Ruijie Reyee RG-EG-W Series Routers

ReyeeOS 1.206

Web-based Configuration Guide

Document Version: V1.0

Date: November 11, 2022

Copyright

Disclaimer

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

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

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

Preface

Intended Audience

This document is intended for:

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

Technical Support

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

Conventions

1. GUI Symbols

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

2. Signs

The signs used in this document are described as follows:

Warning

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

Caution

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

Note

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

✓ **Specification**

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

3. Note

This manual introduces the product model, port type and CLI for your reference. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

1 Login

1.1 Configuration Environment Requirements

1.1.1 PC

- 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.

1.2 Default Configuration

Table 1-1 Default Web Configuration

Item	Default
IP address	192.168.110.1
Username/Password	Username and password are not required at your first login and you can configure the router directly.

1.3 Login to Eweb

1.3.1 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 Configuring the IP Address of the Management Client.

- Wireless Connection

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 Configuring the IP Address of the Management Client.

1.3.2 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.

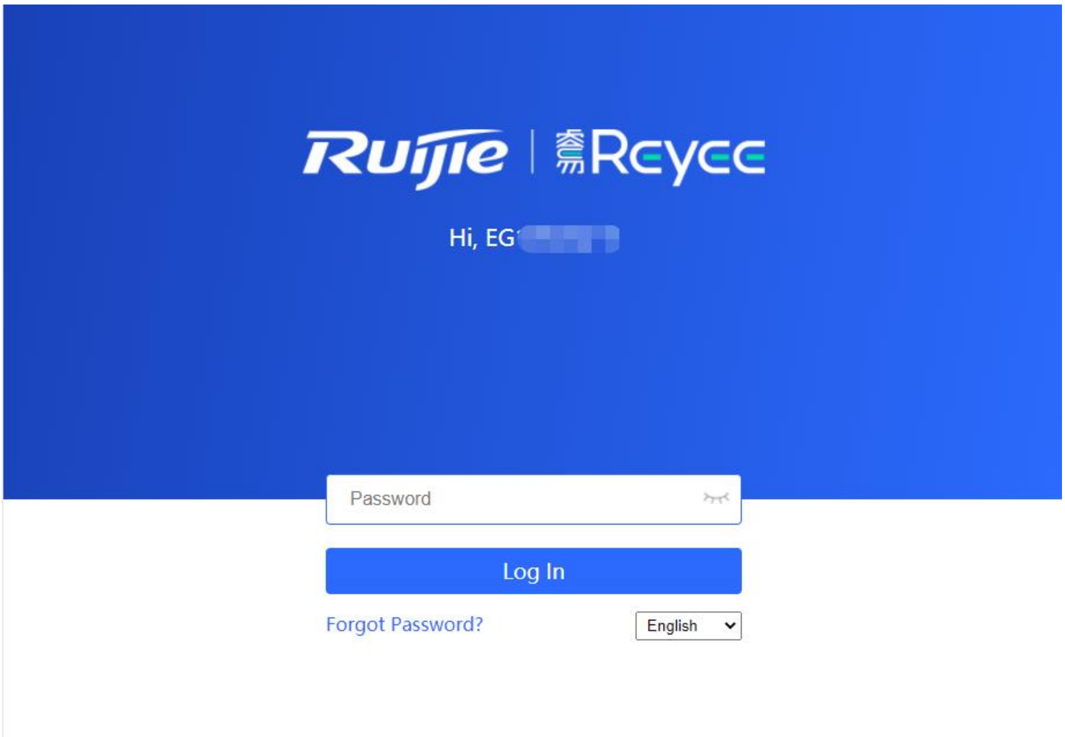
1.3.3 Login

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.



Username and password are not required at your first login and you can configure the router directly.

For device security, you are advised to set the management password after your first login to the web management system. After the password is set, you need to enter the password when you log in to the web management system again.

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.

1.4 Work Mode

The device can work in router mode, AP mode, or wireless repeater mode. The system menu pages and configuration function scope vary depending on the work mode. By default, the EG-W router works in router mode. To modify the work mode, see **错误!未找到引用源。**.

1.4.1 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.

1.4.2 AP Mode

After the AP mode is enabled, the device serves as a fit AP and supports Layer 2 forwarding only. In AP mode, the device does not provide the routing and Dynamic Host Configuration Protocol (DHCP) server functions. By default, the device obtains IP addresses through DHCP and uniformly allocates and manages IP addresses to downlink devices connected to it through the DHCP address pool. In this mode, the AP only transmits data transparently.

Generally, the EG-W router cooperates with devices providing the routing function. On a normally working network, the EG-W router router connects to an uplink router through a network cable to convert wired signals into wireless signals, extending the wireless network coverage range.

1.4.3 Wireless Repeater

Similar to the AP mode, the device does not provide the routing and DHCP server functions in wireless repeater mode. The addresses of end users are allocated and managed by the primary router. This mode is applicable to a normally working network, where the device connects to the primary router in wireless mode to expand the Wi-Fi coverage range and increase the number of network cable ports and wireless access devices.

1.5 Configuration Wizard (Router Mode)

1.5.1 Getting Started

(1) Power on the device. Connect the WAN port 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.

1.5.2 Configuration Steps

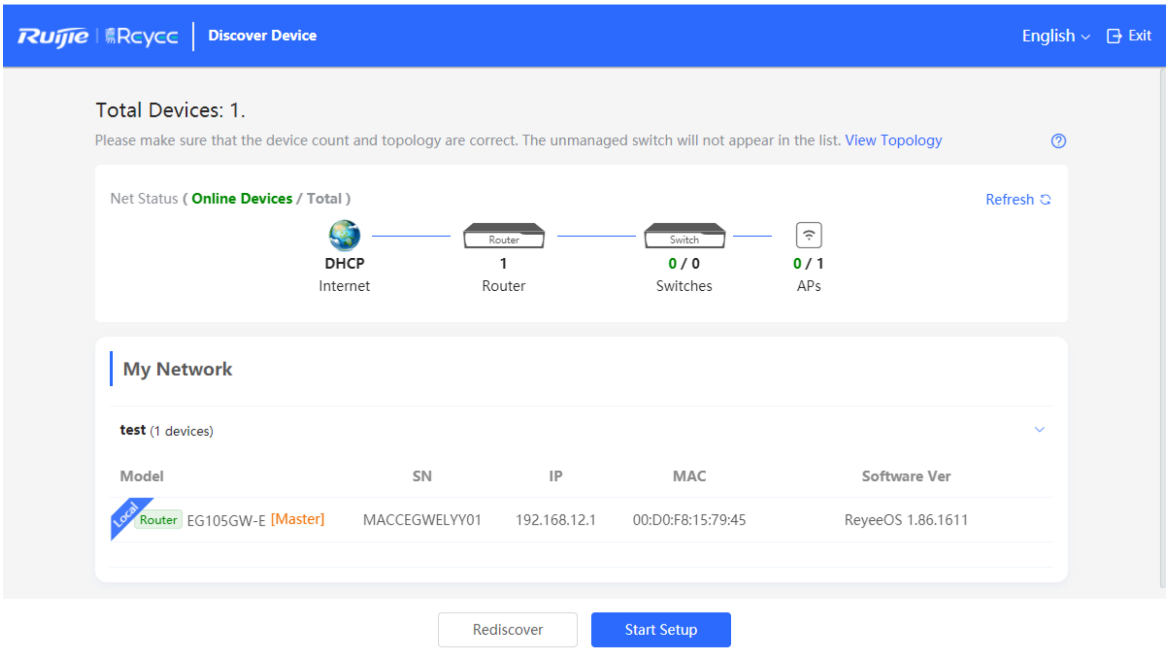
1. Adding a Device to Network

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.



Total Devices: 1.

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

Net Status (Online Devices / Total)

My Network

test (1 devices)

Model	SN	IP	MAC	Software Ver
Local Router EG105GW-E [Master]	MACCEGWELYY01	192.168.12.1	00:D0:F8:15:79:45	ReyeeOS 1.86.1611

2. Creating a Network Project

Click **Start Setup** to configure the Internet connection type, Wi-Fi network and management password.

