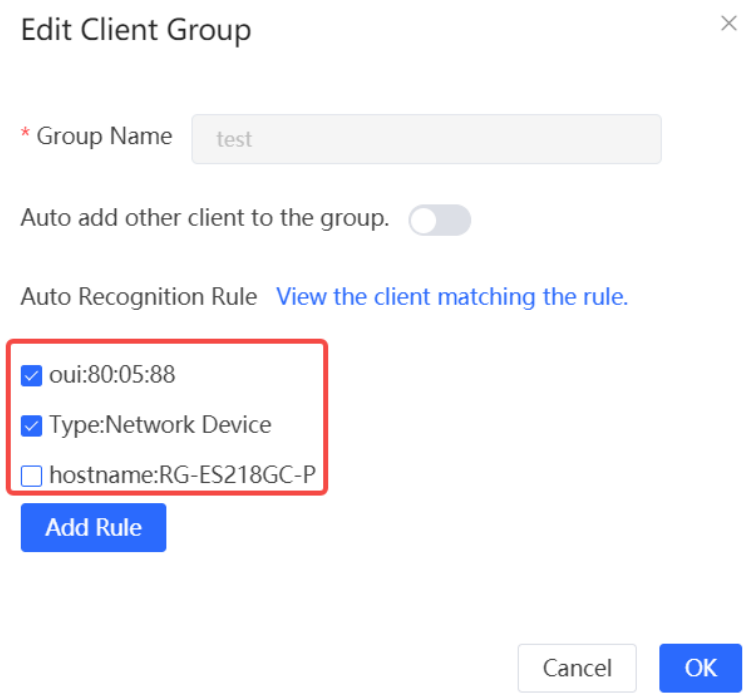
(6) (Optional) Enable **Auto add other client to the group** to add other clients in **Client List** to the group.

(7) Click **OK**.

2. Editing Client Group Information

(1) Select the client group to be edited in **Client Group** and click **Edit**.

(2) Configure grouping rules. Uncheck a rule or add a new rule.



(3) Click **OK**.

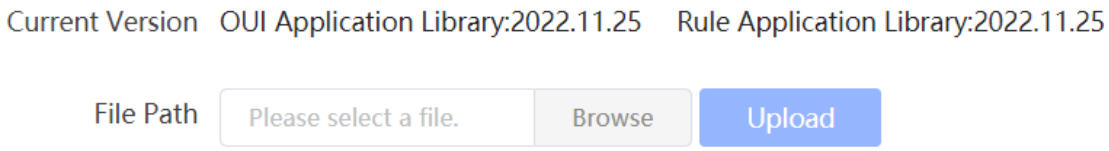
8.8.3 Upgrading a Client Application Library

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Clients Management > Client Library Upgrade**.

Upload an application library upgrade file manually to upgrade a client application library.

Note

You can upgrade a client application library only when the device flash space and memory space are sufficient.



(1) Click **Browse** to select an application library upgrade file.

(2) Click **Upload** to upload the application library upgrade file. Then the system upgrades the application library automatically.

8.9 Upgrading the Application Library

8.9.1 Overview

The app control function relies on the accuracy of the application library, and the application library is updated with the app version. You can upgrade the application library to the latest version on the **Application Library Update** page.

8.9.2 Local Upgrade

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Application Library Update**> **Local Application Library Update**.

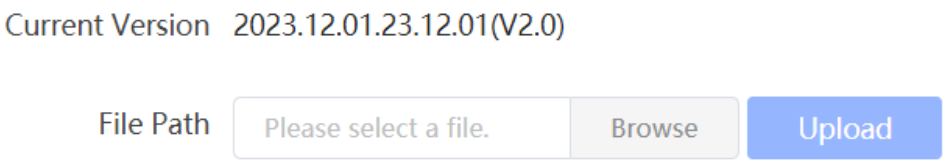
Caution

- Upgrading the application library version takes about one minute to take effect. Do not cut off power during the upgrade. You can view the current application library version on the page.
- Perform subsequent operations based on the memory information displayed on the page. If the memory is insufficient, you are advised to restart the device and then upgrade the application library.
- After the application library is upgraded, the original app control policy may become invalid. Therefore, exercise caution when performing this operation.

(1) Click **Browse**. Select an application library upgrade file.

(2) Click **Upload** to upload the upgrade file.

(3) Click **OK**. Wait for the system to automatically complete the upgrade.



8.9.3 Online Upgrade

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Application Library Management** > **Application Library Management**.

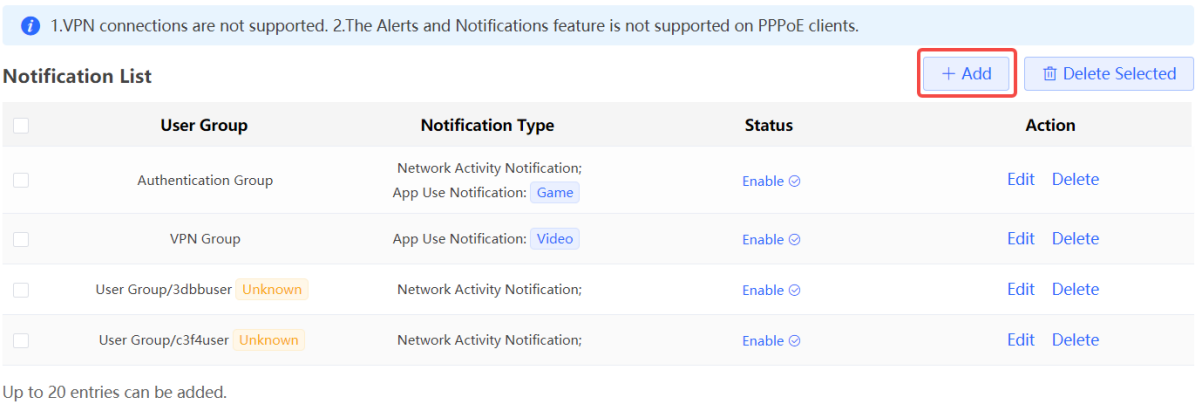
Enable **Auto Update Version**. When the system identifies the latest version, the application library is automatically upgraded.

8.10 Network Behavior Settings

8.10.1 Internet Alert

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Network Settings** > **Internet Alert**.

Click **Add** to create a network access notification policy and notify users of their online behaviors or application usage.



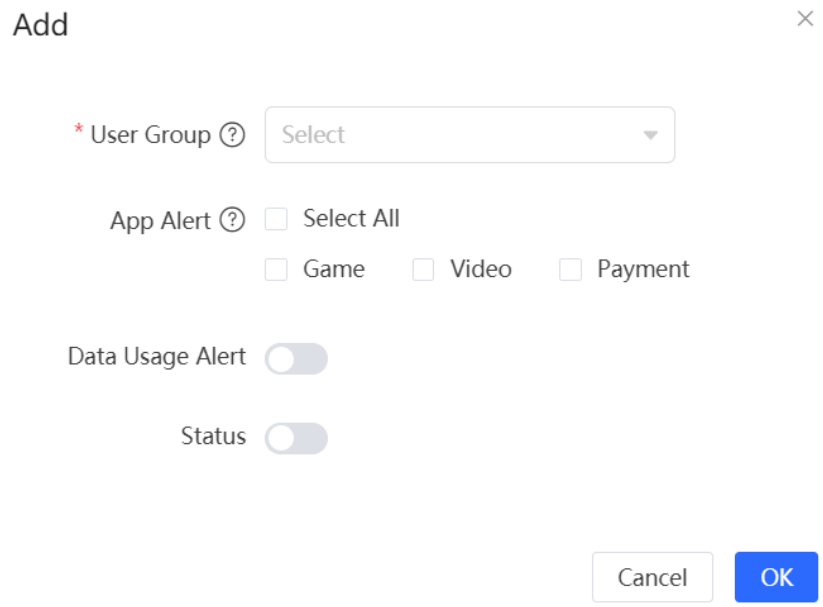


Table 8-15 Internet Access Notification Configuration Parameters

Parameter	Description
User group	Select a user group managed by the policy from the user group list. For details about how to set the user group list, see 8.2 User Management. If you select all members of a user group, the policy takes effect on the entire user group (and members added to the user group later).
App Alert	To enable the **App Alert** function, enable **Traffic Audit** first. For details, see 3.4 Supporting Traffic Monitoring.
App category	When **App Alert** is enabled, you need to select the application category for the policy. When a user uses an application in the corresponding application category, a notification will be received.
Data Usage Alert	After the **Data Usage Alert** function is enabled, you will receive a notification when a specified user accesses the Internet.

Parameter	Description
Status	Enable/disable the **Data Usage Alert** function. If it is disabled, the policy does not take effect.

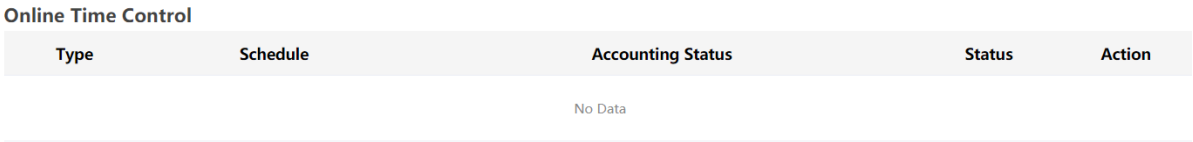
8.10.2 Online Time Control

Note

The **Online Time Control** feature can only be configured on the app, and the web interface only displays the synchronization status.

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Network Settings** > **Online Time Control**.

The **Online Time Control** list displays the type, schedule, accounting status, status, and operation information.



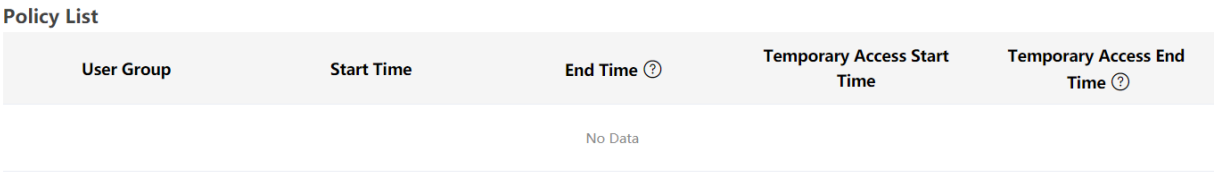
8.10.3 Internet Block Policy

Note

The Internet block policy can be configured only on the app, and the web interface only displays the synchronization status.

Choose **One-Device** > **Gateway** > **Config** > **Behavior** > **Network Settings** > **Internet Block Policy**.

The **Policy List** displays the user group, start time of network disconnection, end time of network disconnection, start time of temporary access, and end time of temporary access.

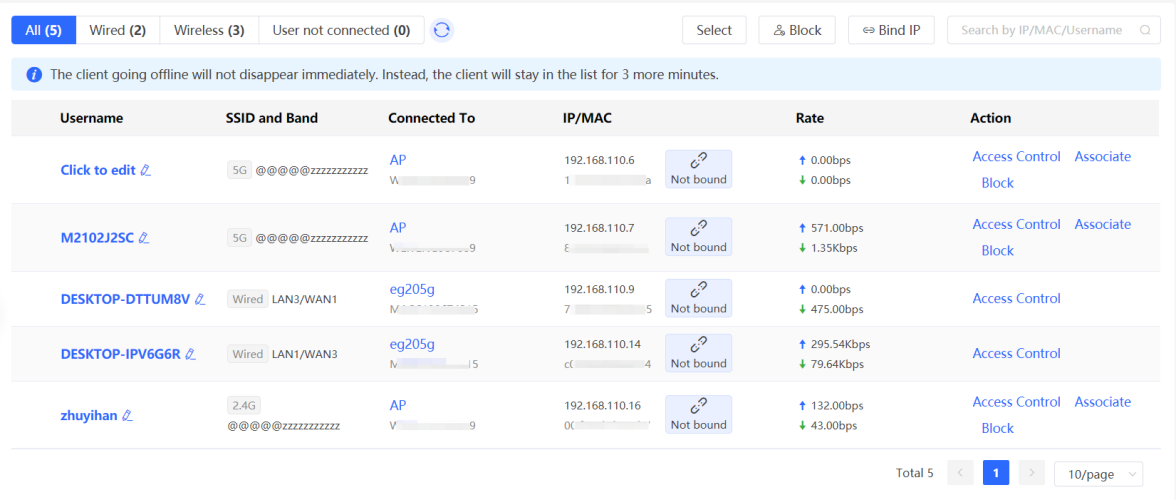


9 Online Client Management

9.1 Overview

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

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



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

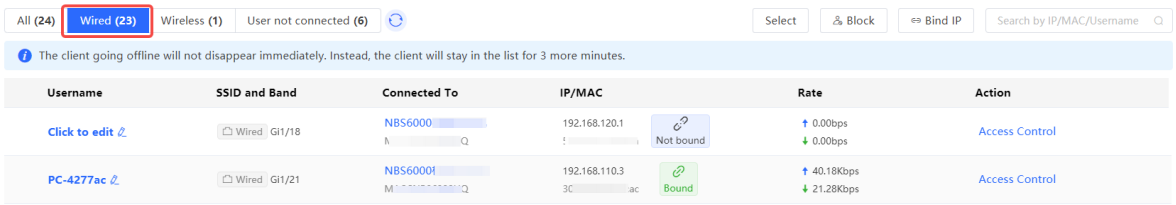
Table 9-1 Online Client Management Configuration Parameters

Parameter	Description
Username	Name of the connected client.
SSID and Band	Indicates the access mode of the client, which can be wireless or wired. The SSID and frequency band is displayed when a client is connected wirelessly.
Connected To	Indicates wired or wireless connection, the associated device and SN.
IP/MAC	Indicates the IP address and MAC address of the client.
Rate	Indicates the uplink and downlink rates of the client.
Action	You can click the corresponding button to perform access control, association, and block operations on online clients.
Signal Quality	The Wi-Fi signal strength of the client and the associated channel. Note: This information is displayed only in the wireless online client list.

Parameter	Description
Negotiation Rate	Negotiation rate between the client and the AP. Note: This information is displayed only in the wireless online client list.
Online Duration	Online duration of the client. Note: This information is displayed only in the wireless online client list.
Limit Speed	Indicates the wireless rate limiting of the current client. For details, see 9.6 Configuring Client Rate Limiting. Note: This information is displayed only in the wireless online client list.

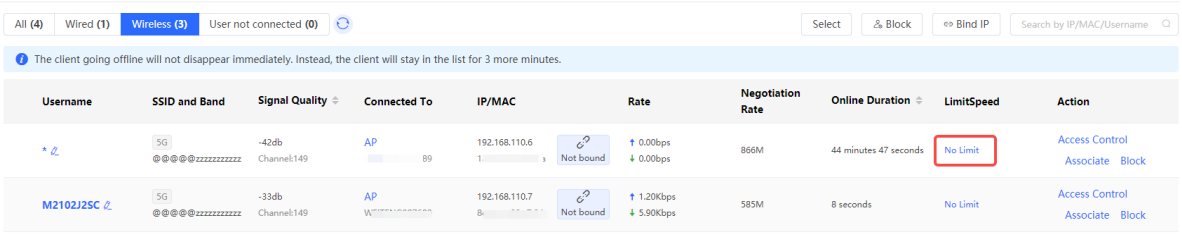
1. Wired Clients

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



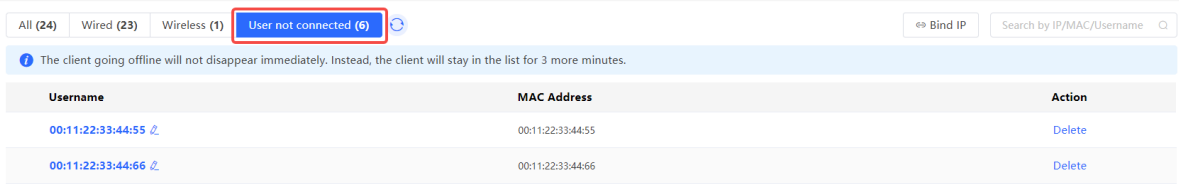
2. Wireless Clients

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



3. User not connected

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



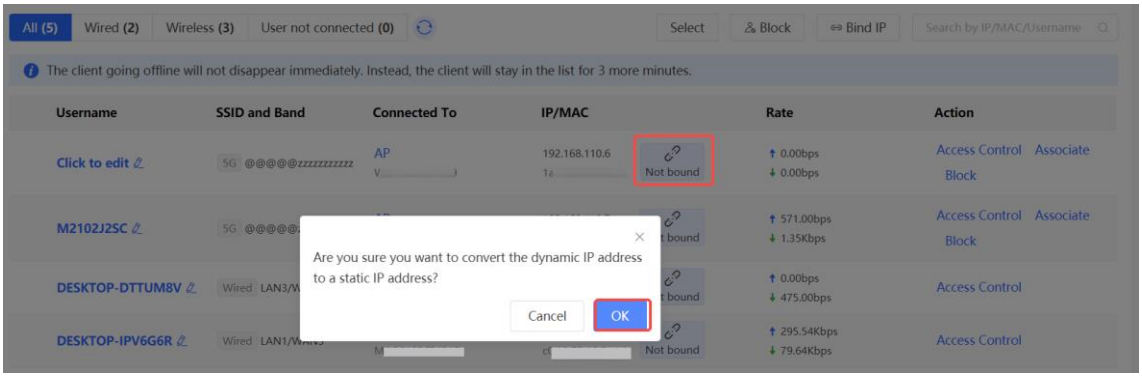
9.2 Configuring Client IP Binding

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

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

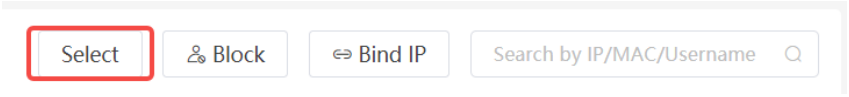
- Single client IP address binding

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

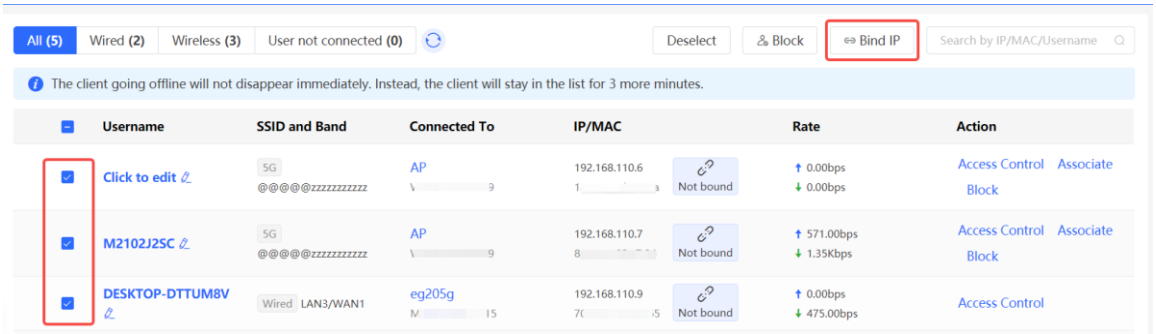


- Batch IP binding

  Click **Select**.

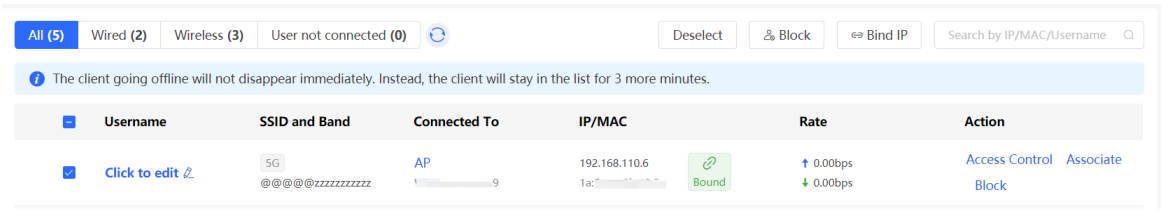


  Select the clients to be bound, click **Bind IP**, and click **OK** in the pop-up box to bind the selected clients to a static IP address.



- Unbind IP address

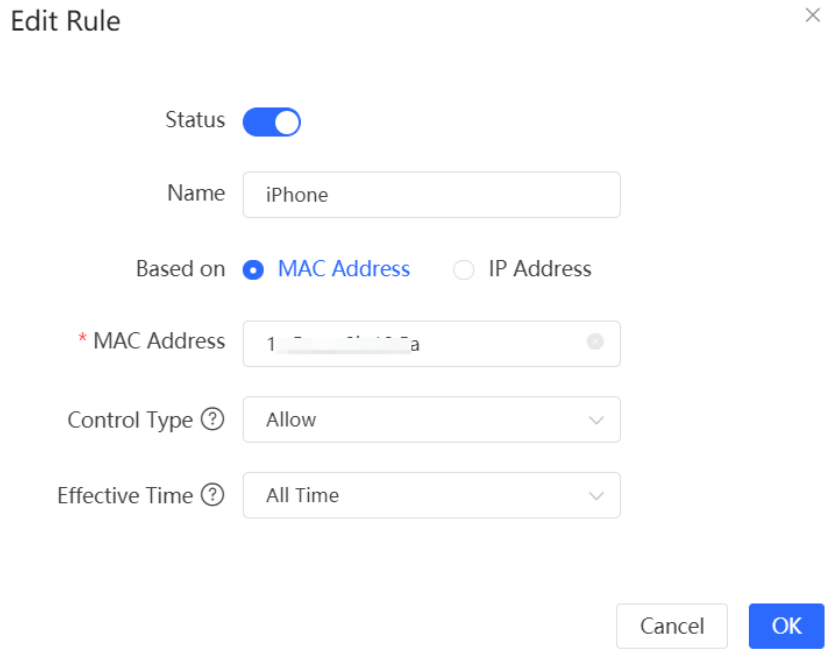
  Select the client to be unbound from the list, click **Bound**, and click **OK** in the pop-up box.



9.3 Configuring Client Access Control

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

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



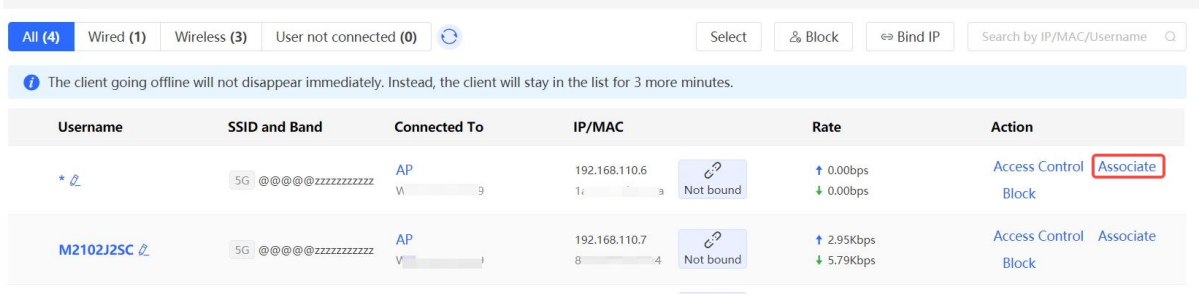
9.4 Configuring Client Association

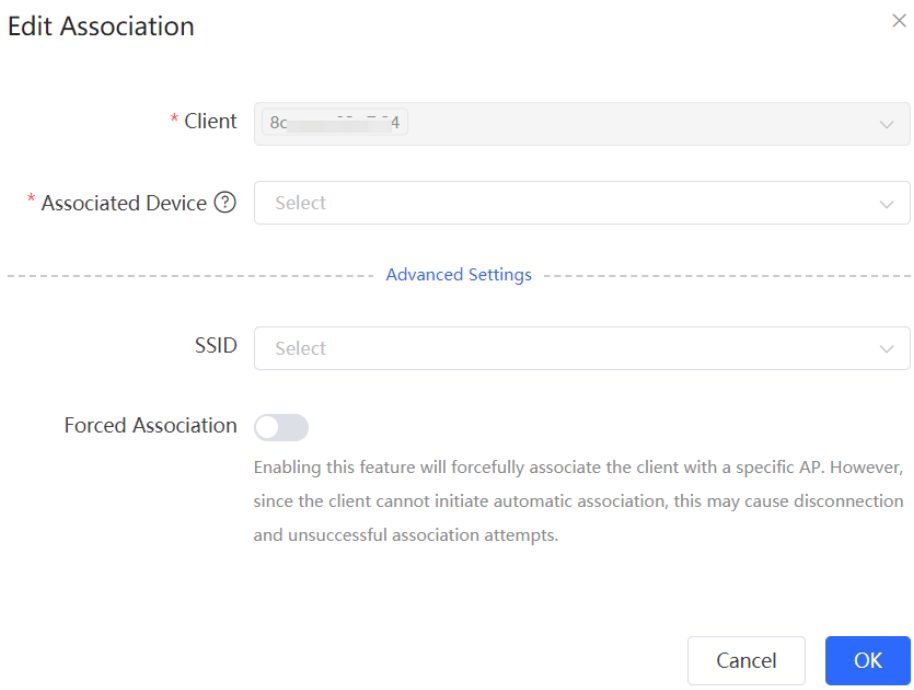
Choose **Network-Wide** > **Clients**.

Note

The Client Association feature applies only to wireless clients.

Select a client in the list and click **Associate** in the **Action** column. You will be redirected to the **Edit Association** page. The **Client** field is populated with the MAC address of the selected client and cannot be modified. The **Associated Device** field is populated with the associated device of the client by default. Set the SSID and the Forced Association feature as required, and click **OK**. For details, see 5.14 Client Association.





9.5 Blocking Clients

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

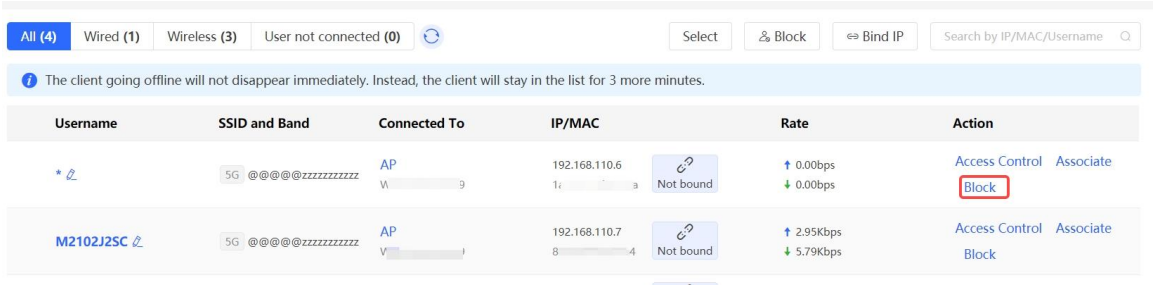
An unauthorized client may occupy network bandwidth and pose security risks. You can block specified clients to solve the unauthorized access problem.

Note

Client Block is available only for wireless clients.

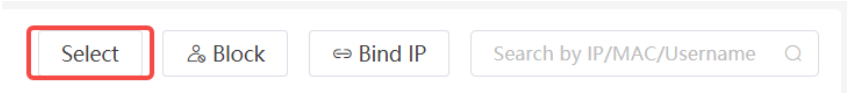
- Block a single client

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

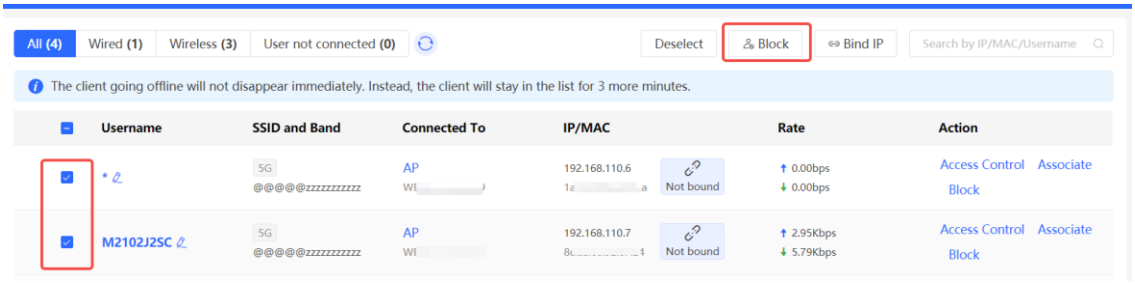


- Batch block clients

  Click **Select**.



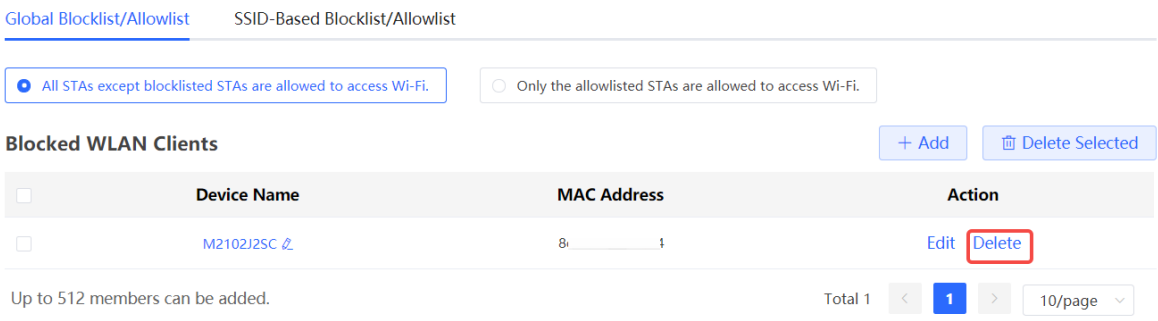
  Select the target clients, click **Block**, and click **OK** in the pop-up box to block the selected clients.



- Cancel Block

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

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



9.6 Configuring Client Rate Limiting

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

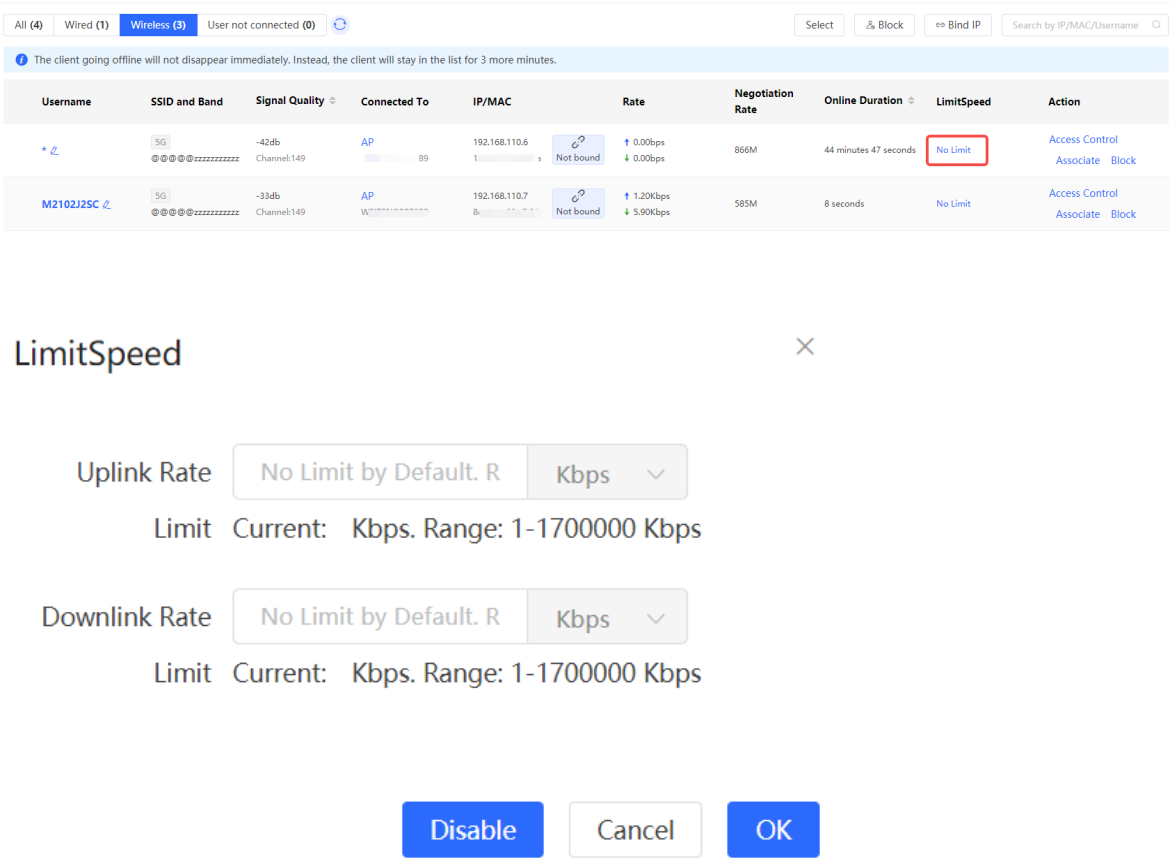
To ensure fair resource allocation, the network administrator can implement wireless rate limiting to prevent some users or devices from occupying a large amount of bandwidth and affecting the network experience of other users.

Note

Rate limiting applies only to wireless clients.

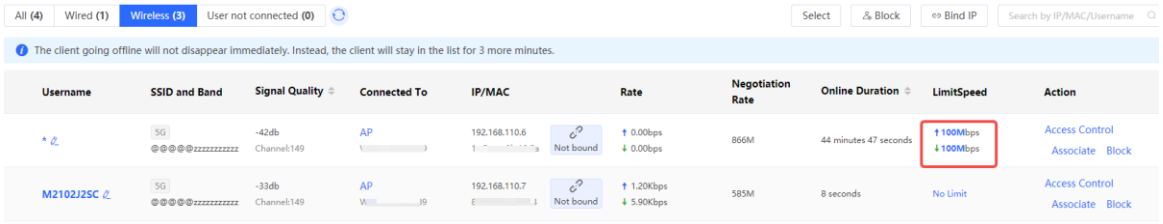
- Configure rate limits for clients

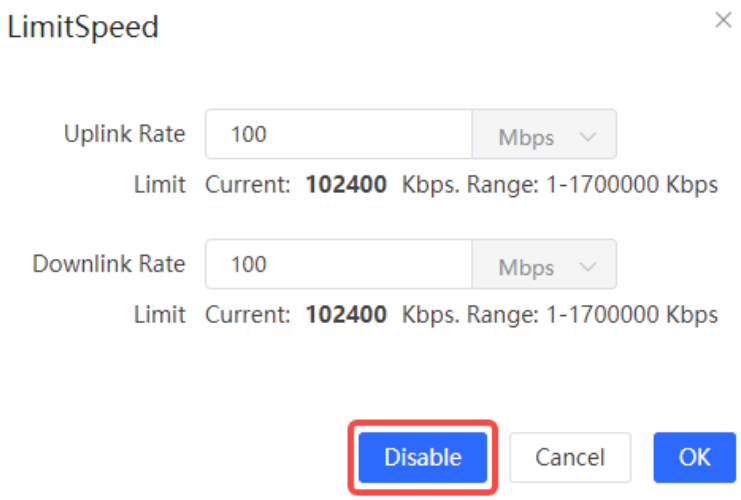
Click the **Wireless** tab, click the **LimitSpeed** column in the table, set the uplink rate limit and downlink rate limit, and click **OK**.



- Cancel rate limits

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




LimitSpeed
Uplink Rate
100
Mbps
Limit Current: 102400 Kbps. Range: 1-1700000 Kbps
Downlink Rate
100
Mbps
Limit Current: 102400 Kbps. Range: 1-1700000 Kbps
Disable
Cancel
OK

10 VPN

10.1 Configuring IPsec VPN

10.1.1 Overview

1. IPsec Overview

IP Security (IPsec) is a Layer 3 tunnel encryption protocol defined by the IETF. IPsec is used to provide end-to-end encryption and verification services in the network to provide high quality and interoperability for data transmission over the network and ensure transmission security by using cryptographic algorithms. The communicating parties obtain the following security services at the IP layer through encryption and data source authentication:

- Confidentiality: The IPsec sender encrypts packets before transmitting the packets over the network.
- Data integrity: The IPsec receiver authenticates packets received from the sender to ensure that data is not tampered with during the transmission.
- Data authentication: The IPsec receiver authenticates whether the sender of IPsec packets is valid.
- Anti-replay: The IPsec receiver detects and denies expired or repeated packets.

The IPsec protocol is widely used for communication between the HQ and branches of an organization. Currently, the device can be deployed as the IPsec server or client. A secure tunnel is established between the HQ and each branch based on the IPsec protocol to ensure the confidentiality of data transmission and improve network security.

2. IKE Overview

IPsec provides secure communication between two endpoints, which are called IPsec peers. Security Association (SA) is the establishment of shared security attributes between the peers to support secure communication. An SA may include attributes such as: security protocol used by the peers, characteristics of data flows to be protected, encapsulation mode of data transmitted between the peers, encryption and authentication algorithms, keys for secure data conversion and transmission, and the SA lifetime. When you configure IPsec, you can use the Internet Key Exchange (IKE) protocol to establish an SA. IKE provides automatically negotiated keys for establishing and maintaining SAs, simplifying IPsec usage and management.

3. IPsec Security Policy

IPsec security policies define security proposals (equivalent to SA) for data flows. You can configure matching security policies on both parties engaged in the communication to establish IPsec tunnels between the IPsec client and the IPsec server, protecting the communication data. An IPsec security policy consists of two parts: basic settings and advanced settings. Advanced settings are optional and include the specific IKE policy and connection policy. You can keep the default settings unless otherwise specified. For details, see the Configuration Steps below.

10.1.2 Configuring the IPsec Server

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **IPsec** > **IPsec Security Policy**.

1. Basic Settings

Click **Add**. In the dialog box that appears, set **Policy Type** to **Server**, enter the policy name and local subnet range, set the pre-shared key, and click **OK**.

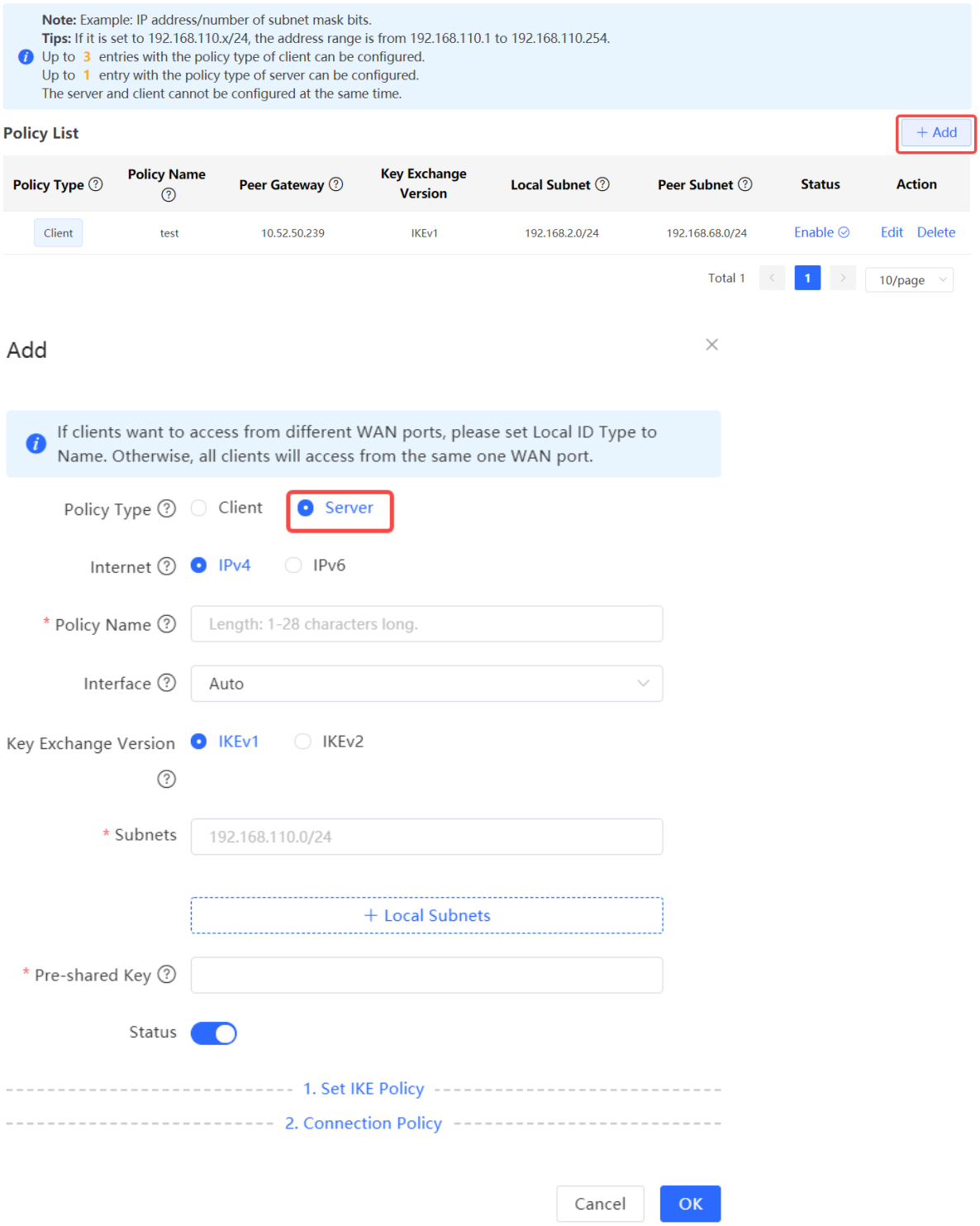


Table 10-1 IPsec server basic settings

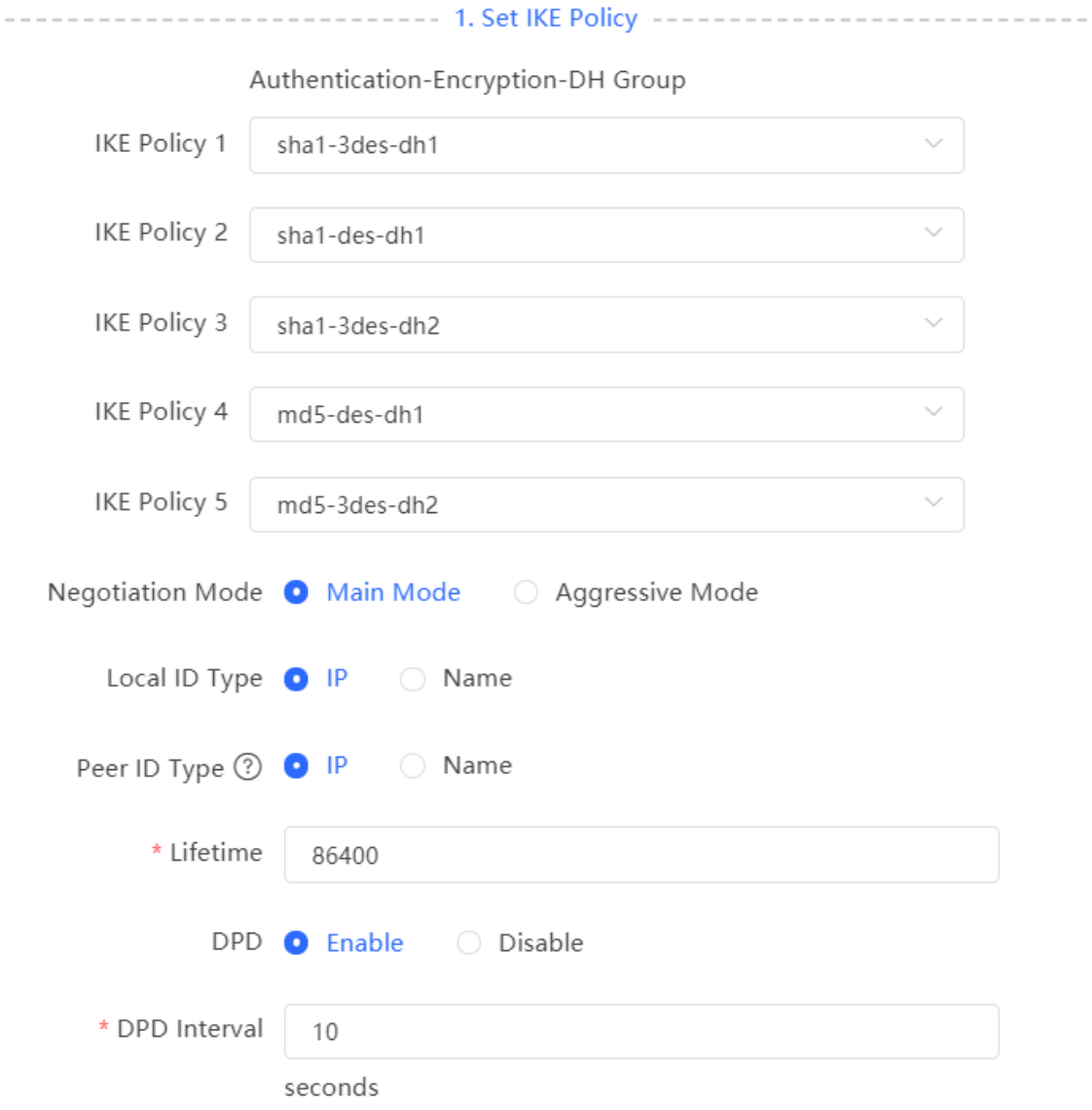
Parameter	Description
Policy Name	Specify the name of the IPsec security policy. The name must be a string of 1 to 28 characters.
Internet	Format of the IP address. Both IPv4 and IPv6 address formats are supported.
Interface	Select a local WAN interface from the drop-down list box. The **Peer Gateway** parameter set for the communication peer (IPsec client) must use the IP address of the WAN interface specified here. In the multi-line scenario, you are advised to set this parameter to **Auto**.
Key Exchange Version	Select the IKE version for SA negotiation. There are two options available: ● IKEv1: The negotiation of SA in IKEv1 primarily consists of two phases. o Phase 1: The purpose is to establish an IKE SA using one of two negotiation modes: Main Mode and Aggressive Mode. Main Mode requires six ISAKMP (Internet Security Association and Key Management Protocol) messages to complete the negotiation, while Aggressive Mode only requires three ISAKMP messages. Aggressive Mode offers faster IKE SA establishment. However, it combines key exchange and identity authentication, which means it does not provide identity protection. o Phase 2: The purpose is to establish an IPsec SA for data transmission, utilizing a fast exchange mode that requires only three ISAKMP messages to complete the negotiation. ● IKEv2: In IKEv2, the negotiation process for SA is simplified. The establishment of one IKE SA and one pair of IPsec SAs can be accomplished using two exchanges with four messages. If there is a need to establish more than one pair of IPsec SAs, only one additional exchange is needed for each pair. This enables the negotiation to be completed with just two messages per pair.
Subnets	Specify the local subnet address range for the data flows to be protected, that is, the LAN port network segment of the server. The value is the combination of IP address and subnet mask.

Parameter	Description
Pre-shared Key	Specify the same pre-shared key as the credential for authentication between communicating parties. For higher security, different peers must be configured with different pre-shared keys. That is, a pair of interface bound to the IPsec server and peer gateway of the IPsec client must be configured with the same unique pre-shared key.
Status	Specify whether to enable the security policy.

2. Advanced Settings (Phase 1)

- The key exchange version in the basic setting is IKEv1:

  Click **1. Set IKE Policy** to expand the configuration items. Keep the default settings unless otherwise specified.



- The key exchange version in the basic setting is IKEv2:

  Click **IKE Policy** to expand the configuration items. Keep the default settings unless otherwise specified.