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

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

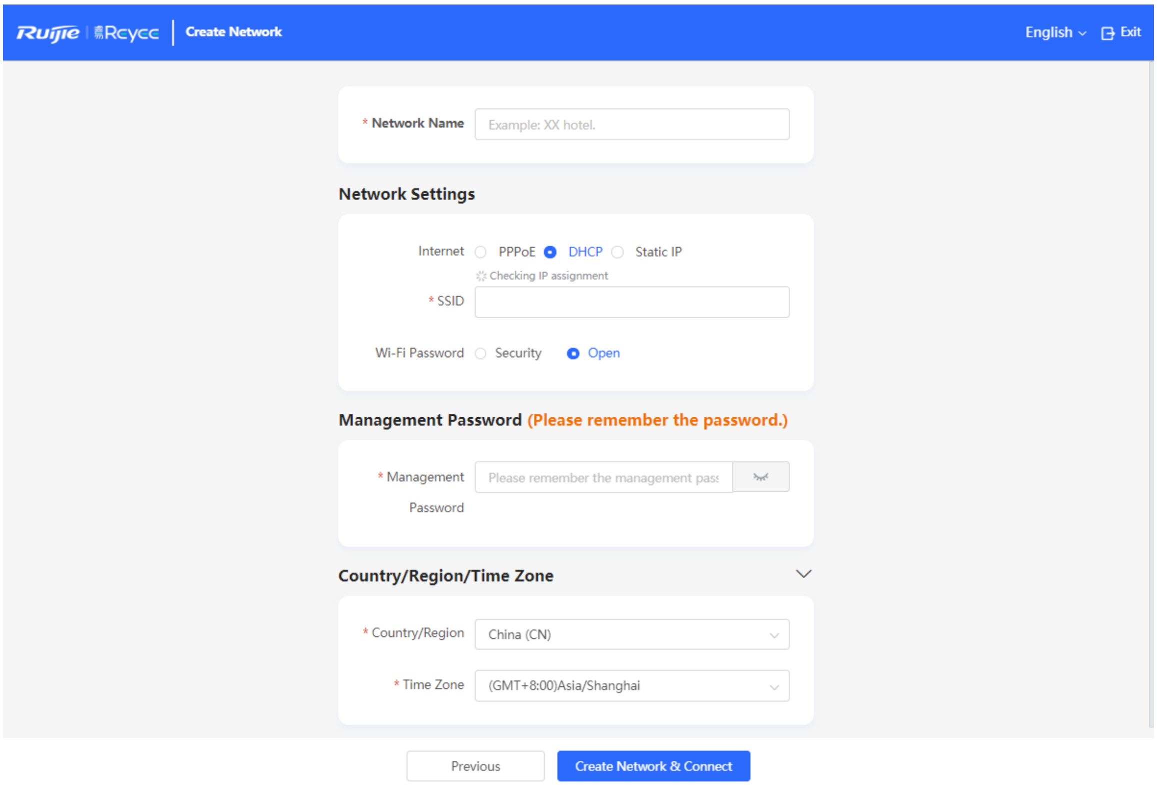
- **DHCP**: The router detects whether it can obtain an IP address via DHCP by default. If the router connects to the Internet successfully, you can click **Next** without entering an account.
- **PPPoE**: Click **PPPoE**, and enter the username, password, and service name. Click **Next**.
- **Static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

(3) **SSID and Wi-Fi Password**: The device has no Wi-Fi password by default, indicating that the Wi-Fi network is an open network. You are advised to configure a complex password to enhance the network security.

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

(5) **Country/Region**: The Wi-Fi channel may vary from country to country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.

(6) **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.



* Network Name: Example: XX hotel.

Network Settings

Internet ○ PPPoE ● DHCP ○ Static IP

Checking IP assignment

* SSID

Wi-Fi Password ○ Security ● Open

Management Password (Please remember the password.)

* Management Password: Please remember the management pass

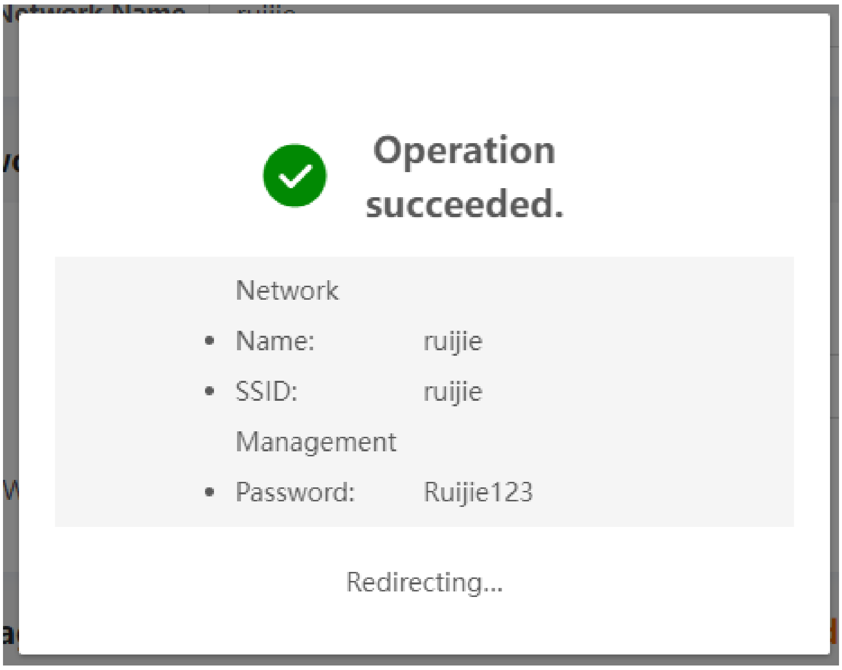
Country/Region/Time Zone

* Country/Region: China (CN)

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

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.



Operation succeeded.

Network Name: ruijie

SSID: ruijie

Management Password: Ruijie123

Redirecting...

Note

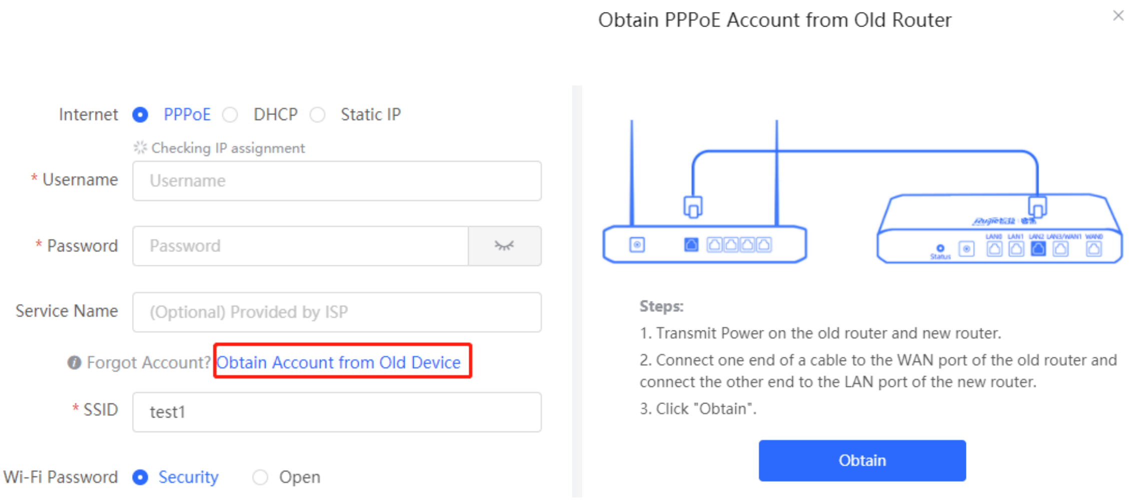
If your device is not connected to the Internet, click Exit to exit the configuration wizard.

Please log in again with the new password if you change the management password.

1.5.3 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 port 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.



Obtain PPPoE Account from Old Router ×

Internet ● PPPoE ○ DHCP ○ Static IP

Checking IP assignment

* Username: Username

* Password: Password

Service Name: (Optional) Provided by ISP

Forgot Account? Obtain Account from Old Device

* SSID: test1

Wi-Fi Password ● Security ○ Open

Steps:

1. Transmit Power on the old router and new router.
2. Connect one end of a cable to the WAN port of the old router and connect the other end to the LAN port of the new router.
3. Click "Obtain".

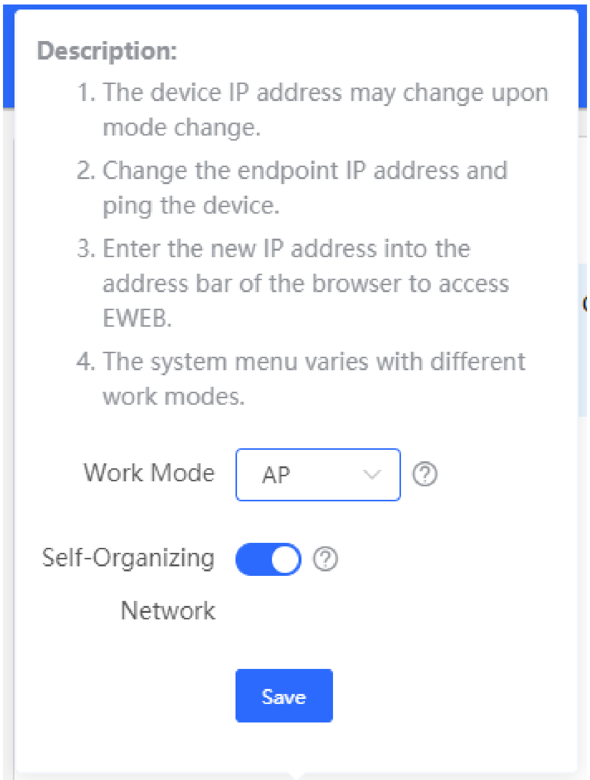
1.6 Configuration Wizard (AP Mode)

1.6.1 Getting Started

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

1.6.2 Configuration Steps

(1) On the work mode setting page, change the work mode from router mode to AP mode. For details, see Section **错误!未找到引用源。**.