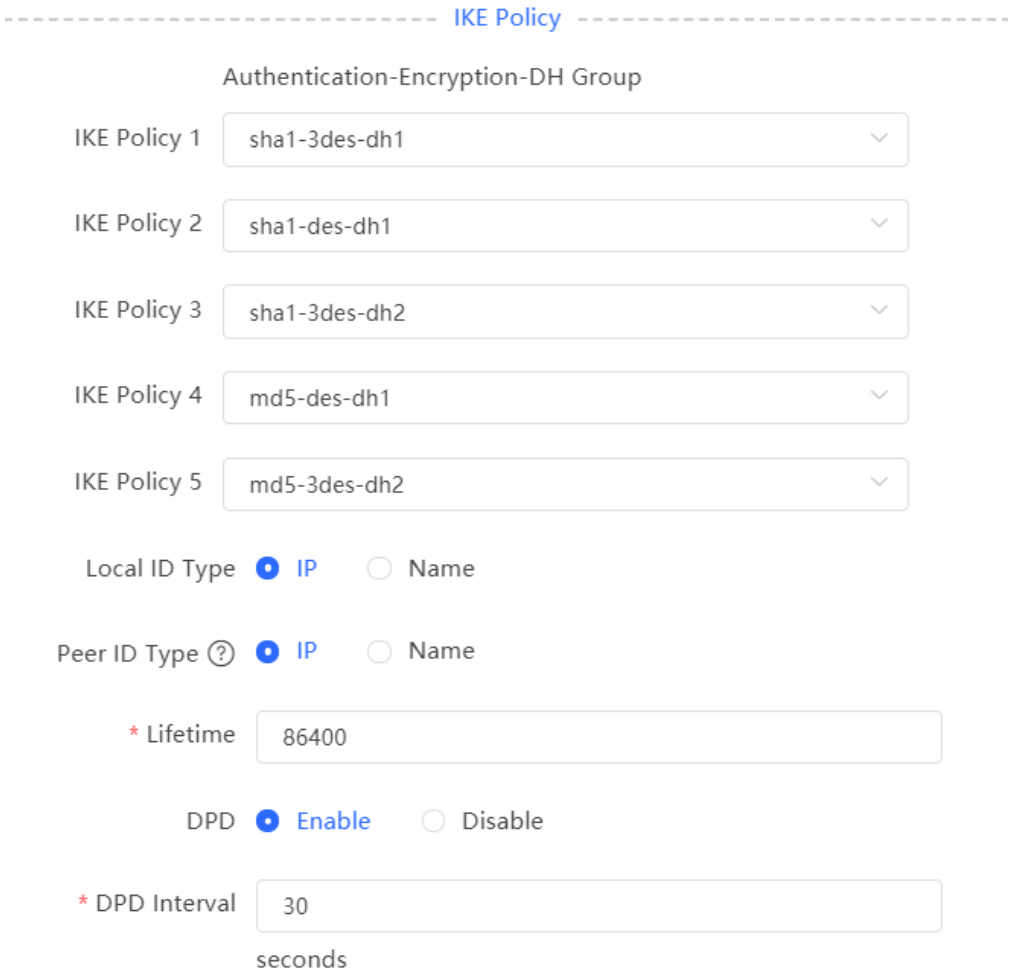


Table 10-2 IPsec server IKE policy configuration

Parameter	Description
IKE Policy	Select the hash algorithm, encryption algorithm, and Diffie-Hellman (DH) group ID used by the IKE protocol. An IKE policy is composed of the three parameters. You can set five sets of IKE policies. To ensure successful IKE negotiation, the two parties engaged in IKE negotiation must have at least one set of consistent IKE policy. ● Hash algorithm: ○ sha1: SHA-1 algorithm ○ md5: MD5 algorithm ● Encryption algorithm: ○ des: DES algorithm using 56-bit keys ○ 3des: 3DES algorithm using 168-bit keys ○ aes-128: AES algorithm using 128-bit keys ○ aes-192: AES algorithm using 192-bit keys ○ aes-256: AES algorithm using 256-bit keys ● DH group ID: ○ dh1: 768-bit DH group ○ dh2: 1024-bit DH group ○ dh5: 1536-bit DH group
Negotiation Mode	Select **Main Mode** or **Aggressive Mode**. The negotiation mode on the IPsec server and IPsec client must be the same. ● **Main Mode**: Generally, this mode is applicable to communication between fixed public network IP addresses and point-to-point communication between devices. In this mode, the peer identity is authenticated to provide high security. ● **Aggressive Mode**: The public network IP addresses obtained by ADSL dial-up users are not fixed and an NAT device may exist. Therefore, the aggressive mode is used to implement NAT traversal. In this mode, you need to set the local and peer ID type to **NAME** as the IP address is not fixed. The aggressive mode does not authenticate the peer identity, so it has low security.
Local/Peer ID Type	Specify the ID type of the local or peer device. The local ID type of the peer device must be the same as the peer ID type of the local device. ● **IP**: The IP address is used as the identity ID. The IDs of the local and peer devices are generated automatically. ● **NAME**: The host character string is used as the identity ID. The IDs of the local and peer devices are generated automatically. When the IP address is not fixed, you need to set **Local ID Type** to **NAME** and modify the peer device settings accordingly. In this case, you also need to configure the host character string that is used as the identity ID.
Local/Peer ID	When the local or peer ID type is set to **NAME**, you also need to host character string that is used as the identity ID. The local ID of the peer device must be the same as peer ID of the local device.

Parameter	Description
Lifetime	Specify the lifetime of the IKE SA. (The negotiated IKE SA lifetime prevails.) You are advised to use the default value.
DPD	Specify whether to enable Dead Peer Detection (DPD) to detect the IPsec neighbor status. After DPD is enabled, if the receiver does not receive IPsec encrypted packets from the peer within the DPD detection interval, DPD query will be triggered and the receiver actively sends a request packet to detect whether the IKE peer exists. You are advised to configure DPD when links are unstable.
DPD Interval	Specify the DPD detection interval. That is, the interval for triggering DPD query. You are advised to keep the default setting.

3. Advanced Settings (Phase 2)

Click **Connection Policy** to expand the configuration items. Keep the default settings unless otherwise specified.

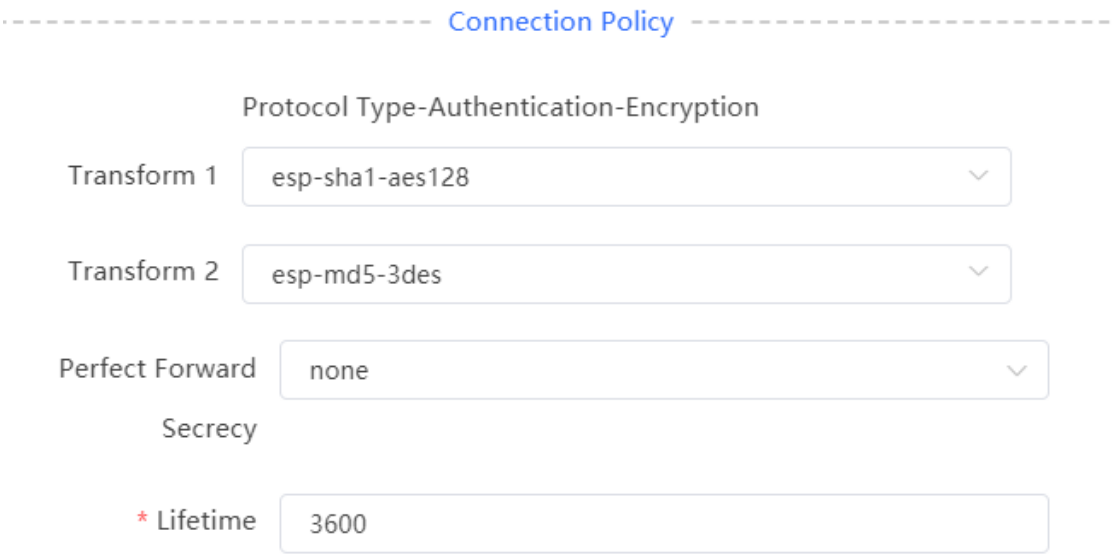


Table 10-3 IPsec server connection policy configuration

Parameter	Description
Transform Set	Specify the set of security protocol and algorithms. During IPsec SA negotiation, the two parties use the same transform set to protect specific data flow. The transform set on the IPsec server and IPsec client must be the same. ● Security protocol: The Encapsulating Security Payload (ESP) protocol provides data source authentication, data integrity check, and anti-replay functions for IPsec connections and guarantees data confidentiality. ● Verification algorithm: o sha1: SHA-1 HMAC o md5: MD5 HMAC ● Encryption algorithm: o des: DES algorithm using 56-bit keys o 3des: 3DES algorithm using 168-bit keys o aes-128: AES algorithm using 128-bit keys o aes-192: AES algorithm using 192-bit keys o aes-256: AES algorithm using 256-bit keys
Perfect Forward Secrecy	Perfect Forward Secrecy (PFS) is a security feature that can guarantee the security of other keys when one key is cracked, because there is no derivative relationship among the keys. After PFS is enabled, temporary private key exchange is performed when an IKE negotiation is initiated using a security policy. If PFS is configured on the local device, it must also be configured on the peer device that initiates negotiation and the DH group specified on the local and peer devices must be the same. Otherwise, negotiation will fail. ● none: Disable PFS. ● d1: 768-bit DH group ● d2: 1024-bit DH group ● d5: 1536-bit DH group By default, PFS is disabled.
Lifetime	Indicates the duration of an IPSec tunnel, which defines the time for data transmission over the IPSec tunnel.

10.1.3 Configuring the IPsec Client

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **IPsec** > **IPsec Security Policy**.

Click **Add**. In the dialog box that appears, set **Policy Type** to **Client**, enter the policy name, peer gateway, local subnet range, and peer subnet range, set the pre-shared key, and click **OK**.

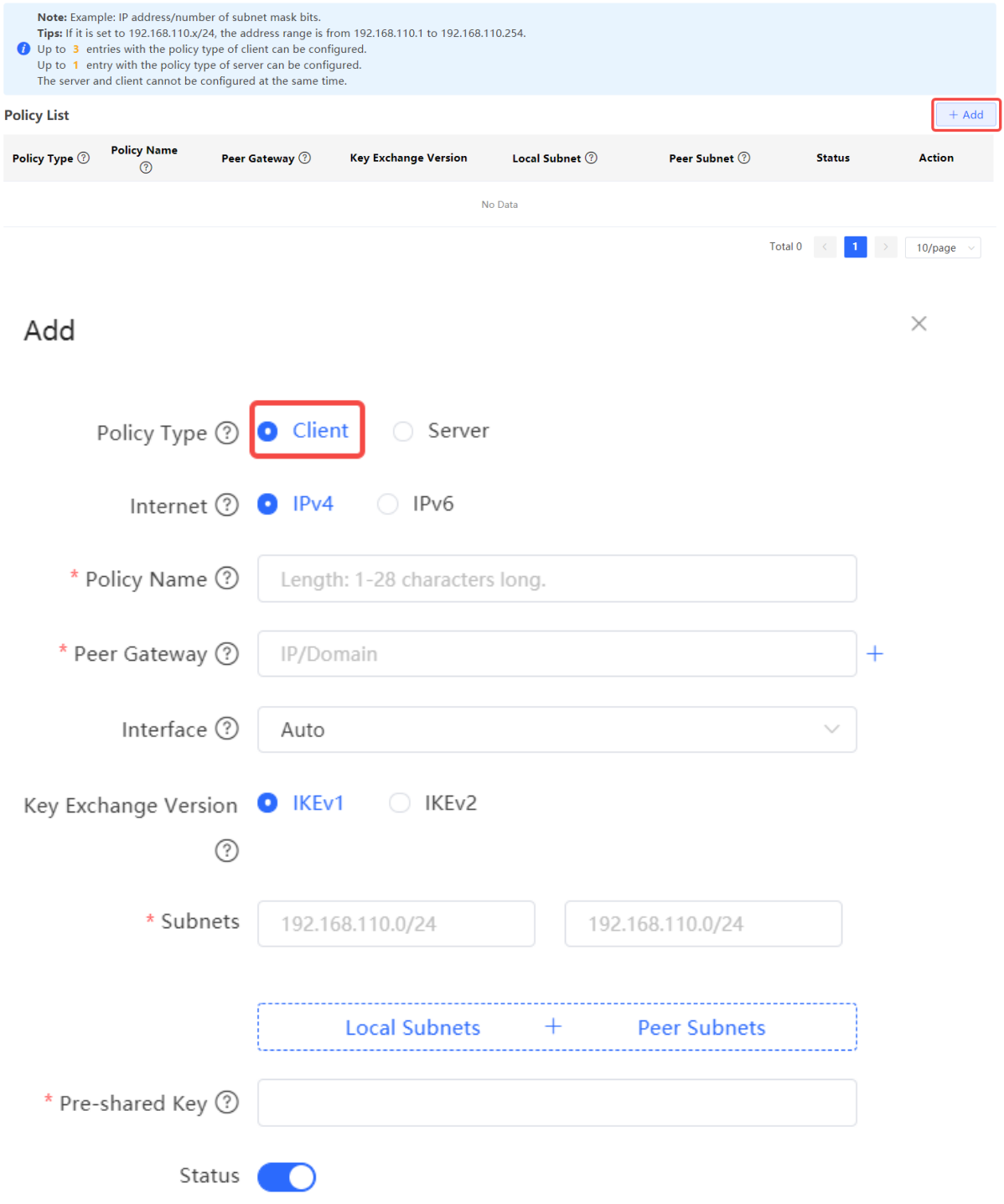


Table 10-4 IPsec client basic settings

Parameter	Description
Policy Name	Specify the name of the IPsec security policy. The name must be a string of 1 to 28 characters.

Parameter	Description
Internet	Format of the IP address. Both IPv4 and IPv6 address formats are supported.
Peer Gateway	Enter the IP address or domain name of the peer device.
Interface	Select a WAN interface used locally from the drop-down list box. In the multi-line scenario, you are advised to set this parameter to **Auto**.
Key Exchange Version	Select the IKE version for SA negotiation. There are two options available: ● IKEv1: The negotiation of SA in IKEv1 primarily consists of two phases. ○ Phase 1: The purpose is to establish an IKE SA using one of two negotiation modes: Main Mode and Aggressive Mode. Main Mode requires six ISAKMP (Internet Security Association and Key Management Protocol) messages to complete the negotiation, while Aggressive Mode only requires three ISAKMP messages. Aggressive Mode offers faster IKE SA establishment. However, it combines key exchange and identity authentication, which means it does not provide identity protection. ○ Phase 2: The purpose is to establish an IPsec SA for data transmission, utilizing a fast exchange mode that requires only three ISAKMP messages to complete the negotiation. ● IKEv2: In IKEv2, the negotiation process for SA is simplified. The establishment of one IKE SA and one pair of IPsec SAs can be accomplished using two exchanges with four messages. If there is a need to establish more than one pair of IPsec SAs, only one additional exchange is needed for each pair. This enables the negotiation to be completed with just two messages per pair.
Local Subnets	Specify the local subnet address range for the data flows to be protected, that is, the LAN port network segment of the server. The value is the combination of IP address and subnet mask.
Peer Subnets	Specify the peer subnet address range for the data flows to be protected, that is, the LAN port network segment of the client. The value is the combination of IP address and subnet mask.
Pre-shared Key	Configure the pre-shared key the same as that on the IPsec server.

Parameter	Description
Status	Specify whether to enable the security policy.

You can configure advanced parameters by referring to the corresponding settings on the IPsec server. For details, see Advanced Settings (Phase 1) and Advanced Settings (Phase 2).

10.1.4 Viewing the IPsec Connection Status

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **IPsec** > **IPsec Connection Status**.

You can view the IPsec tunnel connection status on the current page.

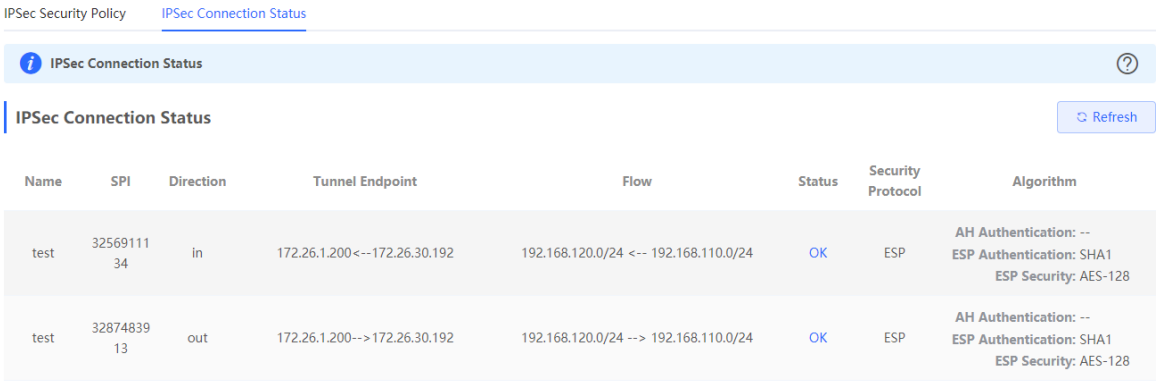


Table 10-5 IPsec tunnel connection status information

Parameter	Description
Name	Indicate the security policy name on the IPsec server or client.
SPI	Indicate the Security Parameter Index (SPI) of the IPsec connection, used to associate the received IPsec data packets with the corresponding SA. The SPI of each IPsec connection must be unique.
Direction	Indicate the direction of the IPsec connection. The value **in** indicates inbound, and the value **out** indicates outbound.
Tunnel Client	Indicate the gateway addresses on two ends of the IPsec connection. The arrow indicates the direction of data flows to be protected by the current tunnel.
Flow	Indicate the subnet range on two ends of the IPsec connection. The arrow indicates the direction of data flows to be protected by the current tunnel.
Status	Indicate the IPsec tunnel connection status.

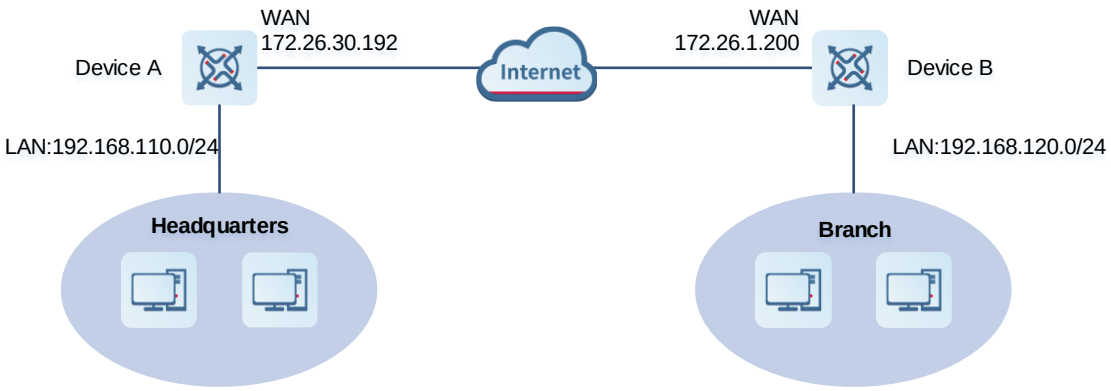
Parameter	Description
Security Protocol	Indicate the security protocol used by the IPsec connection.
Algorithm	Indicate the encryption algorithm and authentication algorithm used by the IPsec connection.

10.1.5 Typical Configuration Example

1. Networking Requirements

The HQ and branch of an enterprise are connected through the Internet. An IPsec tunnel needs to be established between the HQ gateway and branch gateway to ensure the confidentiality of transmitted data.

2. Networking Diagram



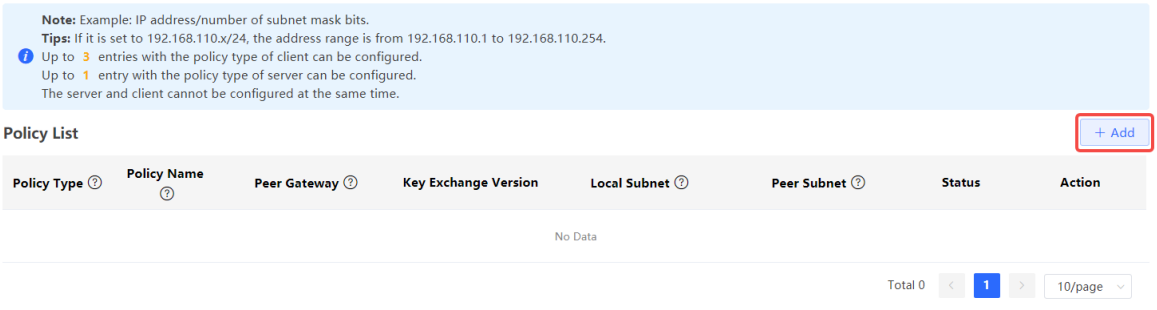
3. Configuration Roadmap

- Configure the HQ gateway Device A as the IPsec server.
- Configure the branch gateway Device B as the IPsec client.

4. Configuration Steps

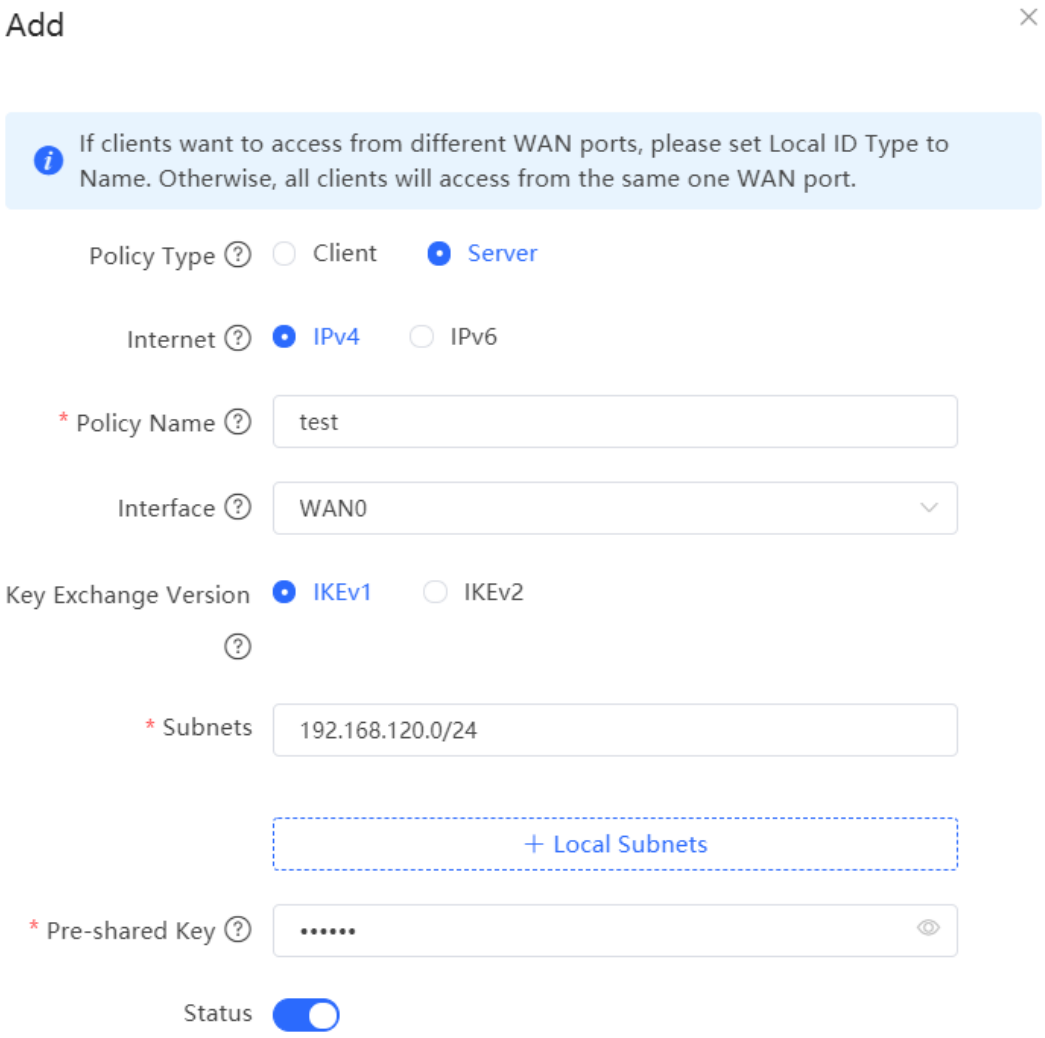
- Configure the HQ gateway.

(1) Log in to the web management system and choose **One-Device** > **Gateway** > **Config** > **VPN** > **IPsec** > **IPsec Security Policy** to access the IPsec Security Policy page.



(2) Click **Add**. In the dialog box that appears, set Policy Type to Server, enter the policy name, select the bound interface, and configure the local subnet to be accessed through IPsec and the pre-shared key.

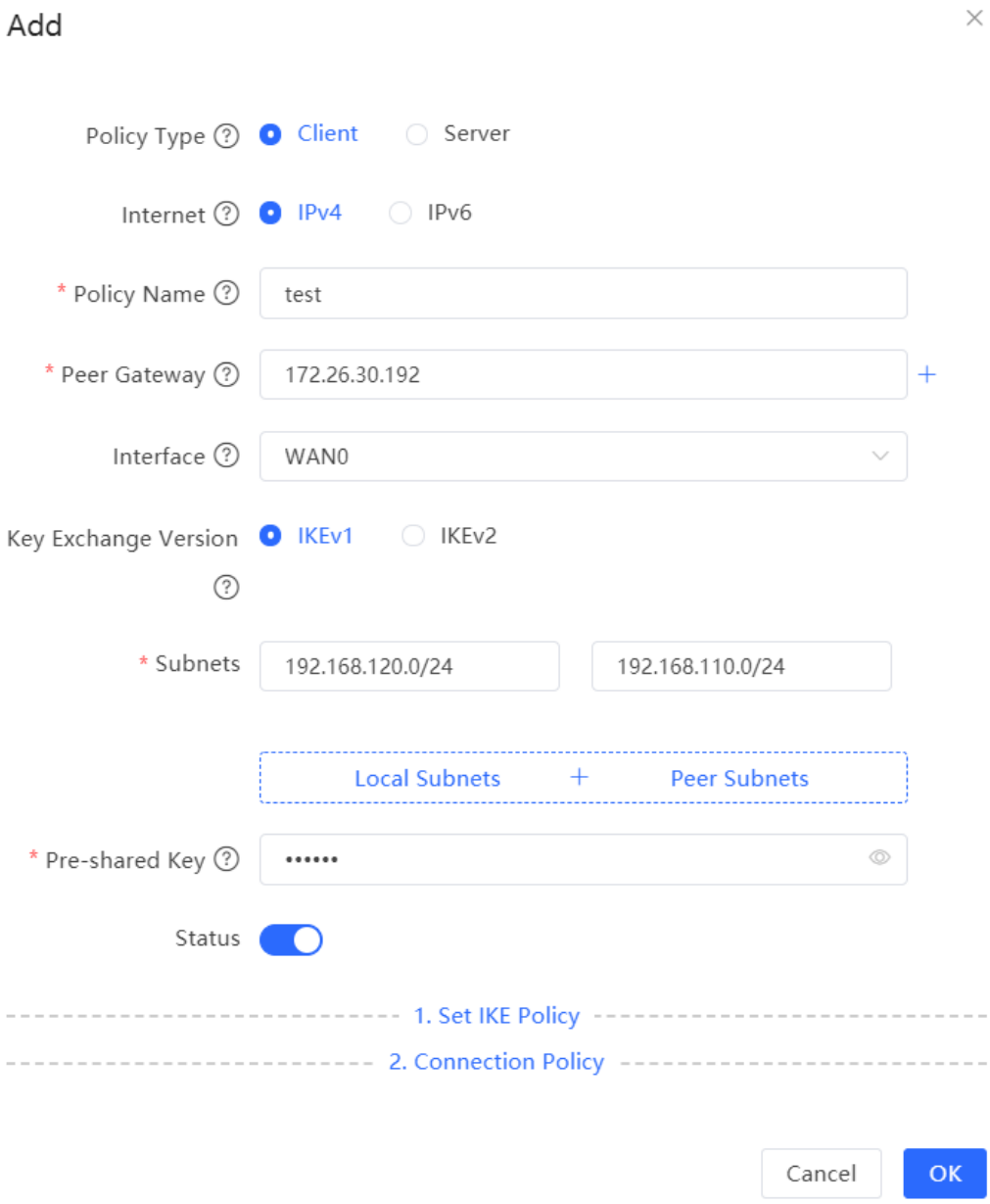
If the device connects to other EG devices in the Reyee network, you are advised to keep the default settings in IKE phase 1 and phase 2. If the device connects to devices from another vendor, keep the parameter settings consistent on the connected devices.



- Configure the branch gateway.

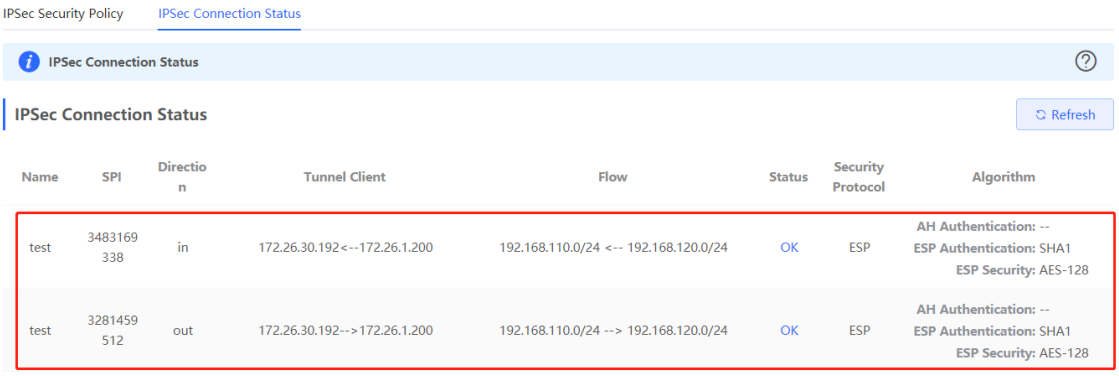
(1) Log in to the web management system and access the IPsec Security Policy page.

(2) Click **Add**. In the dialog box that appears, set Policy Type to Client, enter the policy name, select the peer gateway (WAN interface address or domain name of the HQ gateway), and configure the local subnet that needs to access the peer subnet and the pre-shared key the same as that on the HQ gateway. Keep the other phase 1 and phase 2 parameters consistent with those on the IPsec server.



5. Verifying Configuration

(1) Log in to the web management system of the HQ or branch gateway and choose **One-Device** > **Gateway** > **Config** > **VPN** > **IPsec** > **IPsec Connection Status**. You can view the IPsec connection status between the HQ and branch.



(2) Perform ping test between clients on the two ends that need to access each other. The clients can successfully ping and access each other.

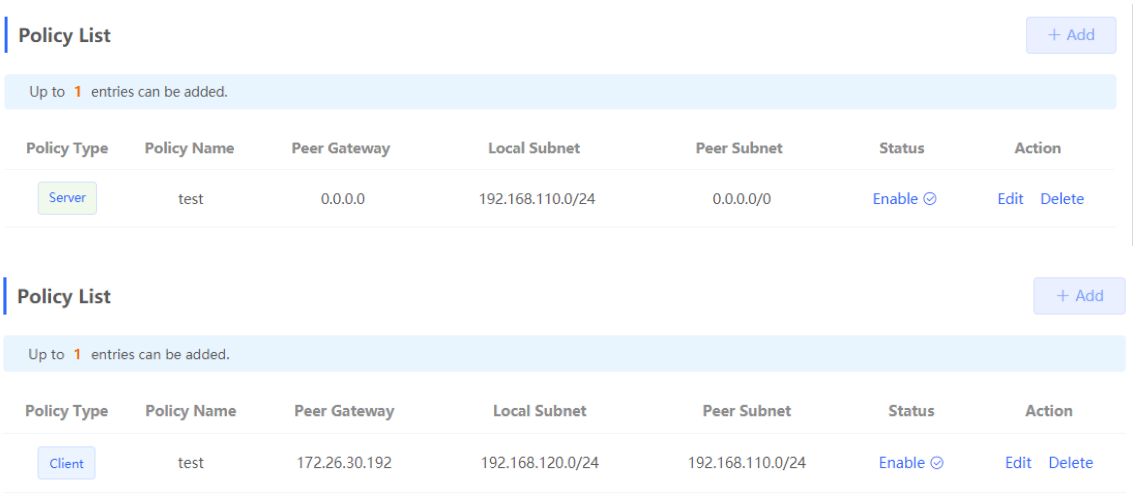
10.1.6 Solution to IPsec VPN Connection Failure

(1) Run the ping command to test the connectivity between the client and server. For details, see Section 12.11.3 Network Tools. If the ping fails, check the network connection settings. Check whether the branch EG can ping to HQ EG. If the ping fails, check the network connection between the two EGs.

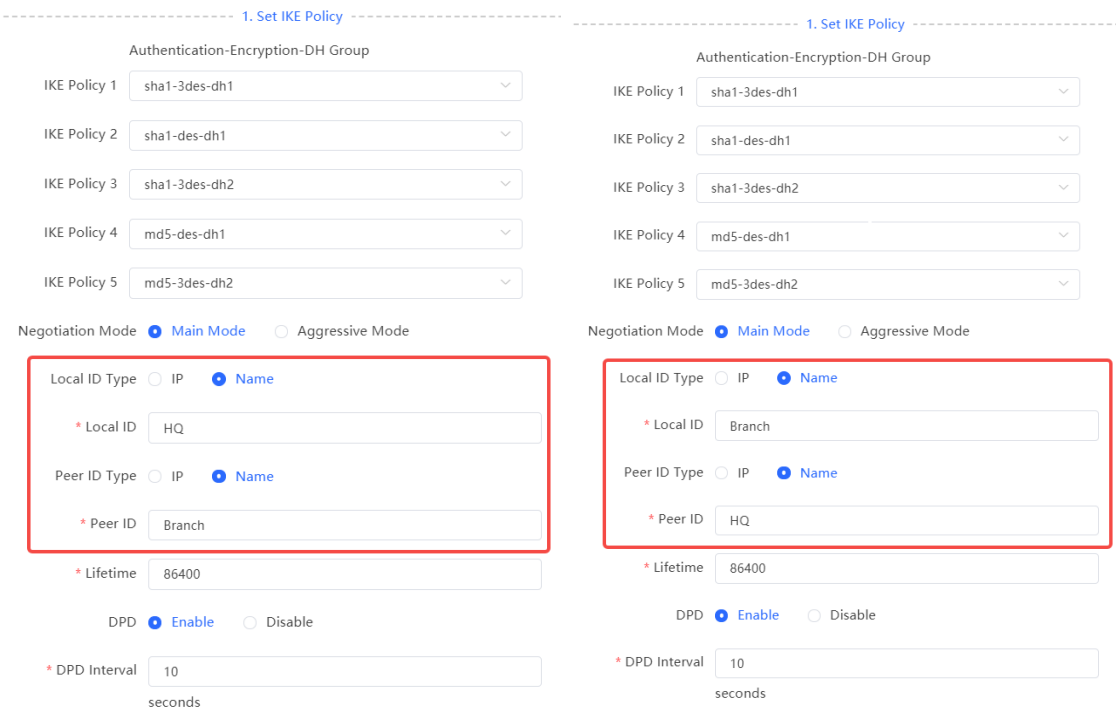
Choose **One-Device** > **Gateway** > **Config** > **Diagnostics** > **Network Tools**. Then, you can start the ping operation. For details, see Section 12.11.3 Network Tools.

(2) Confirm that the configurations on the IPsec server and IPsec client are correct.

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **IPsec** > **IPsec Security Policy** and confirm that the security policies configured on the two ends are matching.



(3) Check whether the WAN IP address of your HQ EG is a public IP address. If not, you need to configure DMZ or port mapping (UDP 500 and 4500 used as IPsec VPN port) on your egress gateway and set **Local ID Type** to **NAME** on HQ and branch gateways.



10.2 Configuring L2TP VPN

10.2.1 Overview

Layer Two Tunneling Protocol (L2TP) is a virtual tunneling protocol, usually used in virtual private networks.

The L2TP protocol does not provide encryption and reliability verification functions, but it can work with a security protocol to implement encrypted data transmission. L2TP is frequently used with IPsec to encapsulate packets using L2TP before encapsulating packets using IPsec. This combination implements user verification and address allocation through L2TP and ensures communication security through IPsec.

L2TP VPN can be used to establish secure tunnels between the enterprise HQ and branches and allow traveling employees to access the HQ. Currently, the device can be deployed as the L2TP server or client.

10.2.2 Configuring the L2TP Server

1. Basic Settings of L2TP Server

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **L2TP** > **L2TP Settings**.

Turn on the L2TP function, set **L2TP Type** to **Server**, set L2TP server parameters, and click **Save**.

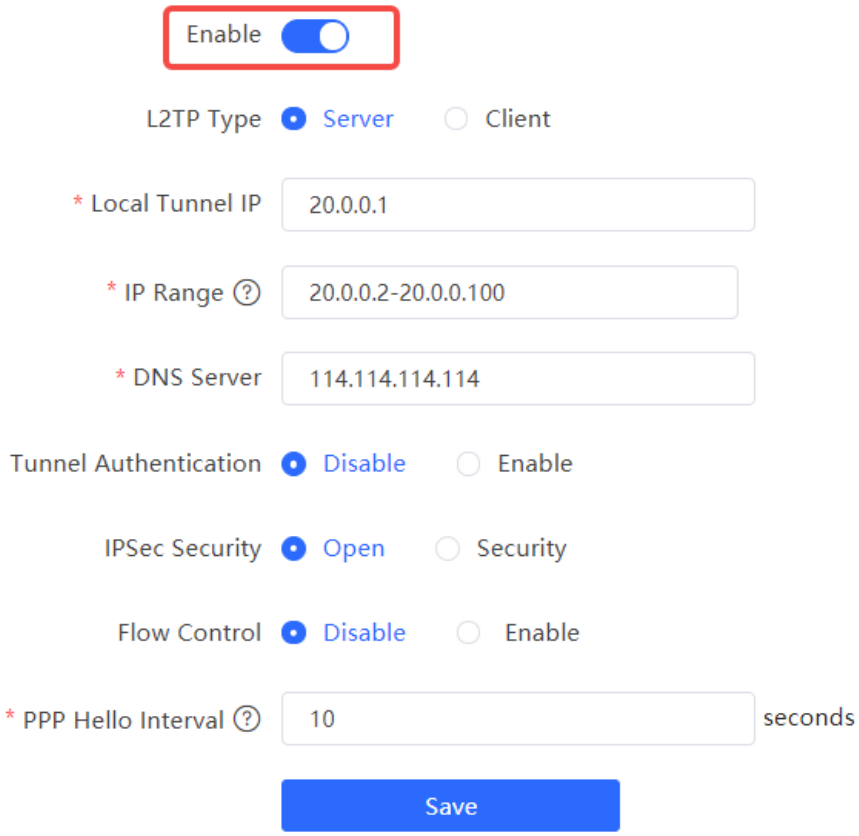


Table 10-6 L2TP server configuration

Parameter	Description
Local Tunnel IP	Specify the local virtual IP address of the L2TP server. Clients can dial up to access the L2TP server through this address.
IP Range	Specify the address pool used by the L2TP server to allocate IP addresses to clients.
DNS Server	Specify the DNS server address pushed by the L2TP server to clients.

Parameter	Description
Tunnel Authentication	Specify whether to enable L2TP tunnel authentication. If you enable this function, you need to configure a tunnel authentication key. By default, tunnel authentication is disabled. The tunnel authentication request can be initiated by clients. If tunnel authentication is enabled on one end, a tunnel to the peer can be established only when tunnel authentication is also enabled on the peer and consistent keys are configured on the two ends. Otherwise, the local end will automatically shut down the tunnel connection. If tunnel authentication is disabled on both ends, no authentication key is required for tunnel establishment. When a PC functions as the client to access the L2TP server, you are advised not to enable tunnel authentication on the L2TP server.
IPsec Security	Specify whether to encrypt the tunnel. If you select **Security**, the device encrypts the L2TP tunnel using IPsec, indicating the L2TP over IPsec mode. If an IPsec security policy is enabled on the current device, you cannot enable IPsec encryption for the L2TP tunnel. If you want to configure L2TP over IPsec, disable the IPsec security policy first. The IPsec encryption configuration on the L2TP server and client must be consistent. For details, see Configuring the L2TP over IPsec Server.
Flow Control	The VPN server has a lower priority to control the traffic of the client than the custom policy. The VPN server can only limit the maximum uplink and downlink bandwidth per user for the client. For details, see 8.6.2 Smart Flow Control.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after L2TP VPN is deployed. You are advised to retain the default configuration.

Caution

The local tunnel address and IP address range of the address pool cannot overlap the network segment of the LAN port on the device.

2. Configuring the L2TP over IPsec Server

Choose **One-Device > Gateway > VPN** > **L2TP** > **L2TP Settings**.

After you complete Basic Settings of L2TP Server, enable IPsec encryption on the L2TP server to guarantee communication security. For details on the IPsec configuration, see Section 10.1 Configuring IPsec VPN.

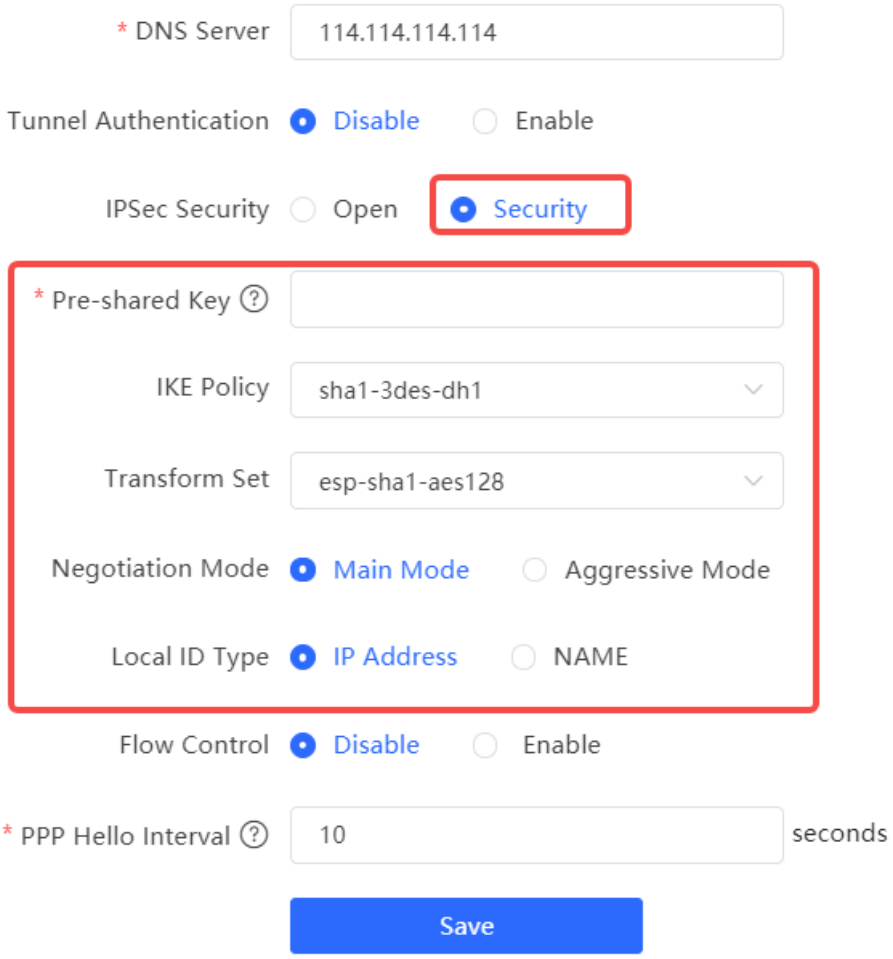


Table 10-7 L2TP over IPsec server configuration

Parameter	Description
Pre-shared Key	Specify the same unique pre-shared key as the credential for mutual authentication between the server and client.

Parameter	Description
IKE Policy	Select the encryption algorithm, hash algorithm, and DH group ID used by the IKE protocol. To ensure successful IKE negotiation, the two parties engaged in IKE negotiation must have at least one set of consistent IKE policy. The IKE policies on the server and client must be consistent. ● Hash algorithm: ○ sha1: SHA-1 algorithm ○ md5: MD5 algorithm ● Encryption algorithm: ○ des: DES algorithm using 56-bit keys ○ 3des: 3DES algorithm using 168-bit keys ○ aes-128: AES algorithm using 128-bit keys ○ aes-192: AES algorithm using 192-bit keys ○ aes-256: AES algorithm using 256-bit keys ● DH group ID: ○ dh1: 768-bit DH group ○ dh2: 1024-bit DH group ○ dh5: 1536-bit DH group
Transform Set	Specify the set of security protocol and algorithms. During IPsec SA negotiation, the two parties use the same transform set to protect specific data flow. The transform set on the server and client must be the same. ● Security protocol: The Encapsulating Security Payload (ESP) protocol provides data source authentication, data integrity check, and anti-replay functions for IPsec connections and guarantees data confidentiality. ● Verification algorithm: ○ sha1: SHA-1 HMAC ○ md5: MD5 HMAC ● Encryption algorithm: ○ des: DES algorithm using 56-bit keys ○ 3des: 3DES algorithm using 168-bit keys ○ aes-128: AES algorithm using 128-bit keys ○ aes-192: AES algorithm using 192-bit keys ○ aes-256: AES algorithm using 256-bit keys

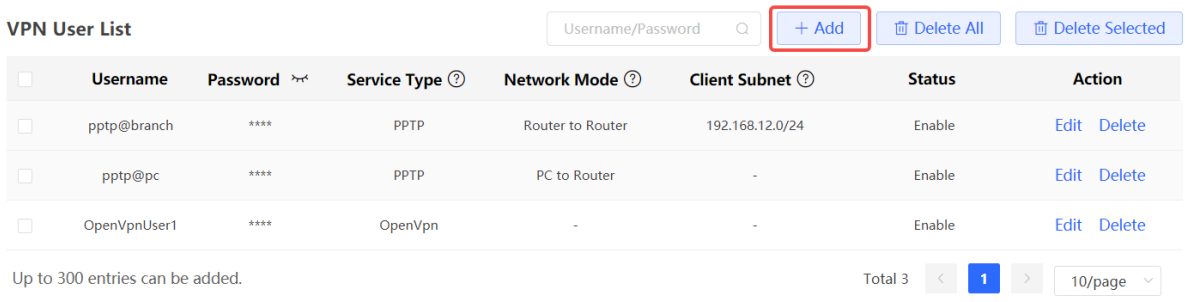
Parameter	Description
Negotiation Mode	Select **Main Mode** or **Aggressive Mode**. The negotiation mode on the server and client must be the same. ● **Main Mode**: This mode is applicable to communication between fixed public network IP addresses and point-to-point communication between devices. In this mode, the peer identity is authenticated to provide high security. ● **Aggressive Mode**: The public network IP addresses obtained by ADSL dial-up users are not fixed and an NAT device may exist. Therefore, the aggressive mode is used to implement NAT traversal. In this mode, you need to set the local and peer ID type to **NAME** as the IP address is not fixed. The aggressive mode does not authenticate the peer identity, so it has low security.
Local ID Type	Specify the ID type of the local device. The peer ID of the client must be the same as local ID of the server. ● **IP**: The IP address is used as the identity ID. The ID of the local device is generated automatically. ● **NAME**: The host character string is used as the identity ID. The ID of the local device is generated automatically. In this case, you also need to configure the host character string that is used as the identity ID. When the WAN interface IP address of the server is a private network address, you need to set **Local ID Type** to **NAME** and configure DMZ on the external device. When the IP address is not fixed, you need to set **Local ID Type** to **NAME** and modify the peer device settings accordingly.
Local ID	When **Local ID Type** is set to **NAME**, the host character string is used as the identity ID. The peer ID of the client must be the same as local ID of the server.

3. Configuring L2TP User

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **VPN Account**

Only user accounts added to the VPN client list are allowed to dial up to connect to the L2TP server. Therefore, you need to manually configure user accounts for clients to access the L2TP server.

Click **Add**. In the dialog box that appears, set **Service Type** to **L2TP** or **ALL**. (If you select **ALL**, the created account can be used to establish all types of VPN tunnels.) Enter the username, password, and peer subnet, select a network mode, and click **OK**.



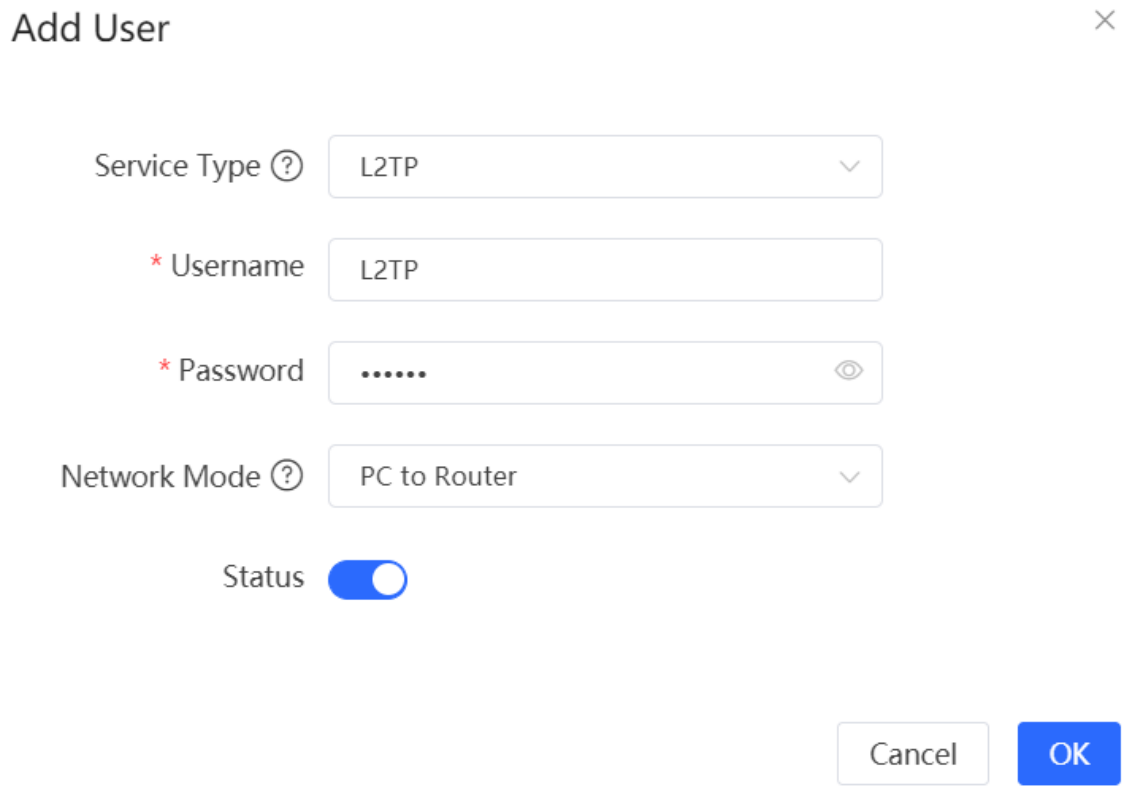


Table 10-8 L2TP user configuration

Parameter	Description
Username/Password	Specify the name and password of the L2TP user allowed to dial up to connect to the L2TP server. The username and password are used to establish a connection between the server and client.
Network Mode	● PC to Router: The dial-up client is an individual. Select this mode when a PC wants to dial up to communicate with the remote PC through the LAN. ● Router to Router: The dial-up client is a user in a network segment. Select this mode when the LANs on two ends of the tunnel need to communicate through router dial-up.
Client Subnet	Specify the IP address range used by the LAN on the peer end of the L2TP tunnel. Generally, the Client Subnet is the IP address network segment of the LAN port on the device. (The LAN network segments of the server and client cannot overlap.) For example, when a branch dials up to connect to the HQ, enter the LAN network segment of the router. Note: When the Network Mode is set to Router to Router, you can click + to set multiple pairs of peer subnets for scenarios where multiple clients are connected to the same server.

Parameter	Description
Status	Specify whether to enable the user account.

10.2.3 Configuring the L2TP Client

1. Basic Settings of L2TP Client

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **L2TP** > **L2TP Settings**.

Turn on the L2TP function, set **L2TP Type** to **Client**, set L2TP client parameters, and click **Save**.

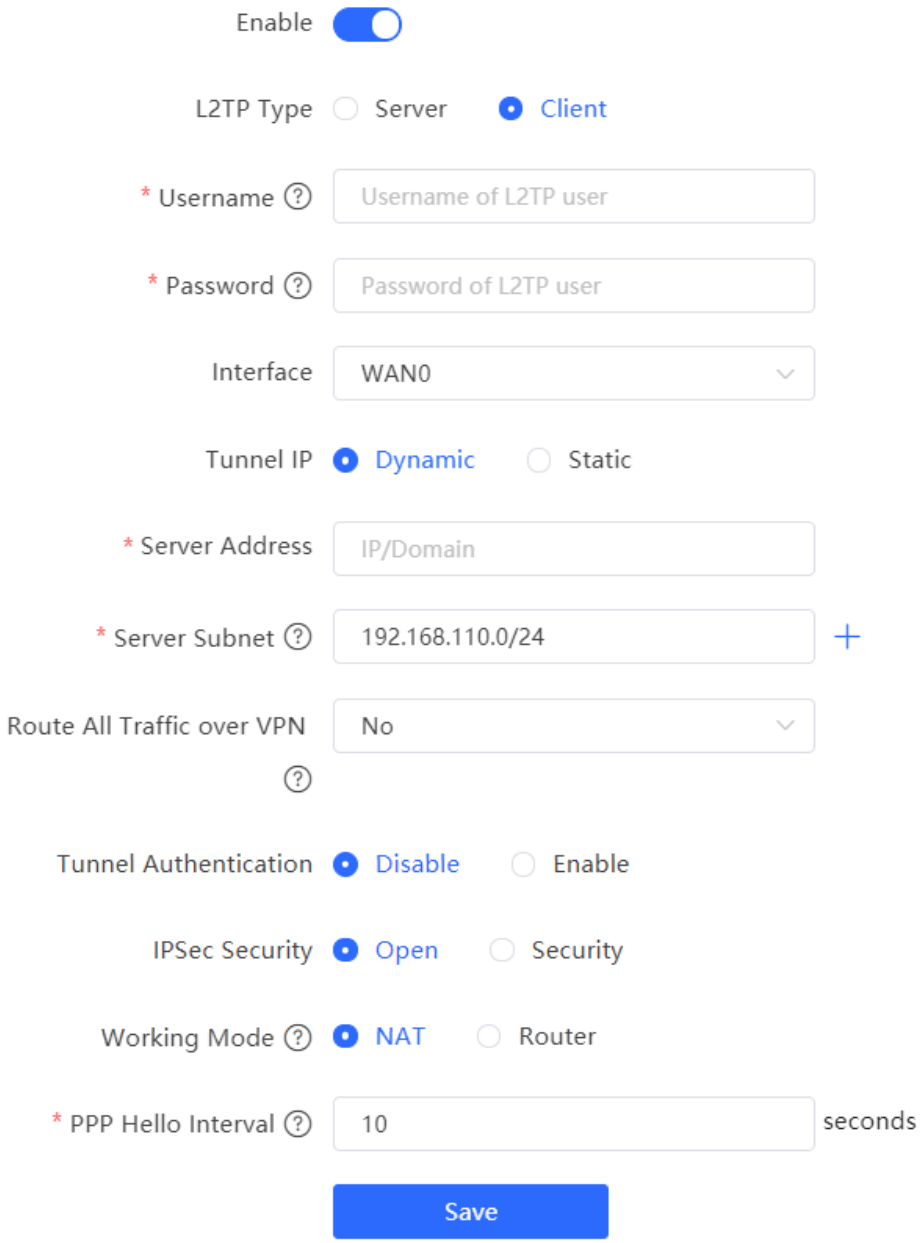


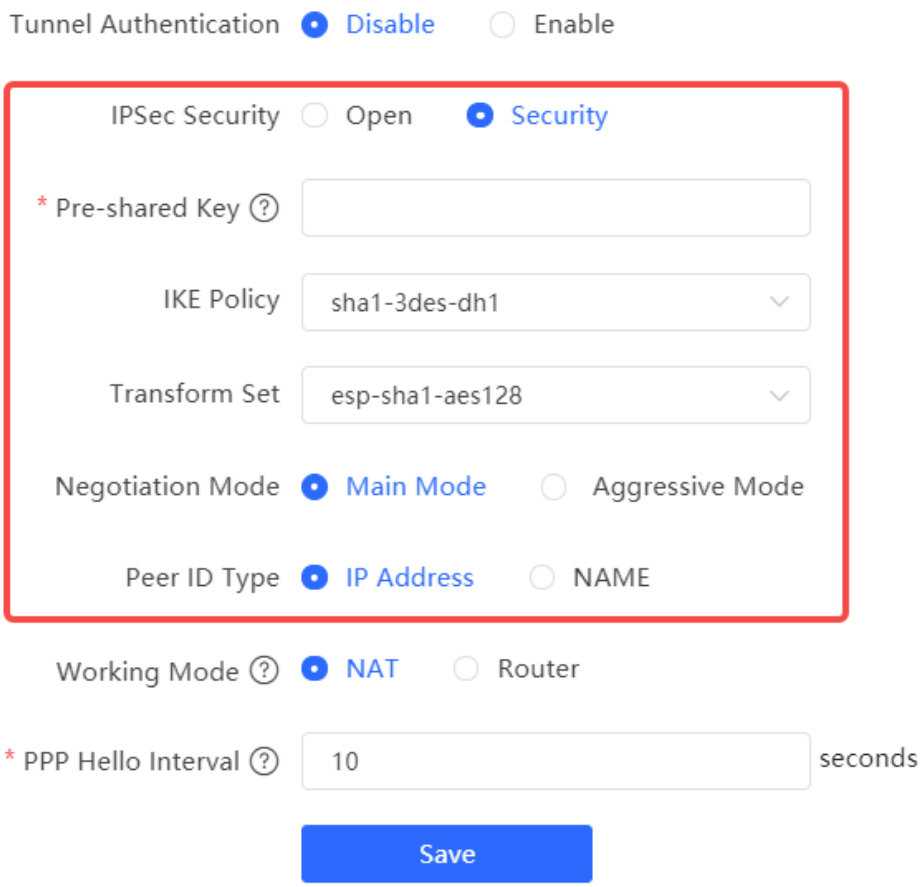
Table 10-9 L2TP client configuration

Parameter	Description
Username/Password	Specify the username and password for identity authentication for communication over the L2TP tunnel. The values must be the same as those configured on the L2TP server.
Interface	Specify the WAN interface used by the client.
Tunnel IP	Specify the virtual IP address of the VPN tunnel client. If you select **Dynamic**, the client obtains an IP address from the server address pool. If you select **Static**, manually configure an idle static address within the range of the server address pool as the local tunnel IP address.
Server Address	Enter the WAN interface IP address or domain name of the server. This address must be a public network IP address.
Server Subnet	Enter the LAN network segment in which clients want to access the server. The value cannot overlap with the LAN network segment of the client.
Route ALL Traffic over VPN	Once this feature is enabled, all traffic will be directed through the VPN connection, that is, VPN is configured as the default route.
Tunnel Authentication	Specify whether to enable L2TP tunnel authentication. If you enable this function, you need to enter tunnel authentication key the same as that configured on the server. By default, tunnel authentication is disabled. To protect tunnel security, you are advised to enable tunnel authentication.
IPsec Security	Specify whether to encrypt the tunnel. If you select **Security**, the device Enable the L2TP tunnel using IPsec, indicating the L2TP over IPsec mode. The IPsec encryption configuration on the server and client must be consistent. For details, see Configuring the L2TP over IPsec Client.
Working Mode	● **NAT**: Perform NAT traversal on the data packet passing through the L2TP tunnel. That is, replace the source IP address of the data packet with the local virtual IP address of the L2TP tunnel. In NAT mode, the server cannot access the LAN where the client resides. ● **Router**: Only route the data packet passing through the L2TP tunnel. In router mode, the server can access the LAN where the client resides.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after L2TP VPN is deployed. You are advised to retain the default configuration.

2. Configuring the L2TP over IPsec Client

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **L2TP** > **L2TP Settings**.

After you complete Basic Settings of L2TP Client, enable IPsec encryption on the L2TP client to guarantee communication security. The IPsec encryption configuration on the server and client must be consistent. For details, see Configuring the L2TP over IPsec Server.



10.2.4 Viewing the L2TP Tunnel Information

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **L2TP** > **Tunnel List**.

It takes some time to establish a VPN connection between the server and client. After the configuration of the server and client is completed, wait for 1 to 2 minutes to refresh the page and view the L2TP tunnel establishment status.

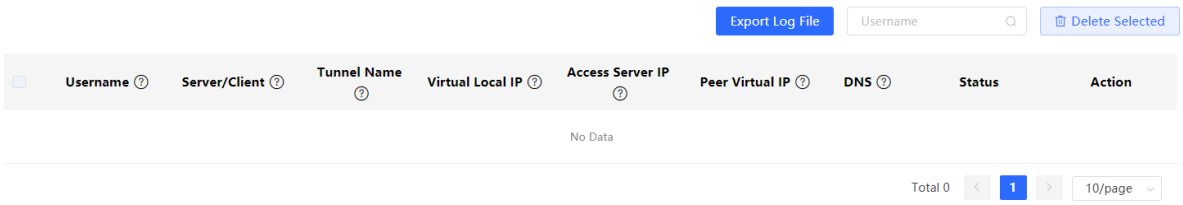


Table 10-10 L2TP tunnel information

Parameter	Description
Username	Indicate the username used by the client for identity authentication.

Parameter	Description
Server/Client	Indicate the role of the current device, which is client or server.
Tunnel Name	Indicate the name of the vNIC generated by L2TP.
Virtual Local IP	Indicate the local virtual IP address of the tunnel. The virtual IP address of the L2TP client is allocated by the L2TP server.
Access Server IP	Indicate the real IP address of the peer connecting to the L2TP tunnel.
Peer Virtual IP	Indicate the peer virtual IP address of the tunnel. The virtual IP address of the L2TP client is allocated by the L2TP server.
DNS	Indicate the DNS server address allocated by the L2TP server.

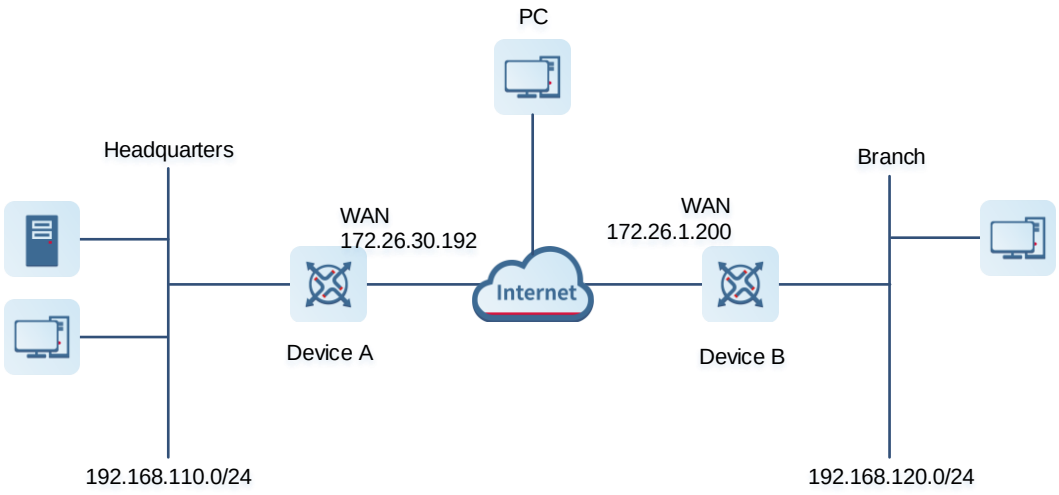
10.2.5 Typical Configuration Example

1. Networking Requirements

An enterprise wants to establish an L2TP tunnel to allow its traveling employees and branch employees to access the servers deployed in the HQ LAN.

- Traveling employees want to access the HQ servers from their PCs through L2TP VPN.
- Branch employees need to frequently access documents on the HQ servers. The enterprise wants to deploy the branch router (Device B) as the L2TP client, so that branch employees can dial up to transparently and directly access documents on the HQ servers, as if they are accessing servers inside the branch.

2. Networking Diagram



3. Configuration Roadmap

- Configure the HQ gateway Device A as the L2TP server.
- Configure the branch gateway Device B as the L2TP client.
- Configure the PC of the traveling employee as the L2TP client.

4. Configuration Steps

- Configure the HQ gateway.

Note

The LAN address of the HQ cannot conflict with that of the branch. Otherwise, resource access will fail.

(1) Log in to the web management system and choose **One-Device** > **Gateway** > **Config** > **VPN** > **L2TP** > **L2TP Settings** to access the L2TP Settings page.

(2) Turn on the L2TP function, set L2TP Type to **Server**, enter the local tunnel IP, IP Range, and DNS Server address, specify whether to enable IPsec encryption and tunnel authentication, and click **Save**.

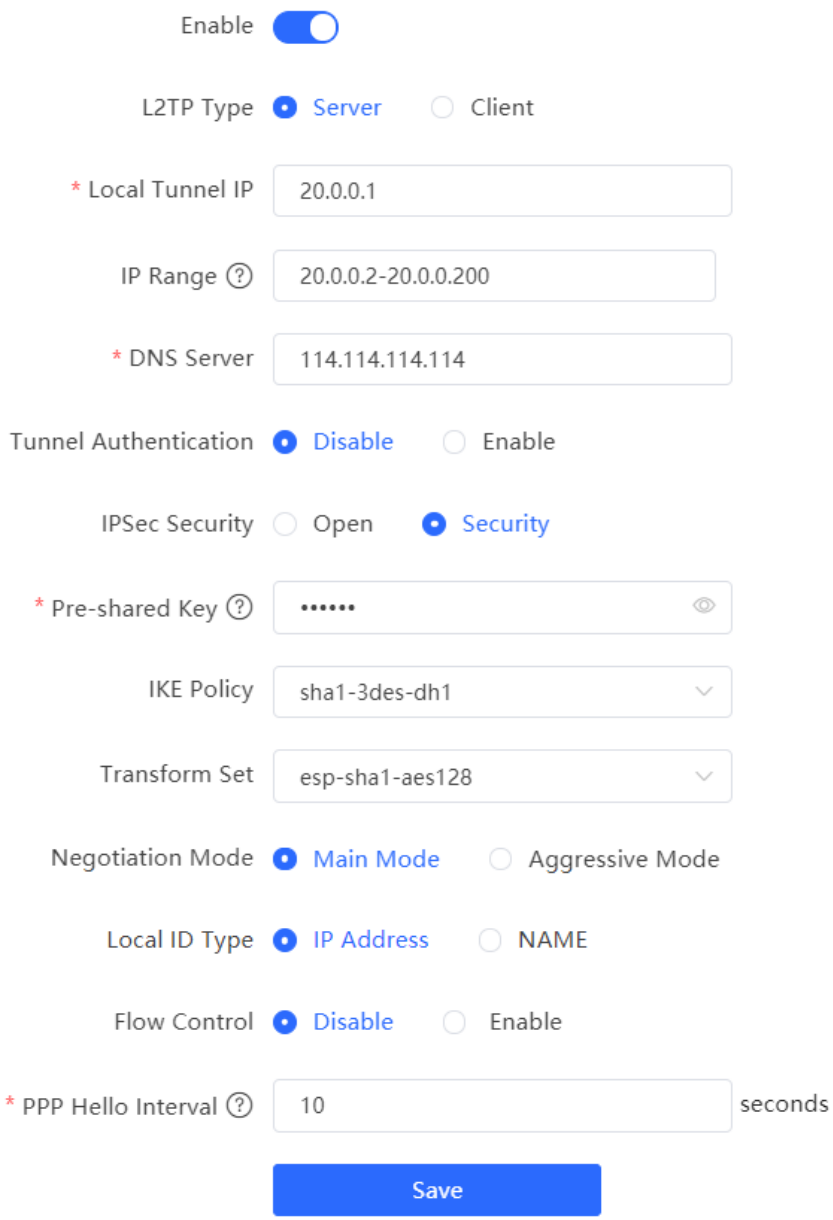


Table 10-11 L2TP server configuration

Parameter	Description
Local Tunnel IP	Enter an IP address not in the LAN network segment. The PC can dial up to access the server through this IP address.
IP Range	Enter an IP address range not in the LAN network segment, which is used to allocate IP addresses to clients.
DNS Server	Enter an available DNS server address.

Parameter	Description
Tunnel Authentication	By default, tunnel authentication is disabled. After this function is enabled, the server and client can be connected only when they use the same tunnel key. You can keep tunnel authentication disabled.
IPsec Security	Specify whether to encrypt the L2TP tunnel using the IPsec protocol. You are advised to select **Security** to guarantee data security. If an IPsec security policy is enabled on the current device, you cannot enable IPsec encryption for the L2TP tunnel. If you want to configure L2TP over IPsec, disable the IPsec security policy first.
Pre-shared Key	Enter the key for IPsec authentication. The client can access the server only when the same pre-shared key is configured on the client.
IKE Policy Transform Set Negotiation Mode Local ID Type Local ID	Keep the default settings unless otherwise specified.
Flow Control	The VPN server has a lower priority to control the traffic of the client than the custom policy. The VPN server can only limit the maximum uplink and downlink bandwidth per user for the client. For details, see 8.6.2 Smart Flow Control.
PPP Hello Interval	Keep the default settings unless otherwise specified.

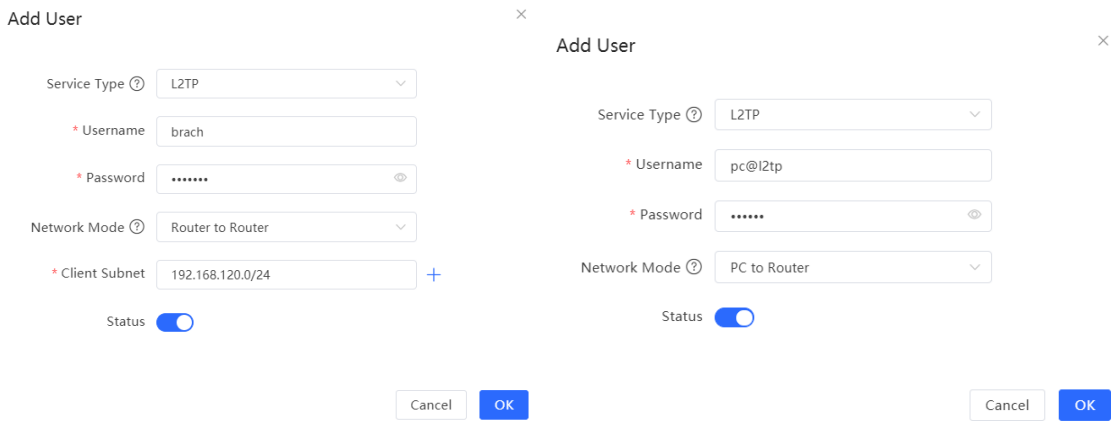
(3) Choose **One-Device** > **Gateway** > **Config** > **VPN** > **VPN Account** and add L2TP user accounts for the traveling employee and branch employee to access the HQ.

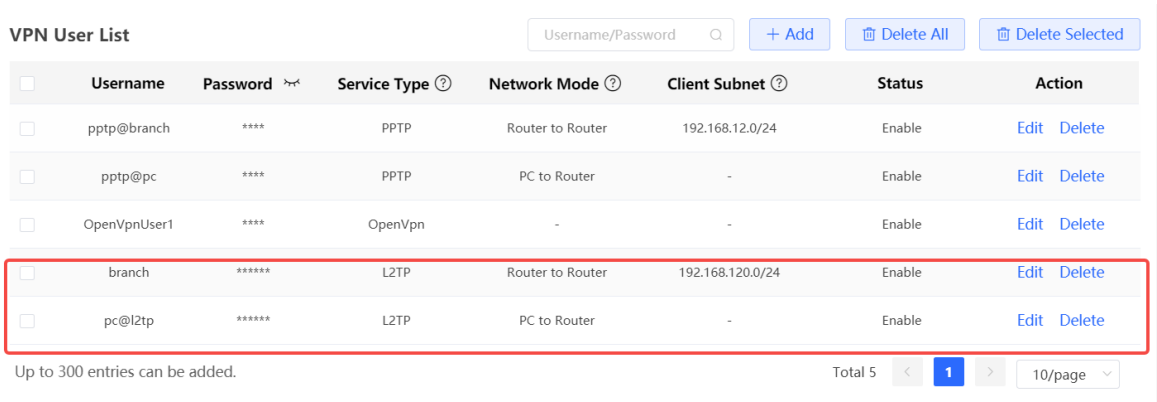
For the traveling employee account, set **Network Mode** to **PC to Router**.

For the branch employee account, set **Network Mode** to **Router to Router** and **Peer Subnet** to the LAN network segment of the branch gateway, which is 192.168.120.0/24.

Caution

The LAN network segments of the server and client cannot overlap.





- Configure the branch gateway.

(1) Log in to the web management system and access the L2TP Settings page.

(2) Turn on the L2TP function, set L2TP Type to Client, enter the username and password configured on the server, server address, and LAN network segment of the peer, configure IPsec encryption parameters the same as those on the server, and click Save.

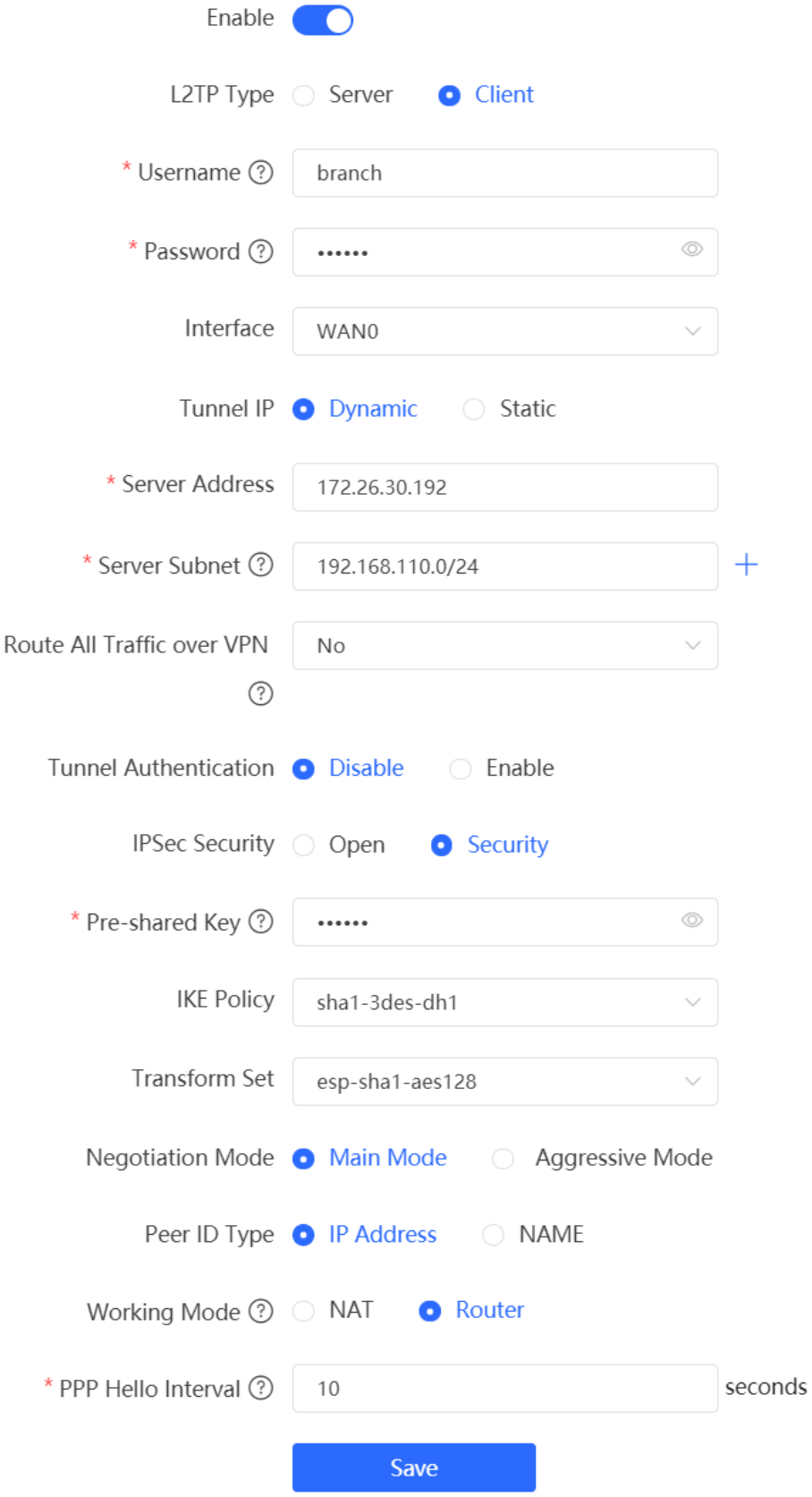

Enable
L2TP Type
Server
Client
* Username
branch
* Password
Interface
WAN0
Tunnel IP
Dynamic
Static
* Server Address
172.26.30.192
* Server Subnet
192.168.110.0/24
Route All Traffic over VPN
No
Tunnel Authentication
Disable
Enable
IPSec Security
Open
Security
* Pre-shared Key
IKE Policy
sha1-3des-dh1
Transform Set
esp-sha1-aes128
Negotiation Mode
Main Mode
Aggressive Mode
Peer ID Type
IP Address
NAME
Working Mode
NAT
Router
* PPP Hello Interval
10
seconds
Save

Table 10-12 L2TP client configuration

Parameter	Description
Username/Password	Enter the username and password configured on the server.
Interface	Select the WAN interface on the client to establish a tunnel with the server.
Tunnel IP	Select **Dynamic** to automatically obtain the tunnel IP address. You can also select Static and enter an IP address in the address pool of the server.
Server Address	Enter the WAN interface address of the server, which is 172.26.30.192.
Server Subnet	Enter the LAN network segment (LAN port IP address range) of the server, which is 192.168.110.0/24.
Route ALL Traffic over VPN	Once this feature is enabled, all traffic will be directed through the VPN connection, that is, VPN is configured as the default route.
Tunnel Authentication	The value must be the same as that on the server. In this example, you need to disable tunnel authentication.
IPsec Security	The value must be the same as that on the server. In this example, you need to set this parameter to **Security**.
Pre-shared Key	Enter the pre-shared key configured on the server.
IKE Policy Transform Set Negotiation Mode Peer ID Type Peer ID	The settings must be the same as those on the server. Set **Peer ID Type** to the same value as that of **Local ID Type** on the server.
Working Mode	If the HQ wants to access the LAN of the branch, set this parameter to **Router**.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after L2TP VPN is deployed. Keep the default settings.

- Configure the PC of the traveling employee.

Note

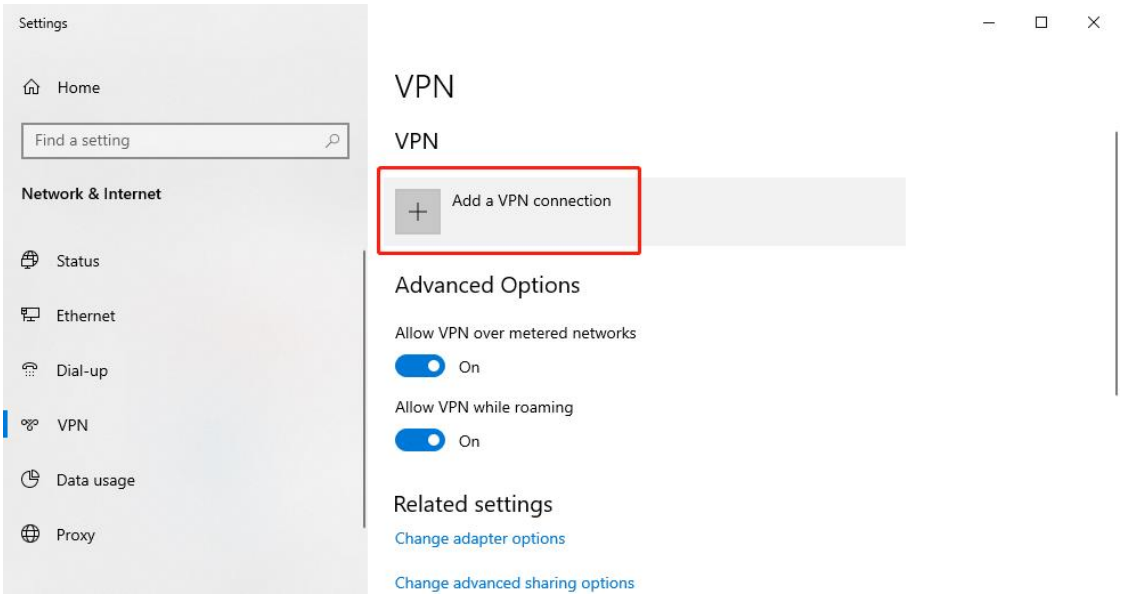
Configure the PC of a traveling employee as the L2TP client. The following uses the PC running Windows 10 operating system as an example.

The Windows XP (shorted as XP) system and Windows 7/Windows 10 (shorted as Win7/10) system differ in their support for L2TP VPN: To enable L2TP VPN in the XP system, you need to modify the service registries. L2TP is supported in the Win7/10 system by default, without the need to modify registries.

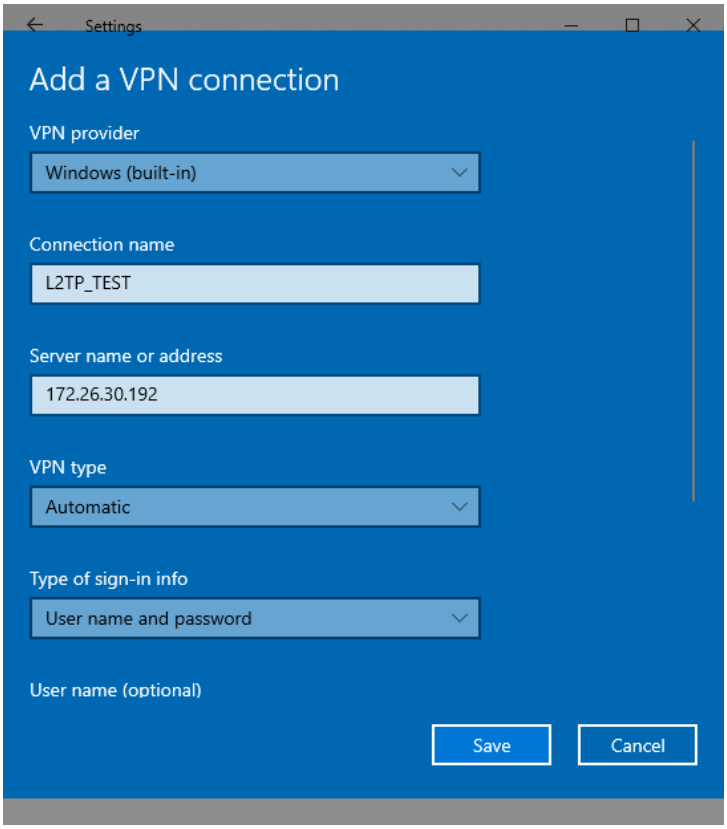
Neither the Win7/Win10 system nor the XP system supports L2TP tunnel authentication. Therefore, tunnel authentication must be disabled on the server.

Apple mobile phones support L2TP over IPsec but do not support IPsec encryption for L2TP dial-up.

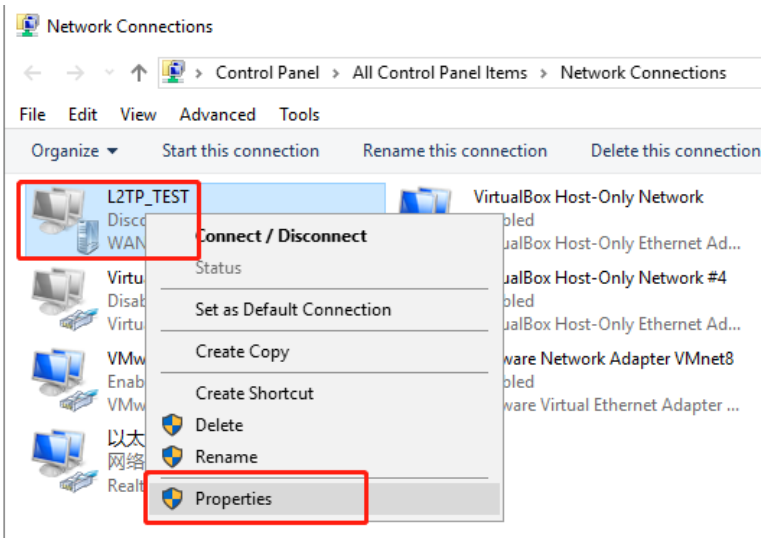
(1) Choose **Settings** > **Network & Internet** > **VPN** to access the VPN page.



(2) Click **Add a VPN connection**. In the dialog box that appears, set VPN provider to **Windows**, enter the connection name and server address or domain name, and click **Save**.



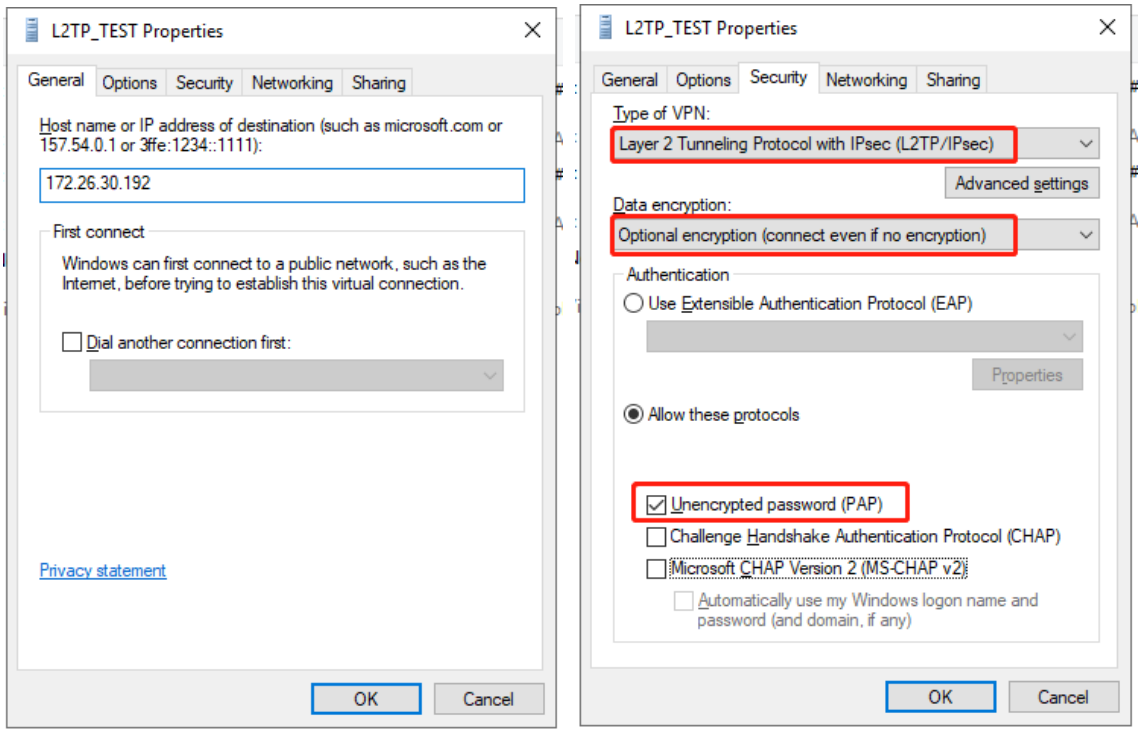
(3) Right-click the created VPN connection named **L2TP_TEST** and select Properties to view the properties of the network connection.



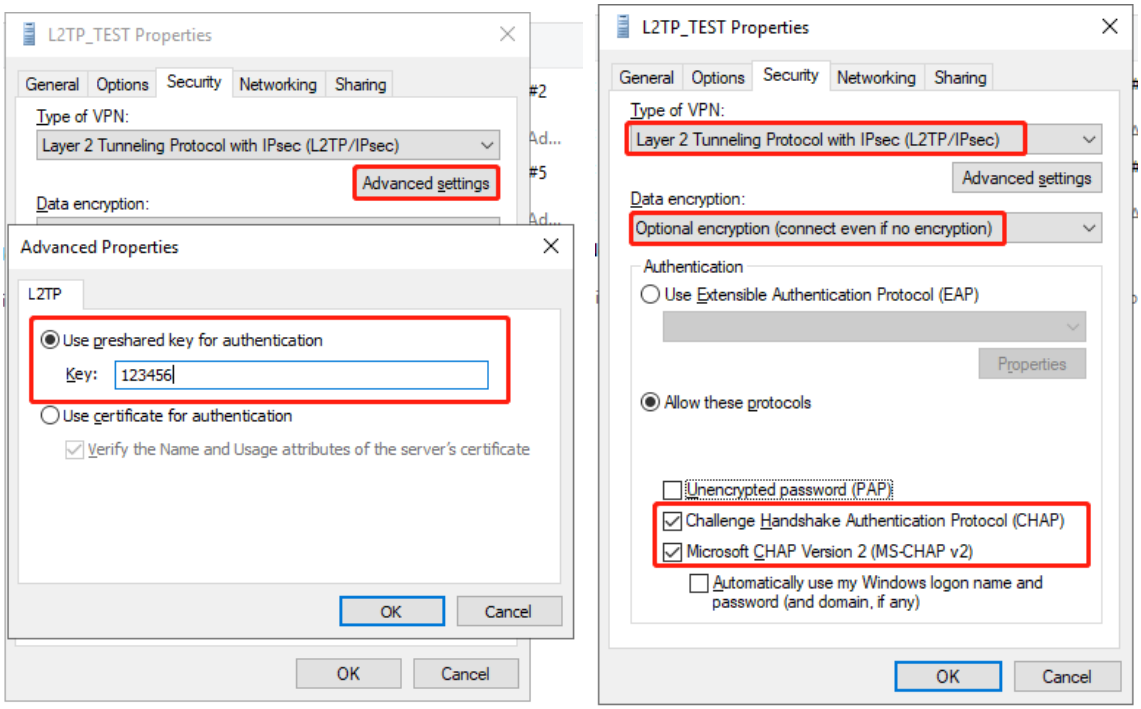
(4) In the dialog box that appears, click the Security tab, and set Type of VPN to Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec) and Data encryption to Optional encryption (connect even if no encryption).

If IPsec encryption is not enabled on the L2TP server, select **Unencrypted password (PAP)** and click **OK**. Skip Step (5) .

If IPsec encryption is enabled on the L2TP server, perform Step (5) .



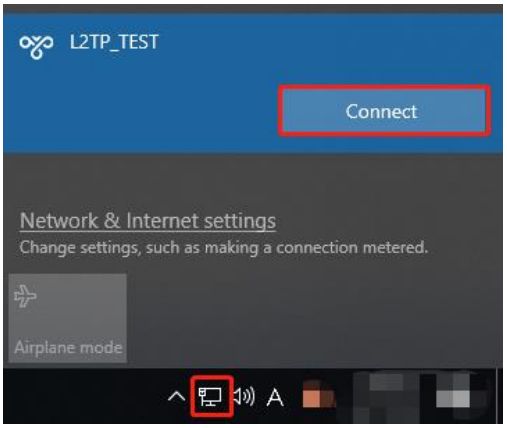
(5) If IPsec encryption is enabled on the server, select **CHAP** and **MS-CHAP v2** as the identity authentication protocols and click **Advanced settings**. In the dialog box that appears, configure the pre-shared key the same as that on the server. After completing the configuration, click **OK**.

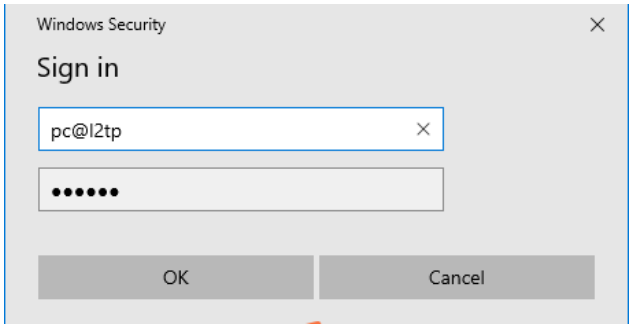


Note

The device does not support EAP for identity authentication. Therefore, you cannot select EAP-related identity authentication options in the Windows client. Otherwise, the VPN connection fails.

(6) After the L2TP client configuration is completed on the PC, initiate a VPN connection on the PC. Click the network icon in the task bar, select the created L2TP VPN connection, and click Connect. In the dialog box that appears, enter the username and password configured on the server.

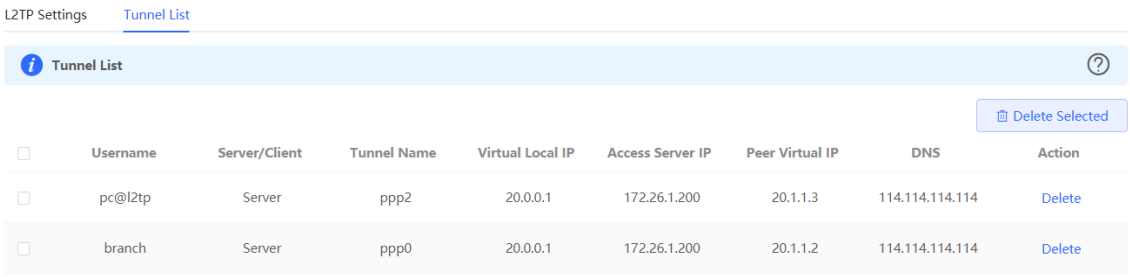




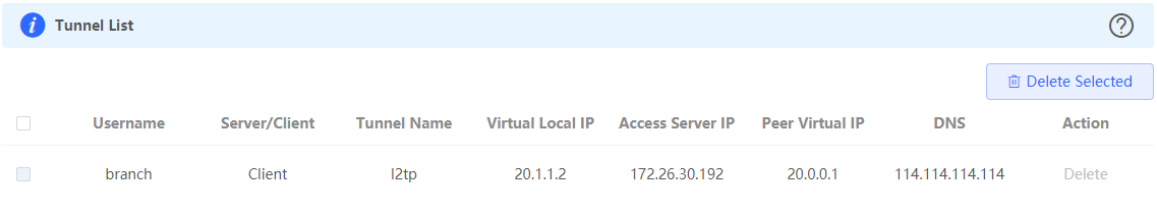
5. Verifying Configuration

(1) After the server and client are configured, wait for about 1 minute. If you can view the L2TP tunnel connection information on the HQ server and branch client, the connection is successful.

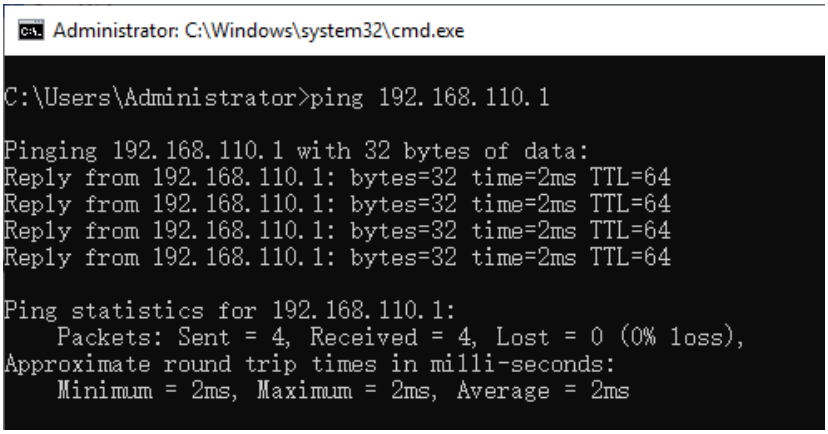
HQ:



Branch:



(2) Ping the LAN address of the peer from the HQ or branch. The HQ and branch can successfully communicate. The PC of the traveling employee and the PC of the branch employee can access the HQ server.