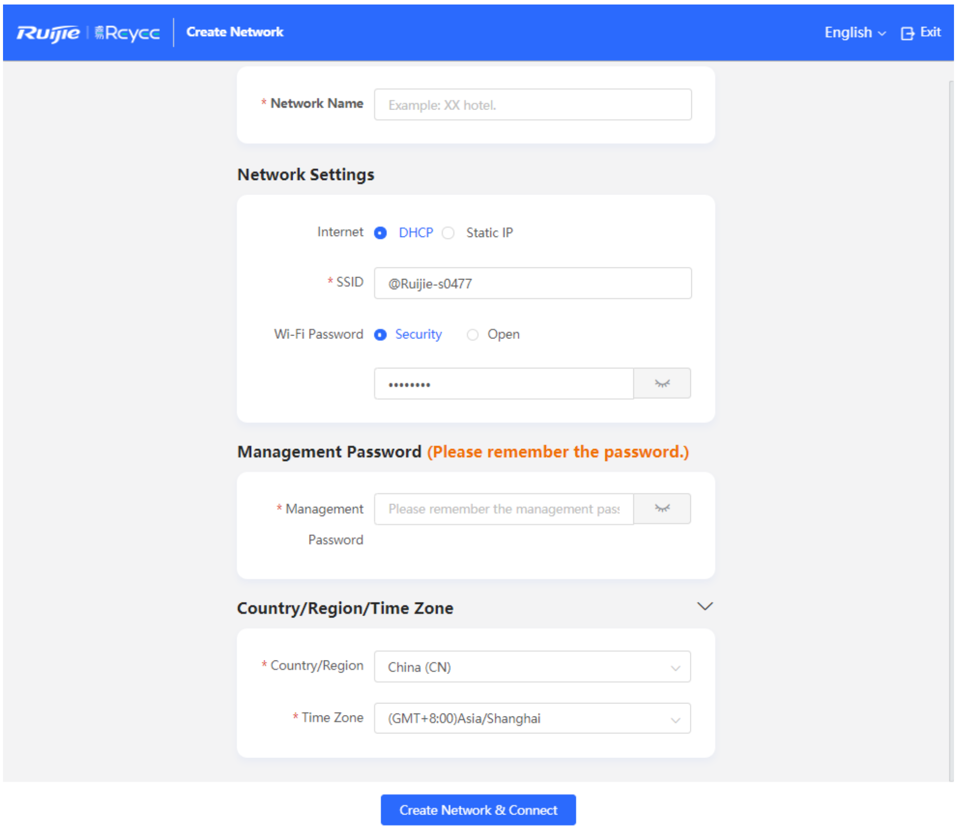
Description:

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

Work Mode: AP

Self-Organizing Network: ●

(2) After mode switching, the device will restart. After restart, the WAN port on the device obtains an IP address through DHCP and accesses the network by using a dynamic IP address. Set the SSID, Wi-Fi password, and management password, and keep the Internet access mode DHCP unchanged. For details, see Section 1.5.1 (2) .



* Network Name: Example: XX hotel.

Network Settings

Internet: ● DHCP ○ Static IP

* SSID: @Ruijie-s0477

Wi-Fi Password: ● Security ○ Open

••••••••

Management Password (Please remember the password.)

* Management Password: Please remember the management pas:

Country/Region/Time Zone

* Country/Region: China (CN)

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

1.7 Configuration Wizard (Wireless Repeater)

1.7.1 Getting Started

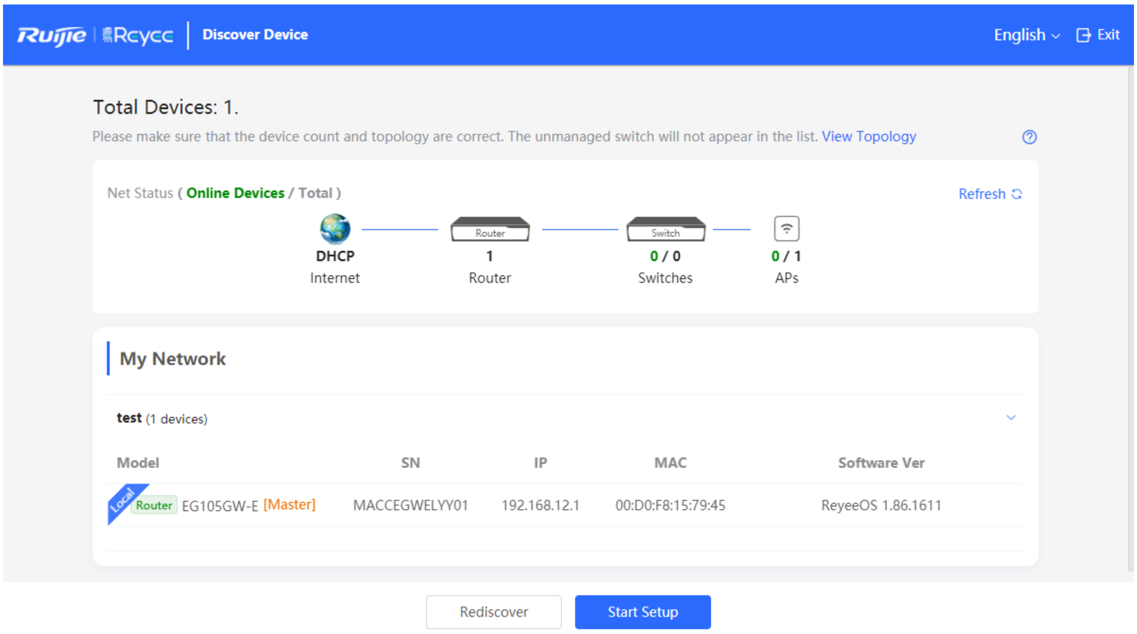
- Before setting the wireless repeater mode, configure the primary router and test that the primary router can normally access the Internet.
- Place the device in a location where Wi-Fi signal of the primary router can be searched and the signal has two or more cells.

Caution

The device does not need to connect to a network cable when working in wireless repeater mode. However, wireless stability is affected by many factors. You are advised to select a wired mode (AP mode).

1.7.2 Configuration Steps

(1) Connect the device to a power supply but not a network cable. Then, click **Start Setup**.



Total Devices: 1.

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

Net Status (Online Devices / Total) Refresh

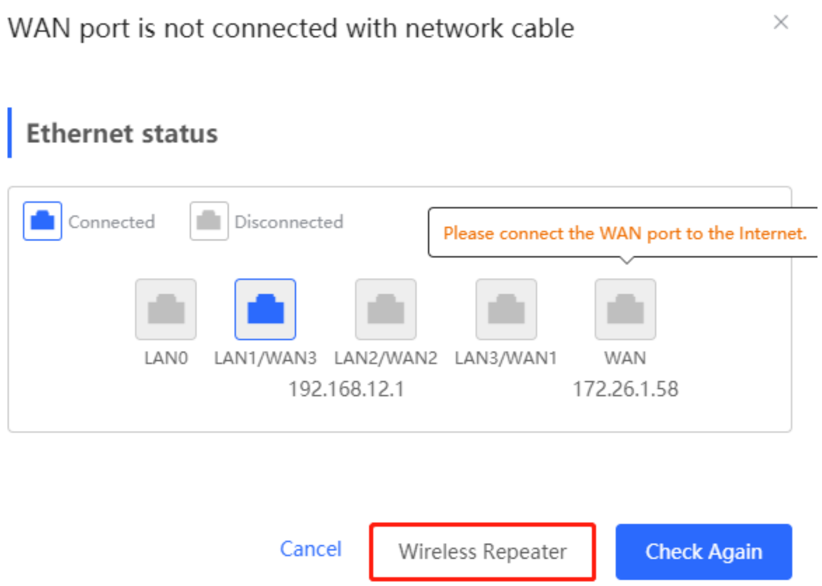
DHCP Internet — 1 Router — 0 / 0 Switches — 0 / 1 APs

My Network

test (1 devices)

Model	SN	IP	MAC	Software Ver
Local Router EG105GW-E [Master]	MACCEGWELYY01	192.168.12.1	00:D0:F8:15:79:45	ReyeeOS 1.86.1611

(2) On the page showing the WAN port is not connected with network cable message, click **Wireless Repeater**.