10.2.6 Solution to L2TP VPN Connection Failure

(1) Run the ping command to test the connectivity between the client and server. For details, see Section 12.11.3 Network Tools. If the ping fails, check the network connection settings. Check whether the branch EG can ping to HQ EG. If the ping fails, check the network connection between the two EGs.

Choose **One-Device** > **Gateway** > **Config** > **Diagnostics** > **Network Tools**. Then, you can start the ping operation. For details, see Section 12.11.3 Network Tools.

(2) Check whether the username and password used by the client are the same as those configured on the server.

(3) Check whether the WAN interface IP address of your HQ EG is a public network IP address. If not, you need to configure DMZ on your egress gateway.

10.3 Configuring PPTP VPN

10.3.1 Overview

Point-to-Point Tunneling Protocol (PPTP) is an enhanced security protocol designed based on the Point-to-Point Protocol (PPP). It allows an enterprise to use private tunnels to expand its enterprise network over the public network. PPTP relies on the PPP protocol to implement security functions such as encryption and identity authentication. Generally, PPTP works with Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv1/v2), or Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) for identity authentication and Microsoft Point-to-Point Encryption (MPPE) for encryption to improve security.

Currently, the device can be deployed as the PPTP server or client. It supports MPPE for encryption MSCHAP-v2 for identity authentication, and does not support EAP authentication.

10.3.2 Configuring the PPTP Service

1. Configuring the PPTP Server

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **PPTP** > **PPTP Settings**.

Turn on the PPTP function, set **PPTP Type** to **Server**, configure PPTP server parameters, and click **Save**.

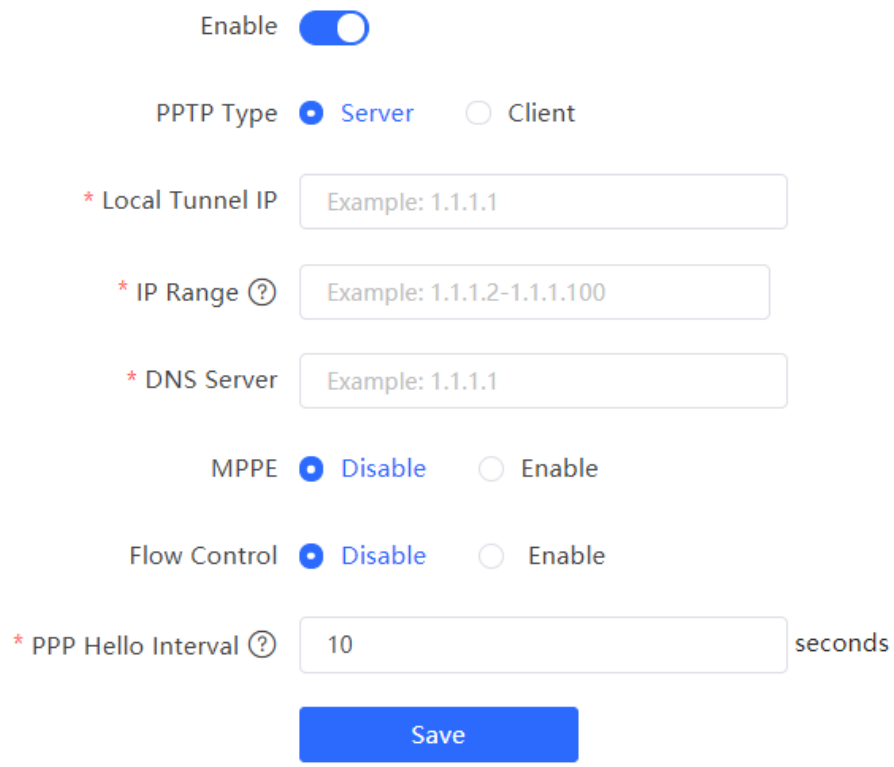


Table 10-13 PPTP server configuration

Parameter	Description
Local Tunnel IP	Specify the local virtual IP address of the L2TP server. Clients can dial up to access the L2TP server through this address.
IP Range	Specify the address pool used by the PPTP server to allocate IP addresses to clients.
DNS Server	Specify the DNS server address pushed by the PPTP server to clients.

Parameter	Description
MPPE	Specify whether to use MPPE to encrypt the PPTP tunnel. After MPPE is enabled on the server: If **Data encryption** is set to **Optional encryption** on the client, the server and client can be connected but the server does not encrypt packets. If **Data encryption** is set to **Require encryption** on the client, the server and client can be connected and the server encrypts packets. If **Data encryption** is set to **No encryption allowed** on the client, the server and client cannot be connected. If MPPE is disabled on the server but the client requires encryption, the server and client connection fails. By default, MPPE is disabled on the server. After you enable MPPE, the bandwidth performance of the device degrades. You are advised to keep MPPE disabled if there are no special security requirements.
Flow Control	The VPN server has a lower priority to control the traffic of the client than the custom policy. The VPN server can only limit the maximum uplink and downlink bandwidth per user for the client. For details, see 8.6.2 Smart Flow Control.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after PPTP VPN is deployed.

Caution

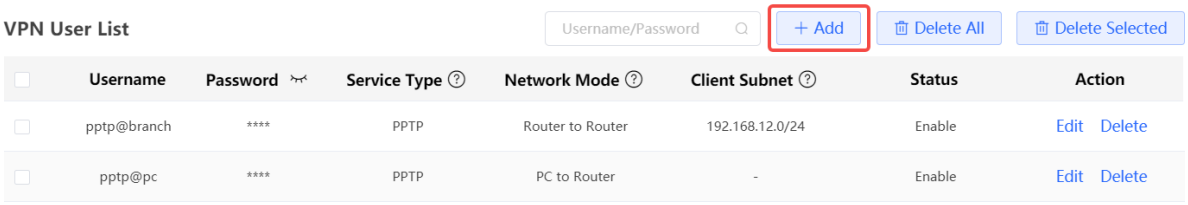
The local tunnel address and IP address range of the address pool cannot overlap the network segment of the LAN port on the device.

2. Configuring PPTP User

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **VPN Account**.

Only user accounts added to the VPN client list are allowed to dial up to connect to the PPTP server. Therefore, you need to manually configure user accounts for clients to access the PPTP server.

Click **Add**. In the dialog box that appears, set **Service Type** to **PPTP** or **ALL**. (If you select **ALL**, the created account can be used to establish all types of VPN tunnels.) Enter the username, password, and peer subnet, select a network mode, and click **OK**.



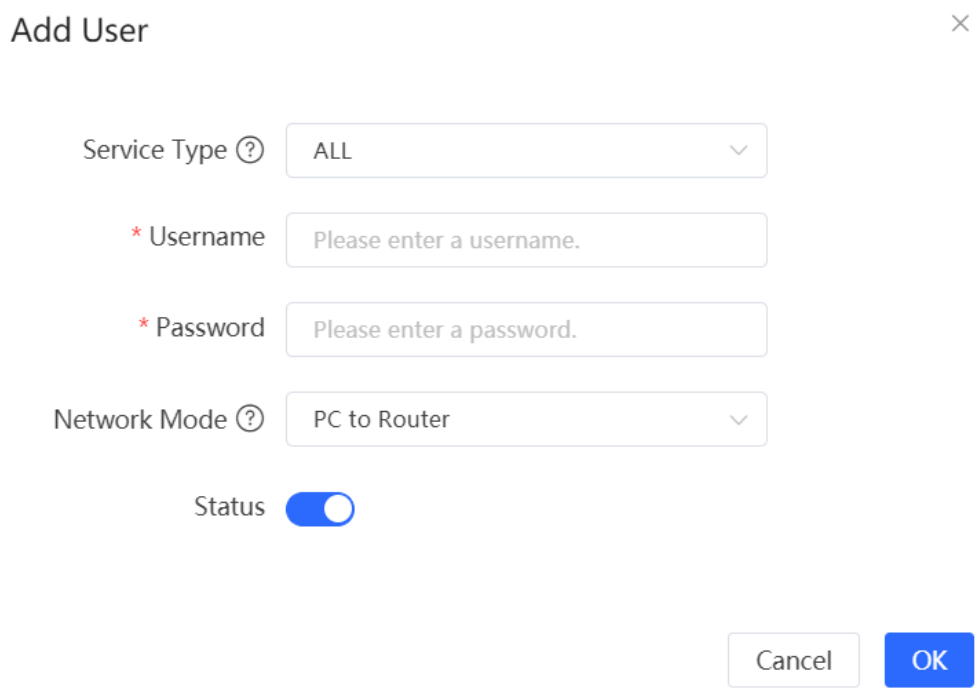


Table 10-14 PPTP user configuration

Parameter	Description
Username/Password	Specify the name and password of the PPTP user allowed to dial up to connect to the PPTP server. The username and password are used to establish a connection between the server and client.
Network Mode	● PC to Router: The dial-up client is an individual. Select this mode when a PC wants to dial up to communicate with the remote PC through the LAN. ● Router to Router: The dial-up client is a user in a network segment. Select this mode when the LANs on two ends of the tunnel need to communicate through router dial-up.
Client Subnet	Specify the IP address range used by the LAN on the peer end of the PPTP tunnel. Generally, the peer subnet is the IP address network segment of the LAN port on the device. (The LAN network segments of the server and client cannot overlap.) For example, when a branch dials up to connect to the HQ, enter the LAN network segment of the router. Note: When the Network Mode is set to Router to Router, you can click + to set multiple pairs of peer subnets for scenarios where multiple clients are connected to the same server.
Status	Specify whether to enable the user account.

10.3.3 Configuring the PPTP Client

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **PPTP** > **PPTP Settings**.

Turn on the PPTP function, set **PPTP Type** to **Client**, configure PPTP client parameters, and click **Save**.

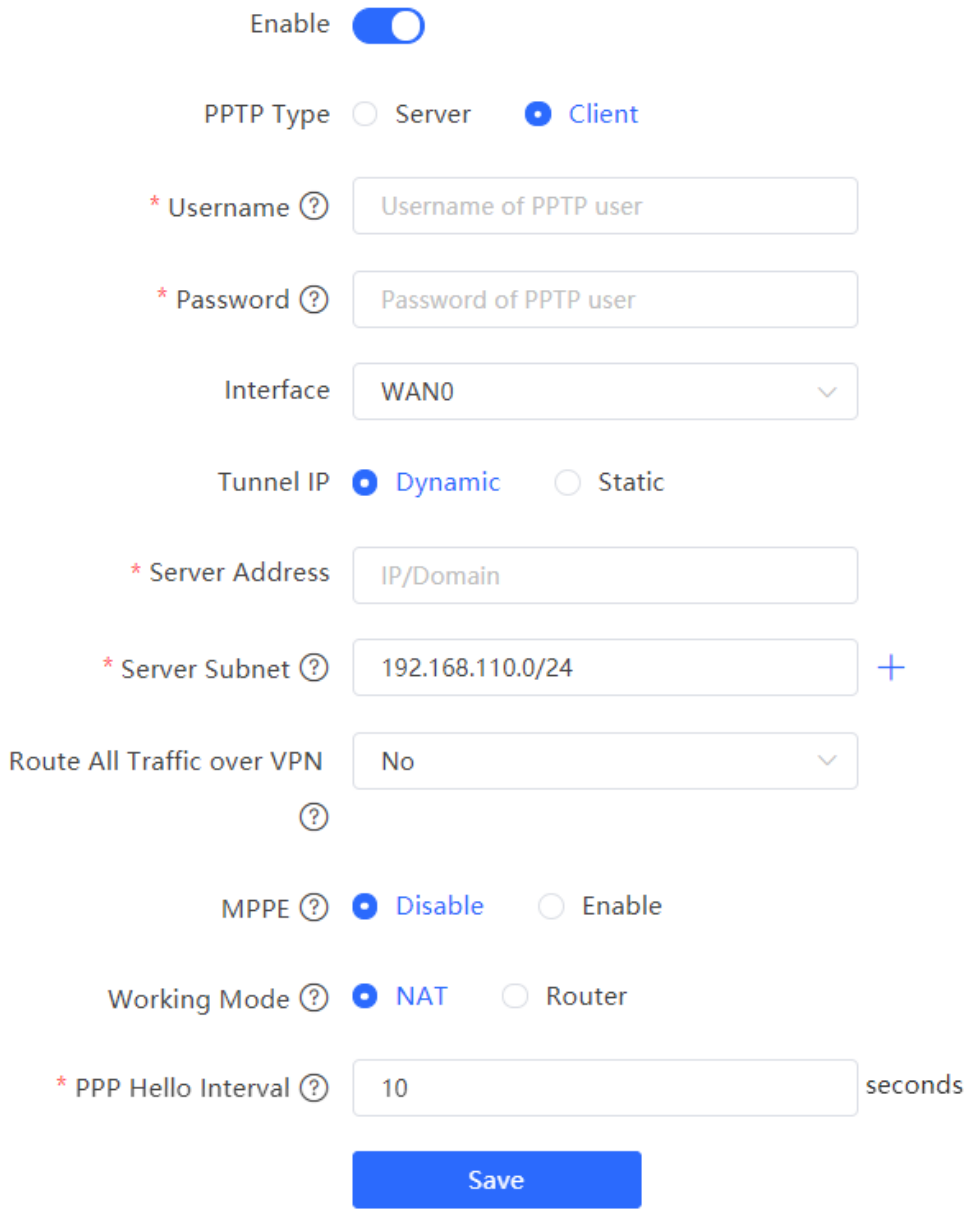


Table 10-15 PPTP client configuration

Parameter	Description
Username/Password	Specify the username and password for identity authentication for communication over the PPTP tunnel. The values must be the same as those configured on the PPTP server.

Parameter	Description
Interface	Specify the WAN interface used by the client.
Tunnel IP	Specify the virtual IP address of the VPN tunnel client. If you select **Dynamic**, the client obtains an IP address from the server address pool. If you select **Static**, manually configure an idle static address within the range of the server address pool as the local tunnel IP address.
Server Address	Enter the WAN interface IP address or domain name of the server. This address must be a public network IP address.
Server Subnet	Enter the LAN network segment in which clients want to access the server. The value cannot overlap with the LAN network segment of the client.
Route All Traffic over VPN	Once this feature is enabled, all traffic will be directed through the VPN connection, that is, VPN is configured as the default route.
MPPE	Specify whether to use MPPE to encrypt the PPTP tunnel. The value must be the same as that on the server.
Working Mode	● **NAT**: The client can access the server network, but the server cannot access the client network. ● **Router**: The server can access the client network.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after a PPTP tunnel is established. You are advised to retain the default configuration.

10.3.4 Viewing the PPTP Tunnel Information

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **PPTP** > **Tunnel List**.

It takes some time to establish a VPN connection between the server and client. After the configuration of the server and client is completed, wait for 1 to 2 minutes to refresh the page and view the PPTP tunnel establishment status.

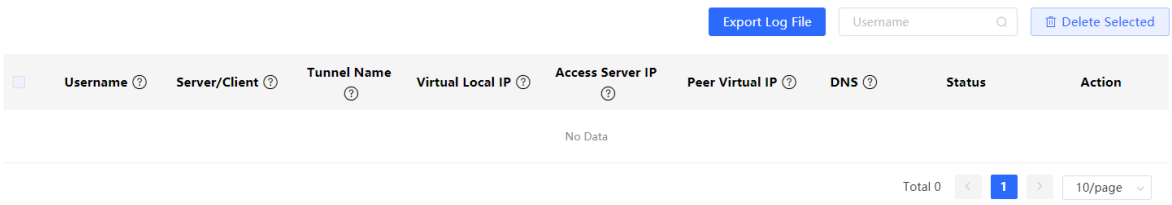


Table 10-16 PPTP tunnel information

Parameter	Description
Username	Indicate the username used by the client for identity authentication.
Server/Client	Indicate the role of the current device, which is client or server.
Tunnel Name	Indicate the name of the vNIC generated by PPTP.
Virtual Local IP	Indicate the local virtual IP address of the tunnel. The virtual IP address of the PPTP client is allocated by the PPTP server.
Access Server IP	Indicate the real IP address of the peer connecting to the PPTP tunnel.
Peer Virtual IP	Indicate the peer virtual IP address of the tunnel. The virtual IP address of the PPTP client is allocated by the PPTP server.
DNS	Indicate the DNS server address allocated by the PPTP server.

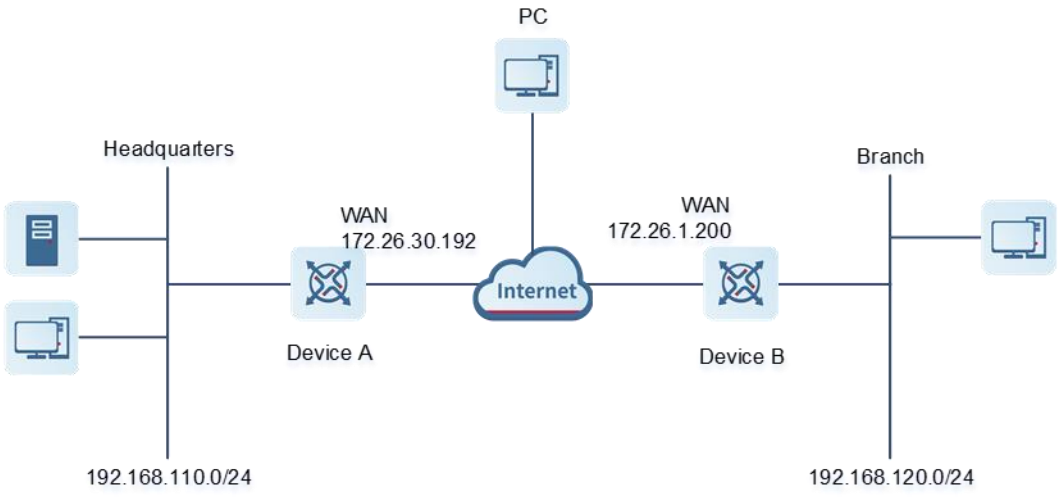
10.3.5 Typical Configuration Example

1. Networking Requirements

An enterprise wants to establish a PPTP tunnel to allow its traveling employees and branch employees to access the servers deployed in the HQ LAN.

- Traveling employees want to access the HQ servers from their PCs through PPTP dial-up.
- Branch employees need to frequently access documents on the HQ servers. The enterprise wants to deploy the branch router (Device B) as the PPTP client, so that branch employees can dial up to transparently and directly access documents on the HQ servers, as if they are accessing servers inside the branch.

2. Networking Diagram



3. Configuration Roadmap

- Configure the HQ gateway Device A as the PPTP server.
- Configure the branch gateway Device B as the PPTP client.
- Configure the PC of the traveling employee as the PPTP client.

4. Configuration Steps

- Configure the HQ gateway.

Note

The LAN address of the HQ cannot conflict with that of the branch. Otherwise, resource access will fail.

(1) Log in to the web management system and choose **One-Device** > **Gateway** > **Config** > **VPN** > **PPTP** > **PPTP Settings** to access the PPTP Settings page.

(2) Turn on the PPTP function, set PPTP Type to Server, enter the local tunnel IP, IP Range, and DNS server address, specify whether to enable MPPE encryption, and click **Save**.

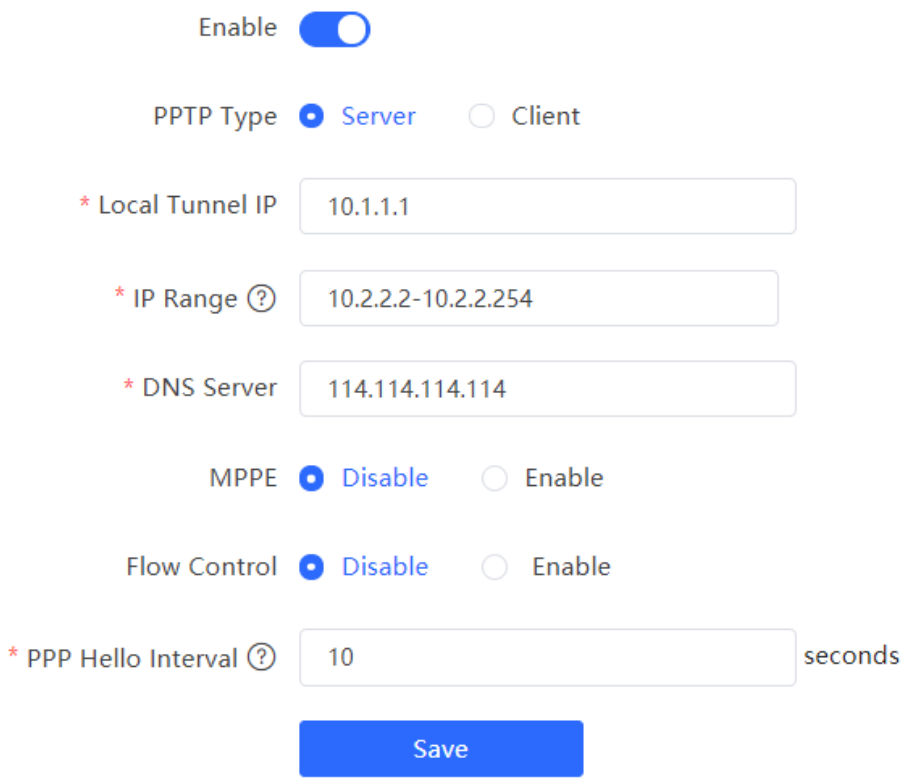


Table 10-17 PPTP server configuration

Parameter	Description
Local Tunnel IP	Enter an IP address not in the LAN network segment. The PC can dial up to access the server through this IP address.

Parameter	Description
IP Range	Enter an IP address range not in the LAN network segment, which is used to allocate IP addresses to clients.
DNS Server	Enter an available DNS server address.
MPPE	Specify whether to use MPPE to encrypt the PPTP tunnel. The value must be the same as that on the client. After you enable MPPE, the device security is improved but the bandwidth performance of the device degrades. You are advised to keep MPPE disabled if there are no special security requirements.
Flow Control	Flow control is disabled by default.
PPP Hello Interval	Keep the default settings unless otherwise specified.

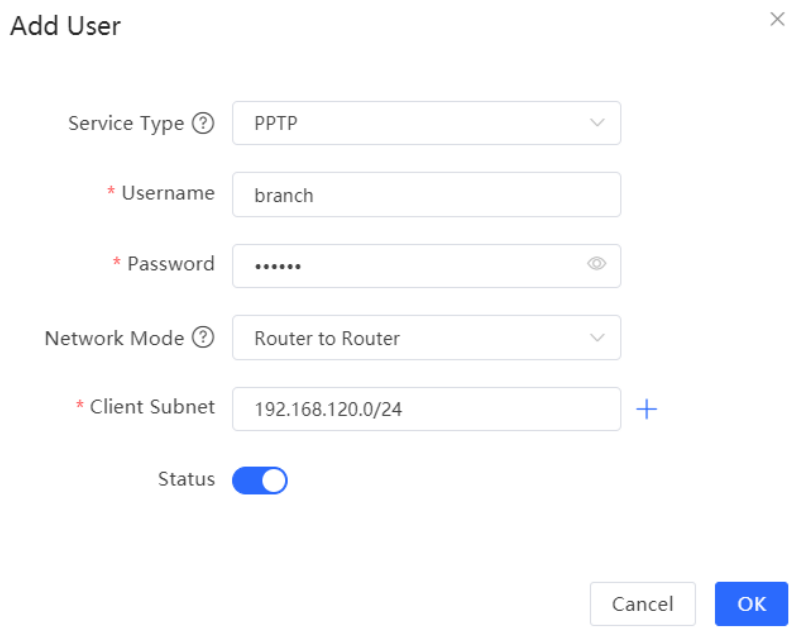
(3) Choose **One-Device** > **Gateway** > **Config** > **VPN** > **VPN Account** and add PPTP user accounts for the traveling employee and branch employee to access the HQ.

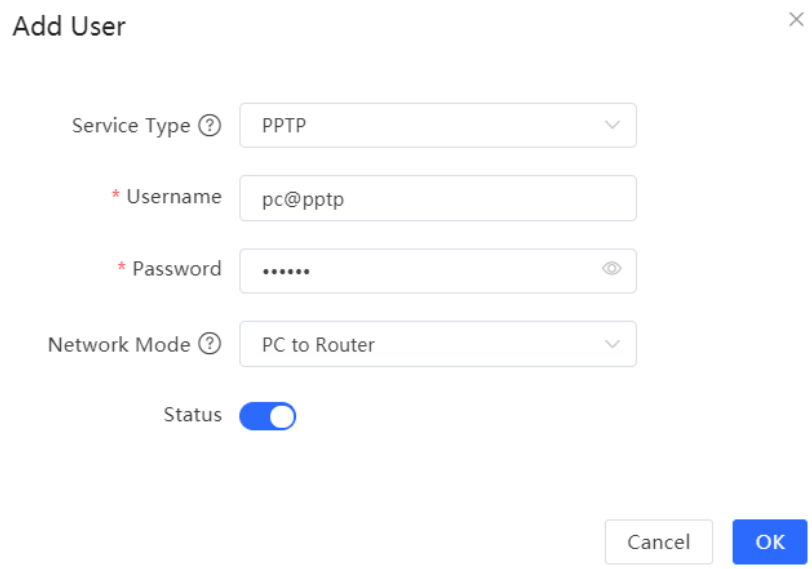
For the traveling employee account, set **Network Mode** to **PC to Router**.

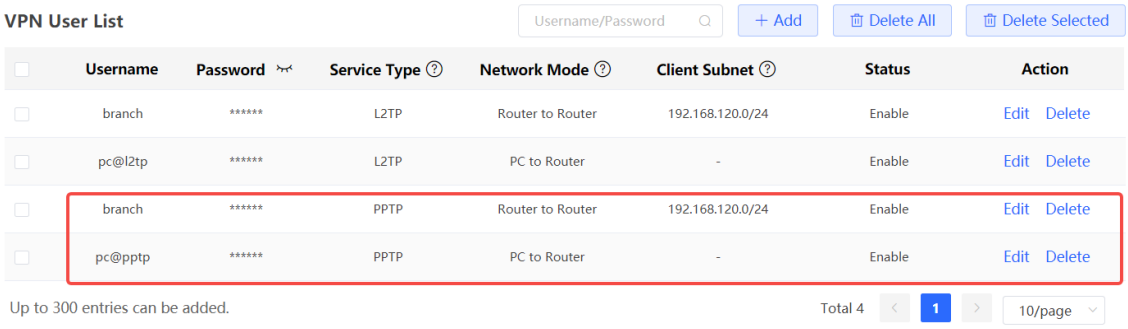
For the branch employee account, set **Network Mode** to **Router to Router** and C**lient Subnet** to the LAN network segment of the branch gateway.

Caution

The LAN network segments of the server and client cannot overlap.







- Configure the branch gateway.

(1) Log in to the web management system and access the PPTP Settings page.

(2) Turn on the PPTP function, set PPTP Type to Client, enter the username and password configured on the server, server address, and LAN network segment of the peer, configure IPsec encryption parameters the same as those on the server, and click Save.

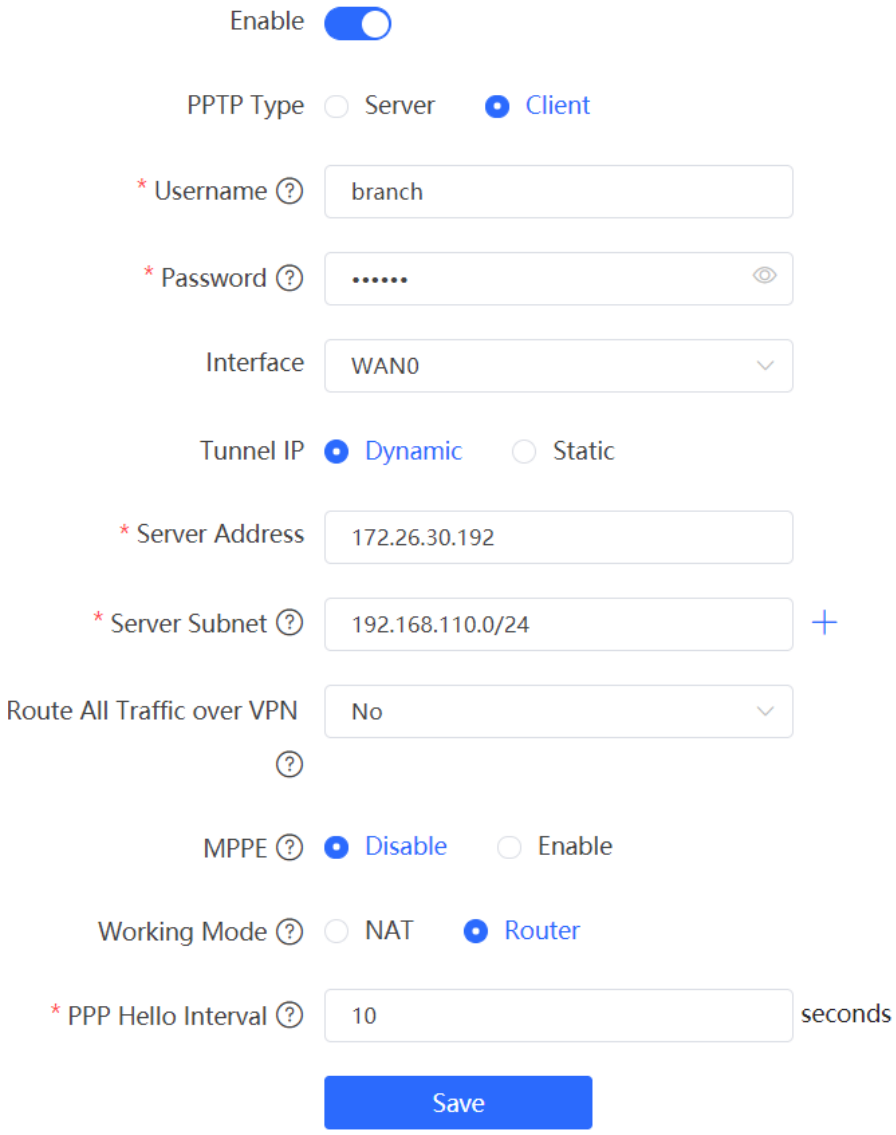


Table 10-18 PPTP client configuration

Parameter	Description
Username/Password	Enter the username and password configured on the server.
Interface	Select the WAN interface on the client to establish a tunnel with the server.
Tunnel IP	Select **Dynamic** to automatically obtain the tunnel IP address. You can also select **Static** and enter an IP address in the address pool of the server.
Server Address	Enter the WAN interface address of the server.
Server Subnet	Enter the LAN network segment (LAN port IP address range) of the server.

Parameter	Description
Route All Traffic over VPN	Once this feature is enabled, all traffic will be directed through the VPN connection, that is, VPN is configured as the default route.
MPPE	The value must be the same as that on the server.
Working Mode	If the HQ wants to access the LAN of the branch, set this parameter to **Router**.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after PPTP VPN is deployed. Keep the default settings.

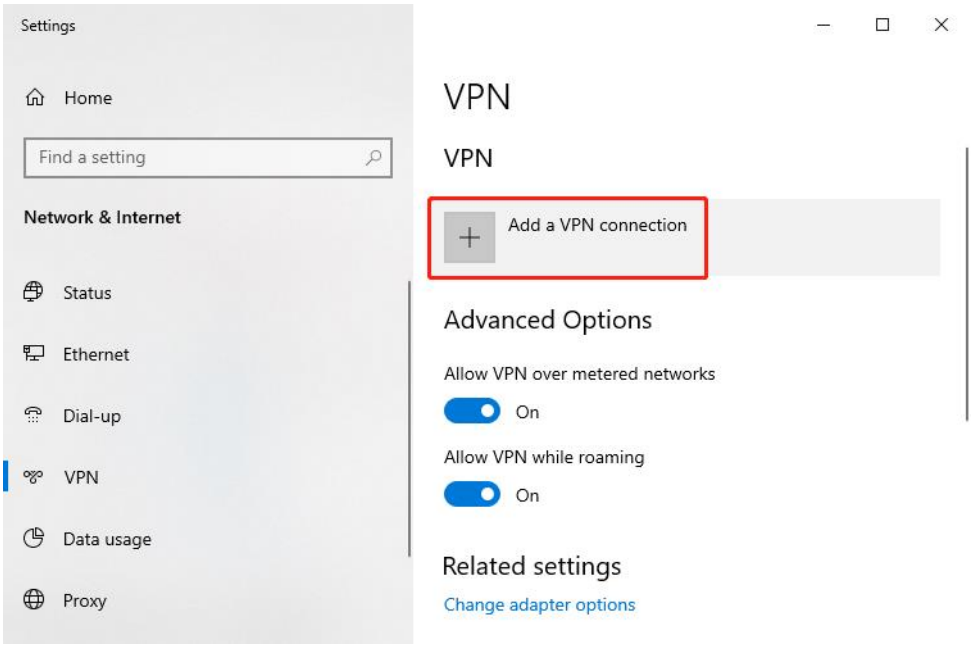
- Configure the PC of the traveling employee.

Note

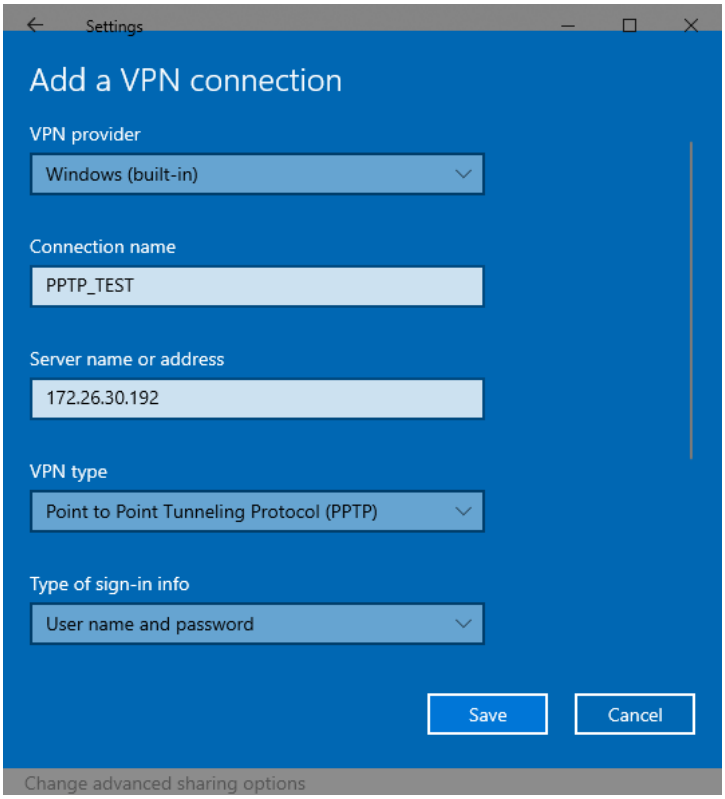
Configure the PC of a traveling employee as the PPTP client. The following uses the PC running Windows 10 operating system as an example.

Enable ports 1723 (PPTP) and 47 (GRE) on the PC firewall.

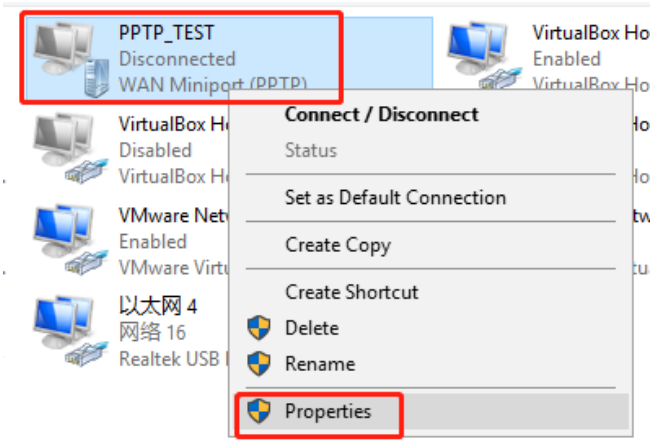
(1) Choose **Settings** > **Network & Internet** > **VPN** to access the VPN page.



(2) Click **Add a VPN connection**. In the dialog box that appears, set VPN provider to **Windows** and VPN type to **Point to Point Tunneling Protocol (PPTP)**, enter the connection name and server address or domain name, and click **Save**.



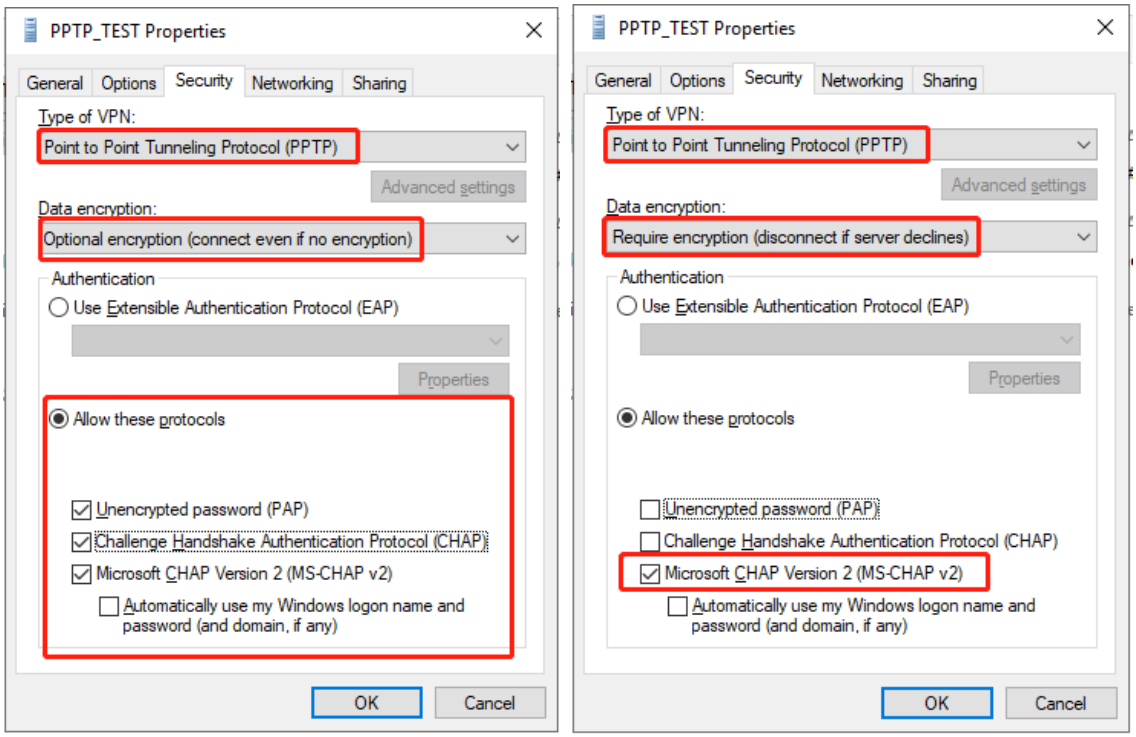
(3) Right-click the created VPN connection named **PPTP_TEST** and select Properties to view the properties of the network connection.



(4) In the dialog box that appears, click the **Security** tab.

If MPPE is not enabled on the PPTP server, set **Data encryption** to **Optional encryption** or **No encryption allowed** and use PAP, CHAP, or MS-CHAP v2 for identity authentication, as shown in the following figure on the left.

If MPPE is enabled on the PPTP server, set **Data encryption** to **Require encryption** or **Maximum strength encryption** and use MS-CHAP v2 for identity authentication, as shown in the following figure on the right.

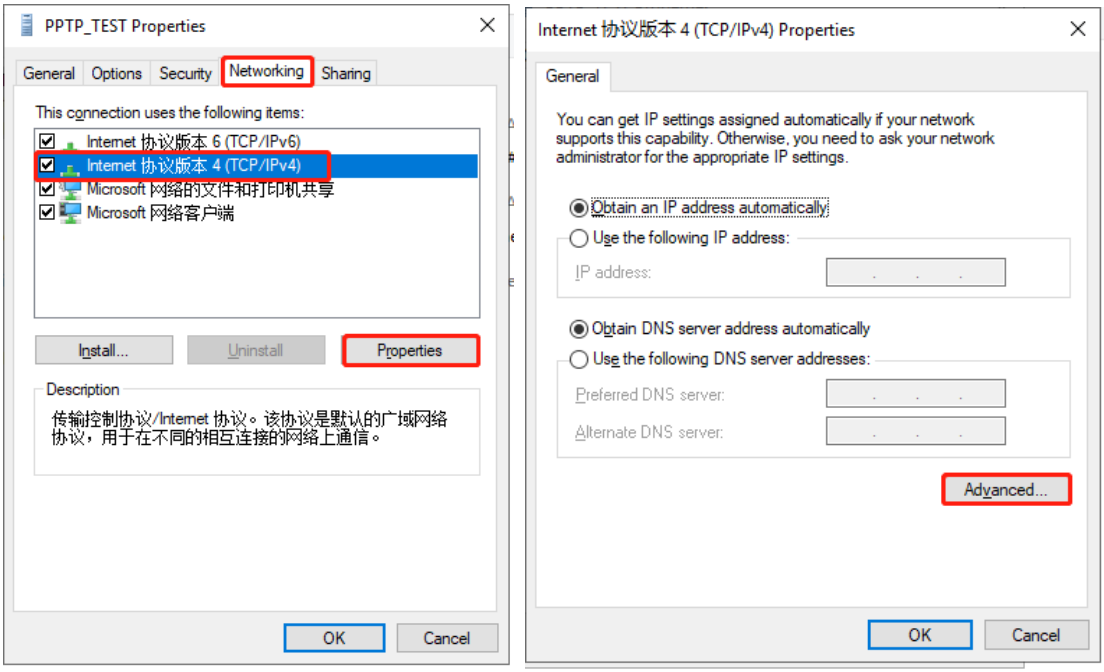


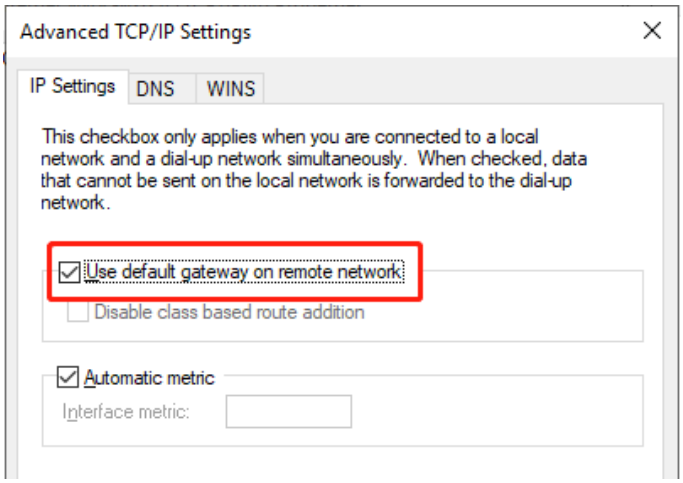
Note

The device does not support EAP for identity authentication. Therefore, you cannot select EAP-related identity authentication options in the Windows client. Otherwise, the VPN connection fails.

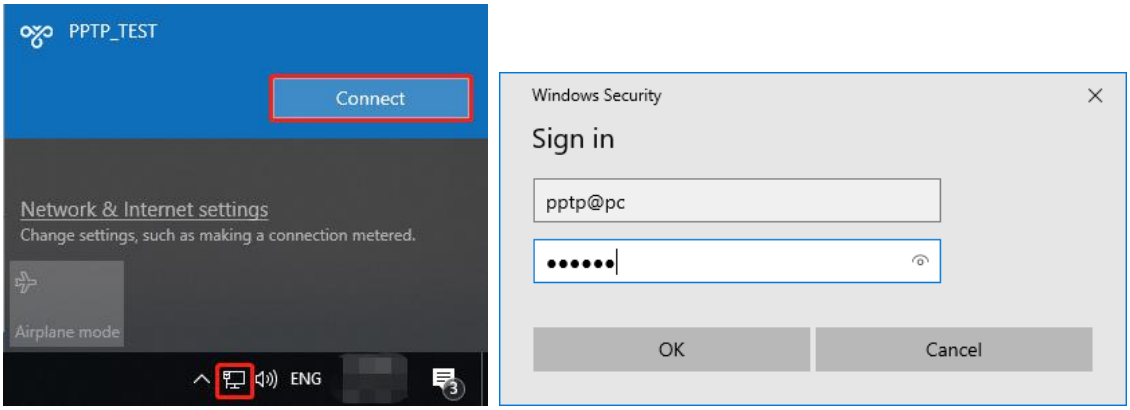
(5) When the PC functions as a dial-up client, configure the PC by using either of the following methods:

- Add a route to the VPN peer network segment on the PC as the administrator.
- In the **Properties** dialog box of the local VPN connection, select **Use default gateway on remote network**. After the VPN connection is successful, all data flows from the PC to the Internet are routed to the VPN tunnel. The following figures show the detailed configuration.





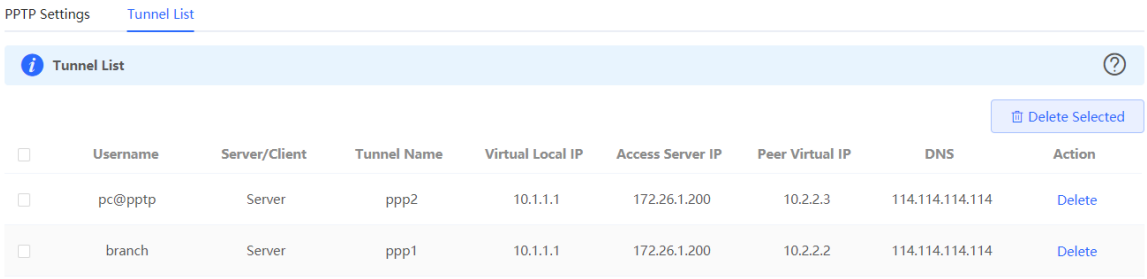
(6) After the PPTP client configuration is completed on the PC, initiate a VPN connection on the PC. Click the network icon  in the task bar, select the PPTP VPN connection, and click **Connect**. In the dialog box that appears, enter the username and password configured on the server.



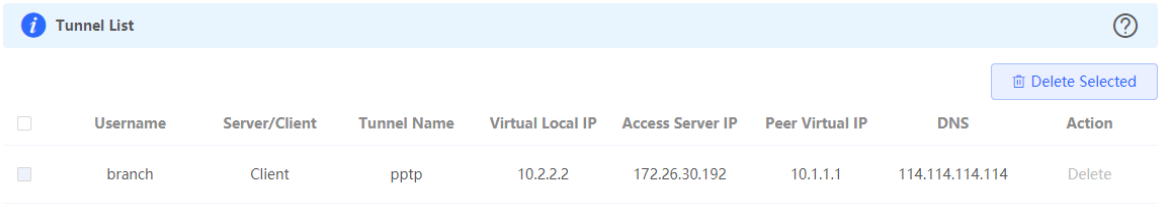
5. Verifying Configuration

(1) After the server and client are configured, wait for about 1 minute. If you can view the L2TP tunnel connection information on the HQ server and branch client, the connection is successful.

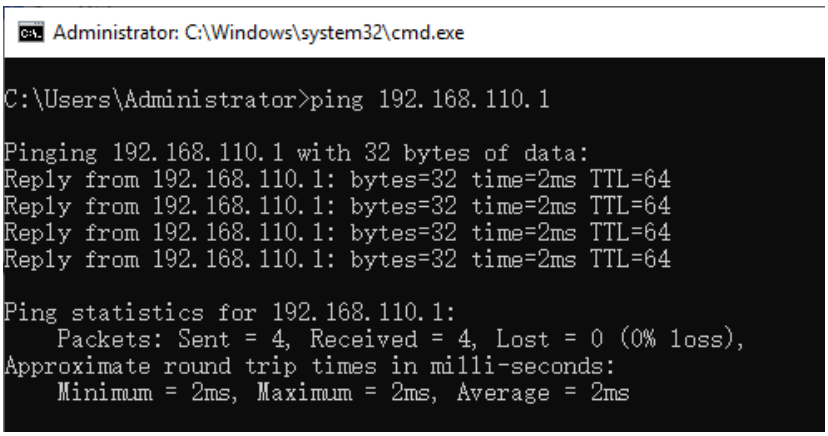
HQ:



Branch:



(2) Ping the LAN address of the peer from the HQ or branch. The HQ and branch can successfully communicate. The PC of the traveling employee and the PC of the branch employee can access the HQ server.