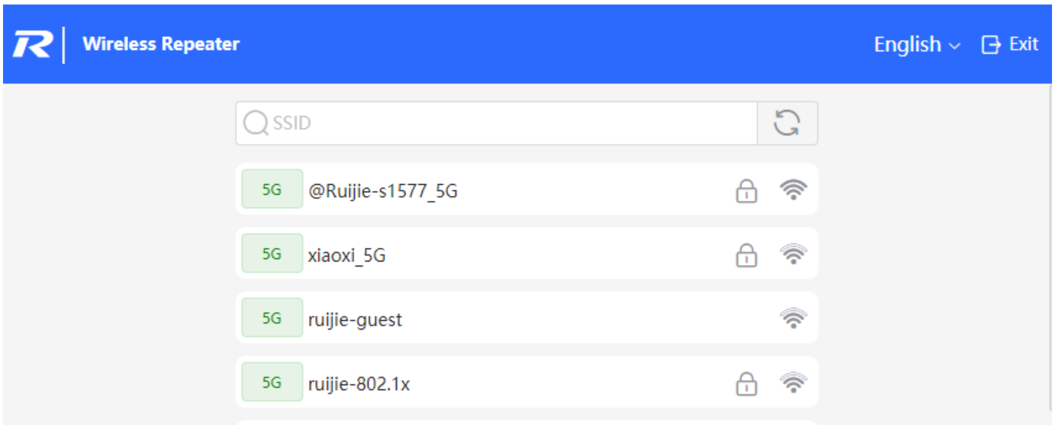


WAN port is not connected with network cable

Ethernet status

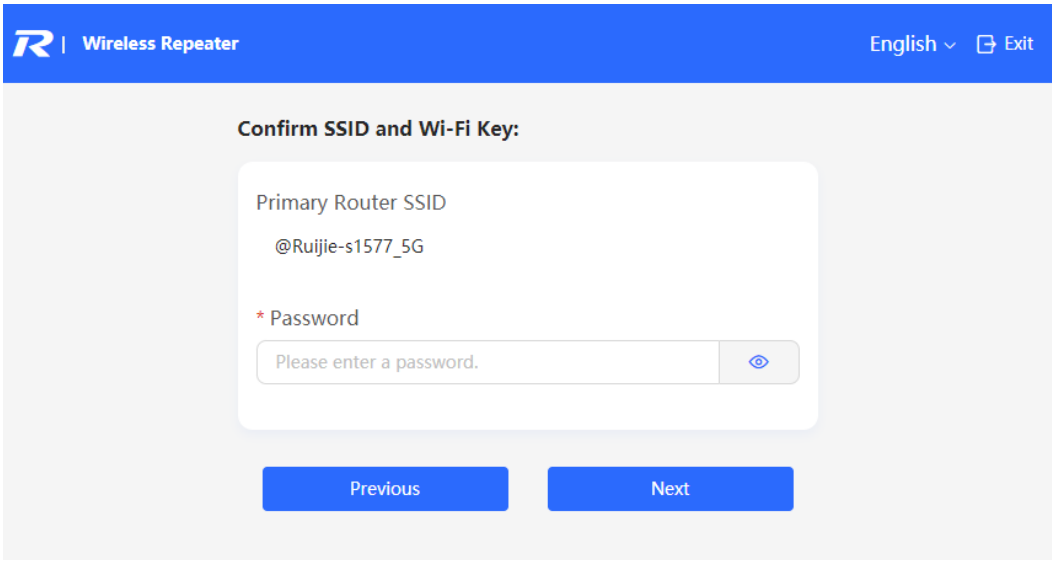
Please connect the WAN port to the Internet.

(3) Select the primary router whose Wi-Fi signal needs to be extended, enter the Wi-Fi password of the primary router, and click **Next**.



Wireless Repeater

5G	@Ruijie-s1577_5G
5G	xiaoxi_5G
5G	ruijie-guest
5G	ruijie-802.1x



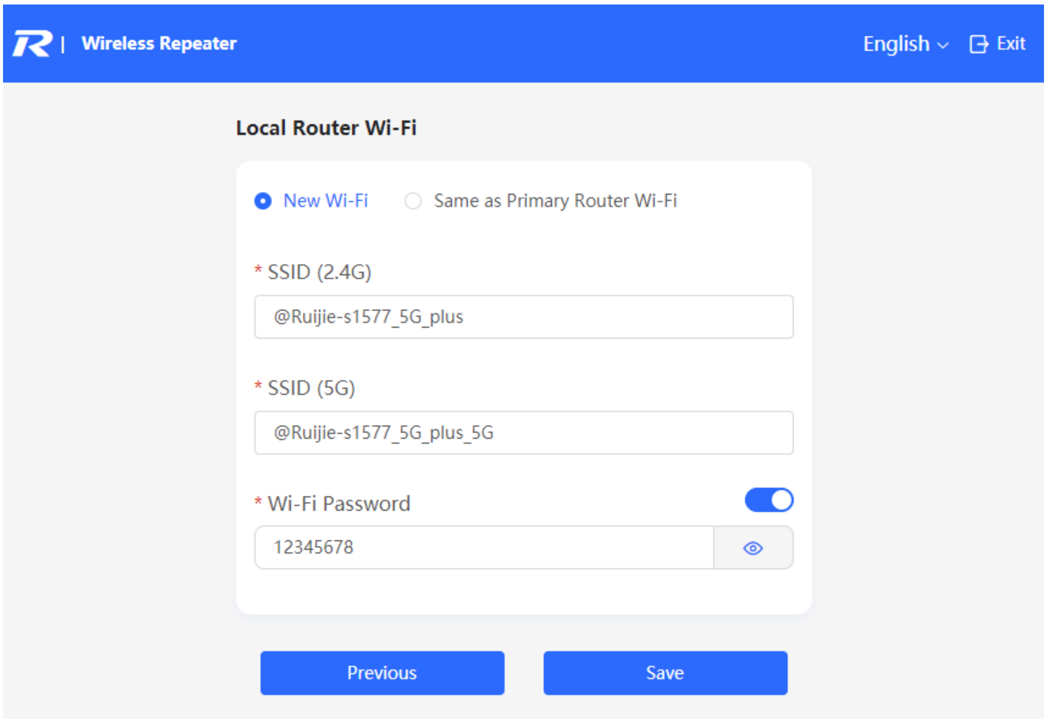
Wireless Repeater

Confirm SSID and Wi-Fi Key:

Primary Router SSID
@Ruijie-s1577_5G

* Password
Please enter a password.

(4) Set the SSID and password and click **Save**. Wi-Fi will restart.



Local Router Wi-Fi

● New Wi-Fi ○ Same as Primary Router Wi-Fi

* SSID (2.4G)
@Ruijie-s1577_5G_plus

* SSID (5G)
@Ruijie-s1577_5G_plus_5G

* Wi-Fi Password
12345678

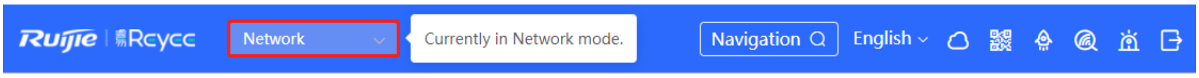
1.8 Switching Between Management Pages

After you disable self-organizing network discovery, the web page is in the Local Device mode. (Self-organizing network discovery is enabled upon delivery. For details, see Section 3.1 Switching the Work Mode.)

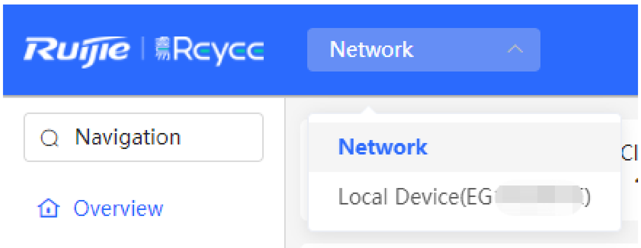
After you enable self-organizing network discovery, you can switch between the Network and Local Device web pages. Click the current management mode in the navigation bar and select the desired mode from the drop-down list box.

Network mode: View the management information of all devices in the network and configure all devices in the current network from the network-wide perspective.

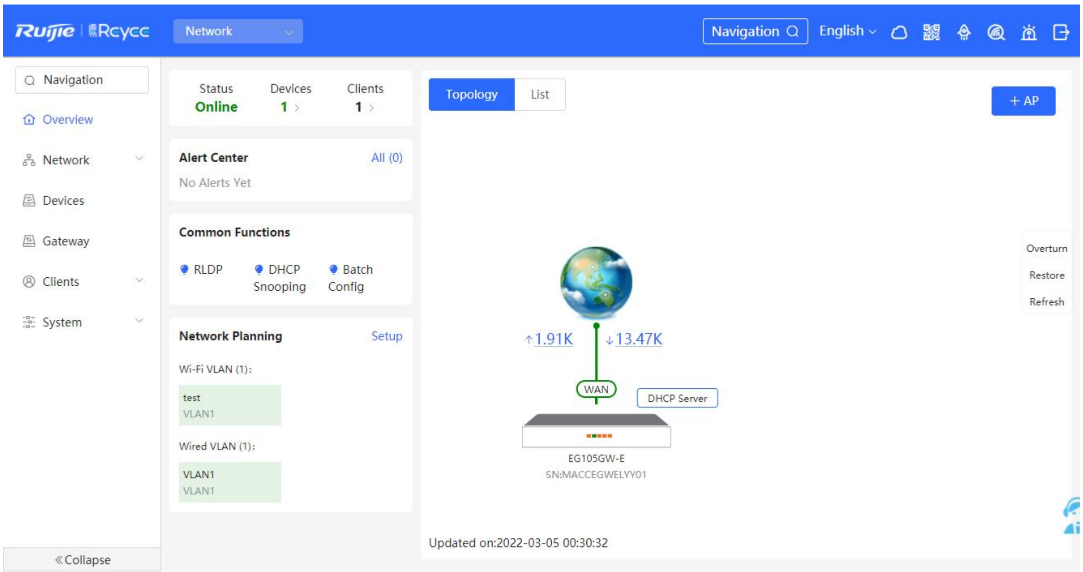
Local Device mode: Configure the device that you log in to.



Currently in Network mode.



Network page:



Status	Devices	Clients
Online	1	1

Alert Center All (0)

No Alerts Yet

Common Functions

- RLDP
- DHCP Snooping
- Batch Config

Network Planning Setup

Wi-Fi VLAN (1):

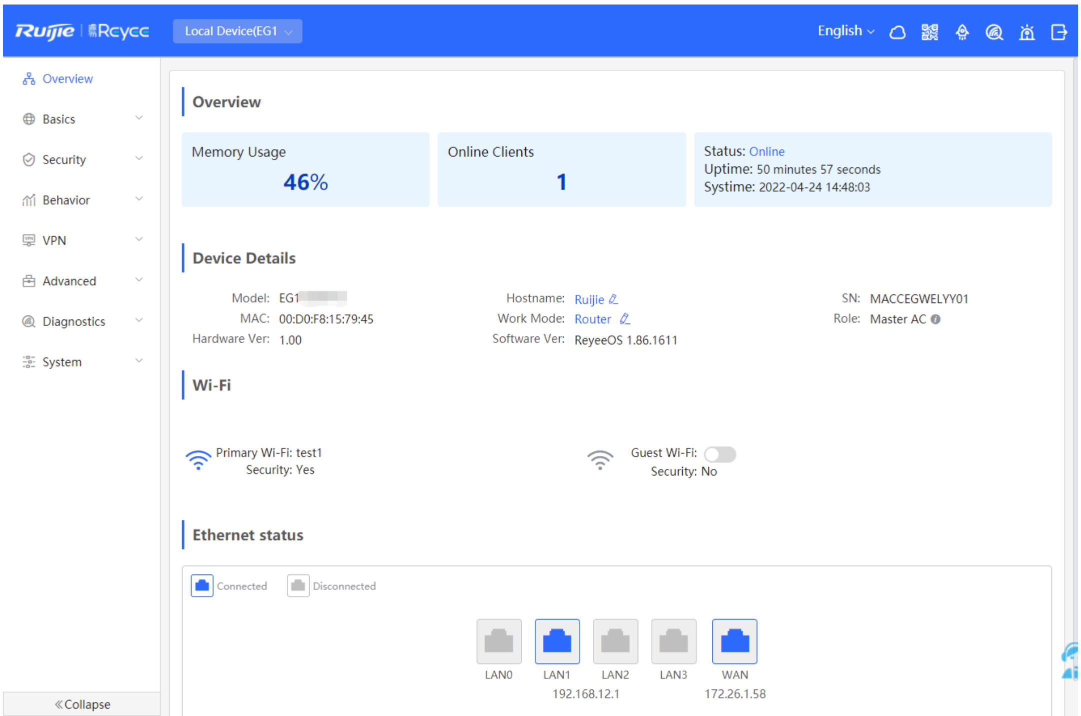
test
VLAN1

Wired VLAN (1):

VLAN1
VLAN1

Updated on:2022-03-05 00:30:32

Local Device page:



Overview

Memory Usage
46%

Online Clients
1

Status: Online
Uptime: 50 minutes 57 seconds
Systime: 2022-04-24 14:48:03

Device Details

Model: EG1[redacted]
MAC: 00:D0:F8:15:79:45
Hardware Ver: 1.00
Hostname: Ruijie
Work Mode: Router
Software Ver: ReyeeOS 1.86.1611
SN: MACCEGWELYY01
Role: Master AC

Wi-Fi

Primary Wi-Fi: test1
Security: Yes

Guest Wi-Fi:
Security: No

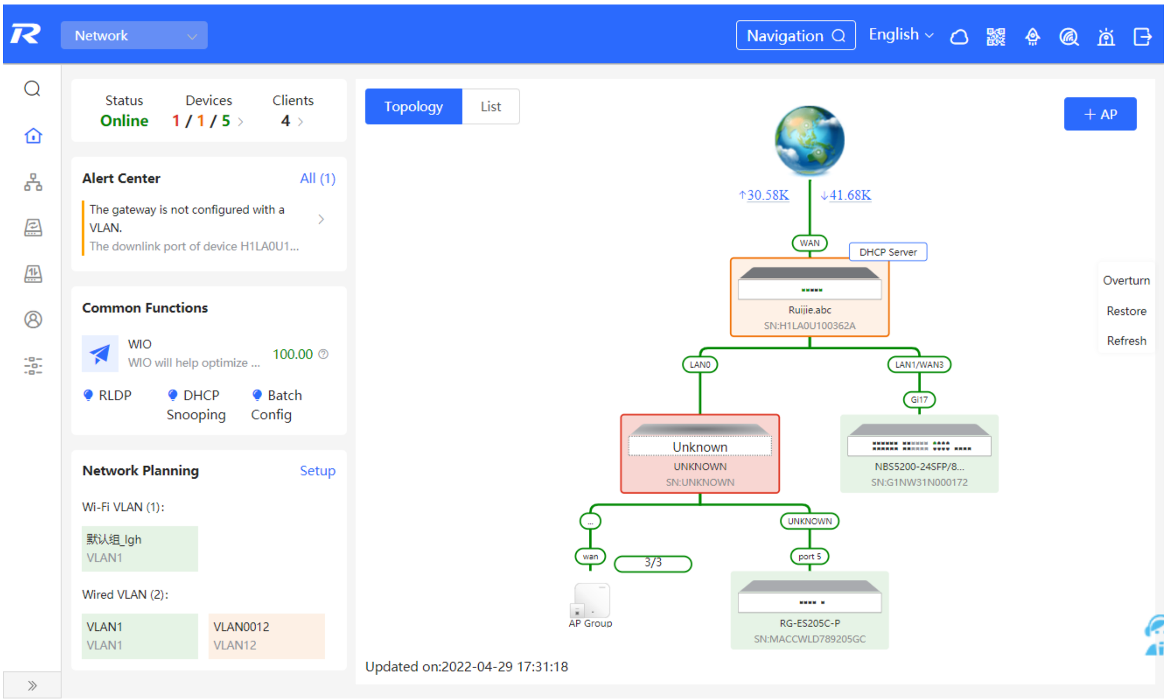
Ethernet status

LAN1 192.168.12.1
WAN 172.26.1.58

2 Network-Wide Monitoring

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

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

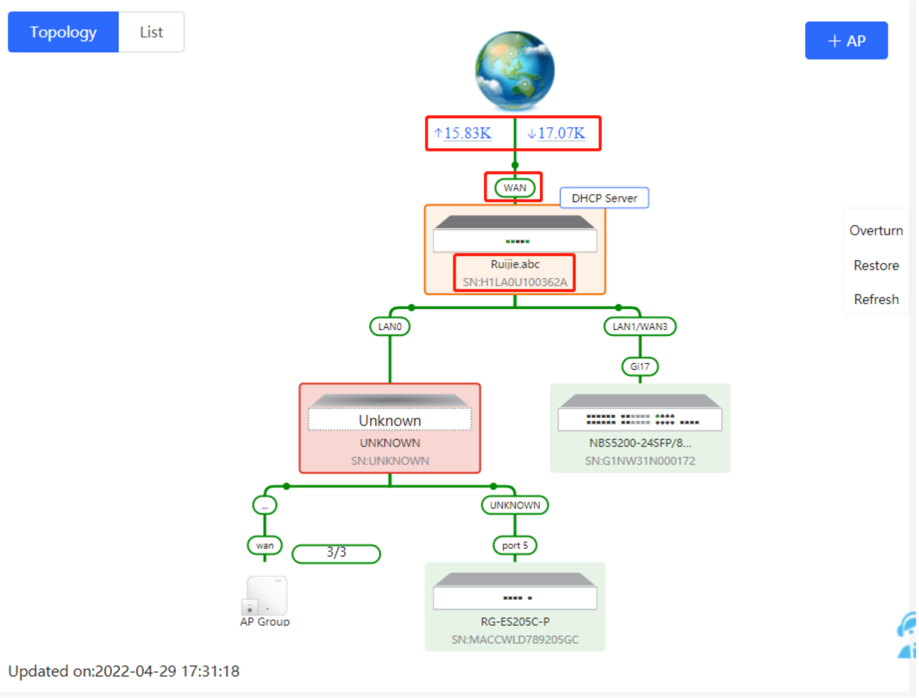


The gateway is not configured with a VLAN.
The downlink port of device H1LA0U1...