10.3.6 Solution to PPTP VPN Connection Failure

(1) iPhones and other IOS devices do not support PPTP VPN. Please use L2TP VPN instead

(2) Run the ping command to test the connectivity between the client and server. For details, see Section 12.11.3 Network Tools. If the ping fails, check the network connection settings. Check whether the branch EG can ping to HQ EG. If the ping fails. Check the network connection between the two EGs.

Choose **One-Device** > **Gateway** > **Config** > **Diagnostics** > **Network Tools**. Then, you can start the ping operation. For details, see Section 12.11.3 Network Tools.

(3) Check whether the username and password used by the client are the same as those configured on the server.

(4) Check whether the WAN interface IP address of your HQ EG is a public network IP address. If not, please configure DMZ on your egress gateway.

10.4 Configuring OpenVPN

Caution

IPTV connection is not supported only in the Chinese environment. To connect to IPTV in the Chinese environment, switch the system language. For details, see Section 12.13 Switching System Language.

10.4.1 Overview

1. OpenVPN Overview

Due to security considerations or cross-NAT communication needs, private channels need to be established between enterprises or between individual and enterprise. OpenVPN is used to establish Layer 2 or Layer 3 VPN tunnels by using the vNIC. OpenVPN supports flexible client authorization modes, supports authentication through certificate or username and password, and allows users to connect to VPN virtual interfaces through the firewall. It is easier to use than other types of VPN technologies. OpenVPN can run in the Linux, xBSD, Mac OS X, and Windows 2000/XP systems. The device can establish VPN connections to PCs, Android/Apple mobile phones, routers, and Linux devices, and it is compatible with most OpenVPN products in the market.

OpenVPN connections can traverse most proxy servers and can function well in the NAT environment. The OpenVPN server can push the following network configuration to clients: IP address, routes, and DNS settings.

2. Certificate Overview

The major advantage of OpenVPN lies in its high security, but OpenVPN security requires the support of certificates.

The OpenVPN client supports certificates **ca.crt**, **ca.key**, **client.crt**, and **client.key** and the OpenVPN server supports certificates **ca.crt**, **ca.key**, **server.crt**, and **server.key**.

10.4.2 Configuring the OpenVPN Server

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **OpenVPN**.

1. Basic Settings

Turn on **Enable** to enable the OpenVPN function, set **OpenVPN Type** to **Server**, set other parameters, and click **Save**. After the basic settings are completed, you can view the tunnel information of the server in the tunnel list.

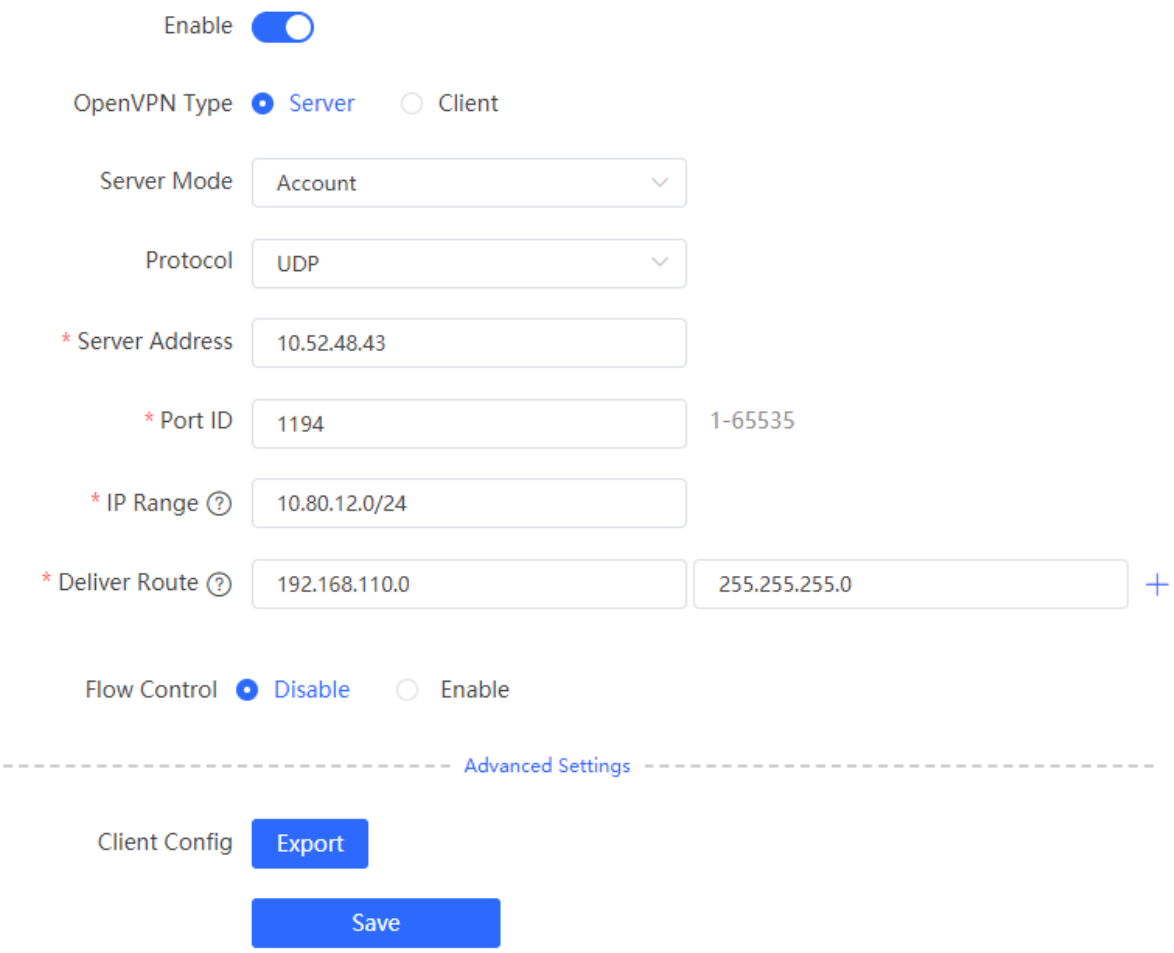


Table 10-19 OpenVPN server basic settings

Parameter	Description
Server Mode	Select a server authentication mode. The options are **Account**, **Certificate**, and **Account & Certificate**. ● **Account**: Enter the correct username and password and upload the CA certificate on the client to connect to the server. The configuration is simple. ● **Certificate**: Upload the CA certificate and client certificate and enter the correct private key on the client to connect to the server. ● **Account & Certificate**: Upload the CA certificate and client certificate and enter the correct username, password, and private key. This mode is applicable to scenarios with high security requirements.
Protocol	Select a protocol for all OpenVPN communications based on a single IP port. The options are **UDP** and **TCP**. The default value is **UDP**, which is recommended. When you select a protocol, pay attention to the network status between two encrypted tunnel ends. If high latency or heavy packet loss occurs, select **TCP** as the underlying protocol.

Parameter	Description
Server Address	Specify the server address for client connection. You can set this parameter to a domain name.
Port ID	Specify the port used by the OpenVPN service process. Internet Assigned Numbers Authority (IANA) specifies port 1194 as the official port for the OpenVPN service. If the port is in use or disabled in the local network, the server log prompts port binding failure and you are asked to change the port number.
IP Range	Specify the network segment of the OpenVPN address pool. The first available in the address pool is allocated to the server, and the other addresses are allocated to clients. For example, if this parameter is set to **10.80.12.0/24**, the VPN virtual address of the server is 10.80.12.1.
Deliver Route	Specify the VPN dial-up line for clients to access the LAN network segment of the server. The server informs clients that want to access the server LAN of the route information. You can configure a maximum of three routes.
Flow Control	The VPN server has a lower priority to control the traffic of the client than the custom policy. The VPN server can only limit the maximum uplink and downlink bandwidth per user for the client. For details, see 8.6.2 Smart Flow Control.
Client Config	Click **Export** to export the parameter configuration of the client connected to the server in the .tar compressed package. The decompressed information is used for setting the OpenVPN client. In account mode, the compressed package contains the configuration file **client.ovpn**, CA certificate **ca.crt**, and CA private key **ca.key**. If certificate authentication is configured, the compressed package contains the configuration file **client.ovpn**, CA certificate **ca.crt**, CA private key **ca.key**, client certificate **client.cart**, and client private key **client.key**. If TLS authentication is enabled, the compressed package contains the TLS identity authentication key **tls.key** apart from the preceding files. For details on TLS authentication, see Advanced Settings.
Server Log	Click **Export** to export server log files, including the server start time and client dial-up logs.

Caution

The IP address range of the device cannot overlap the network segment of the LAN port on the device.

2. Advanced Settings

Click **Advanced Settings** to configure the advanced parameters. Keep the default settings unless otherwise specified.

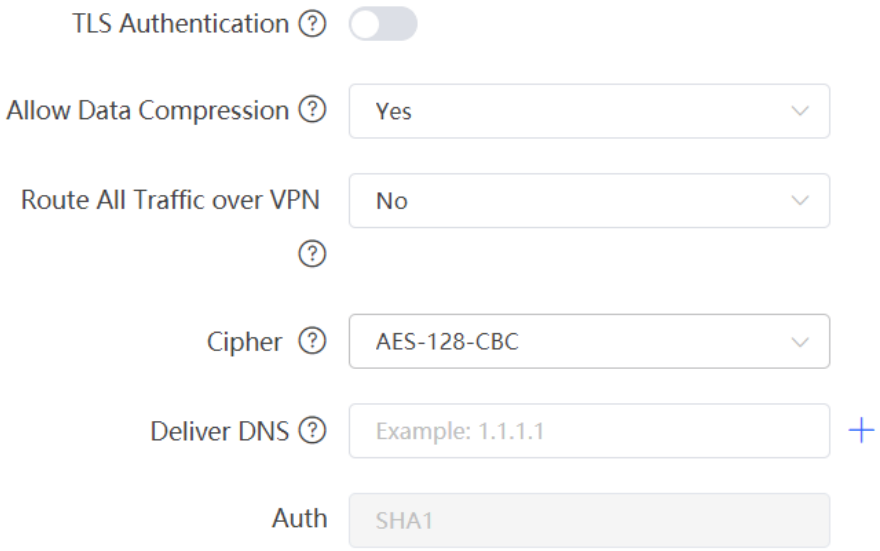


Table 10-20 OpenVPN server advanced settings

Parameter	Description
TLS Authentication	Specify the TLS key for enhanced OpenVPN security by allowing the communicating parties to possess the shared key before TLS handshake. After TLS authentication is enabled, you must import the TLS key on the client. (The version of the peer OpenVPN client must be higher than 2.40.)
Allow Data Compression	Specify whether to enable data compression. If this function is enabled, transmitted data is compressed using the LZO algorithm. Data compression saves bandwidth but consumes certain CPU resources. The setting on the client must be the same as that on the server. Otherwise, the connection fails.
Route All Traffic over VPN	Specify whether to route all traffic over VPN. After this function is enabled, all the traffic is routed over the VPN tunnel. This means that the VPN tunnel is the default route.

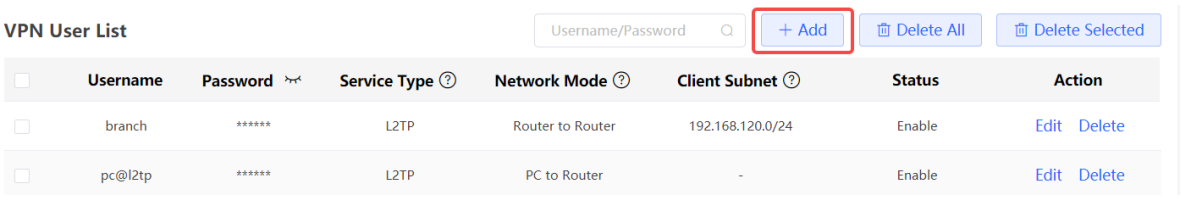
Parameter	Description
Cipher	Select the data encryption mode before data transmission to ensure that even data packets are intercepted during transmission, the leaked data cannot be interpreted. If this parameter is set to **Auto** on the server, you can set this parameter to any option on the client. If a specific encryption algorithm is configured on the server, you must select the same encryption algorithm on the client. Otherwise, the connection fails.
Deliver DNS	Specify the DNS server address pushed by the server to clients. Currently, the device can push the DNS server address to Windows clients only.
Auth	Specify the MD5 algorithm used by the server. The server will inform the clients of this information. The default value is **SHA1**.

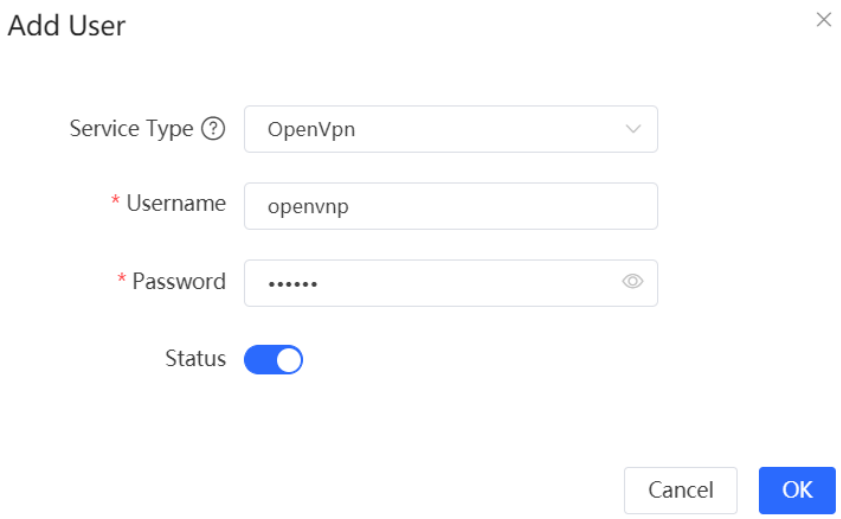
3. Configuring OpenVPN User

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **VPN Account**.

Only user accounts added to the VPN client list are allowed to dial up to connect to the OpenVPN server. Therefore, you need to manually configure user accounts for clients to access the OpenVPN server.

Click **Add**. In the dialog box that appears, set **Service Type** to **OpenVpn**, enter the username and password, and click **OK**. The **Status** parameter specifies whether to enable the user account.





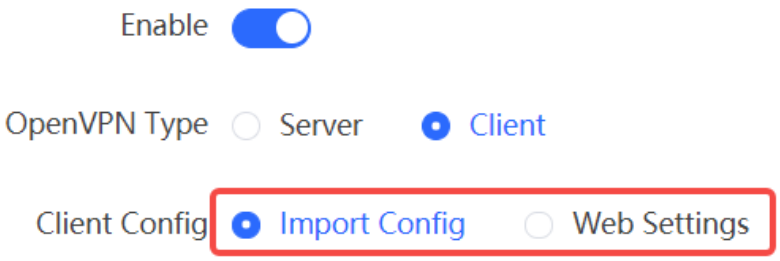
10.4.3 Configuring the OpenVPN Client

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **OpenVPN**.

Currently, you can configure the device as the OpenVPN client in either of the following methods:

Web Settings: Configure OpenVPN client on the web page. This method is used when the device is connected to a non-EG server.

Import Config: Manually import the configuration file. This method is used when the device is connected to a similar device. The client configuration file **client.ovpn** can be directly exported from the connected OpenVPN server.



1. Import Config

Turn on **Enable** to enable the OpenVPN function, set **OpenVPN Type** to **Client** and **Client Config** to **Import Config**, select a server mode, set relevant parameters, and click **Browse** to import the client configuration file. Then, click **Save** to make the configuration take effect.

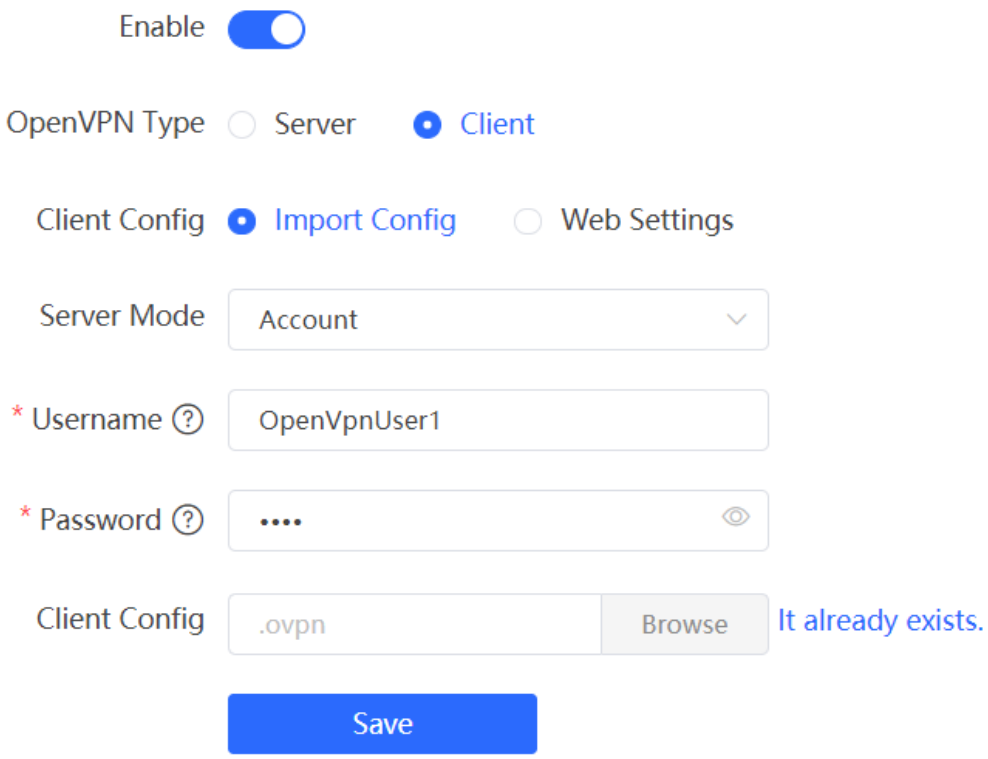


Table 10-21 OpenVPN client configuration in Import Config method

Parameter	Description
Server Mode	Select a server authentication mode. The options are **Account**, **Certificate**, **Account & Certificate** and **Pre-Shared Key**. ● **Account**: Enter the correct username and password and upload the CA certificate on the client. The CA certificate information is embedded in the client configuration file. ● **Certificate**: Upload the CA certificate and client certificate and enter the correct private key on the client. All the information is embedded in the client configuration file. ● **Account & Certificate**: Enter the correct username, password, and private key and upload the CA certificate, and client certificate on the client. The information of the CA certificate, client certificate, and private key is embedded in the client configuration file. ● **Static Key**: Upload the pre-shared key file apart from the client configuration file.
Username/Password	Enter the username and password configured on the server.
Client Config	Click **Browse**, select the client configuration file exported from the server, and upload the file.
Pre-Shared Key	This parameter is available only when **Server Mode** is set to **Static Key**. Click **Browse**, select the pre-shared key file, and upload the file.

Parameter	Description
Working Mode	This parameter is available only when **Server Mode** is set to **Static Key**. ● **NAT**: The client can access the server network, but the server cannot access the client network. ● **Router**: The server can access the client network.

2. Web Settings

Turn on **Enable** to enable the OpenVPN function, set **OpenVPN Type** to **Client** and **Client Config** to **Web Settings**, configure parameters such as **Device Mode** and **Device Mode**, and click **Save** to make the configuration take effect.

(1) Basic Settings

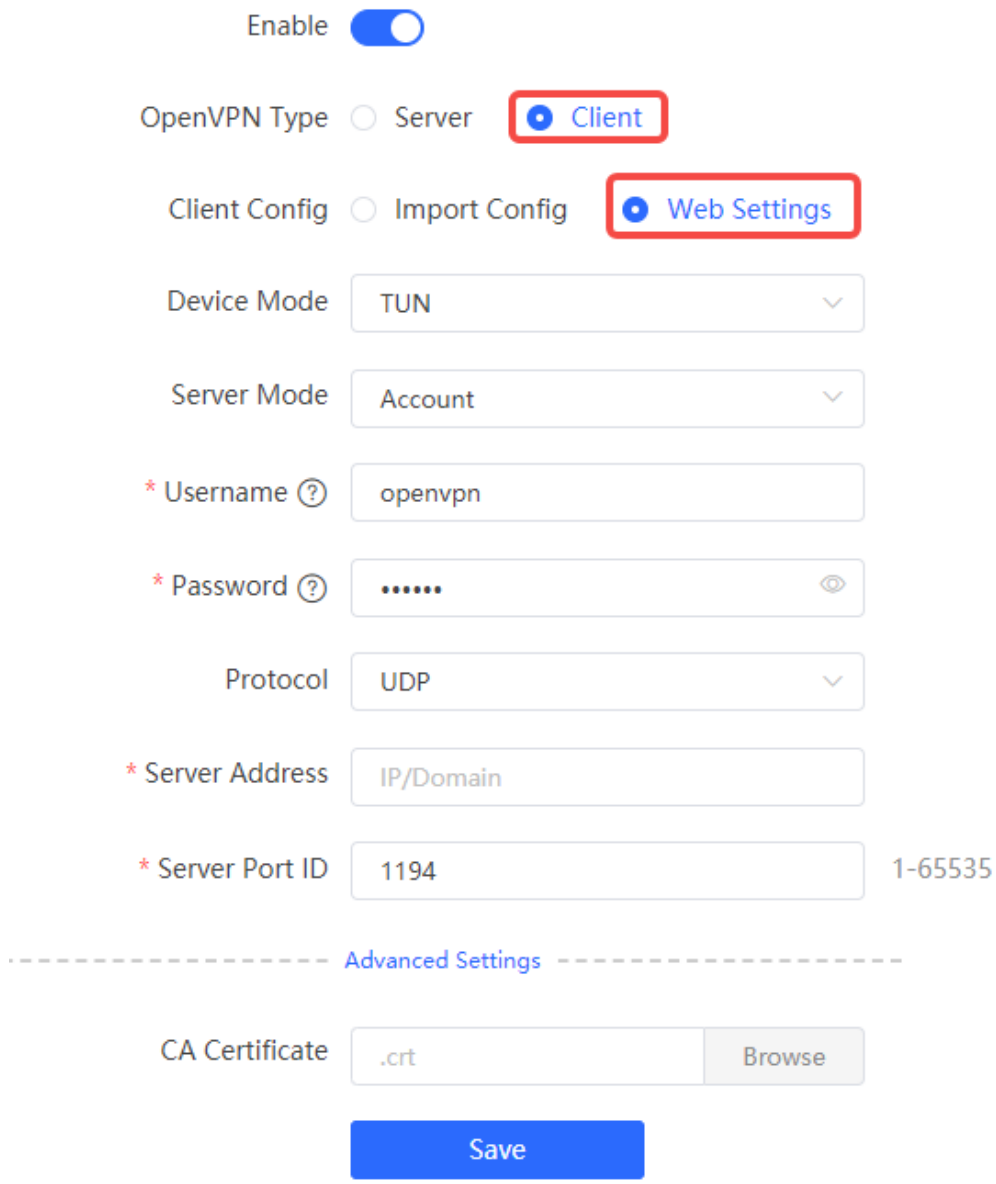


Table 10-22 OpenVPN client configuration in Web Settings method

Parameter	Description
Device Mode	Specify the mode of the EG device that functions as a client. The options are **TUN** and **TAP**. The value must be the same as that configured on the server. When the EG device works as a server, it supports the TUN mode only.
Server Mode	Select a client authentication mode. The options are **Account**, **Certificate**, and **Account & Certificate**. ● **Account**: Enter the correct username and password and upload the CA certificate on the client. ● **Certificate**: Upload the correct CA certificate, client certificate, and private key file on the client. ● **Account & Certificate**: Enter the correct username and password, and upload the CA certificate, client certificate, and private key file on the client.
Username/Password	Enter the username and password configured on the server.
Protocol	Select the protocol running on the device. The options are **UDP** and **TCP**. The value must be the same as that configured on the server.
Server Address	Enter the address or domain name of the server to be connected.
Server Port ID	Enter the port number of the server to be connected.
CA Certificate	Click **Browse**, select the CA certificate file with the file name extension **.ca**, and upload the file.
Client Key	Click **Browse**, select the client private file with the file name extension **.key**, and upload the file.
Client Certificate	Click **Browse**, select the client certificate file with the file name extension **.crt**, and upload the file.
Client Certificate Key	Specify the client certificate key if the client certificate provided by the server (such as the MikroTik server) is encrypted twice.

(2) Advanced Settings

Click **Advanced Settings** to configure the advanced parameters. Keep the default settings unless otherwise specified.

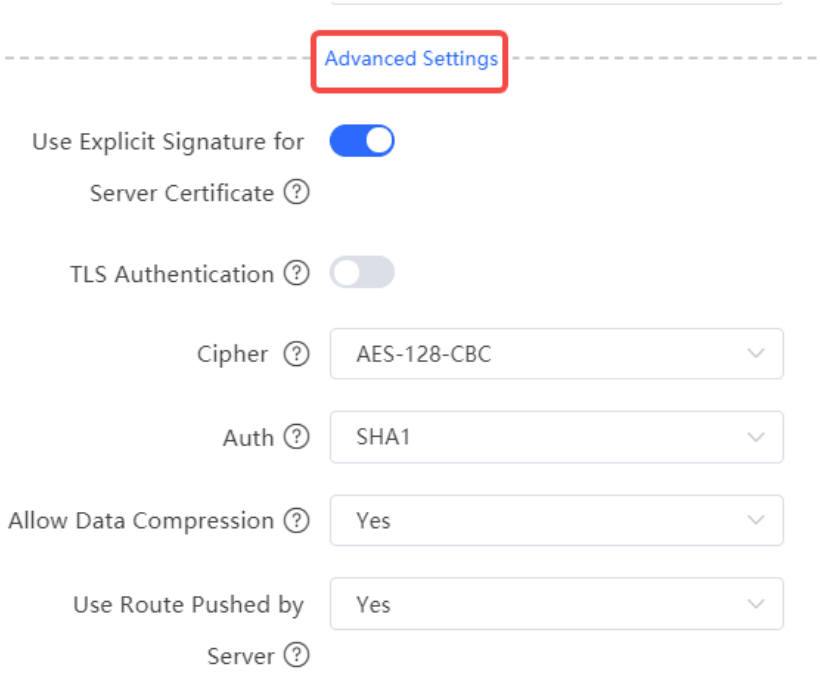


Table 10-23 OpenVPN client configuration in Web Settings method

Parameter	Description
Use Explicit Signature for Server Certificate	Specify whether to verify the server certificate using explicit signature. By default, this function is enabled. If the server certificate does not use explicit signature, for example, the MikroTik server, you need to disable this function. Otherwise, the connection fails.
TLS Authentication	Specify whether to enable TLS authentication for the server. If this function is enabled, you need to upload the TLS certificate file.
Cipher	Select a data compression algorithm. The value must be the same as that configured on the server. Otherwise, the connection fails.
Auth	Select an MD5 algorithm for data packet verification. The options are **SHA1**, **MD5**, **SHA256**, and **NULL**. The value must be the same as that configured on the server. Otherwise, the connection fails.
Allow Data Compression	Specify whether to allow data compression. After this function is enabled, the transmitted data can be compressed by using the LZO algorithm. The value must be the same as that configured on the server.

Parameter	Description
Use Route Pushed by Server	Specify whether to use the routes pushed by the server. If this function is disabled, the device cannot accept the routes pushed by the server. If the server needs to access LAN devices, you must set this parameter to **Yes**.

10.4.4 Viewing the OpenVPN Tunnel Information

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **OpenVPN** > **Tunnel List**.

After the server and client are configured, you can view the OpenVPN tunnel connection status. If the tunnel is established successfully, the client tunnel information is displayed in the tunnel list of the server.

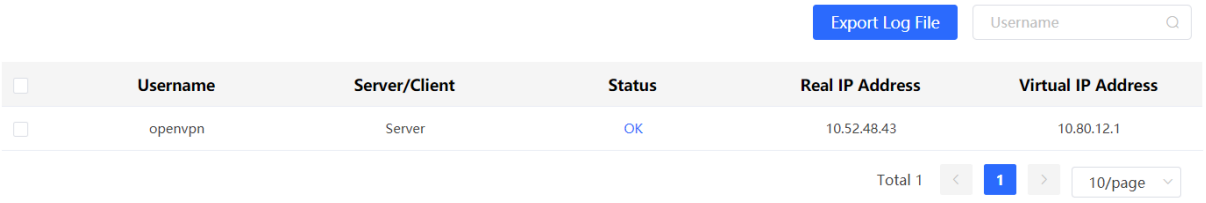


Table 10-24 OpenVPN tunnel information

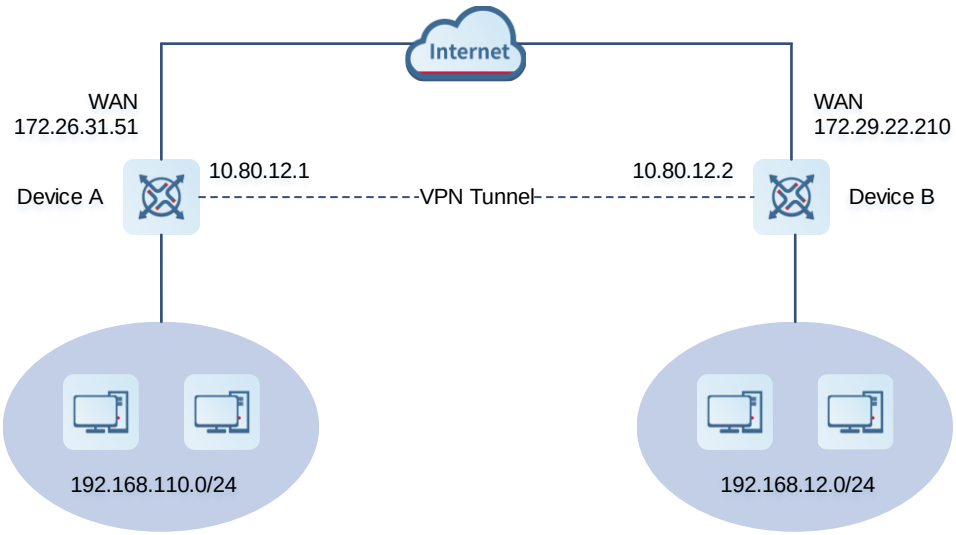
Parameter	Description
Username	Indicate the username used by the client for identity authentication. By default, the username displayed on the server is **openvpn**.
Server/Client	Indicate the role of the local end of the tunnel, which can be client or server.
Status	Indicate the tunnel establishment status.
Real IP Address	Indicate the real IP address used by the local end to connect to the VPN.
Virtual IP Address	Indicate the local virtual IP address of the tunnel. The virtual IP address of the OpenVPN client is allocated by the OpenVPN server.

10.4.5 Typical Configuration Example

1. Networking Requirements

The enterprise wants to allow the client network to dial up to the server through OpenVPN, implementing mutual access between the server and client.

2. Networking Diagram



3. Configuration Roadmap

- Configure Device A as the OpenVPN server.
- Configure Device B as the OpenVPN client.
- The server needs to push the local LAN network segment to the client to allow the client to access the server in the LAN.

4. Configuration Steps

- Configure Device A.

(1) Log in to the web management system and choose **One-Device** > **Gateway** > **Config** > **VPN** > **OpenVPN** > **OpenVPN** to access the OpenVPN page.

(2) Turn on Enable to enable the OpenVPN function, set OpenVPN Type to Server, select a server mode and protocol, enter the port number (1194 by default) and server address (external IP address of the local device), and click **Save**.

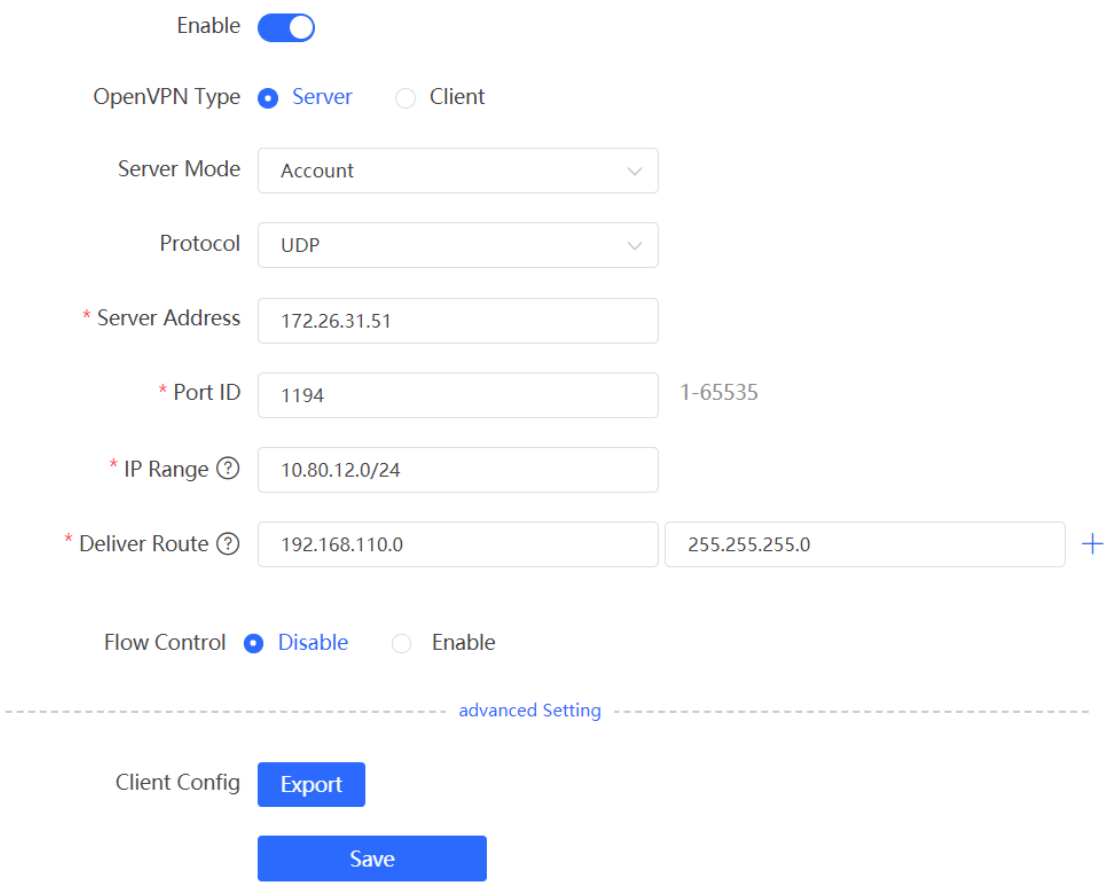
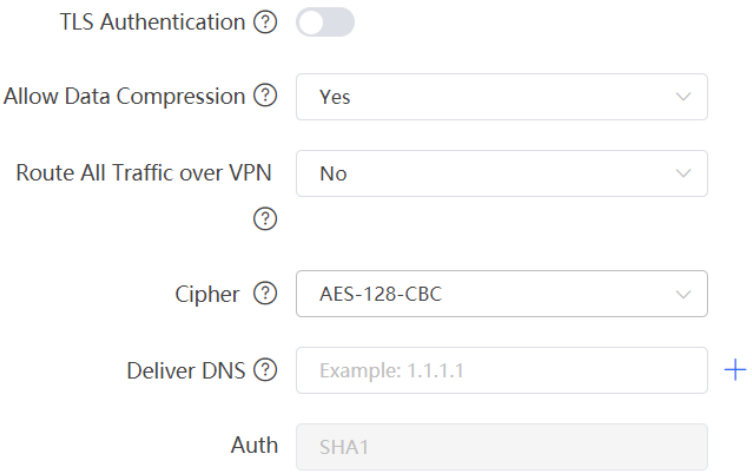


Table 10-25 OpenVPN server configuration

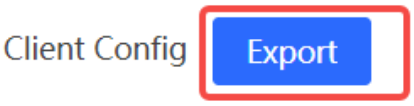
Parameter	Description
Server Mode	Select an authentication mode. In this example, select **Account**. In scenarios with high security requirements, select **Account & Certificate**.
Protocol	Select **UDP** unless otherwise specified. When the network status between two encrypted tunnel ends is poor, such as high latency or heavy packet loss, select **TCP**.
Server Address	Enter the WAN interface address of the server, which is **172.26.31.51**.
Port ID	The default value is **1194**. Keep the default value unless otherwise specified. If the port is in use of disabled in the current network, change to an available port number.
IP Range	Specify the network segment of the OpenVPN address pool. The first available in the address pool is allocated to the server, and the other addresses are allocated to clients. For example, if this parameter is set to **10.80.12.0/24**, the VPN virtual address of the server is 10.80.12.1.

Parameter	Description
Deliver Route	Add routes to the corresponding network segment if the client wants to the LAN network segment where the server resides.

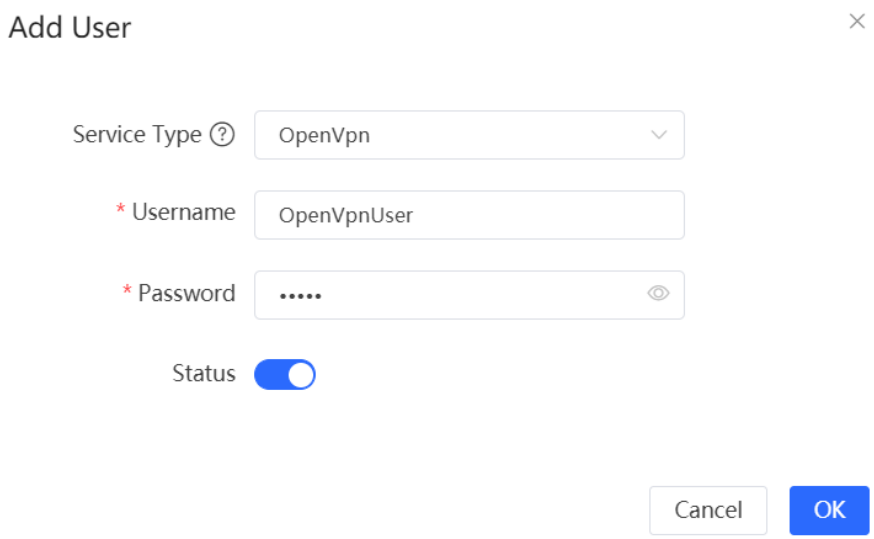
(3) Click **Advanced Settings** to configure more advanced parameters. If the device connects to other EG devices in the Reyee network, you are advised to keep the default values for advanced settings. If the device connects to devices from another vendor, keep the parameter settings consistent on the connected devices.



(4) Click **Export** to export the compressed package of the client parameter configuration. Download the compressed package to the local device and decompress it for setting the OpenVPN client in subsequent steps.



(5) Choose **One-Device** > **Gateway** > **Config** > **VPN** > **VPN Account** and add an OpenVPN user account.

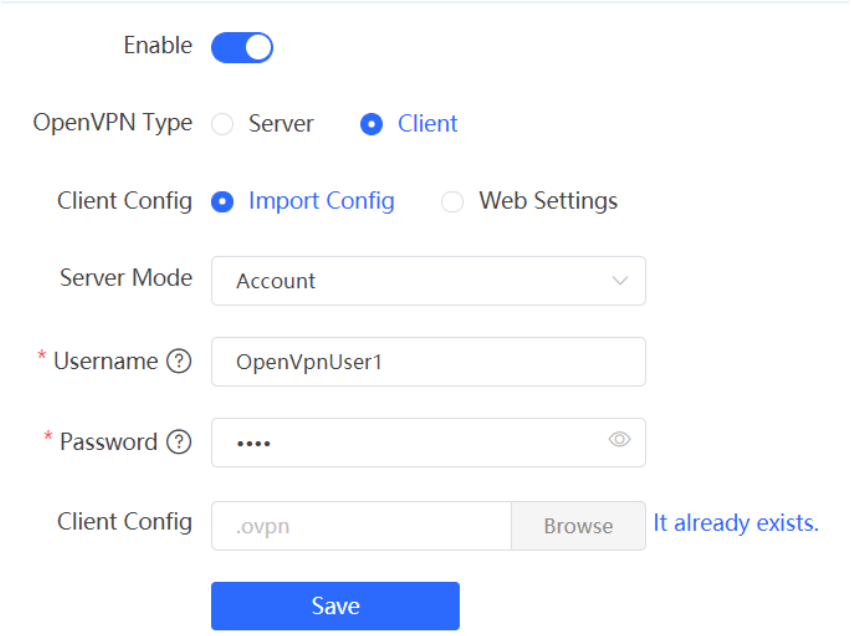


- Configure Device B

(1) Log in to the web management system and access the OpenVPN page.

(2) Turn on Enable to enable the OpenVPN function and set OpenVPN Type to Client. Two methods are available for configuring the client. The Import Config method is recommended.

- **Import Config**:

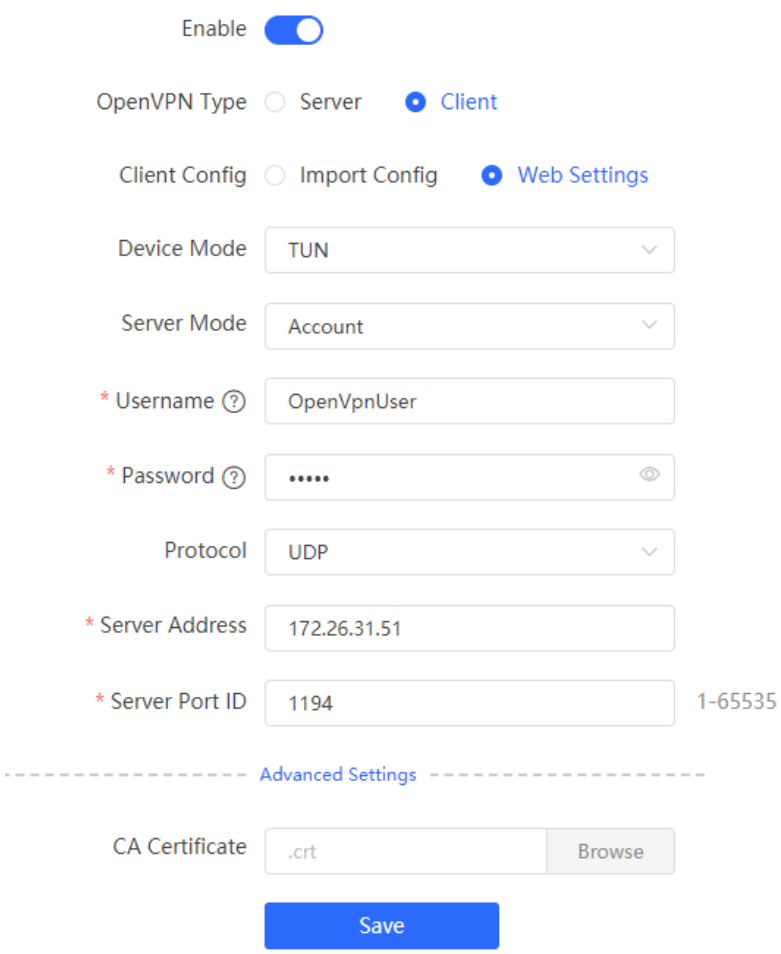


OpenVPN client configuration in Import Config method

Parameter	Description
Client Config	Select **Import Config**.
Server Mode	The value must be the same as that on the server. In this example,

Parameter	Description
	select **Account**.
Username & Password	Enter the username and password configured on the server.
Client Config	Click **Browse**, select the client configuration file exported from the server, and upload the file.

- **Web Settings**:



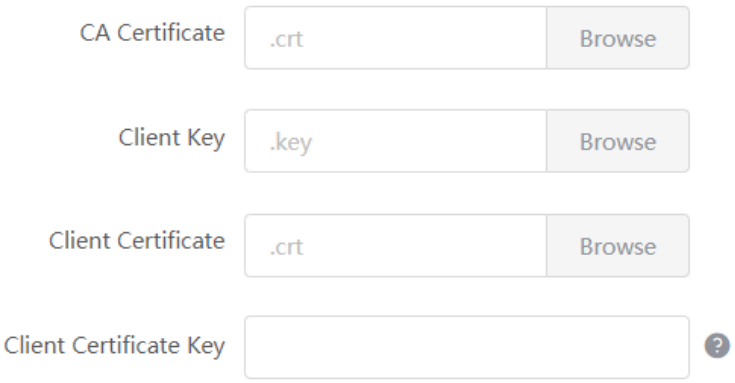
OpenVPN client configuration in Web Settings method

Parameter	Description
Client Config	Select **Web Settings**.
Device Mode	The value must be the same as that on the server. In this example, select **TUN**.

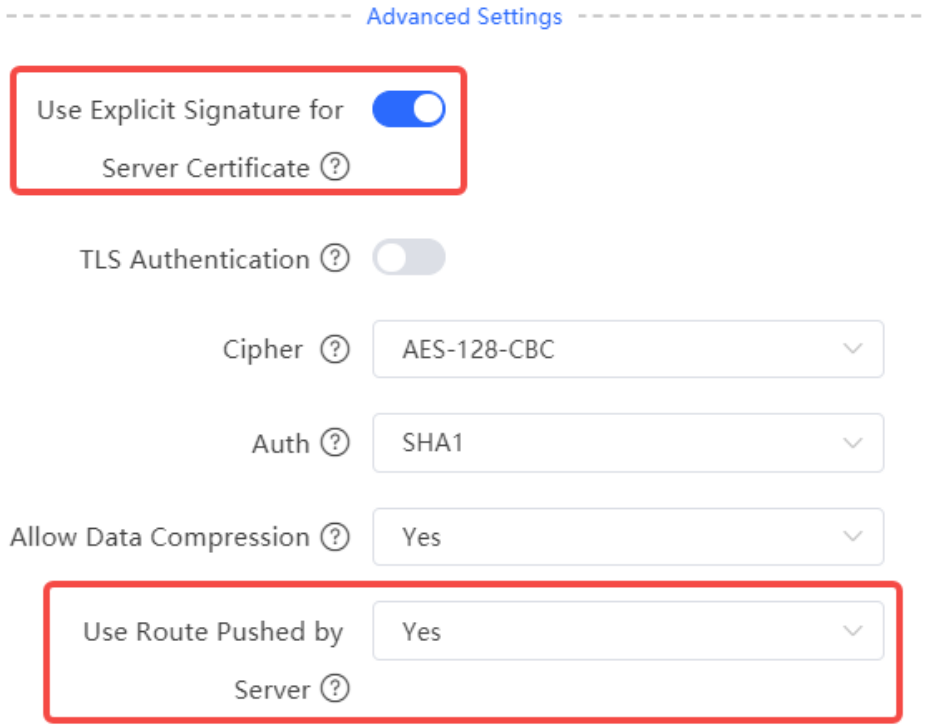
Parameter	Description
Server Mode	The value must be the same as that on the server. In this example, select **Account**.
Username & Password	Enter the username and password configured on the server.
Protocol	The value must be the same as that on the server. In this example, select **UDP**.
Server Address	Enter the public network IP address of the server, which is **172.26.31.51**.
Server Port ID	Enter the port number used by the server, such as **1194**.

Import the corresponding files according to the value of **Server Mode**.

If **Server Mode** is set to **Certificate** or **Account & Certificate**, you need to import the CA certificate file, client certificate file, and client private key file. If **Server Mode** is set to **Account**, you only need to import the CA certificate file. If the client certificate is encrypted, you also need to enter the pre-shared key specified by **Client Certificate Key**.



Click **Advanced Settings** to configure more parameters. Configure **Use Route Pushed by Server** to specify whether to accept routes pushed by the server. The value must be the same as that on the server. If the client is connected to a non-EG device, such as MikroTik server outside China, you need to turn off **Use Explicit Signature for Server Certificate**.