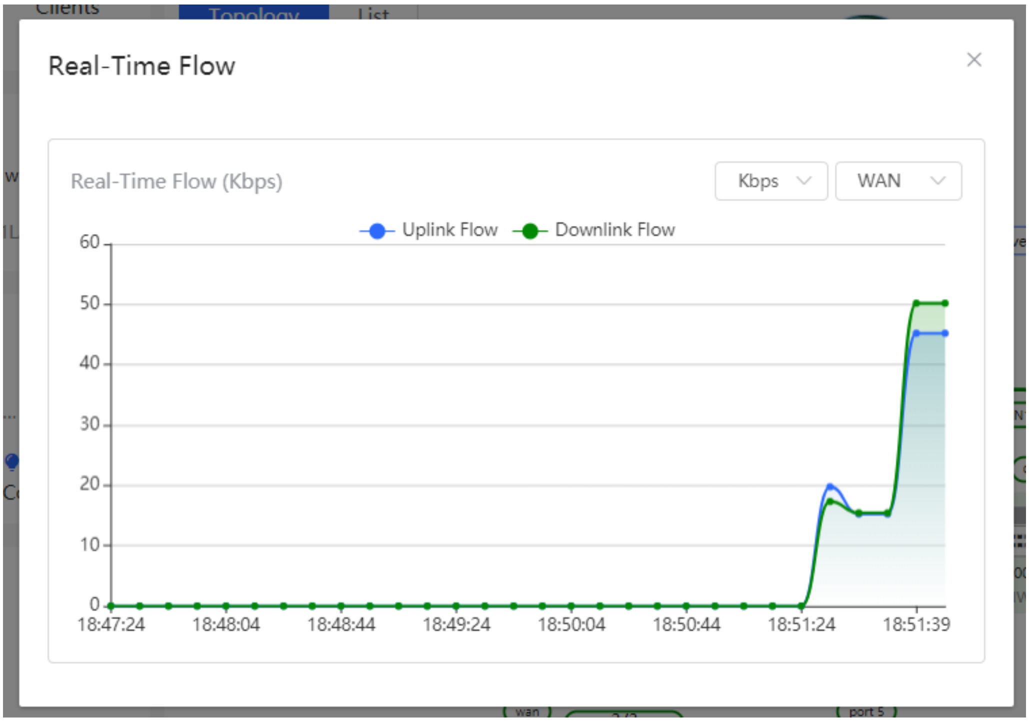
Updated on:2022-04-29 17:31:18

2.1 Viewing Networking Information

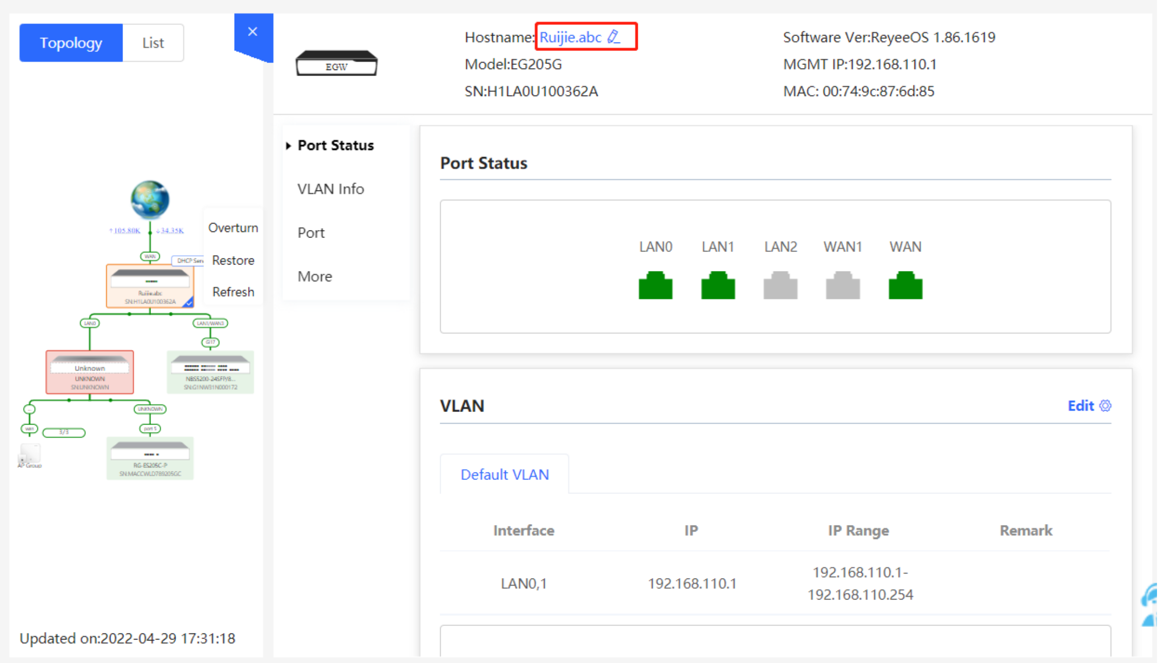
The networking topology contains information about online devices, connected port numbers, device SNs, and uplink and downlink real-time traffic.



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



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



Hostname: Ruijie.abc
Model:EG205G
SN:H1LA0U100362A
Software Ver:ReyeeOS 1.86.1619
MGMT IP:192.168.110.1
MAC: 00:74:9c:87:6d:85

Port Status

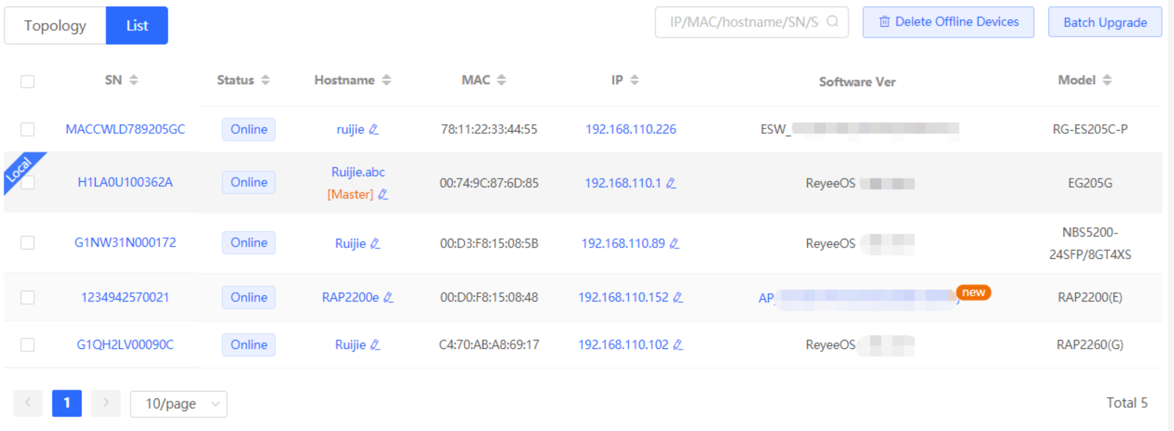
VLAN

Default VLAN

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

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

- Click **List** in the upper-left corner of the topology to switch to the device list view. Then, you can view device information in the current networking. Click an item in the list to configure and manage the device separately.

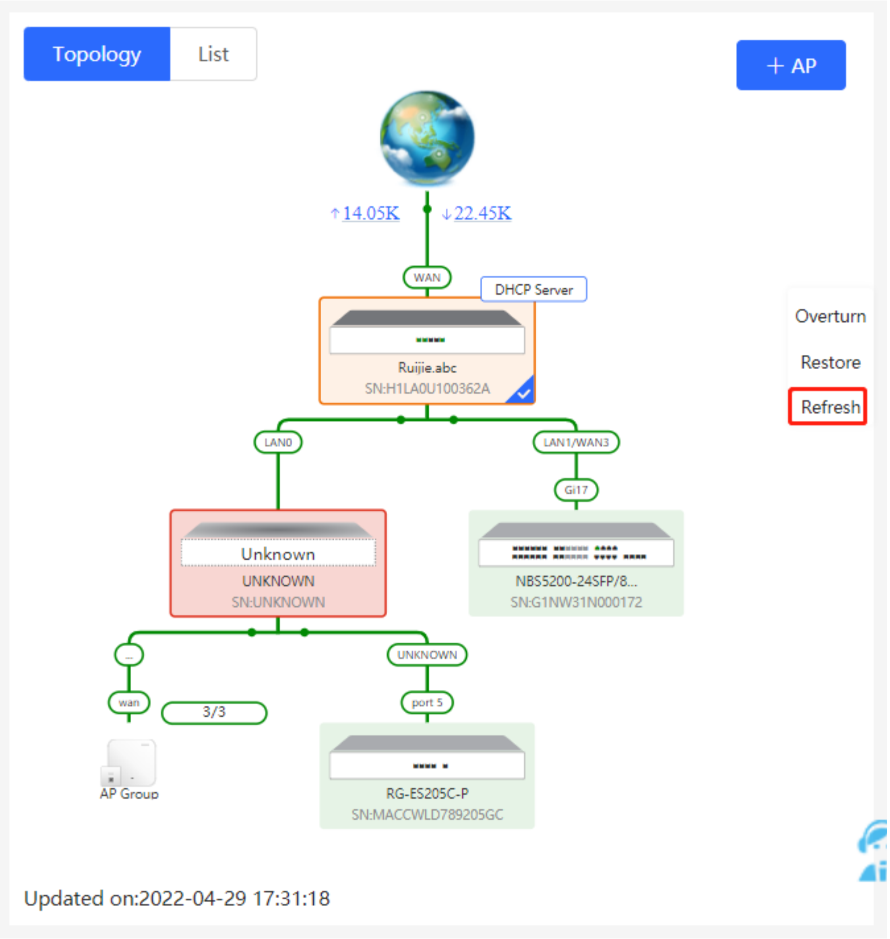


□	SN	Status	Hostname	MAC	IP	Software Ver	Model
□	MACCWLD789205GC	Online	ruijie	78:11:22:33:44:55	192.168.110.226	ESW_[redacted]	RG-ES205C-P
□	H1LA0U100362A	Online	Ruijie.abc [Master]	00:74:9C:87:6D:85	192.168.110.1	ReyeeOS [redacted]	EG205G
□	G1NW31N000172	Online	Ruijie	00:D3:F8:15:08:5B	192.168.110.89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