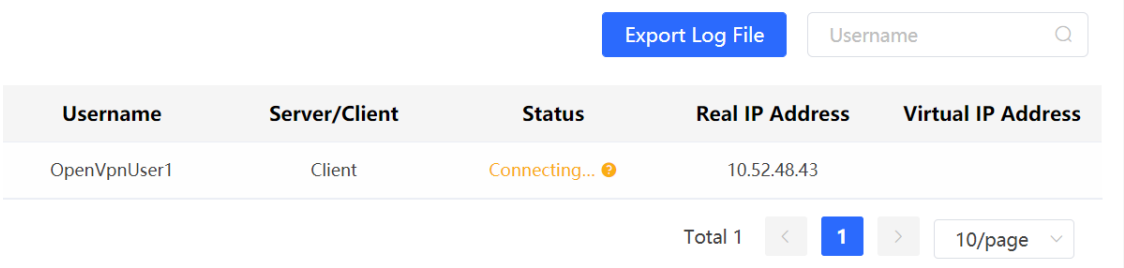


(3) After the configuration is completed, click Save to make the configuration take effect.

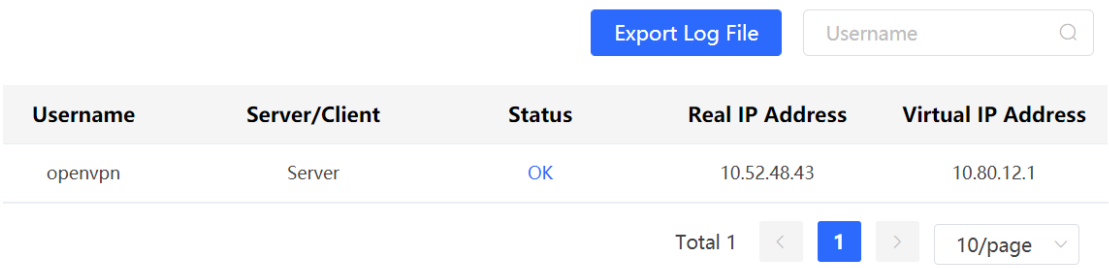
5. Verifying Configuration

After the server and client are configured, view the two tunnel end information in the tunnel list.

- Client:



- Server:



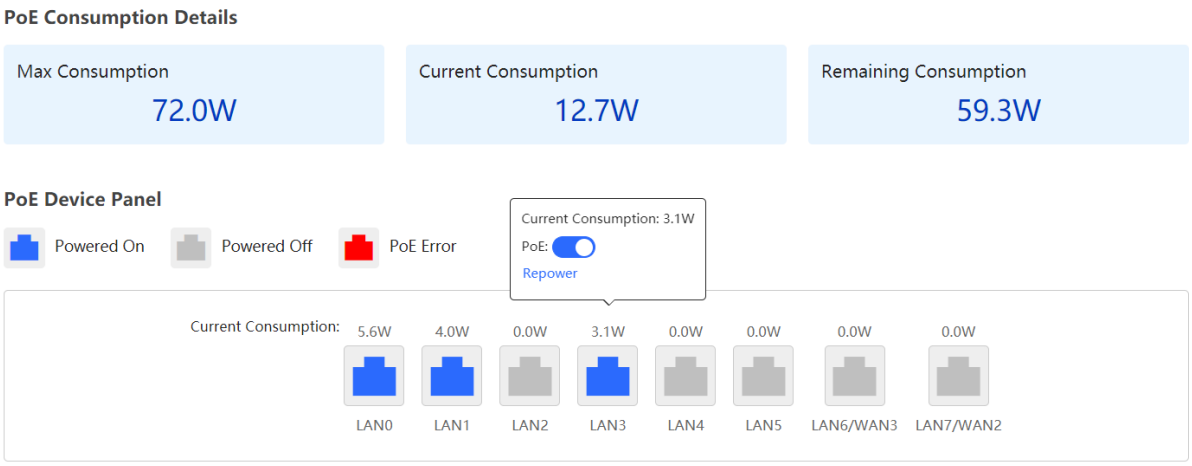
11 Configuring PoE

Caution

This feature is supported by only the models ending with -P, for example, RG-EG105G-P and RG-EG210G-P.

Choose **One-Device** > **Gateway** > **Config** > **Network** > **PoE**.

The device supplies power to PoE powered devices through ports. You can check the total power, current consumption, remaining consumption, and whether PoE power supply status is normal. Move the cursor over a port. The **PoE** toggle appears. You can click it to control whether to enable PoE on the port.



12 System Management

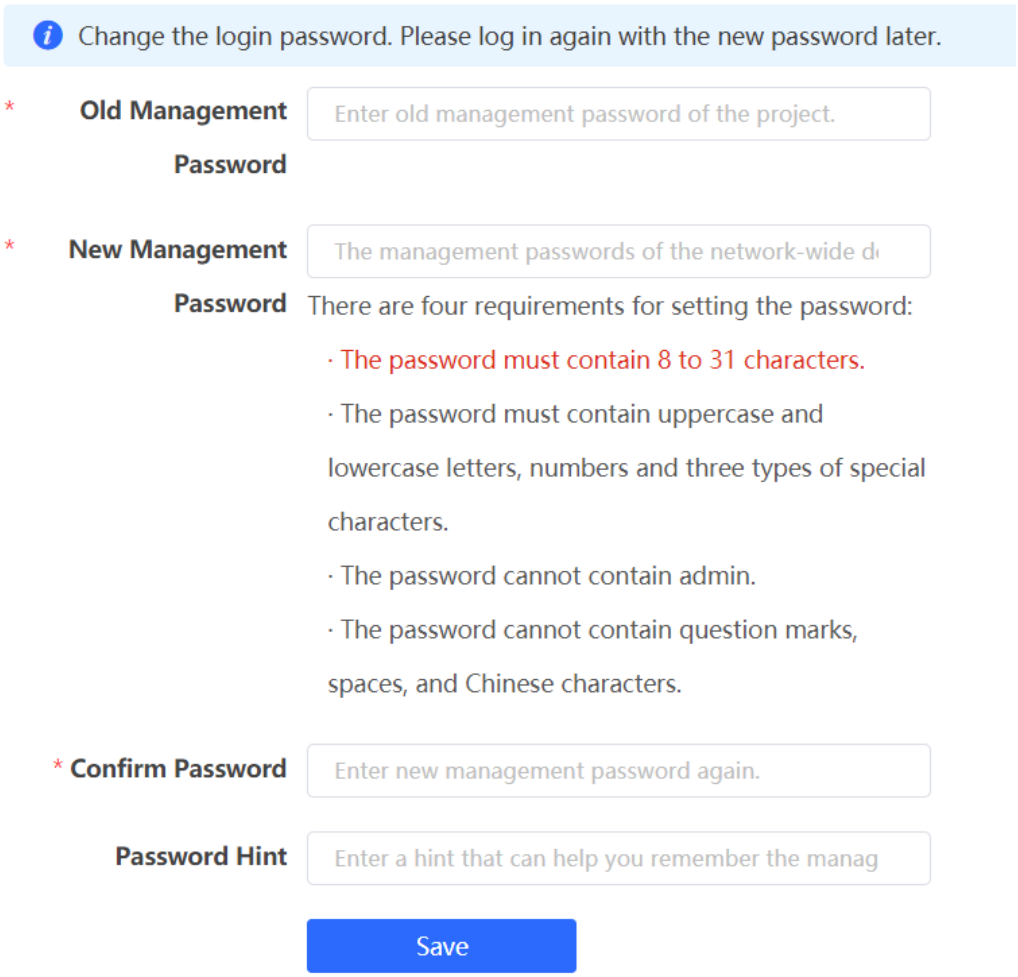
12.1 Setting the Login Password

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

Enter the old password and new password. After saving the configuration, log in again using the new password.

Caution

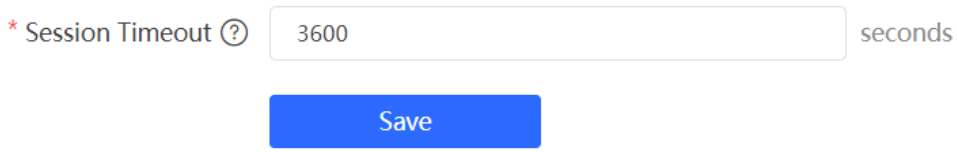
In the self-organizing network mode, the login password of all devices in the network will be changed synchronously.



12.2 Setting the Session Timeout Duration

Choose **One-Device** > **Gateway** > **Config** > **System** > **Login** > **Session Timeout**.

If no operation is performed on the Web page within a period of time, the session is automatically disconnected. When you need to perform operations again, enter the password to log in again. The default timeout duration is 3600 seconds, that is, 1 hour.

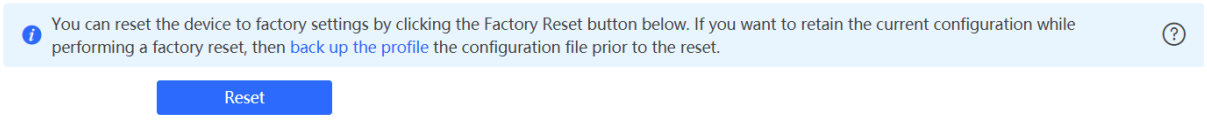


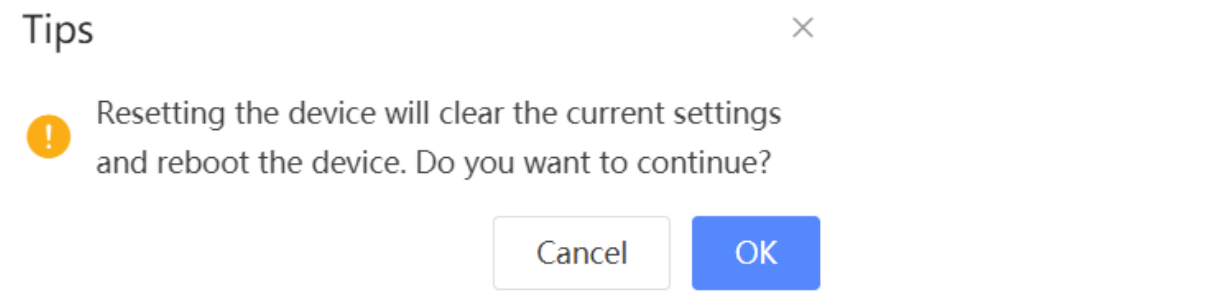
12.3 Restoring Factory Settings

12.3.1 Restoring the Current Device to Factory Settings

Choose **One-Device** > **Gateway** > **Config** > **System** > **Backup > Reset**.

Click **Reset** to restore the current device to the factory settings.





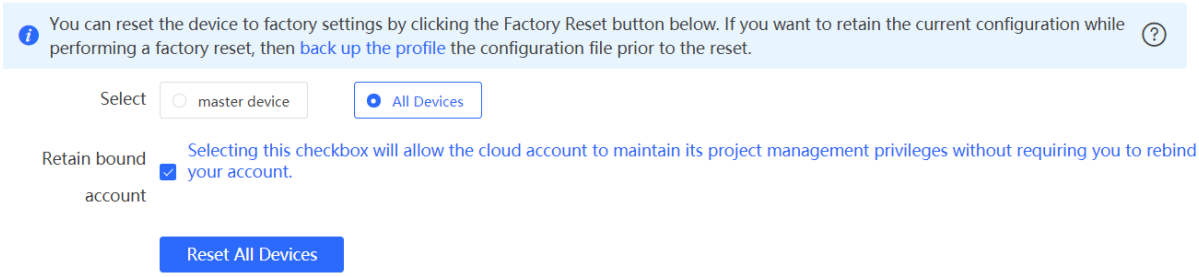
Caution

The operation will clear all configuration of the current device. If you want to retain the current configuration, back up the configuration first. (For details, see 12.9 Configuring Backup and Import.) Therefore, exercise caution when performing this operation.

12.3.2 Restoring All Devices to Factory Settings

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

Click **All Devices**, select whether to enable **Keep Account and Password,** and click **Reset All Devices**. All devices in the network will be restored to factory settings.



Caution

The operation will clear all configuration of all devices in the network. Therefore, exercise caution when performing this operation.

12.4 Configuring SNMP

12.4.1 Overview

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

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

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

12.4.2 Global Configuration

1. Overview

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

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

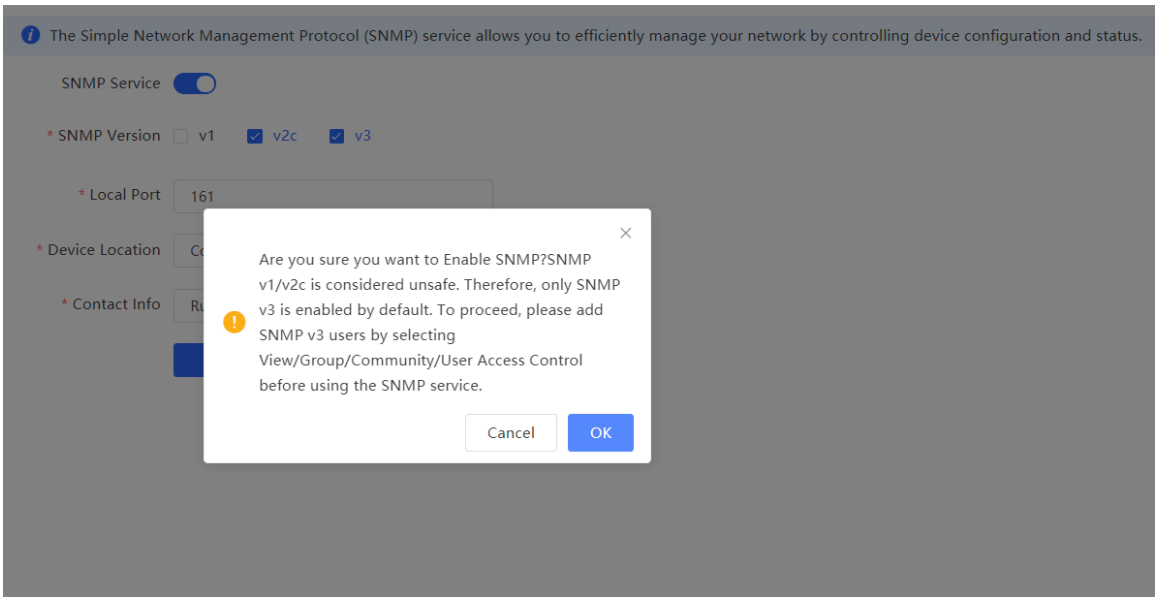
SNMP v2c: As an improved version of SNMP v1, SNMP v2c supports richer functions and more complex data types, with enhanced security. SNMP v2c performs better than SNMP v1 in terms of security and functionality, and is more flexible. It can be configured according to different needs.

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

2. Configuration Steps

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **Global Config**

(1) Enable the SNMP service.



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

(2) Set SNMP service global configuration parameters.

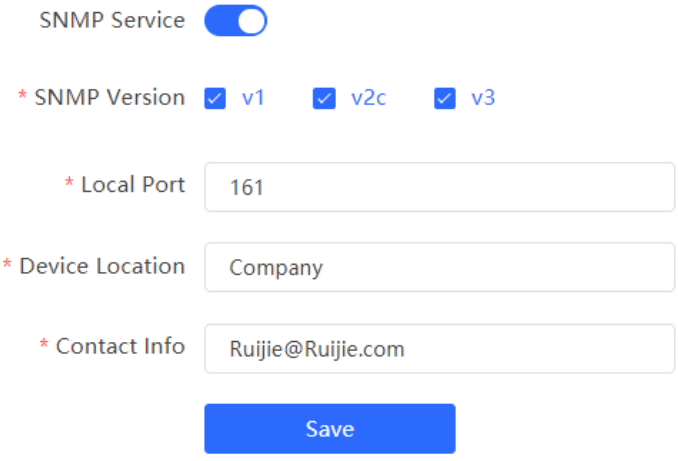


Table 12-1 Global Configuration Parameters

Parameter	Description
SNMP Server	Indicates whether SNMP service is enabled.
SNMP Version	Indicates the SNMP protocol version, including v1, v2c, and v3 versions.
Local Port	The port range is 1 to 65535.

Parameter	Description
Device Location	1-64 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.
Contact Info	1-64 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.

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

12.4.3 View/Group/Community/User Access Control

1. Configuring Views

- Overview

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

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

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

- Configuration Steps

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **View/Group/Community/Client Access Control**

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

(2) Configure basic information of a view.

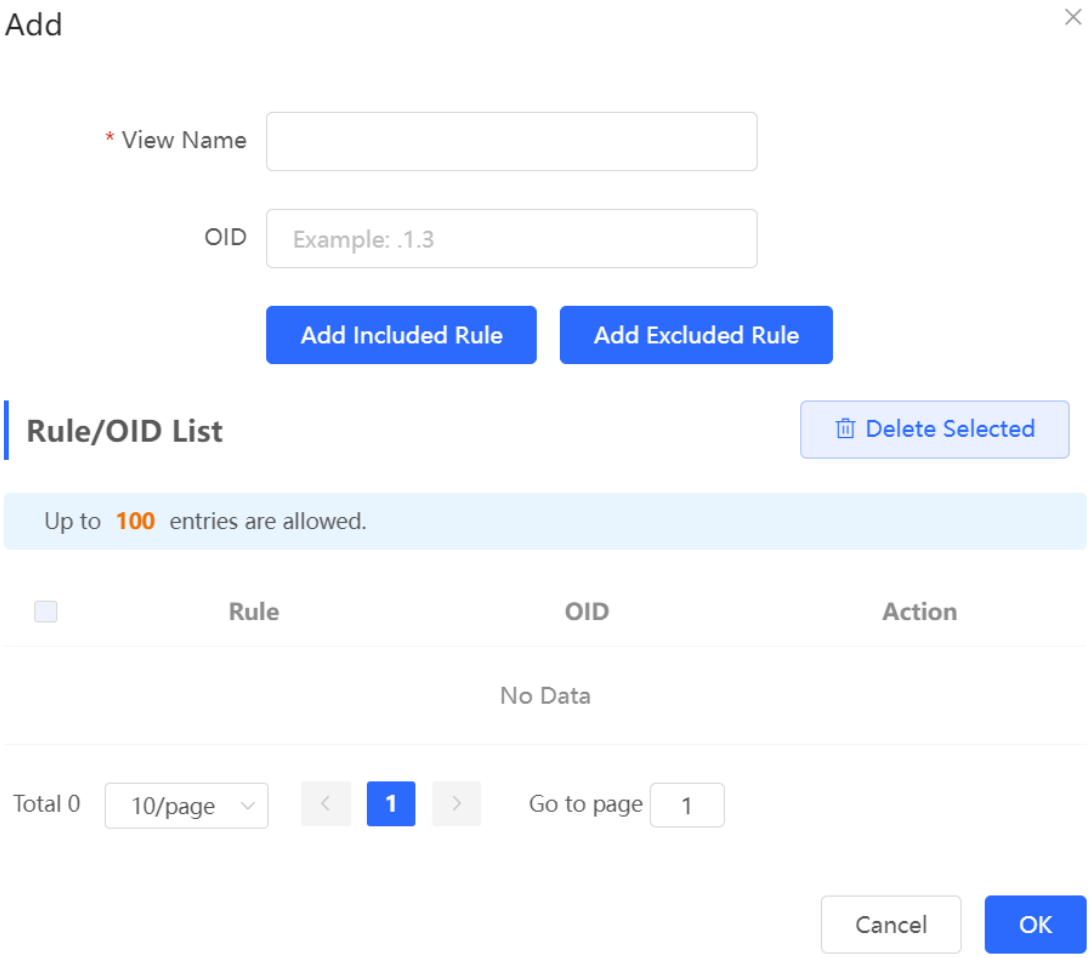


Table 12-2 View Configuration Parameters

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

Note

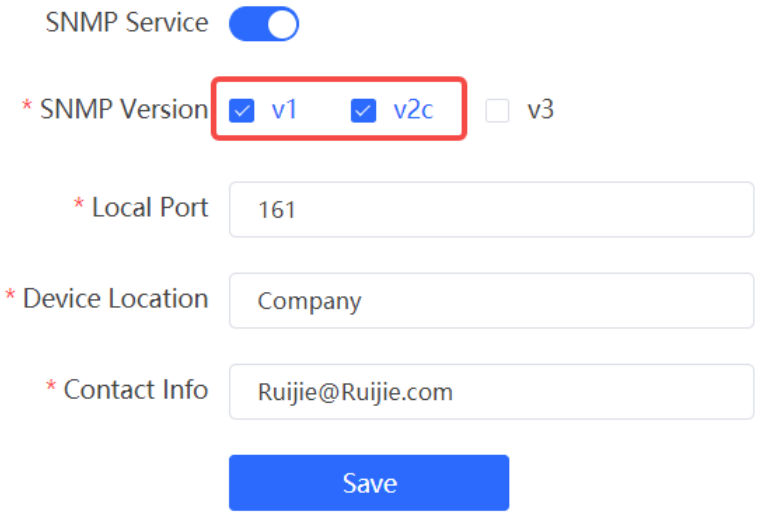
A least one OID rule must be configured for a view. Otherwise, an alarm message will appear.

(3) Click **OK**.

2. Configuring v1/v2c Users

- Overview

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



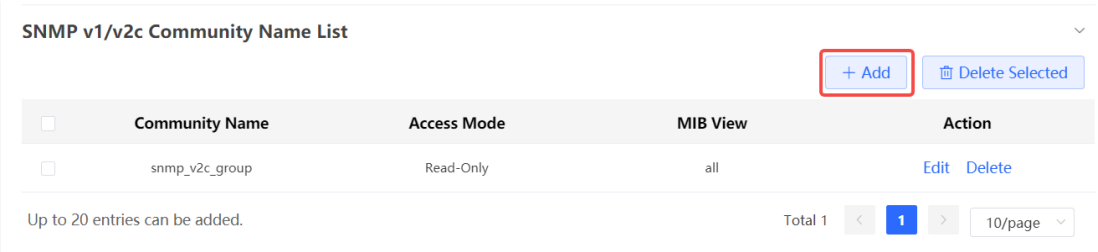
Note

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

- Configuration Steps

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **View/Group/Community/Client Access Control**

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



(2) Add a v1/v2c user.

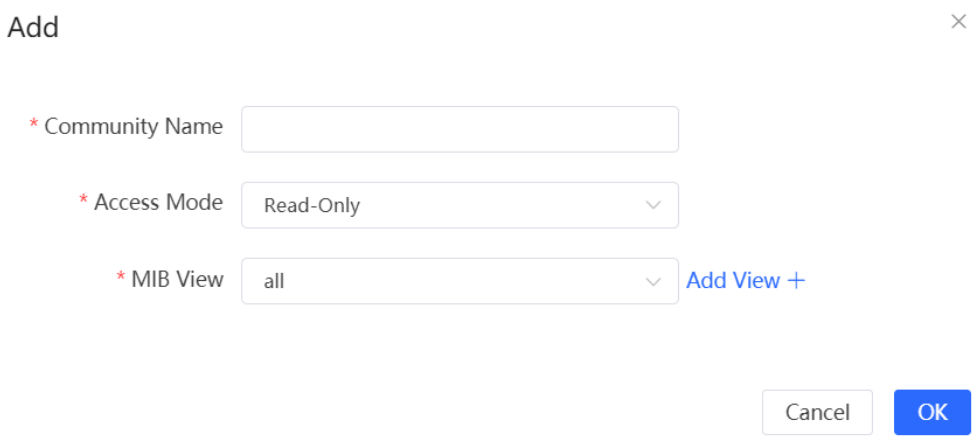


Table 12-3 v1/v2c User Configuration Parameters

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

Note

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

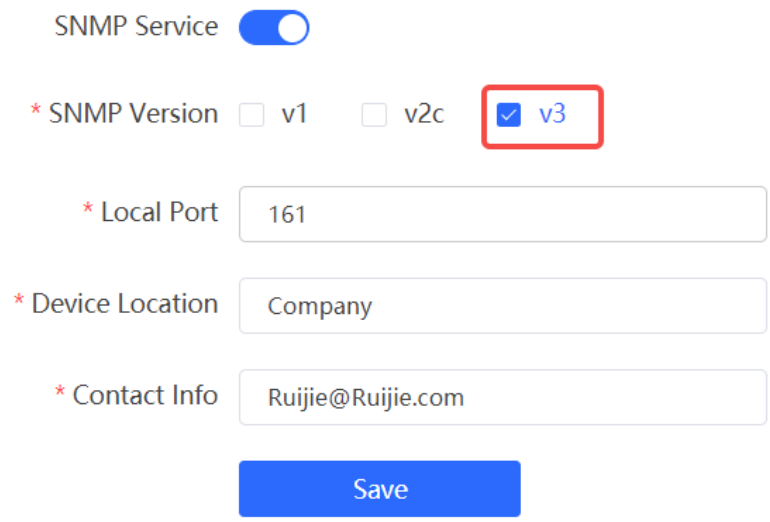
3. Configuring v3 Groups

- Overview

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

- Prerequisites

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



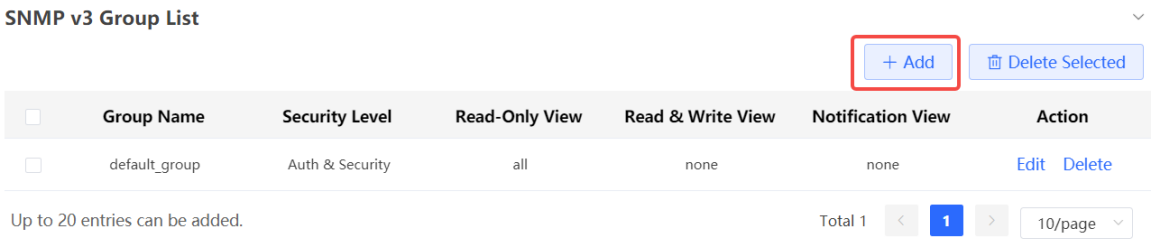
Note

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

- Configuration Steps

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **View/Group/Community/Client Access Control**

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



(2) Configure v3 group parameters.

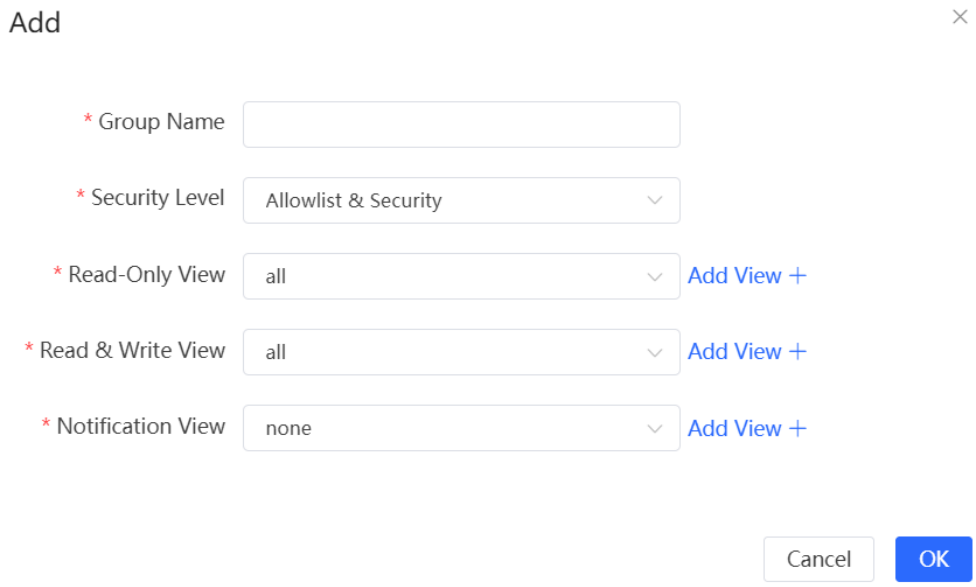


Table 12-4 v3 Group Configuration Parameters

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

Note

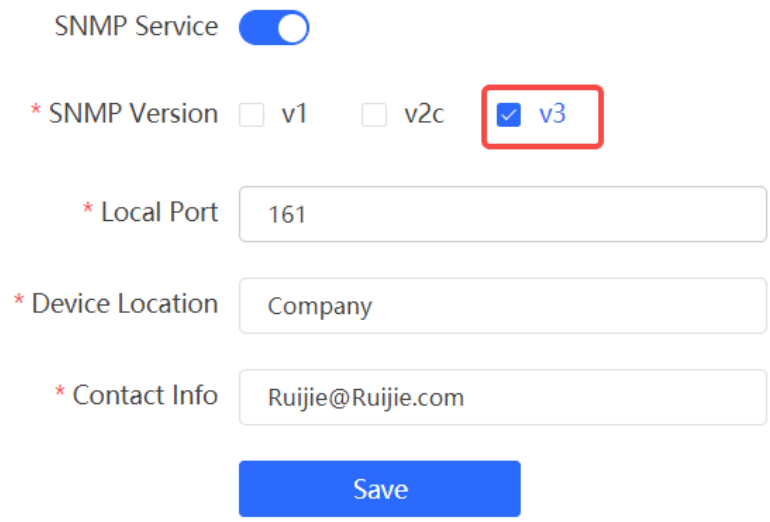
- A group defines the minimum security level, read and write permissions, and scope for users within the group.
- The group name must be unique. To add a view, click **Add View**.

(3) Click **OK**.

4. Configuring v3 Users

- Prerequisites

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



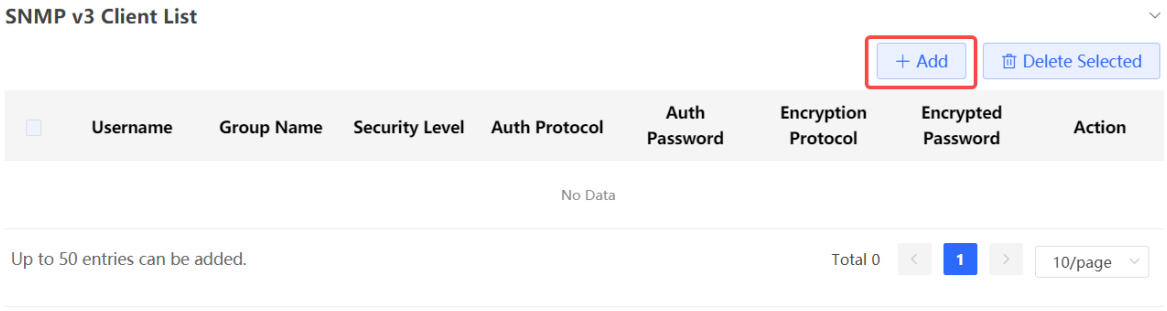
Note

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

- Configuration Steps

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **View/Group/Community/Client Access Control**.

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



(2) Configure v3 user parameters.

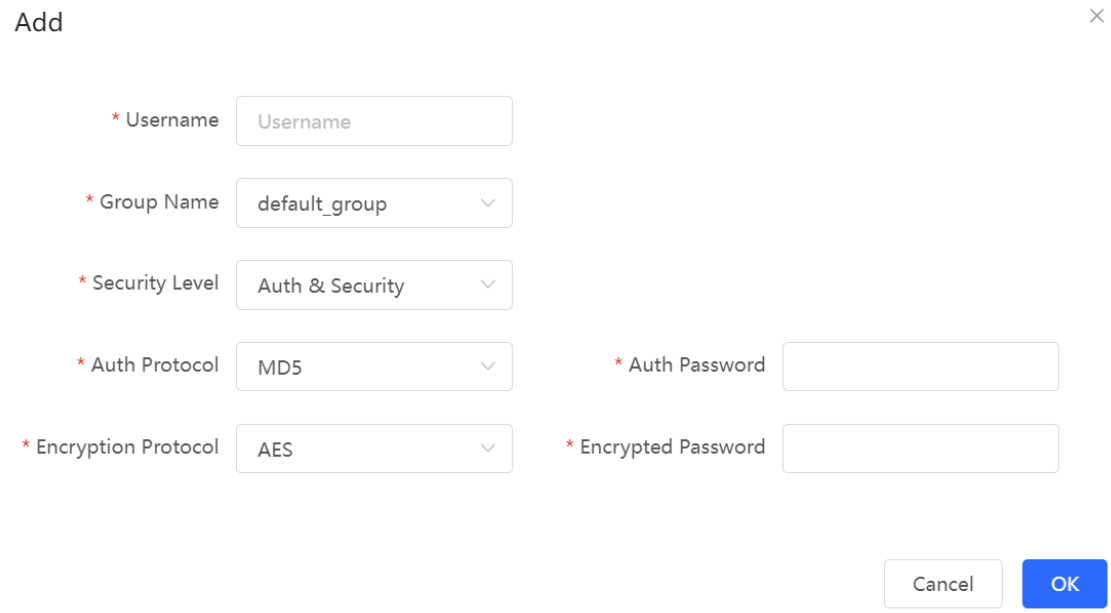


Table 12-5 v3 User Configuration Parameters

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

Parameter	Description
Encryption Protocol, Encryption Password	Encryption protocols supported: DES/AES/AES192/AES256. Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption.

Note

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

12.4.4 SNMP Service Typical Configuration Examples

1. Configuring SNMP v2c

- Application Scenario

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

- Configuration Specification

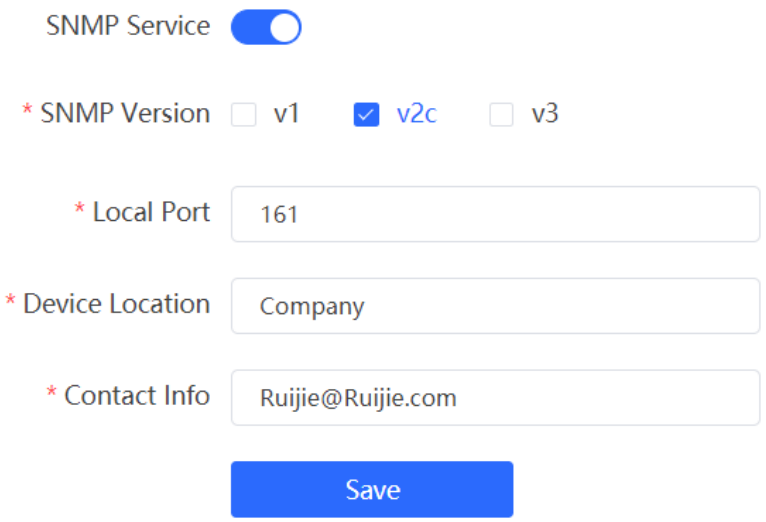
According to the user's application scenario, the requirements are shown in the following table:

Table 12-6 User Requirement Specification

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1.1, and the custom view name is "system".
Version	For SNMP v2c, the custom community name is "snmp_v2c_group", and the default port number is 161.
Read & write permission	Read-only permission.

- Configuration Steps

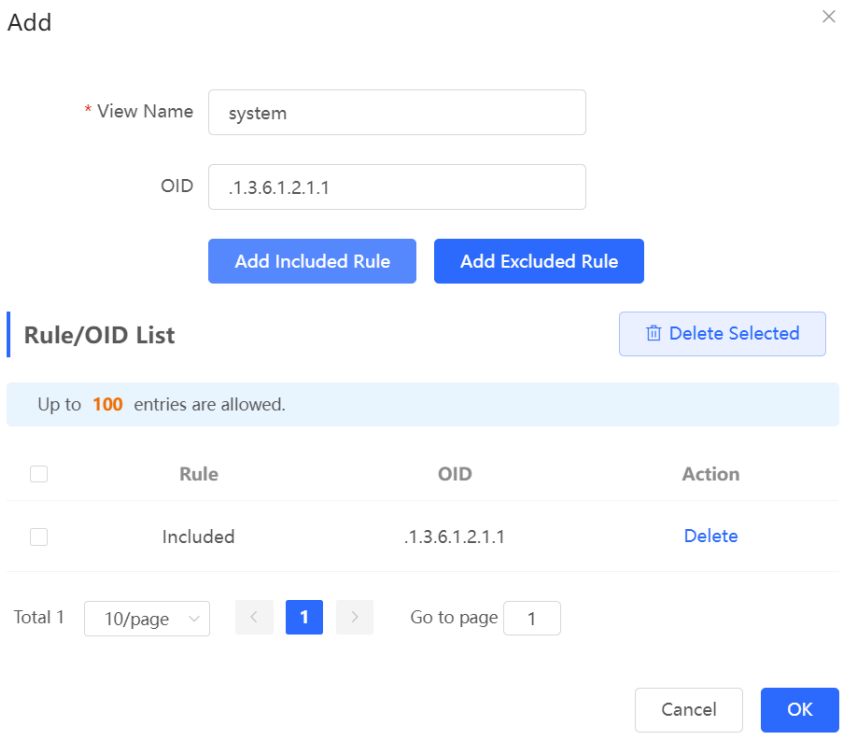
(1) In the global configuration interface, select v2c and set other settings as default. Then, click **Save**.



(2) Add a view on the **View/Group/Community/Client Access Control** interface.

a Click **Add** in the **View List** pane to add a view.

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

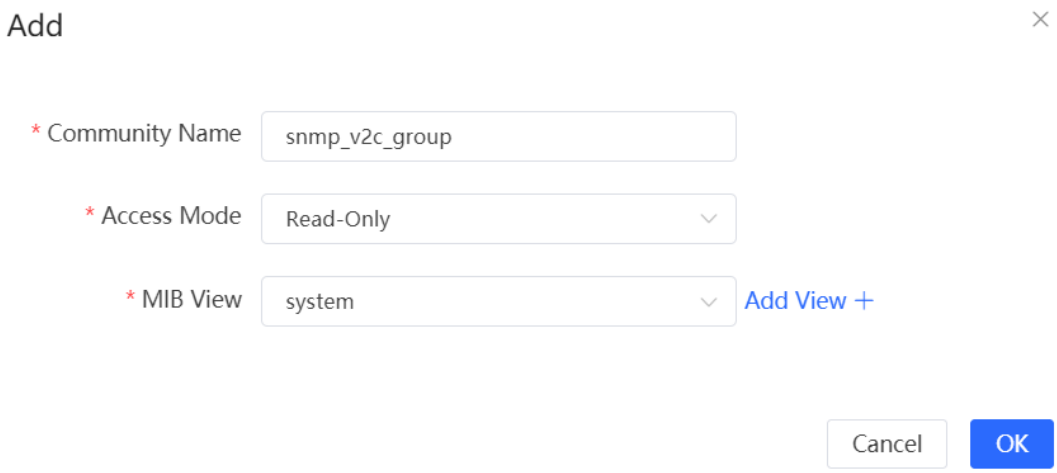


c Click **OK**.

(3) On the View/Group/Community/Client Access Control interface, enter the SNMP v1/v2c community name.

a Click **Add** in the **SNMP v1/v2c Community Name List** pane.

b Enter the group name, access mode, and view in the pop-up window.



c Click **OK**.

2. Configuring SNMP v3

- Application Scenario

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

- Configuration Specification

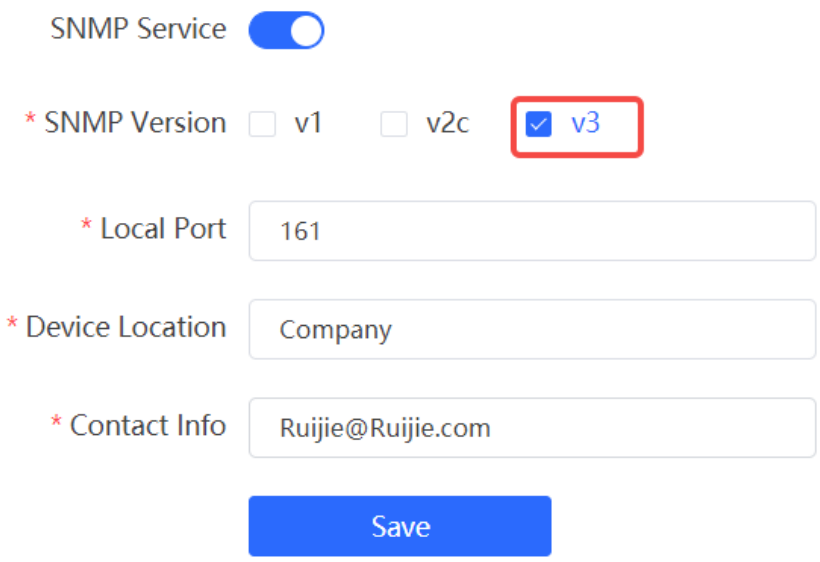
According to the user's application scenario, the requirements are shown in the following table:

Table 12-7 User Requirement Specification

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1, and the custom view name is "public_view".
Group configuration	Group name: default_group Security level: authentication and encryption Select **public_view** for a read-only view. Select **public_view** for a read & write view. Select **none** for a notify view.
Configuring v3 Users	User name: snmp _v3_user Group name: default_group Security level: authentication and encryption Authentication protocol/password: MD5/Ruijie123 Encryption protocol/password: AES/Ruijie123
Version	For SNMP v3, the default port number is 161.

- Configuration Steps

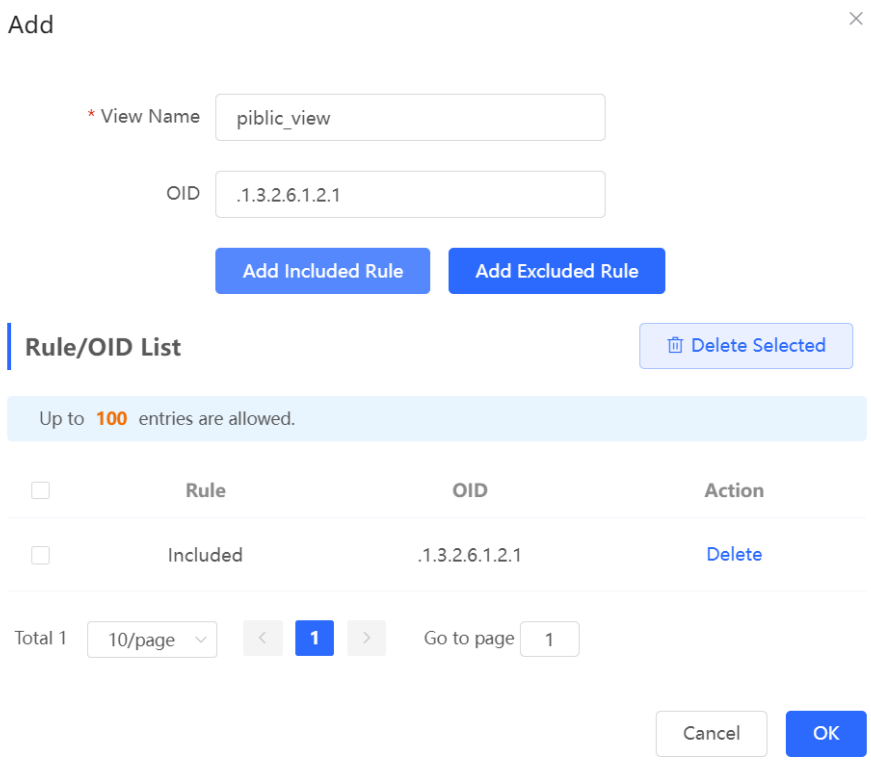
(1) On the global configuration interface, select v3, and change the port number to 161. Set other settings to defaults. Then, click **Save**.



(2) Add a view on the **View/Group/Community/Client Access Control** interface.

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

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

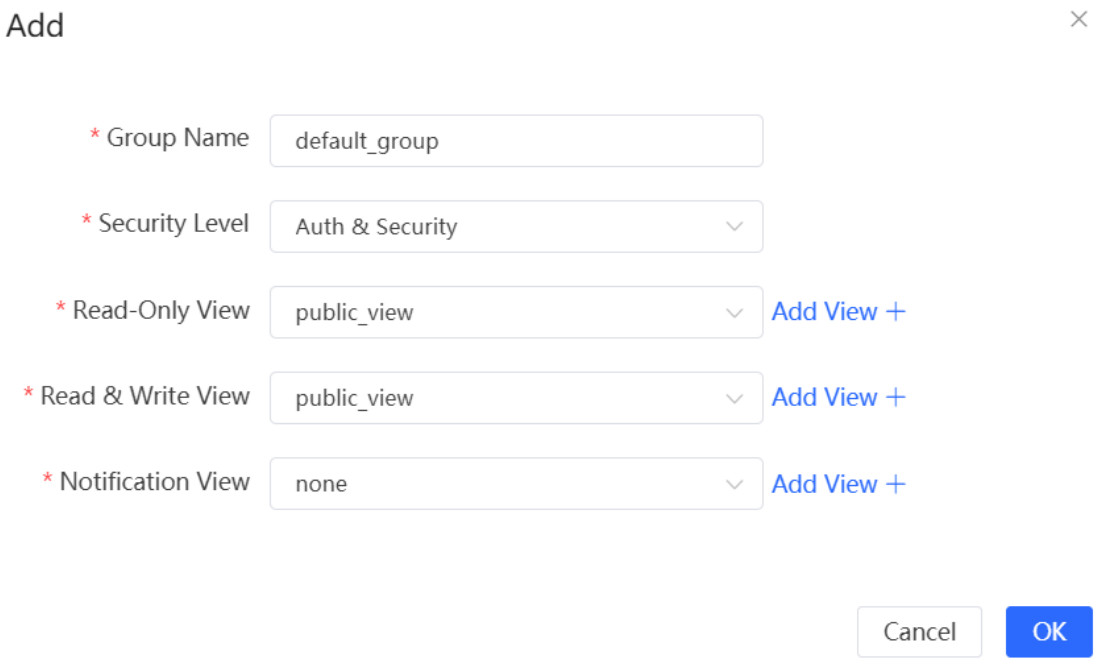


c Click **OK**.

(3) On the View/Group/Community/Client Access Control interface, add an SNMP v3 group.

a Click **Add** in the **SNMP v3 Group List** pane.

b Enter the group name and security level on the pop-up window. As this user has read and write permissions, select public_view for read-only and read & write views, and select none for notify views.

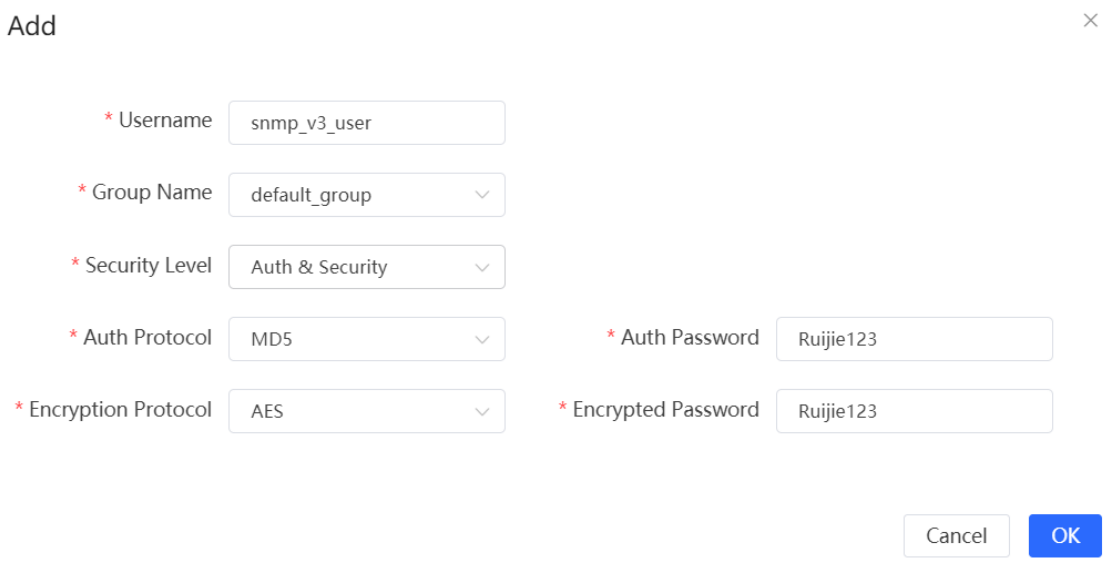


c Click **OK**.