1

Total 5

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

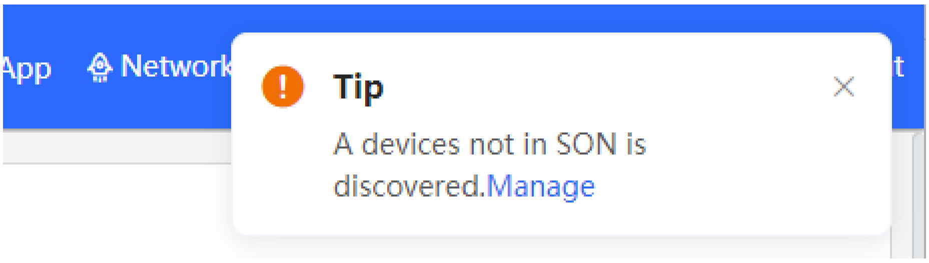


Updated on:2022-04-29 17:31:18

2.2 Adding Networking Devices

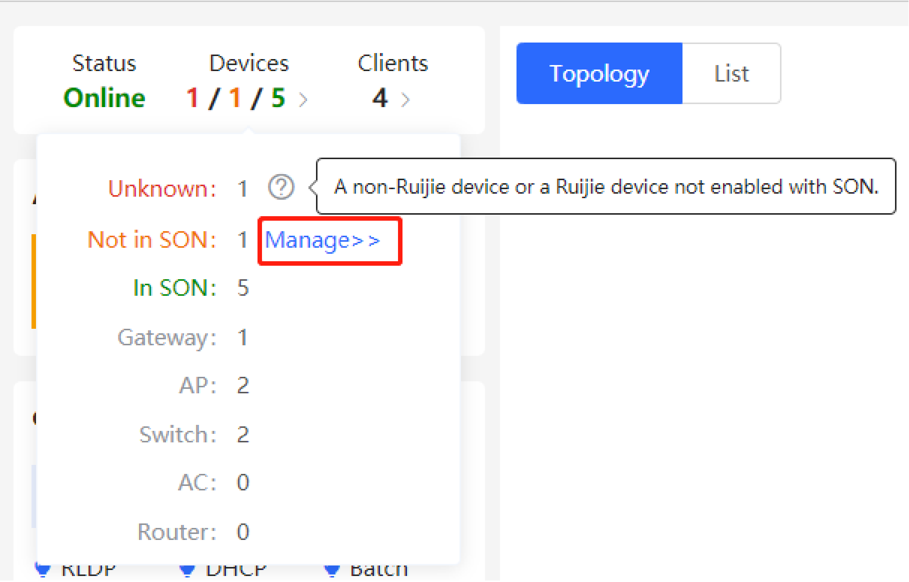
2.2.1 Wired Connection

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



Tip

A devices not in SON is discovered.Manage



Status: Online

Devices: 1 / 1 / 5 >

Clients: 4 >

Unknown: 1 ⓘ A non-Ruijie device or a Ruijie device not enabled with SON.

Not in SON: 1 Manage>>

In SON: 5

Gateway: 1

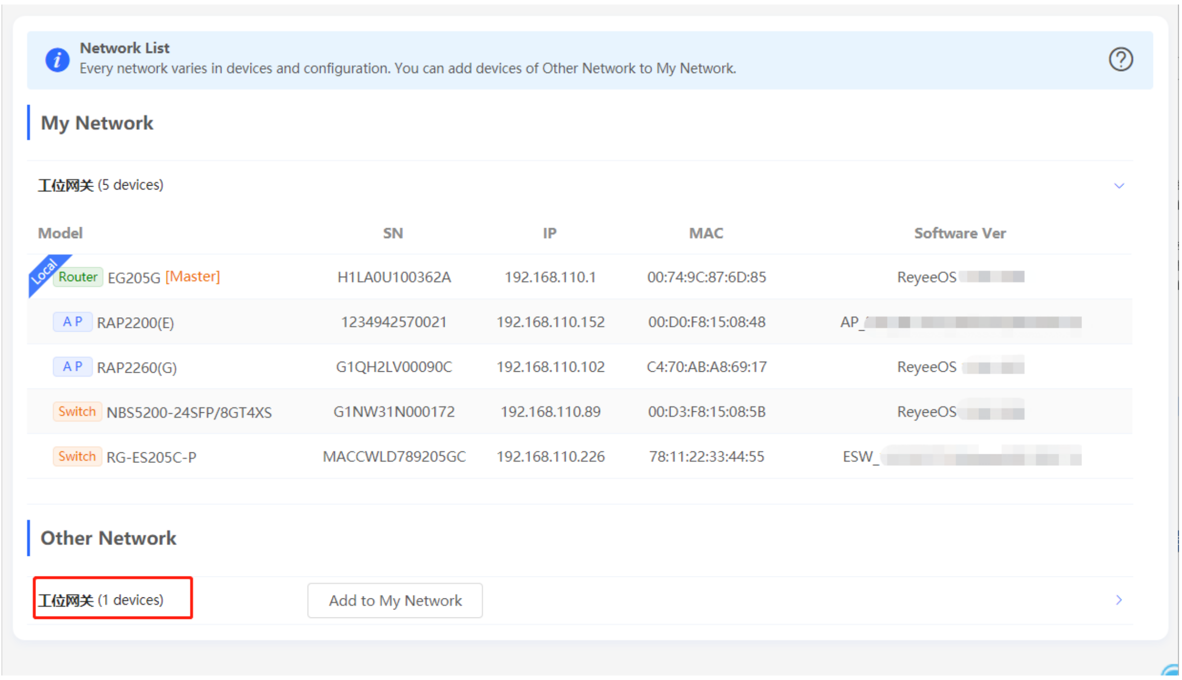
AP: 2

Switch: 2

AC: 0

Router: 0

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



Network List

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

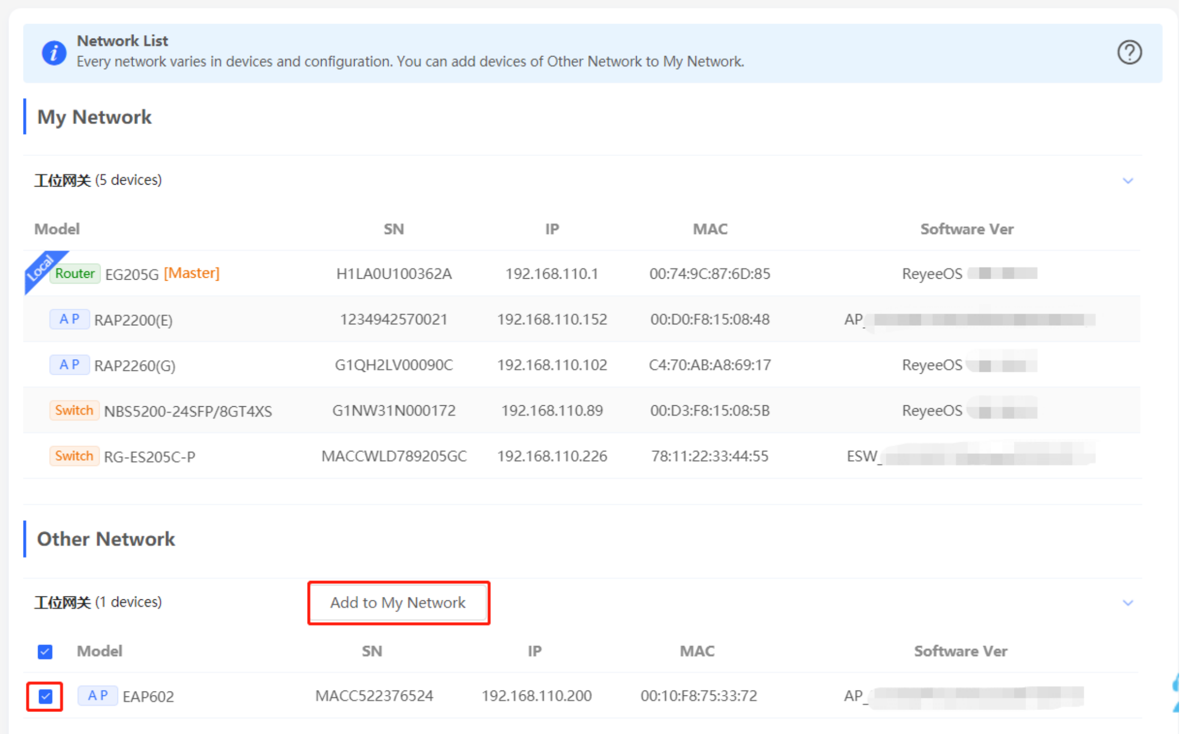
My Network

工位网关 (5 devices)

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

Other Network

工位网关 (1 devices) Add to My Network



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

My Network

工位网关 (5 devices)

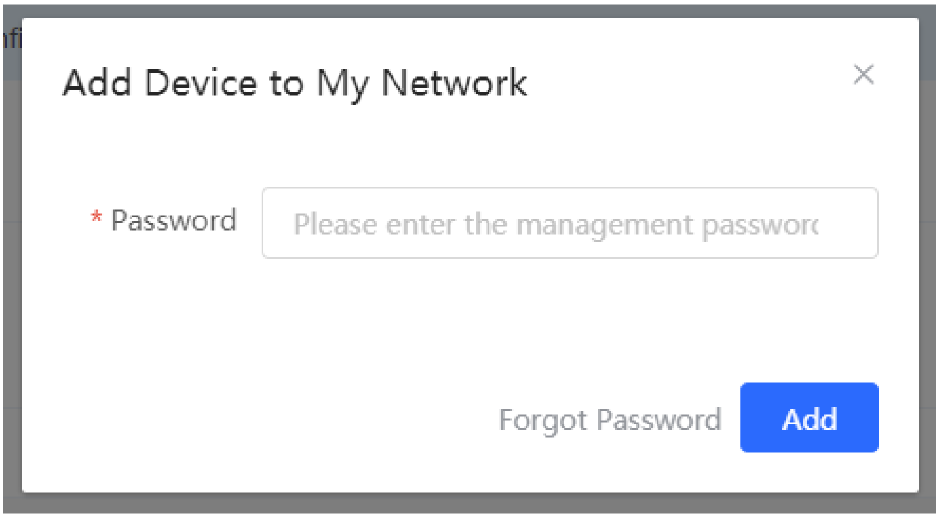
Model	SN	IP	MAC	Software Ver
Local Router EG205G [Master]	H1LA0U100362A	192.168.110.1	00:74:9C:87:6D:85	ReyeeOS [redacted]
AP RAP2200(E)	1234942570021	192.168.110.152	00:D0:F8:15:08:48	AP_[redacted]
AP RAP2260(G)	G1QH2LV00090C	192.168.110.102	C4:70:AB:A8:69:17	ReyeeOS [redacted]
Switch NBS5200-24SFP/8GT4XS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

Other Network

工位网关 (1 devices)   Add to My Network

☑ Model	SN	IP	MAC	Software Ver
☑ AP EAP602	MACC522376524	192.168.110.200	00:10:F8:75:33:72	AP_[redacted]

(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.