(4) On the View/Group/Community/Client Access Control interface, add an SNMP v3 user.

a Click Add in the SNMP v3 Client List pane.

b Enter the user name and group name in the pop-up window. As the user's security level is authentication and encryption, enter the authentication protocol, authentication password, encryption protocol, and encryption password.



c Click **OK**.

12.4.5 Configuring Trap Service

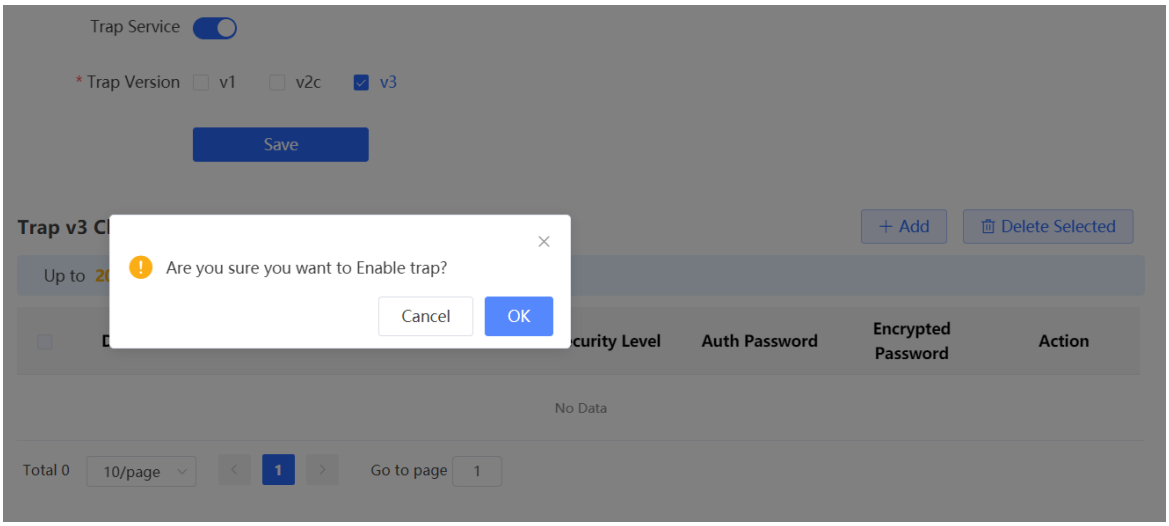
Trap is a notification mechanism of the Simple Network Management Protocol (SNMP) protocol. It is used to report the status and events of network devices to administrators, including device status, faults, performance, configuration, and security management. Trap provides real-time network monitoring and fault diagnosis services, helping administrators discover and solve network problems in a timely manner.

1. Enabling Trap Service

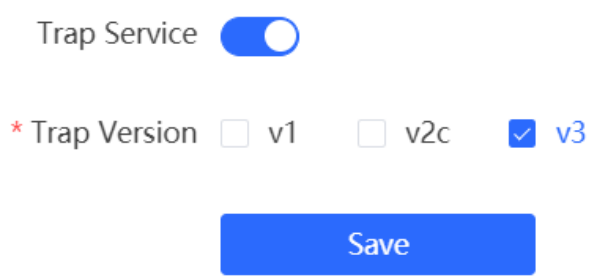
Enable the trap service and select the effective trap version, including v1, v2c, and v3 versions.

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **Trap Setting**

(1) Enable the trap service. When the trap service is enabled for the first time, the system will pop up a prompt message. Click **OK**.



(2) Set the trap version. The trap versions include v1, v2c, and v3.



(3) After the trap service is enabled, click **Save** for the configuration to take effect.

2. Configuring Trap v1/v2c Users

- Overview

Trap is a notification mechanism that is used to send alerts to administrators when important events or failures occur on devices or services. Trap v1/v2c are two versions in the SNMP protocol for network management and monitoring.

Trap v1 is the first version that supports basic alert notification functionality. Trap v2c is the second version, which supports more alert notification options and advanced security features.

By using trap v1/v2c, administrators can promptly understand problems on the network and take corresponding measures.

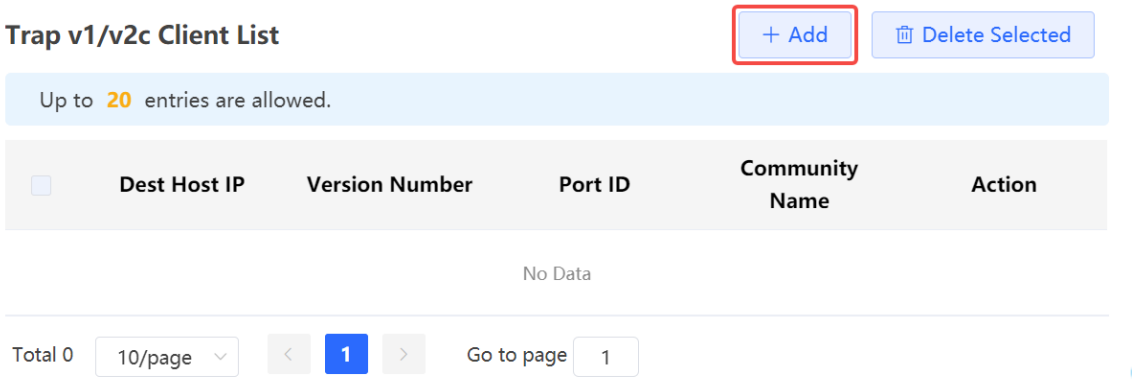
- Prerequisites

Once trap v1 and v2c versions are selected, it is necessary to add trap v1v2c users.

- Procedure

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **Trap Setting**

(1) Click **Add** in the **Trap v1/v2c Client List** pane to add a trap v1/v2c user.



(2) Configure trap v1/v2c user parameters.

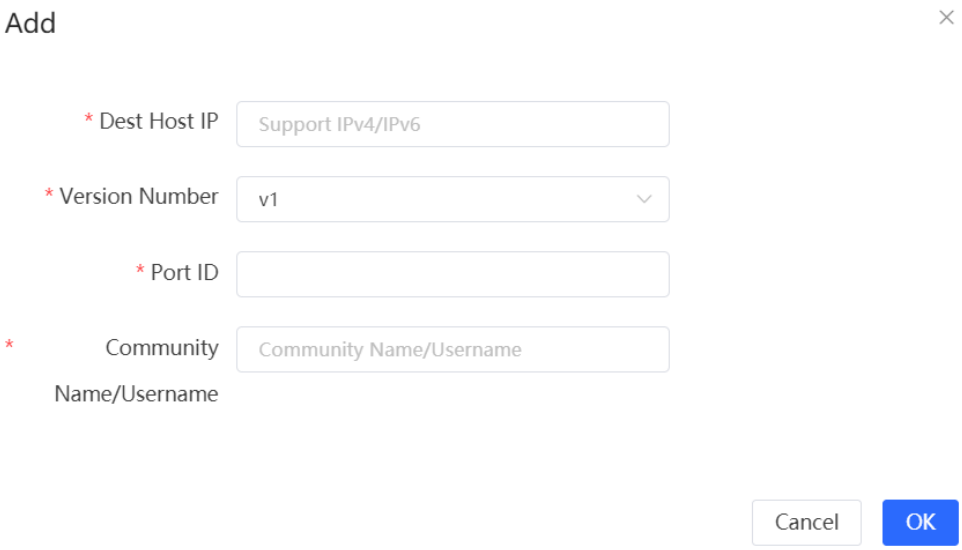


Table 12-8 Trap v1/v2c User Configuration Parameters

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

Note

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

(3) Click **OK**.

3. Configuring Trap v3 Users

- Overview

Trap v3 is a network management mechanism based on the SNMP protocol. It is used to send alert notifications to administrators. Unlike previous versions, trap v3 provides more secure and flexible configuration options, including authentication and encryption features.

Trap v3 offers custom conditions and methods for sending alerts, as well as the recipients and notification methods for receiving alerts. This enables administrators to have a more accurate understanding of the status of network devices and to take timely measures to ensure the security and reliability of the network.

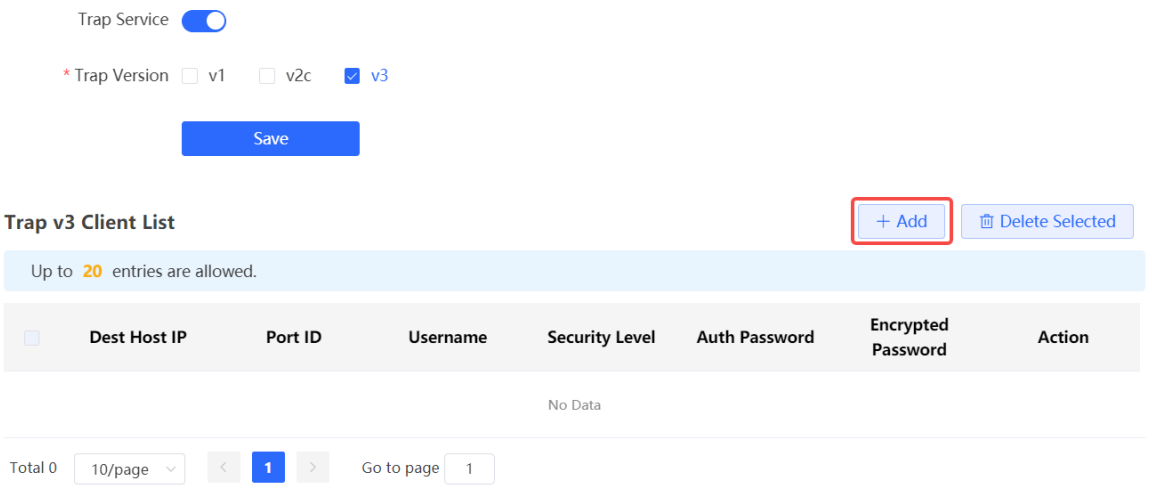
- Prerequisites

When the v3 version is selected for the trap service, it is necessary to add a trap v3 user.

- Configuration Steps

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **SNMP** > **Trap Setting**

(1) Click **Add** in the **Trap v3 User** pane to add a trap v3 user.



(2) Configure trap v3 user parameters.

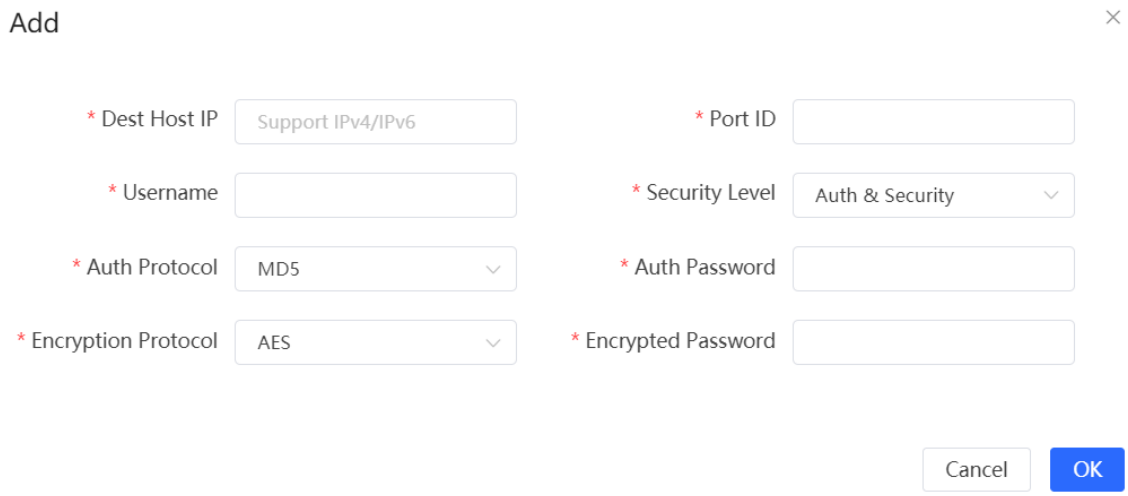


Table 12-9 Trap v3 User Configuration Parameters

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.
Port ID	The port range of the trap peer device is 1 to 65535.
Username	Name of the trap v3 user. ● At least 8 characters. ● It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. ● Admin, public or private community names are not allowed. ● Question marks, spaces, and Chinese characters are not allowed.
Security Level	Indicates the security level of the trap v3 user. The security levels include authentication and encryption, authentication but no encryption, and no authentication and encryption.

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

Note

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

12.4.6 Trap Service Typical Configuration Examples

1. Configuring Trap v2c

- Application Scenarios

During device monitoring, if the device is suddenly disconnected or encounters an abnormality, and the third-party monitoring software cannot detect and handle the abnormal situation in a timely manner, you can configure the device with a destination IP address of 192.168.110.85 and a port number of 166 to enable the device to send a v2c trap in case of an abnormality.

- Configuration Specification

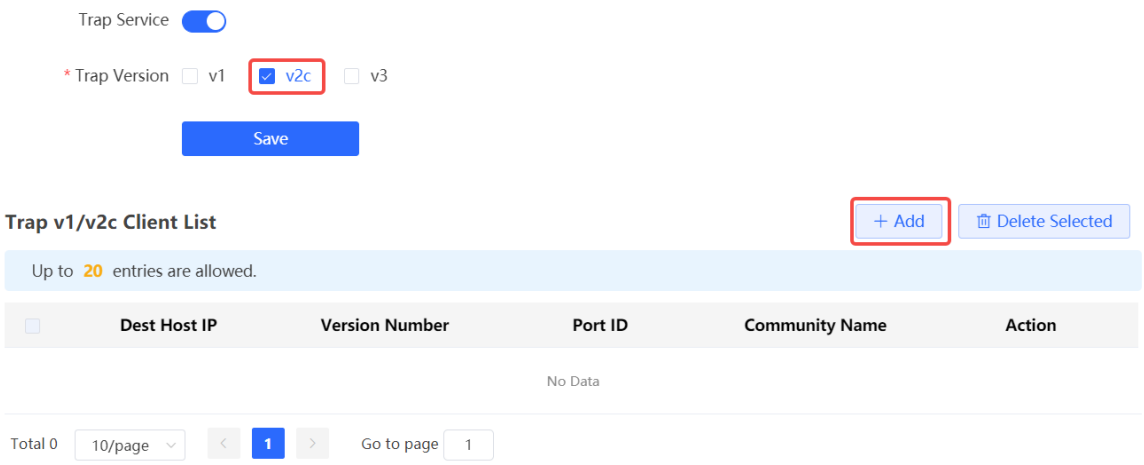
According to the user's application scenario, the requirements are shown in the following table:

Table 12-10 User Requirement Specification

Item	Description
IP address and port number	The destination host IP is 192.168.110.85, and the port number is 166.
Version	Select the v2 version.
Community name/User name	Trap_user

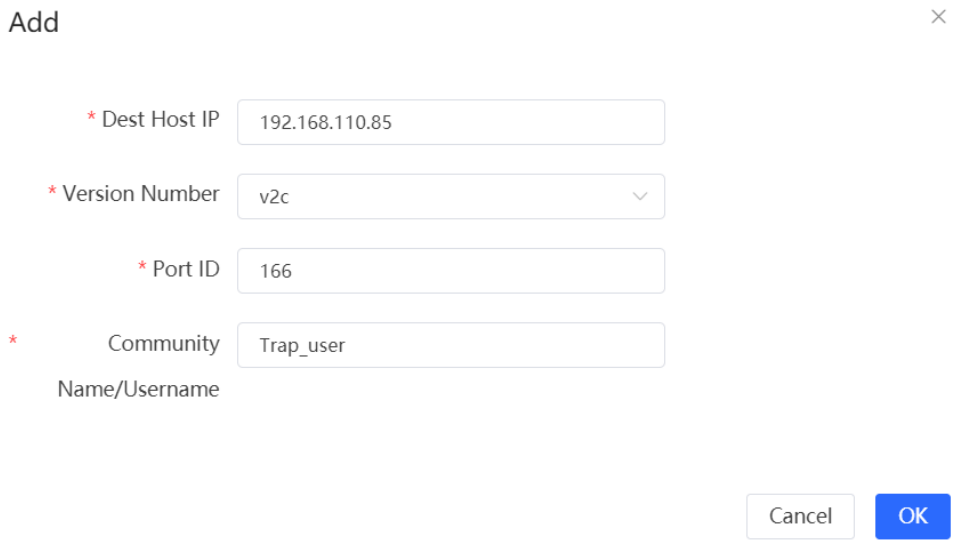
- Configuration Steps

(1) Select the v2c version in the **Trap Setting** interface and click **Save**.



(2) Click **Add** in the Trap v1/v2c Client List to add a trap v2c user.

(3) Enter the destination host IP address, version, port number, user name, and other information. Then, click **OK**.



2. Configuring Trap v3

- Application Scenarios

During device monitoring, if the device is suddenly disconnected or encounters an abnormality, and the third-party monitoring software cannot detect and handle the abnormal situation in a timely manner, you can configure the device with a destination IP address of 192.168.110.87 and a port number of 167 to enable the device to send a v3 trap, which is a safer trap compared with v1/v2c traps.

- Configuration Specification

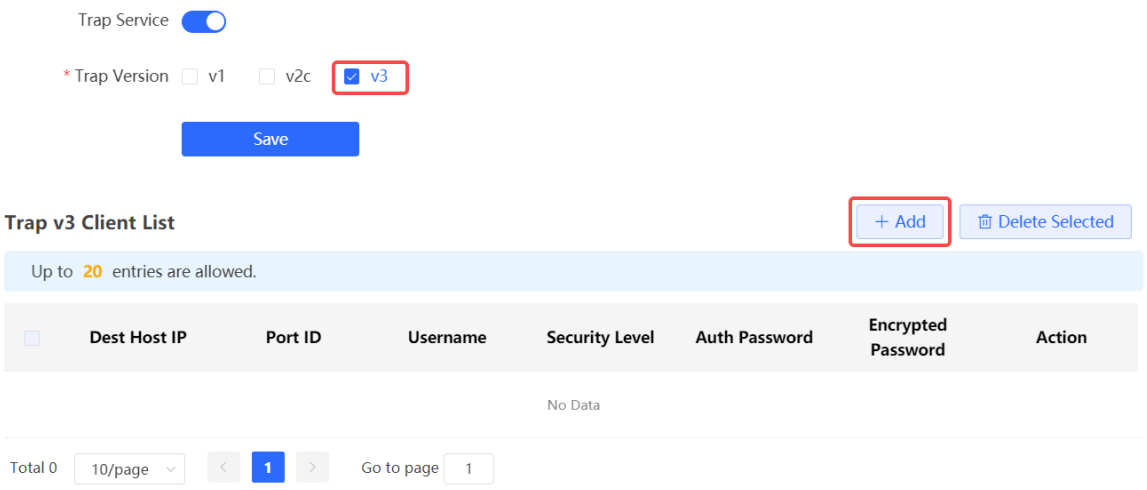
According to the user's application scenario, the requirements are shown in the following table:

Table 12-11 User Requirement Specification

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

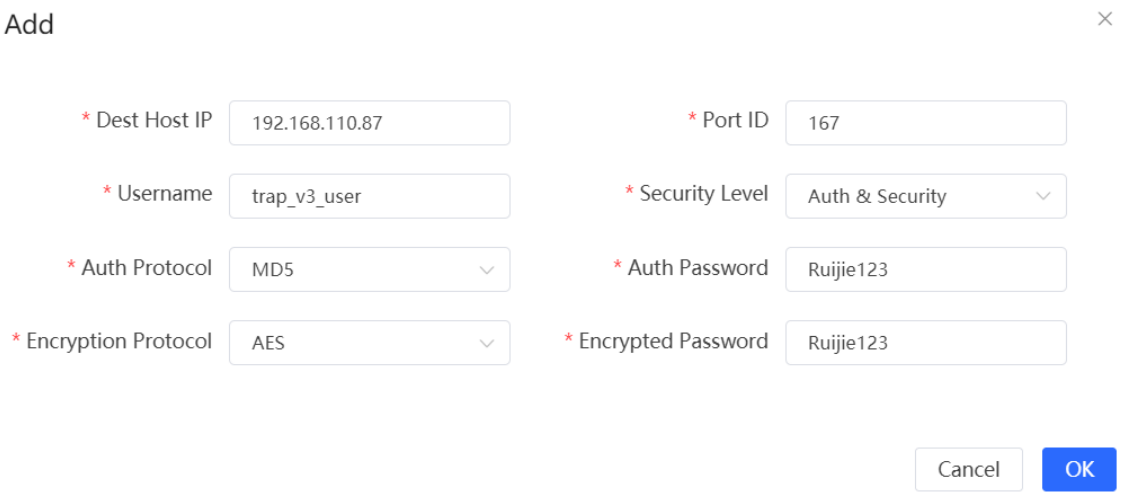
- Configuration Steps

(1) Select the v3 version in the **Trap Setting** interface and click **Save**.



(2) Click **Add** in the Trap v3 Client List to add a trap v3 user.

(3) Enter the destination host IP address, port number, user name, and other information. Then, click **OK**.



12.5 Configure IEEE 802.1X authentication

Note

This feature is supported on RG-EG105G-V3, RG-EG105G-P-V3, RG-EG209GS, RG-EG210G-P-V3, RG-EG310GH-E, RG-EG305GH-P-E, RG-EG310GH-P-E and RG-EG1510XS.

12.5.1 Overview

IEEE 802.1X is a port-based network access control standard that provides secure access services for LANs.

On an IEEE 802 LAN, a user can directly access network resources without authentication and authorization as long as it can connect to a network device. This uncontrolled behavior can bring security risks to the network. The IEEE 802.1X protocol was proposed to address the security issues on an IEEE 802 LAN.

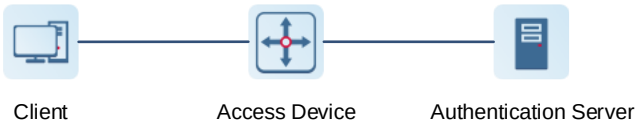
The IEEE 802.1X protocol supports three security applications: Authentication, Authorization, and Accounting, abbreviated as AAA.

- Authentication: Determines whether a user can obtain access, and restricts unauthorized users.
- Authorization: Authorizes services available for authorized users, and controls the permissions of unauthorized users.
- Accounting: Records the usage of network resources by users, and provides a basis for traffic billing.

The 802.1X feature can be deployed on networks to control user authentication, authorization, and more.

An 802.1X network uses a typical client/server architecture, consisting of three entities: client, access device, and authentication server. A typical architecture is shown here.

Figure 12-1 Typical Architecture of 802.1X Network



- The client is usually an endpoint device which can initiate 802.1X authentication through the client software. The client must support the Extensible Authentication Protocol over LANs (EAPoL) on the local area network.
- The access device is usually a network device (AP or switching device) that supports the IEEE 802.1X protocol. It provides an interface for clients to access the local area network, which can be a physical or a logical interface.

  Note
  - The RG-EG gateway device itself does not support the IEEE 802.1X authentication, and can only serve as the primary device to support 802.1X global configuration and deliver the configuration to APs and switching devices on the entire network.
  - To achieve IEEE 802.1X authentication, ensure that the network includes an AP or switching device.

- The authentication server can realize user authentication, authorization, and accounting. Usually a RADIUS server is used as the authentication server.

12.5.2 Configuring 802.1X Globally

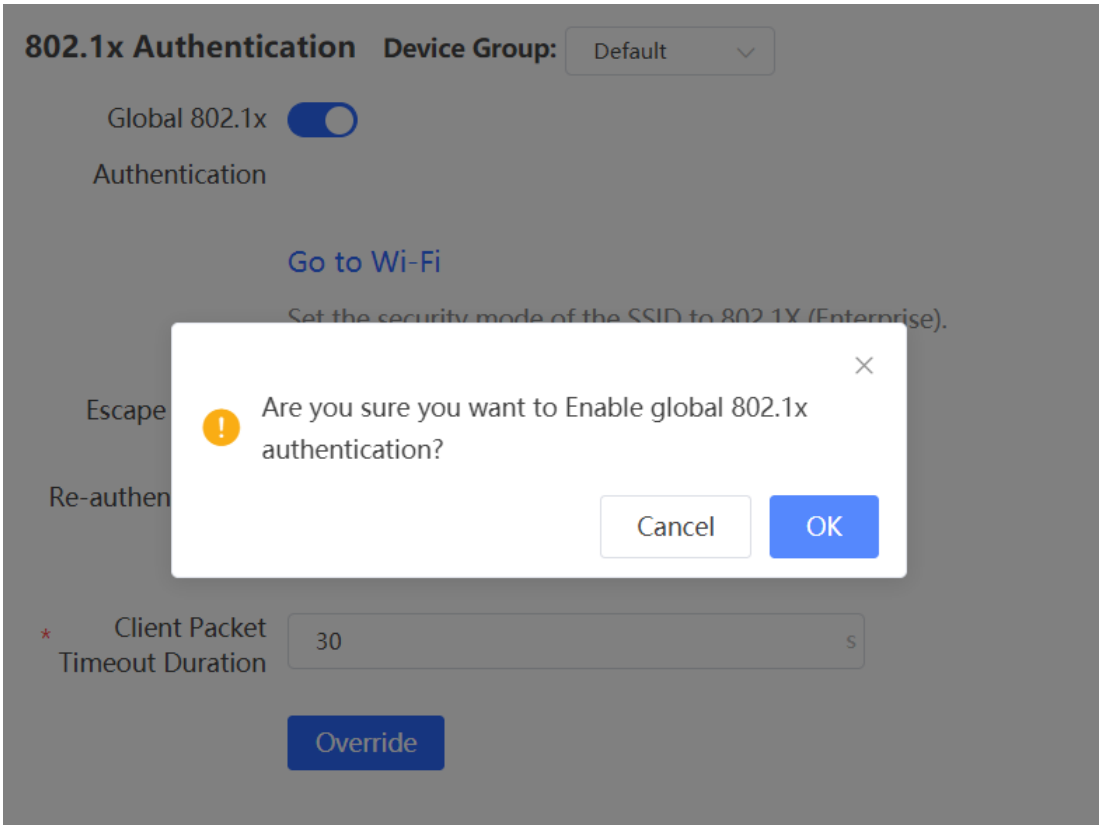
The gateway device supports the 802.1X global configuration, and can synchronously deliver the configuration to APs and switching devices on the network.

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **802.1x Authentication** > **802.1x Authentication.**

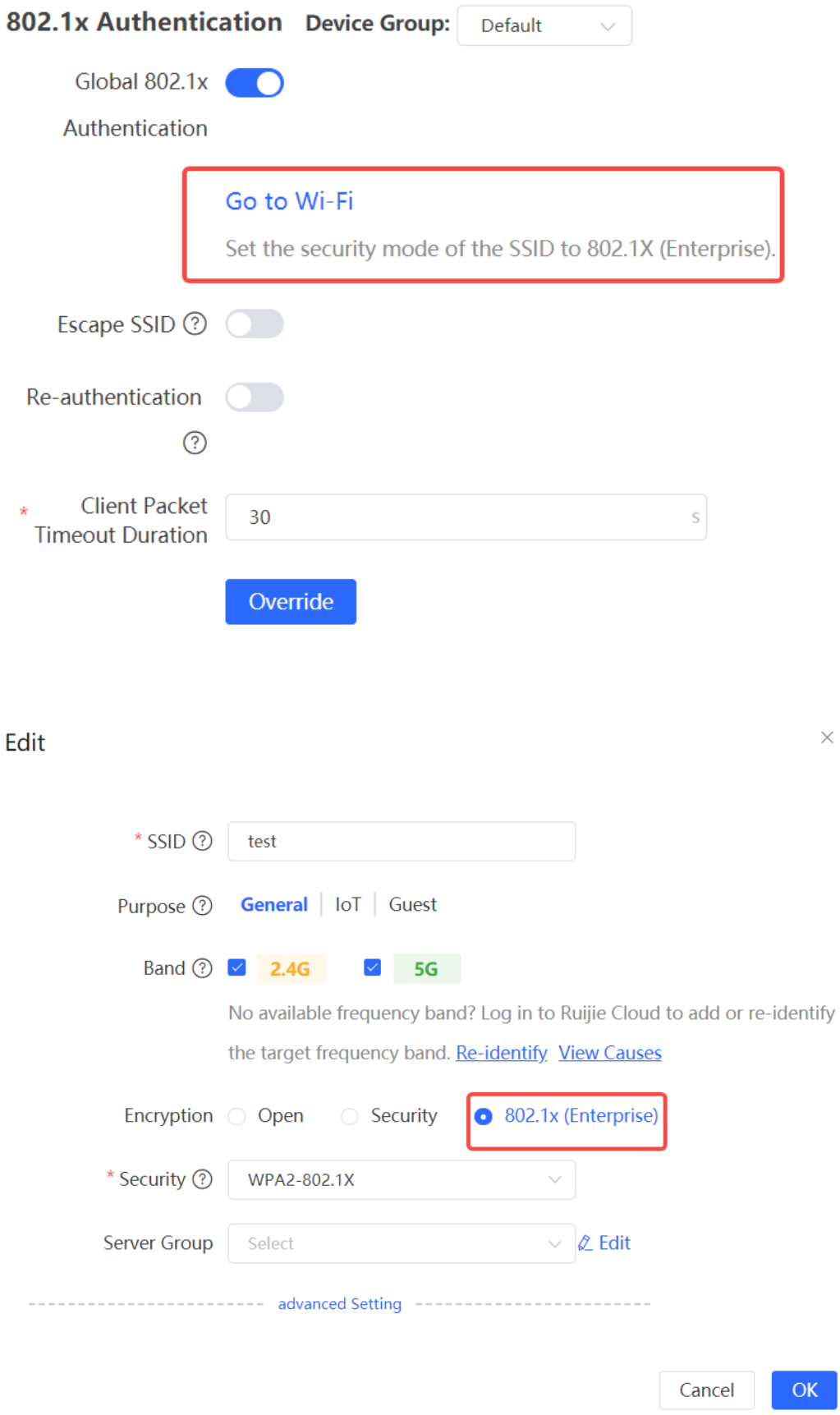
(1) Click the **802.1x Authentication** tab to configure global configuration for 802.1x wireless authentication.

(2) Select the authentication device group, and enable the global 802.1x authentication.

You will be prompted to enable this feature or not. Click **OK**.



(3) Click **Go to Wi-Fi,** and set the encryption method of SSID to **802.1x (Enterprise)**.



(4) Configure global parameters.

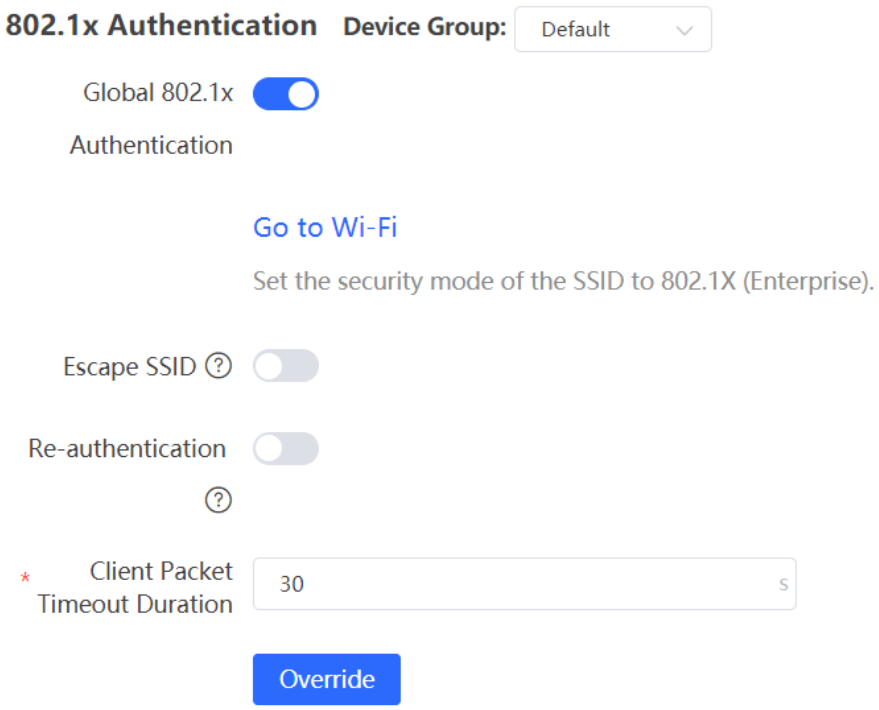


Table 12-12 Description of Global 802.1x Authentication Configuration

Parameter	Description
Escape SSID	Once this feature is enabled, when the authentication server is unavailable, the system will create a temporary Wi-Fi network for users. If this function is enabled, it is necessary to set the Escape SSID, encryption type, and Wi-Fi password.
Re-authentication	Once this feature is enabled, the system regularly re-authenticates users. Users who do not match the information on the server will be automatically disconnected. If this function is enabled, it is necessary to set the re-authentication cycle, which is 21600 seconds by default.
Client Packet Timeout Duration	The timeout period during which the client waits for a response from the authentication server. If this timer expires, authentication is considered failed. The value range is 10 seconds to 60 seconds. The default value is 30 seconds.

(5) Click **Override**.

12.5.3 Configuring the RADIUS Server

1. Prerequisites

Before configuration, ensure that the RADIUS server is ready, and that the IP address and shared key of the RADIUS server are configured.

2. Configuration Steps

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **802.1x Authentication** > **RADIUS Server Management.**

(1) Click the **RADIUS Server Management** tab.

(2) Click **Add Server Group** to configure related server parameters.

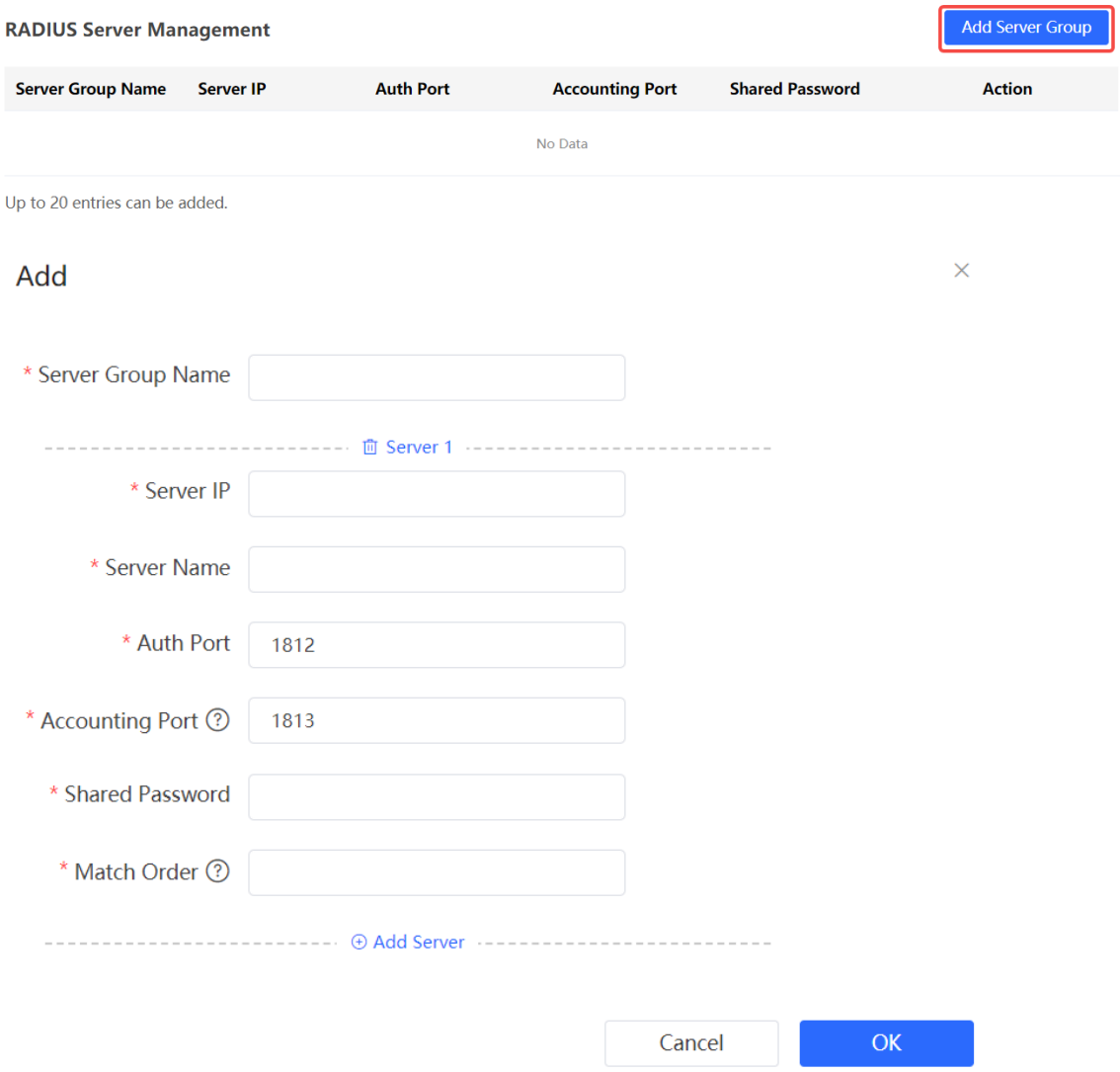


Table 12-13 Description of RADIUS Server Management Configuration

Parameter	Description
Server IP	IP address of the RADIUS server.
Auth Port	The port number for the RADIUS server to perform user authentication.
Accounting Port	The port number for the RADIUS server to perform user accounting.
Shared Password	Shared key of the RADIUS server.

Parameter	Description
Match Order	The system supports up to five RADIUS servers. A larger value indicates a higher priority.

(3) Enter the server global configuration parameters, and click **Save**.

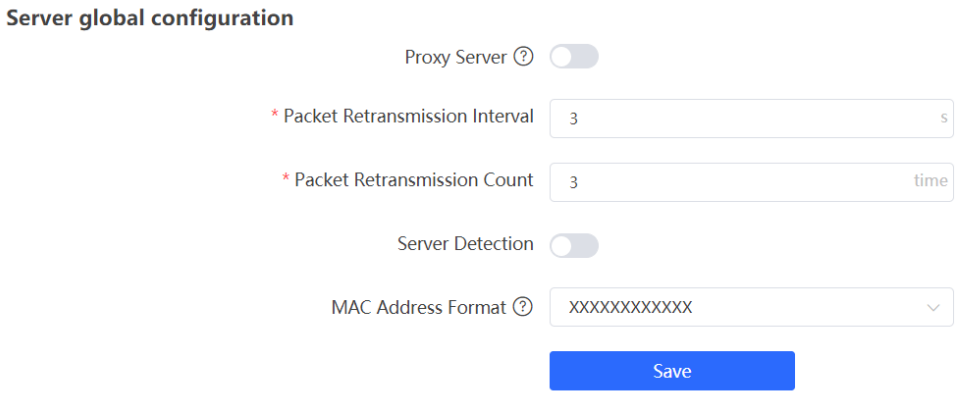


Table 12-14 Description of Server Global Configuration

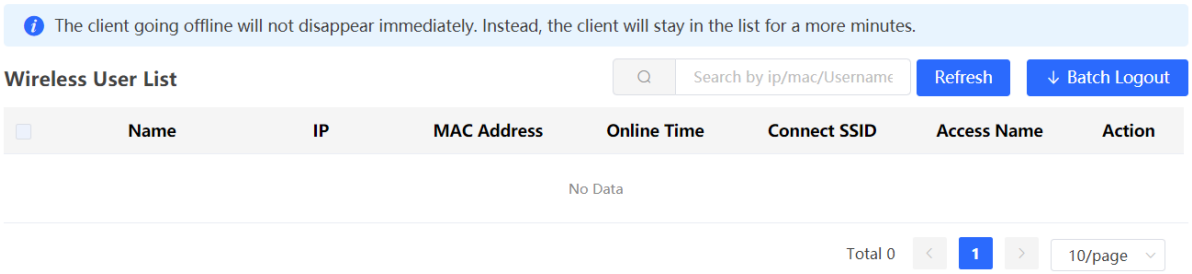
Parameter	Description
Proxy Server	After this function is enabled, local device will act as a proxy for the RADIUS server to send RADIUS messages.
Packet Retransmission Interval	Configure the interval during which the device sends a request to a RADIUS server before confirming that the RADIUS server is unreachable.
Packet Retransmission Count	Configure the number of times that the device sends requests to a RADIUS server before confirming that the RADIUS server is unreachable.
Server Detection	If this function is enabled, it is necessary to set the server detection cycle, server detection times, and server detection username. Determines the server status and whether to enable functions such as the escape function.
MAC Address Format	Configure the format of the MAC address used in attribute 31 (**Calling-Station-ID**) of a RADIUS message. The following formats are supported: ● Dotted hexadecimal format. For example, 00d0.f8aa.bbcc. ● IETF format. For example: 00-D0-F8-AA-BB-CC. ● Unformatted (default). For example: 00d0f8aabbcc

12.5.4 Checking Authentication User List

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

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **802.1x Authentication** > **Wireless User List/ Wired User List.**

Click **Wireless User List** or **Wired User List** to view specific user information.



Click **Refresh** to view the latest user list.

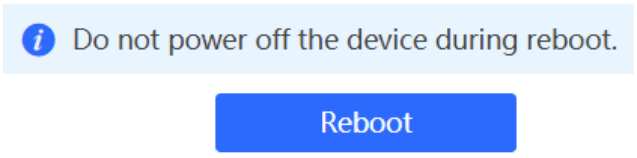
If you want to disconnect a user from the network, select the user and click **Logout** under the **Action** column. You can also select multiple users and click **Batch Logout** to disconnect selected users.

12.6 Configuring Reboot

12.6.1 Rebooting the Current Device

Choose **One-Device** > **Gateway** > **Config** > **System** > **Reboot** > **Reboot**.

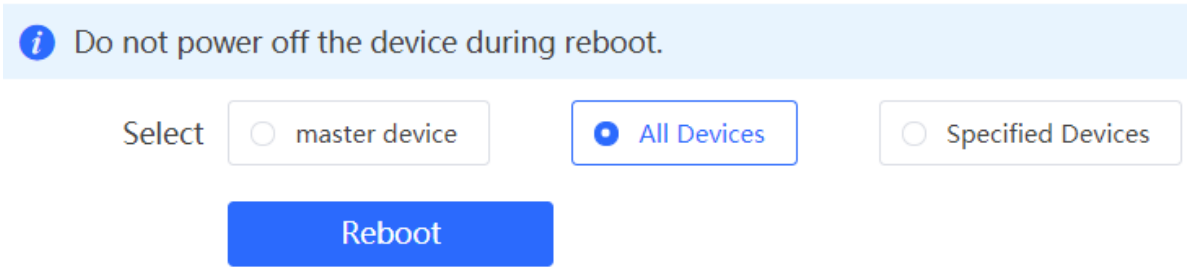
Click **Reboot**, and the device will be restarted. Please do not refresh or close the page during the reboot process. After the device is rebooted, the browser will be redirected to the login page.



12.6.2 Rebooting All Devices in the Network

Choose **Network-wide** > **System** > **Reboot** > **Reboot**.

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



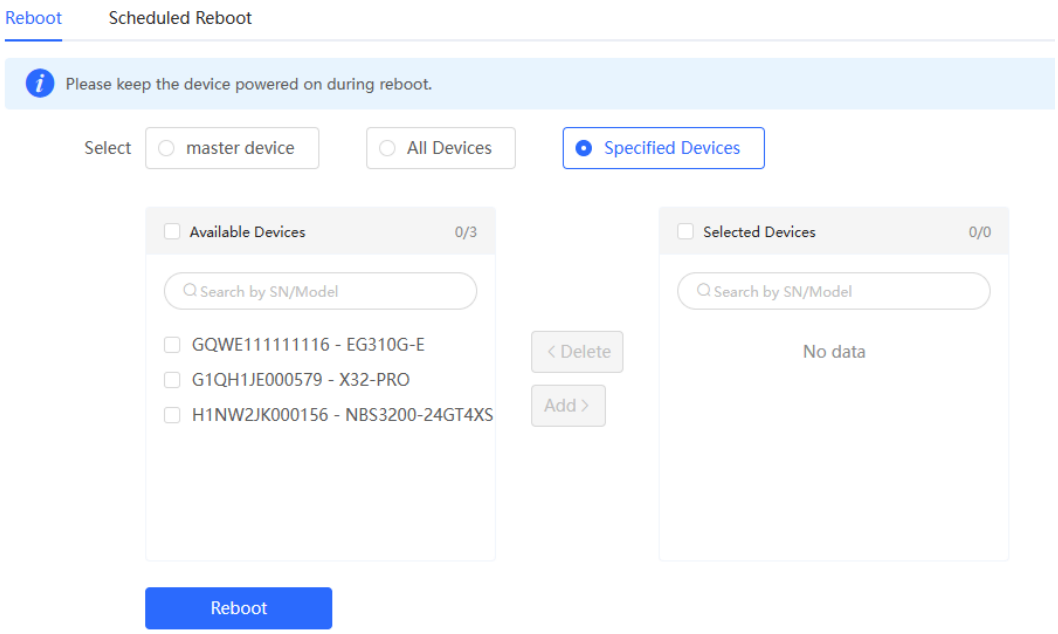
Caution

The operation takes some time and affects the whole network. Therefore, exercise caution when performing this operation.

12.6.3 Rebooting the Specified Device

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

Click **Specified Devices**, select required 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.



12.7 Configuring Scheduled Reboot

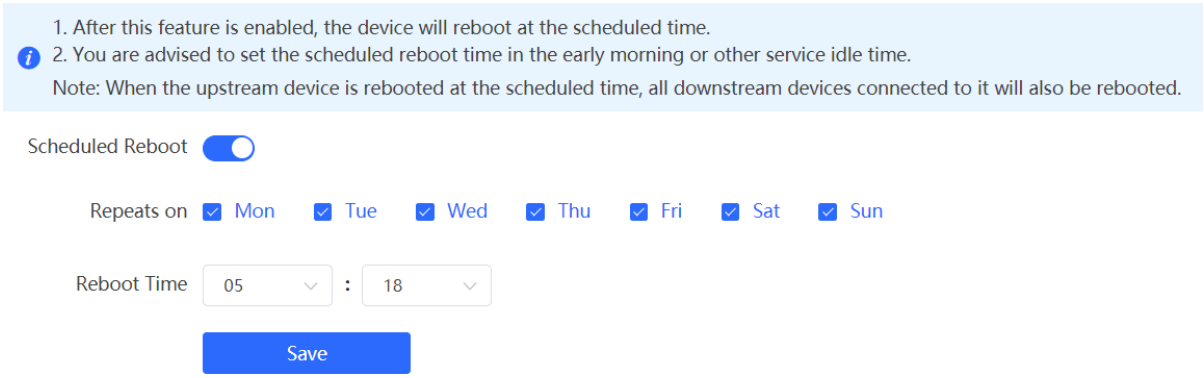
Confirm that the system time is accurate to avoid network interruption caused by device reboot at wrong time. For details about how to configure the system time, see Section 12.8 Setting and Displaying System Time.

Choose **Network-Wide** > **Workspace** > **Network-Wide** > **Reboot** > **Scheduled Reboot**.

Turn on **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. You are advised to set scheduled reboot time to off-peak hours.

Caution

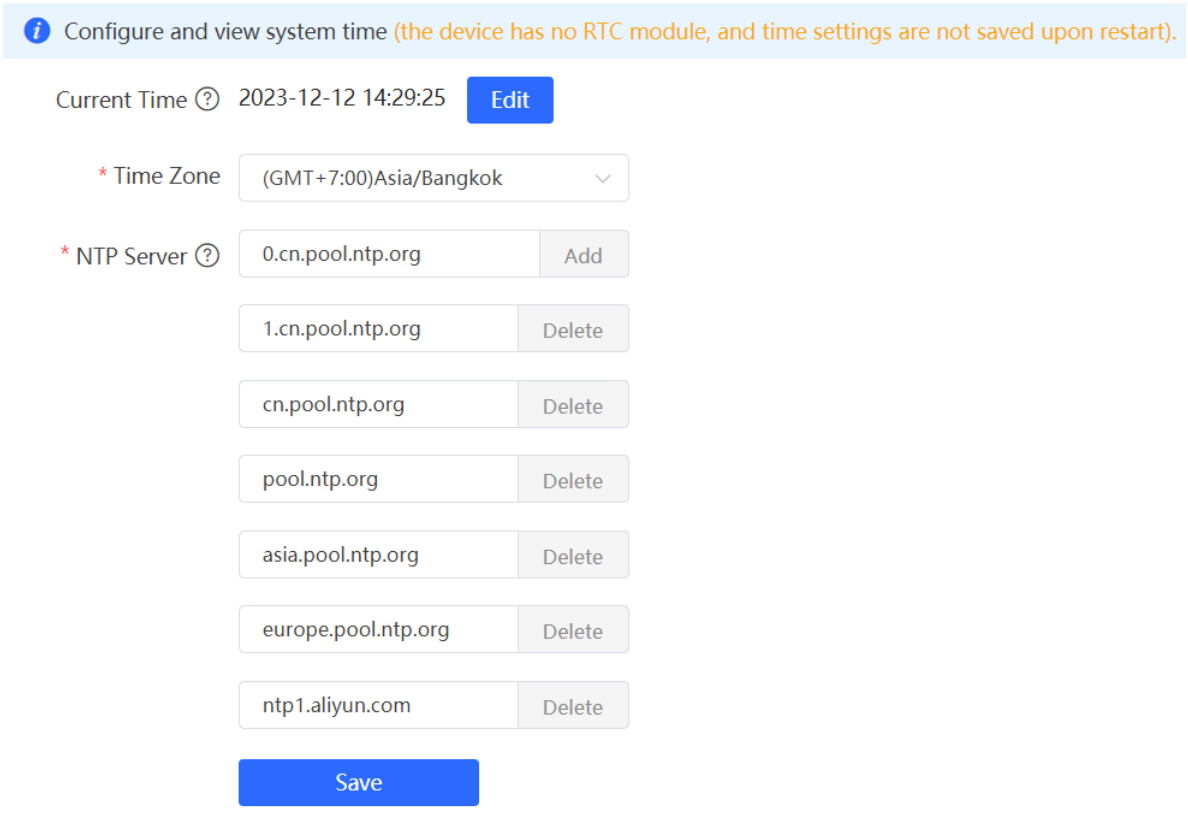
The operation affects the whole network. Therefore, exercise caution when performing this operation.



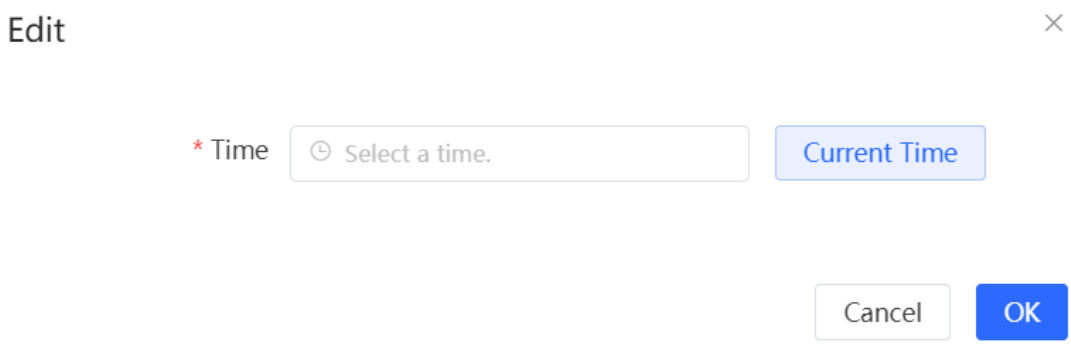
12.8 Setting and Displaying System Time

Choose **Network-Wide** > **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**, and the current system time will be filled in automatically.

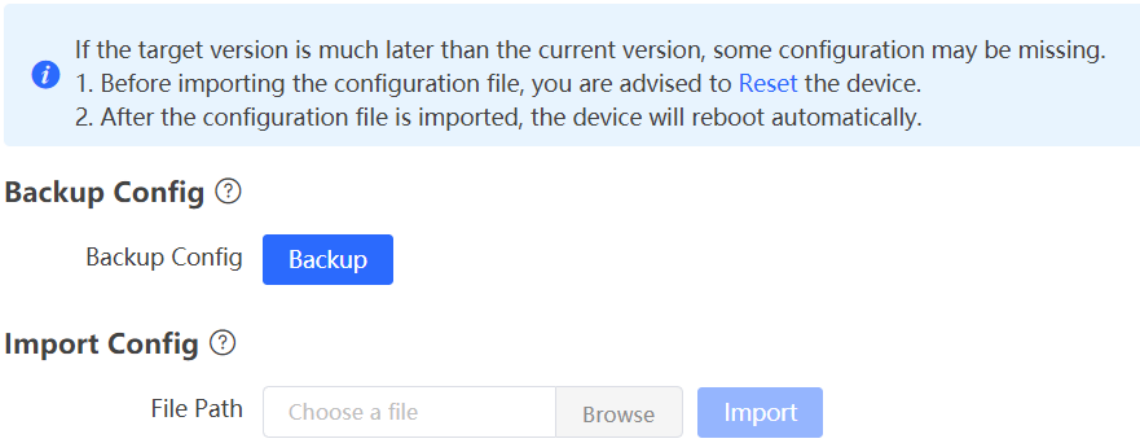


12.9 Configuring Backup and Import

Choose **Network-Wide** > **System** > **Backup & Import**.

Configuration backup: Click **Backup** to download a configuration file locally.

Configuration import: Click **Browse**, select a backup file on the local PC, and click **Import** to import the configuration file. The device will restart.

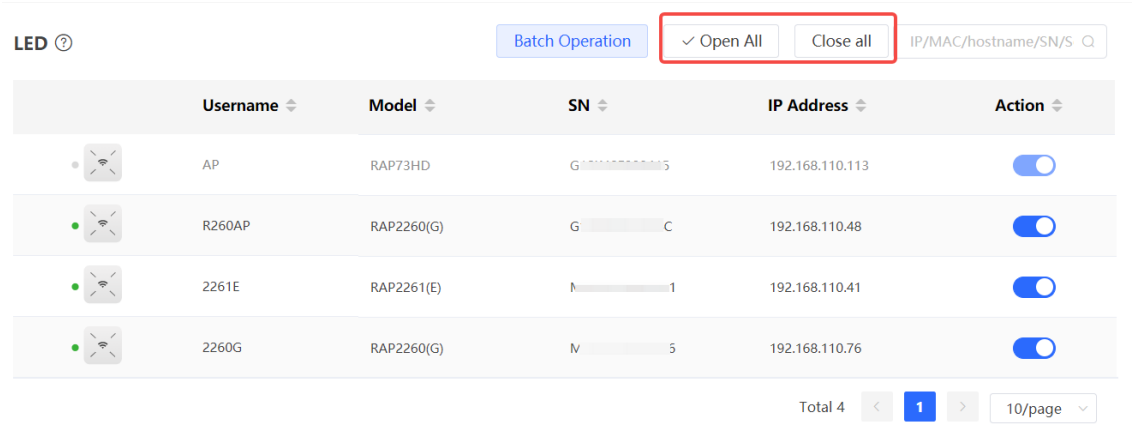


12.10 Configuring LEDs

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

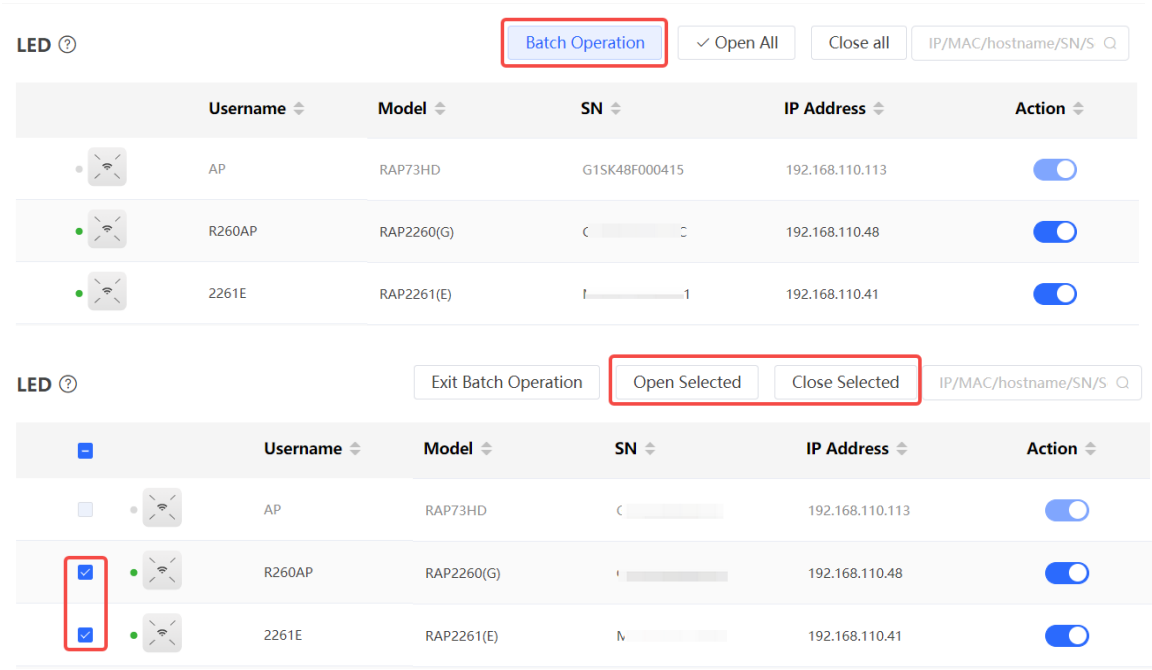
- Configuring the LED status of network-wide APs

  Click **Open All** or **Close All** to enable or disable the LEDs of all APs on the network.



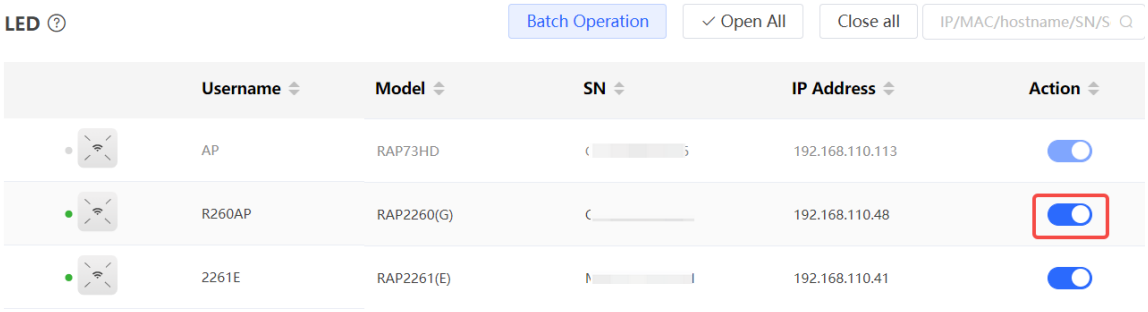
- Configuring the LED status of selected APs

  Click **Batch Operation**, select the desired APs, and click **Open Selected** or **Close Selected** to enable or disable the LED status of the selected APs.



- Configuring the LED status of a single AP

  Toggle on or off the switch in the **Action** column to enable or disable the LED status of the corresponding AP.



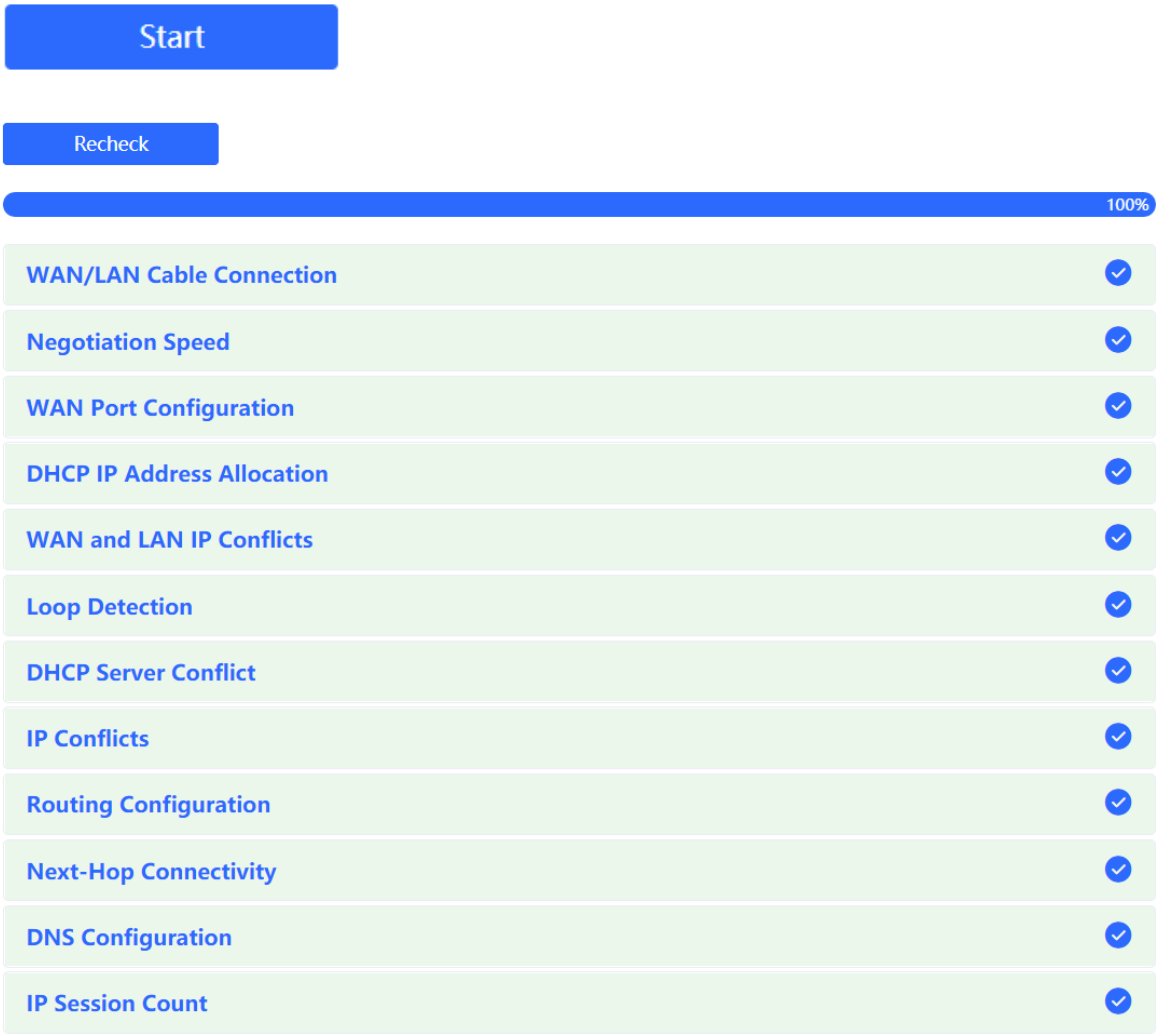
12.11 Configuring Diagnostics

12.11.1 Network Check

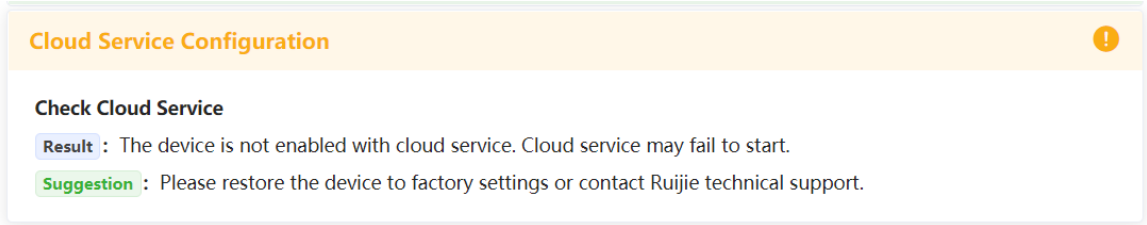
When a network error occurs, perform **Network Check** to identify the fault and take the suggested action.

Choose **One-Device** > **Gateway** > **Config** > **Diagnostics** > **Network Check**.

Click **Start** to perform the network check and show the result.



If a network error occurs, its symptom and suggested action will be displayed.



12.11.2 Alerts

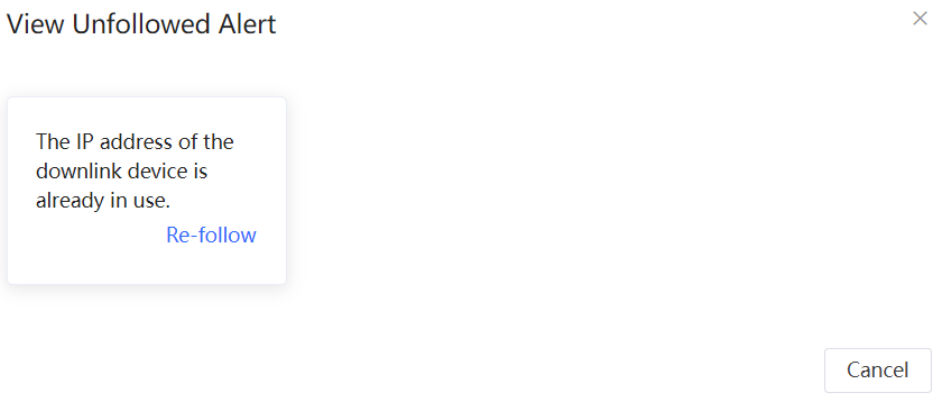
Click **Alert Center** in the navigation bar.

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

Caution

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

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



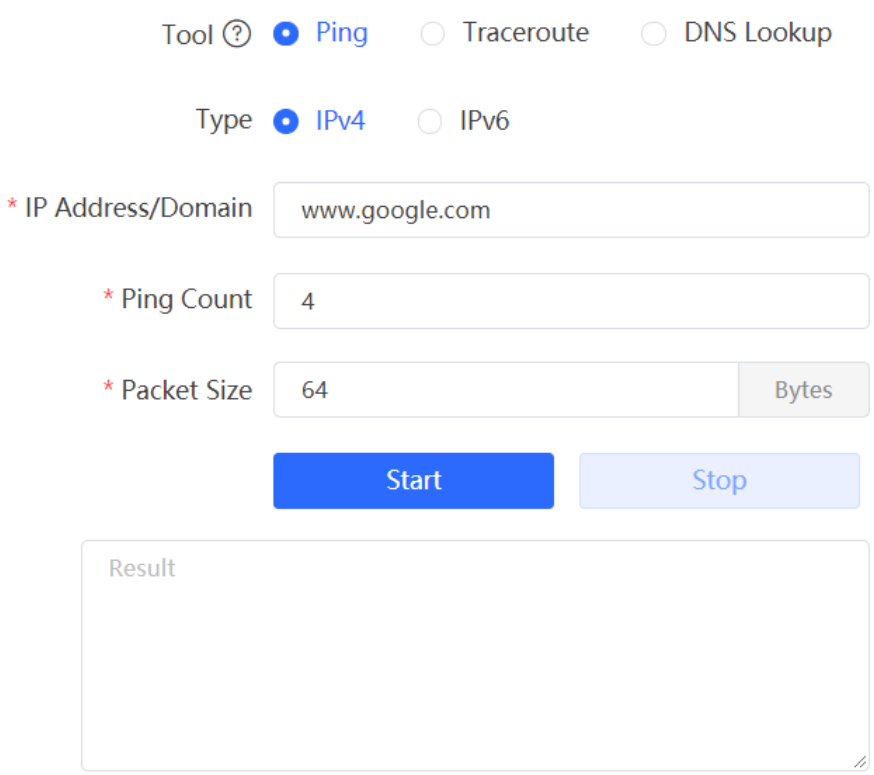
12.11.3 Network Tools

1. Ping

Choose **One-Device** > **Gateway** > **Config** > **Diagnostics** > **Network Tools**.

The **Ping** command is used to detect the network connectivity.

Select **Ping** as the diagnosis mode, select the IP type, 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.

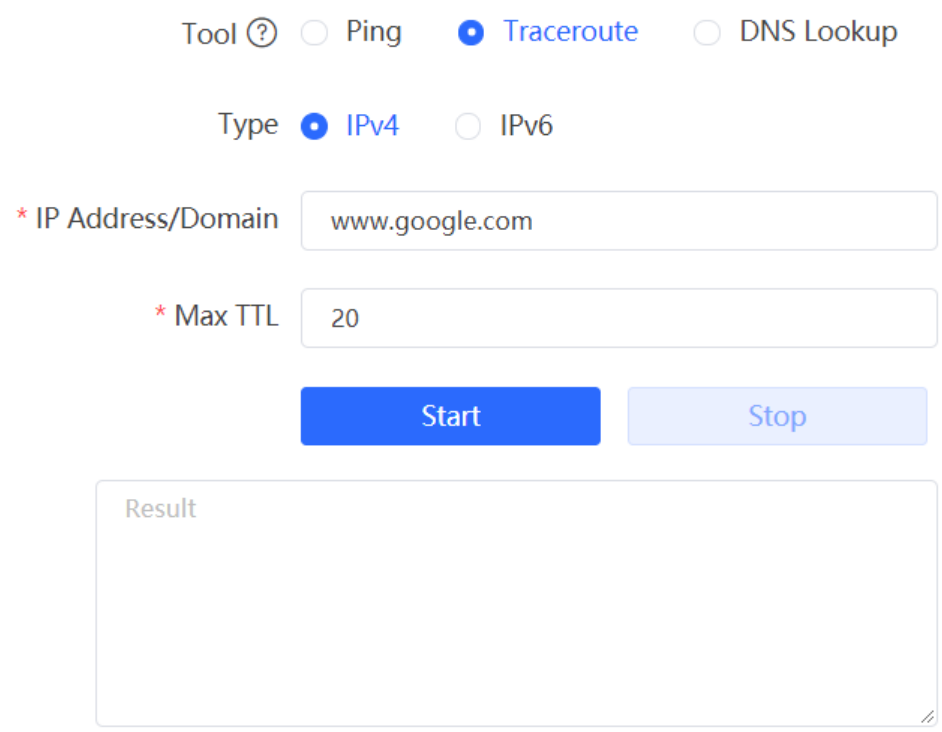


2. Traceroute

Choose **One-Device** > **Gateway** > **Config** > **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, select the IP type, and enter a destination IP address or the maximum TTL value used by the URL and traceroute, and click **Start**.

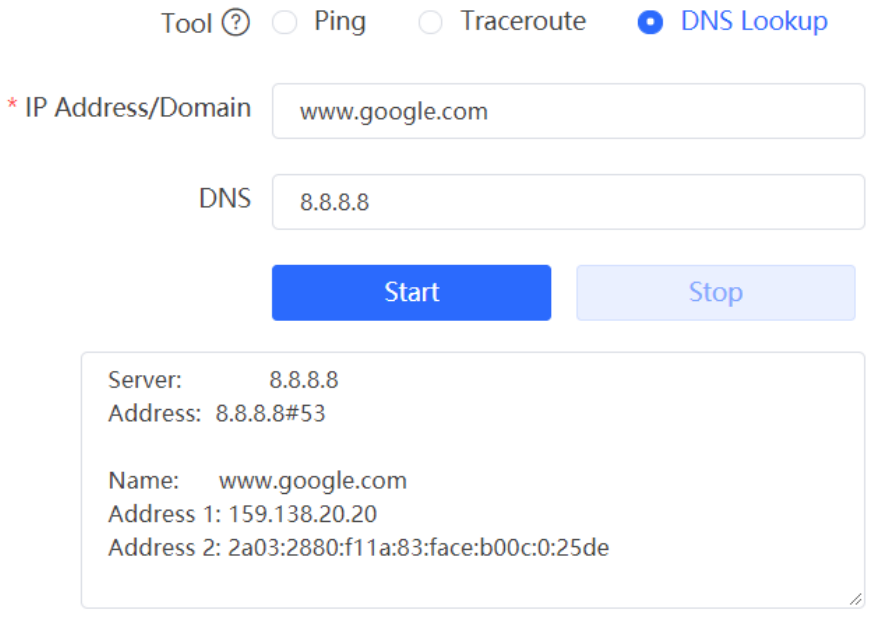


3. DNS Lookup

Choose **One-Device** > **Gateway** > **Config** > **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**.



12.11.4 Packet Capture

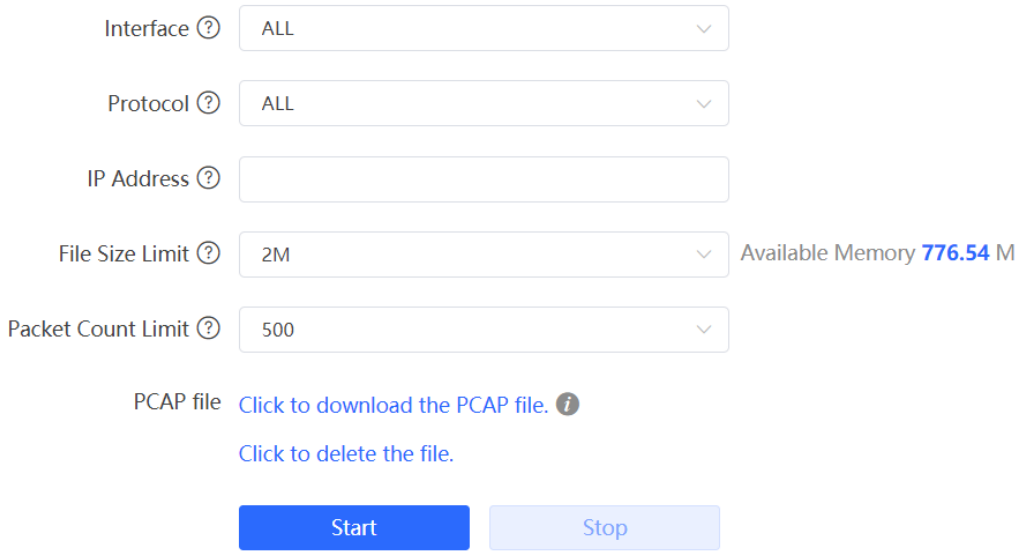
Choose **One-Device** > **Gateway** > **Config** > **Diagnostics** > **Packet Capture**.

If the device fails and troubleshooting is required, the packet capture result can be analyzed to locate and rectify the fault.

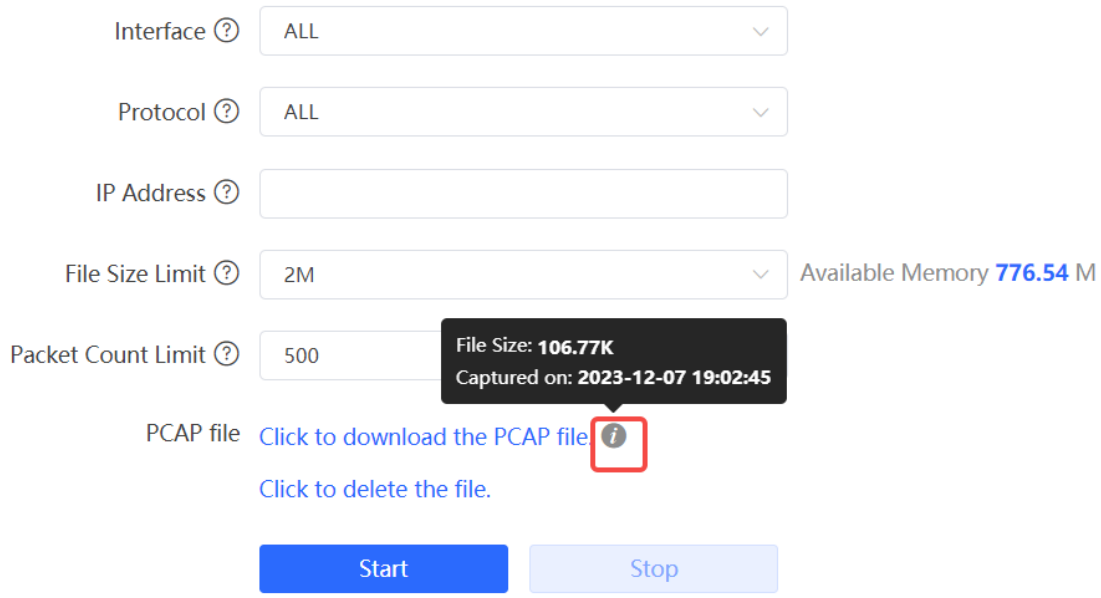
Select an interface and a protocol and specify the host IP address to capture the content in data packets. Select the file size limit and packet count limit to determine the conditions for automatically stopping packet capture. (If the file size or number of packets reaches the specified threshold, packet capture stops and a diagnostic package download link is generated.) Click **Start** to execute the packet capture command.

Caution

The packet capture operation may occupy many system resources, causing network freezing. Therefore, exercise caution when performing this operation.



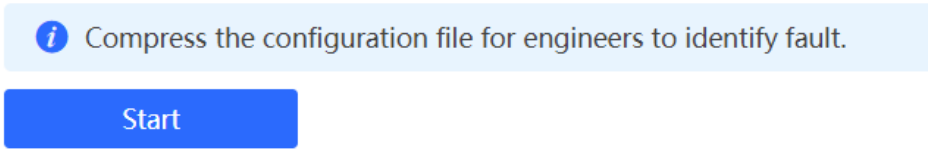
Packet capture can be stopped at any time. After that, a download link is generated. Click this link to save the packet capture result in the PCAP format locally. Use analysis software such as Wireshark to view and analyze the result.



12.11.5 Fault Collection

Choose **One-Device** > **Gateway** > **Config** > **Diagnostics** > **Fault Collection**.

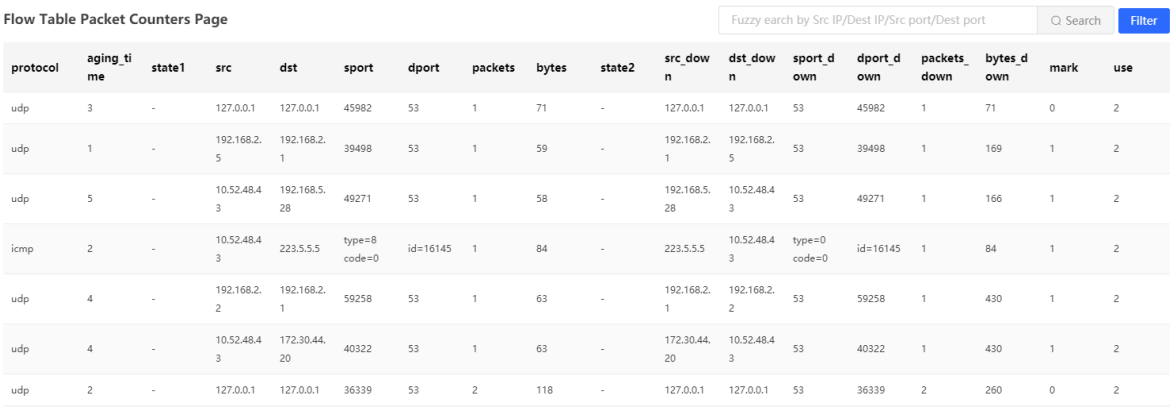
When the device fails, you need to collect the fault information. Click **Start**. The configuration files of the device will be packed into a compressed file. Download the compressed file locally and provide it to R&D personnel for fault locating.



12.11.6 Viewing Flow Statistics

Choose **One-Device** > **Gateway** > **Config** > **Diagnostics** > **Flow Statistic**.

On the **Flow Table Packet Counters Page**, you can view the details of packets received by the device, including protocol, aging time, state, source IP address, destination IP address, source port, destination port, and so on.



protocol	aging_time	state1	src	dst	sport	dport	packets	bytes	state2	src_down	dst_down	sport_down	dport_down	packets_down	bytes_down	mark	use
udp	3	-	127.0.0.1	127.0.0.1	45982	53	1	71	-	127.0.0.1	127.0.0.1	53	45982	1	71	0	2
udp	1	-	192.168.2.5	192.168.2.1	39498	53	1	59	-	192.168.2.1	192.168.2.5	53	39498	1	169	1	2
udp	5	-	10.52.48.43	192.168.5.28	49271	53	1	58	-	192.168.5.28	10.52.48.43	53	49271	1	166	1	2
icmp	2	-	10.52.48.43	223.5.5.5	type=8 code=0	id=16145	1	84	-	223.5.5.5	10.52.48.43	type=0 code=0	id=16145	1	84	1	2
udp	4	-	192.168.2.2	192.168.2.1	59258	53	1	63	-	192.168.2.1	192.168.2.2	53	59258	1	430	1	2
udp	4	-	10.52.48.43	172.30.44.20	40322	53	1	63	-	172.30.44.20	10.52.48.43	53	40322	1	430	1	2
udp	2	-	127.0.0.1	127.0.0.1	36339	53	2	118	-	127.0.0.1	127.0.0.1	53	36339	2	260	0	2

Note

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

12.12 Performing Upgrade and Checking System Version

Caution

You are advised to back up the configuration before upgrading the router.

Version upgrade will restart the device. Do not refresh or close the browser during the upgrade process.

12.12.1 Online Upgrade

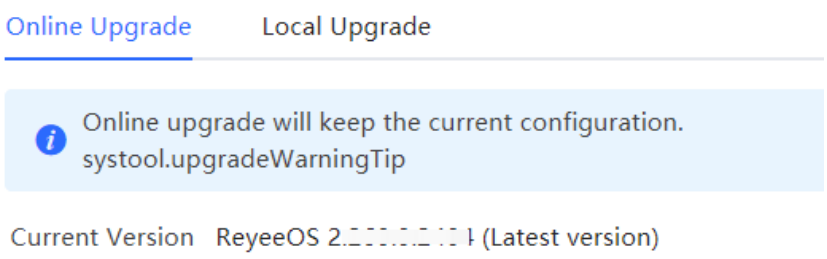
Choose **One-Device** > **Gateway** > **Config** > **System** > **Upgrade** > **Online Upgrade**.

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.

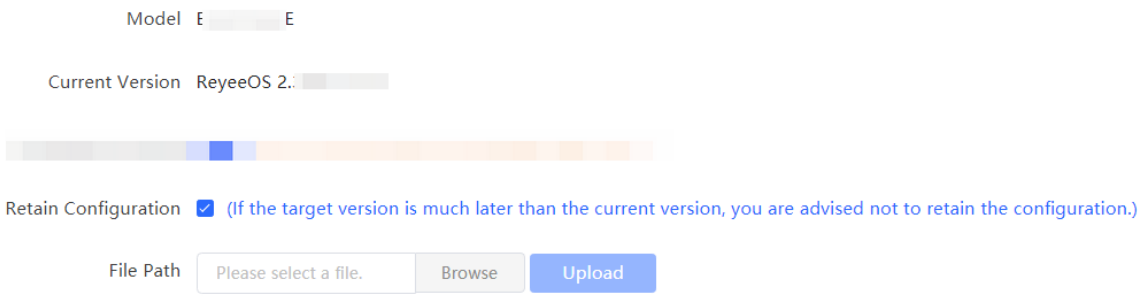
Do not refresh the page or close the browser during the upgrade process. After successful upgrade, you will be redirected to the login page automatically.



12.12.2 Local Upgrade

Choose **One-Device** > **Gateway** > **Config** > **System** > **Upgrade** > **Local Upgrade**.

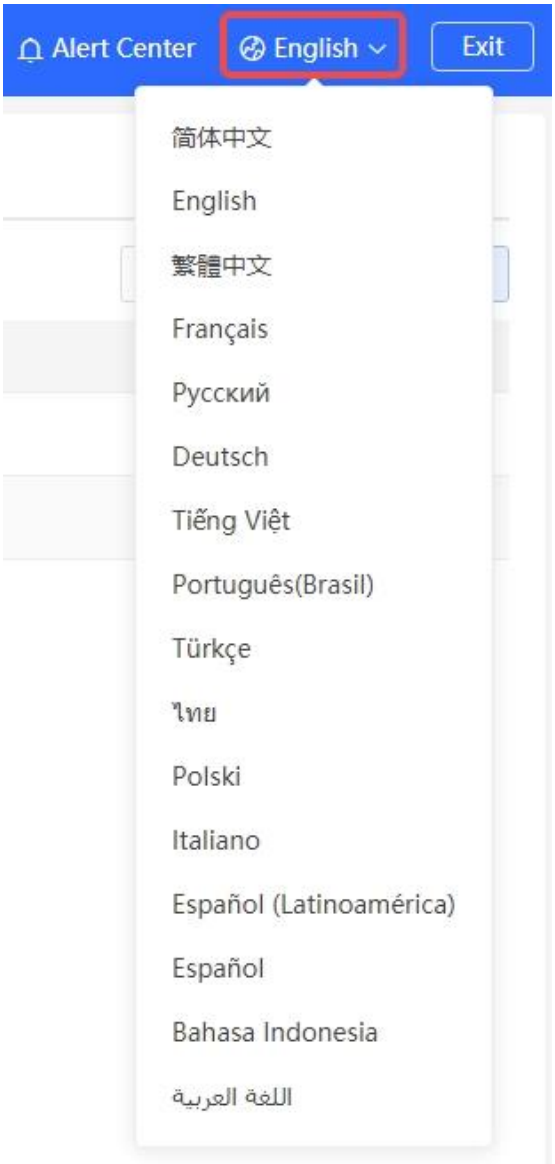
You can view the current software version and device model. If you want to upgrade the device with the configuration retained, select **Keep Config**. Click **Browse**, select an upgrade package on the local PC, and click **Upload** to upload the file. The device will be upgraded.



12.13 Switching System Language

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

Click a required language to switch the system language.



12.14 Configuring Cloud Service

12.14.1 Overview

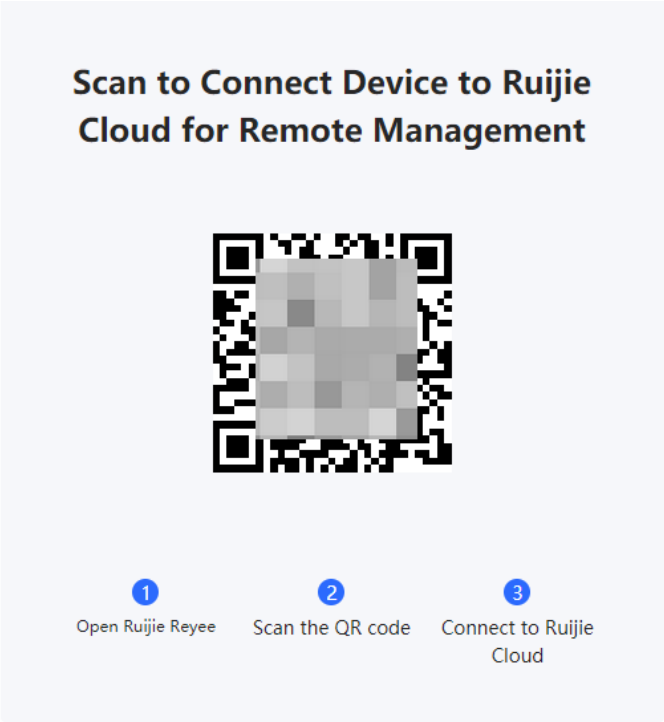
The Cloud Service feature provides powerful remote network management and operation capabilities, making it convenient and efficient to manage geographically dispersed networks with diverse device types. This feature supports wireless devices, switches, and gateways, enabling unified network management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

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

12.14.2 Configuration Steps

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

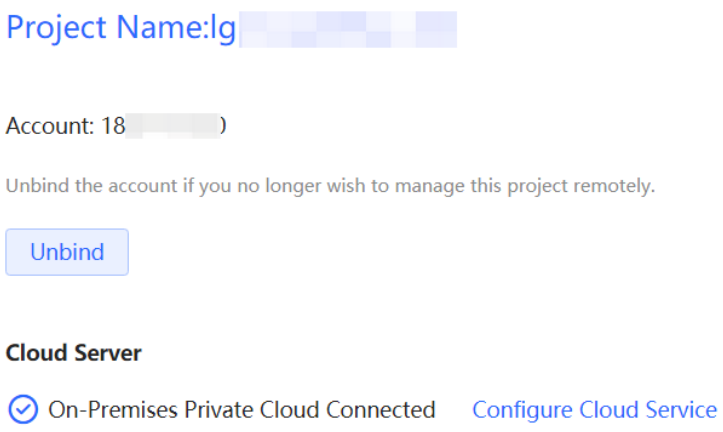
If the device is not currently associated with a cloud account, simply follow the on-screen instructions to add it to the network. Open up the Ruijie Reyee app, click the scan icon at the upper left corner on the **Project** page, and enter the device's management password.



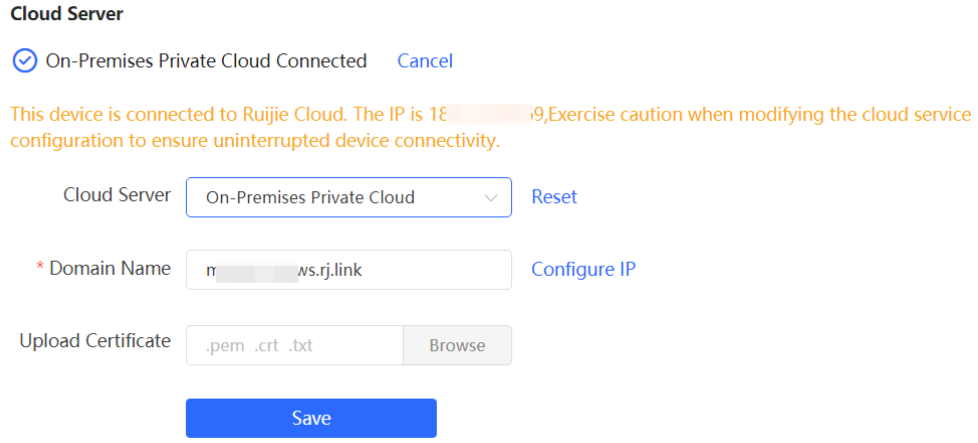
Once the device is associated with a cloud account, it will automatically be bound to a cloud server based on its geographic location.

Caution

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



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



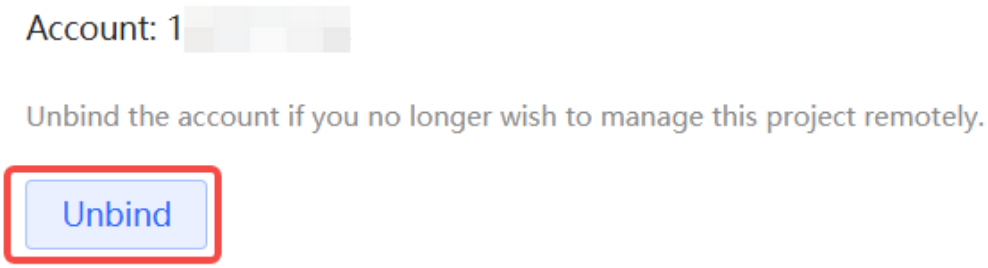
Note

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

12.14.3 Unbinding Cloud Service

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

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



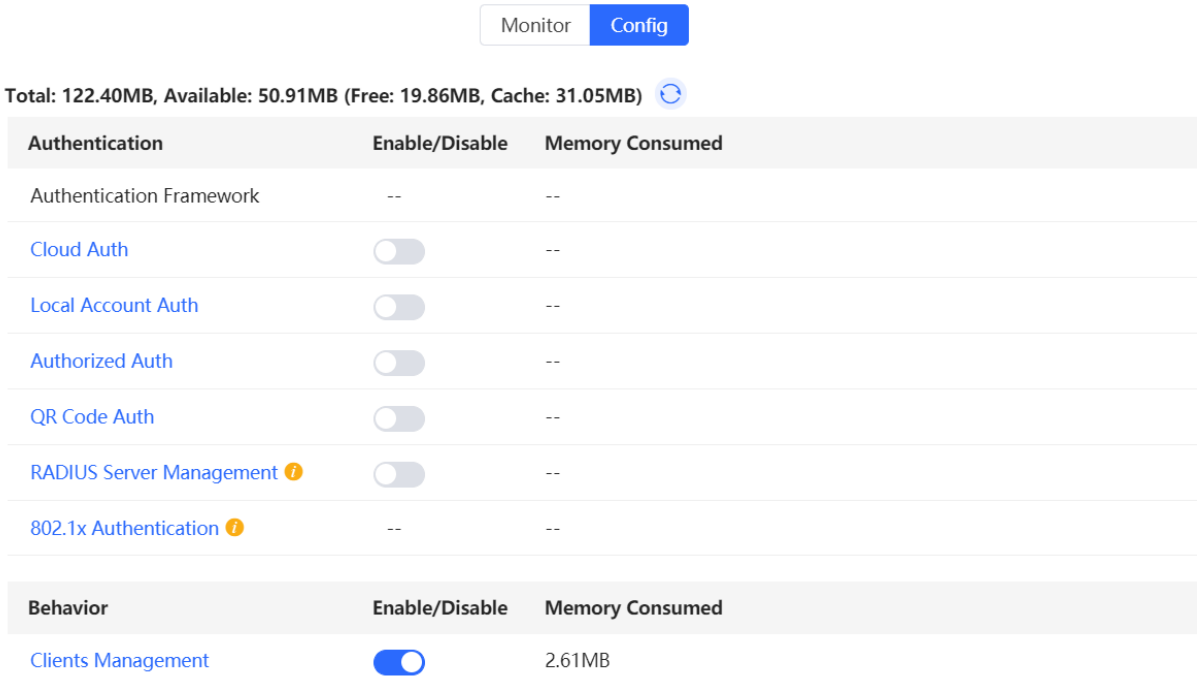
12.15 Feature Configuration

Note

Only RG-EG105G-V3, RG-EG105G-P-V3, RG-EG210G-P-V3 and RG-EG209GS support this function.

Choose **One-Device** > **Gateway** > **Config** > **System** > **Feature Configuration**.

On the page, you can view the current configuration status of some device functions and the amount of memory space they occupy. This allows users to make informed decisions about which functions to enable or disable based on their device's memory consumption. This can help prevent device lagging and ensure a smoother internet browsing experience.



13 FAQs

13.1 Login Failure

- What can I do if I fail to log in to the Web management system?

(1) Confirm that the network cable is correctly connected to the LAN port of the device, and the corresponding indicator is flashing or solid on.

(2) Before you access the Web management system page, you are advised to configure the PC to automatically obtain an IP address, so the DHCP-enabled device automatically allocates an IP address to the PC. If you want to specify a static IP address to the PC, ensure that the IP address of the PC and the IP address of the device's LAN port are in the same network segment. For example, if the LAN port IP address is 192.168.110.1 and subnet mask is 255.255.255.0, set the PC IP address to 192.168.110.X (X representing any integer in the range of 2 to 254) and the subnet mask to 255.255.255.0.

(3) Run the ping command to test the connectivity between the PC and device. If ping fails, check the network settings.

(4) If you still cannot log in to the **Device Management** page after the preceding steps, restore the device to factory settings.

13.2 Password Loss/Factory Setting Restoration

- What can I do if I forget the login password? How can I restore the device to factory settings?

When the device is powered, press and hold the **Reset** button on the panel for 5 seconds. The device will restore factory settings after restart. Then, you can log in to the Web page of the device using the default IP address 192.168.110.1.

13.3 Internet Access Failure

- What can I do if the Internet access through PPPoE Dial-Up fails?

(1) Check whether the PPPoE account and password are correct. Please see Section 2.5.3 Forgetting the PPPoE Account for details.

(2) Check whether the IP address allocated by the ISP conflicts with the IP address existing on the router.

(3) Check whether the MTU setting of the device meets the requirements of the ISP.

The default MTU is 1500. Please see Section 4.3.3 Modifying the MTU for details.

(4) Check whether VLAN tagging should be configured for PPPoE.

VLAN tagging is disabled by default. Please see Section 4.3.5 Configuring the VLAN Tag for details.