Add Device to My Network

* Password: Please enter the management passworc

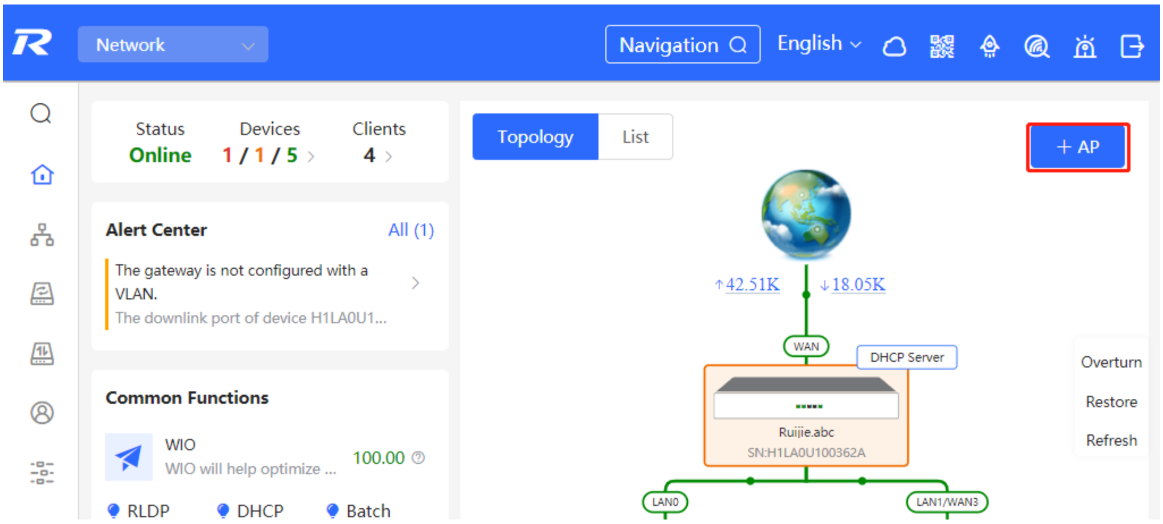
2.2.2 AP Mesh

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 Reyee Mesh Settings.) The AP should be powered on nearby. It may fail to be scanned in case of long distance or obstacle blocking.

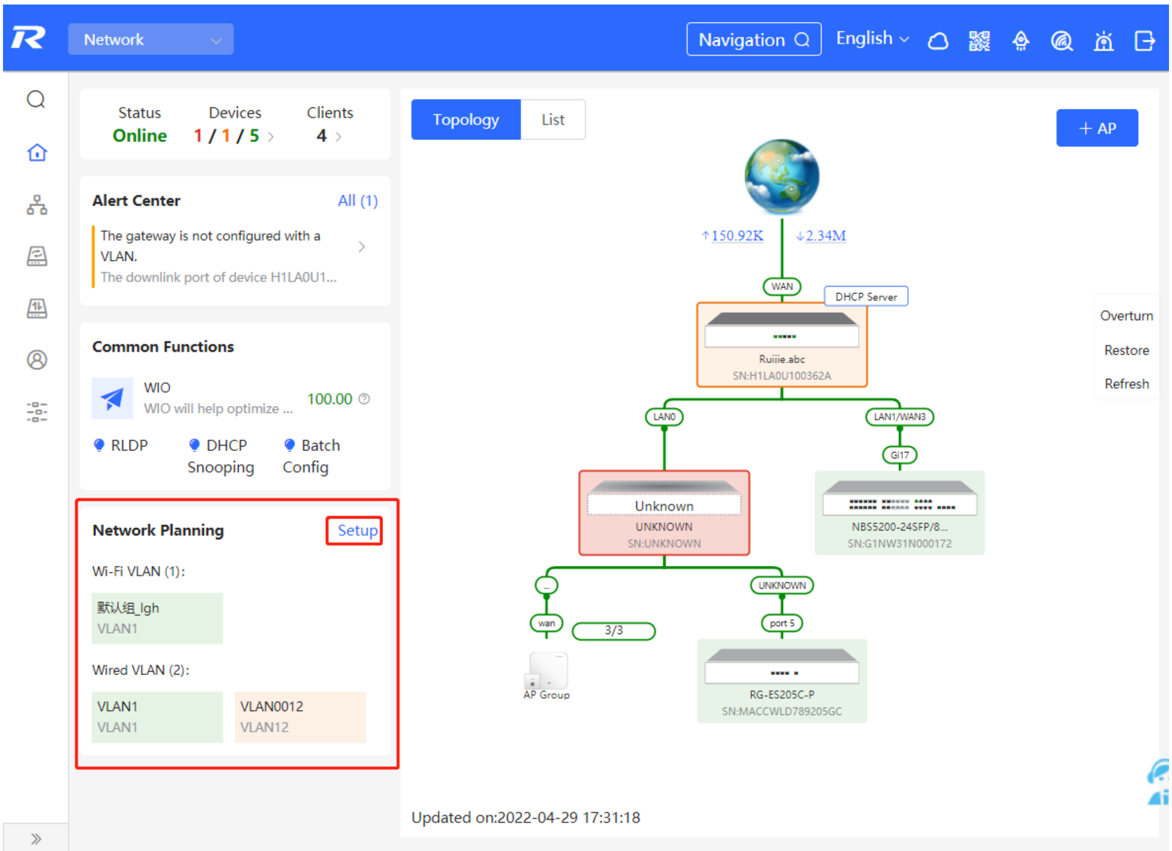
(1) Place the powered new AP near an existing AP, where the new AP can receive Wi-Fi signals from the existing AP. Log in to a device in the network. On the **Overview** page, click **+AP** in the upper-right corner of the topology to scan nearby APs that do not belong to the current network and are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



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

2.3 Configuring the Service Network

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



The gateway is not configured with a VLAN.

The downlink port of device H1LA0U1...

Wi-Fi VLAN (1):

默认组_lgh
VLAN1

Wired VLAN (2):

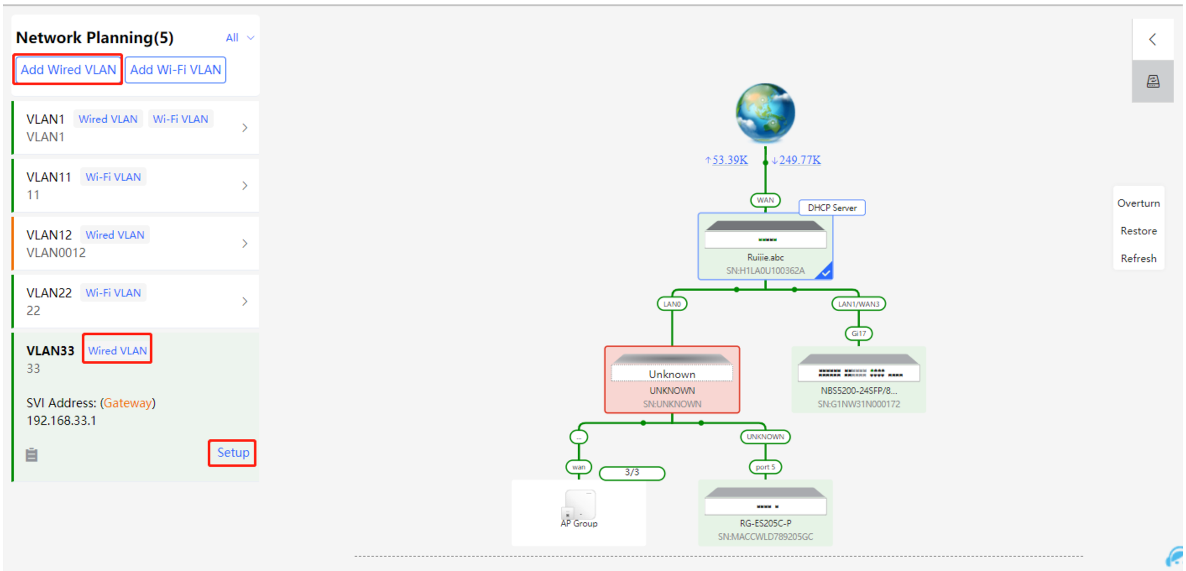
VLAN1
VLAN1

VLAN0012
VLAN12

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

2.3.1 Configuring the Wired Network

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



VLAN1 Wired VLAN Wi-Fi VLAN
VLAN1

VLAN11 Wi-Fi VLAN
11

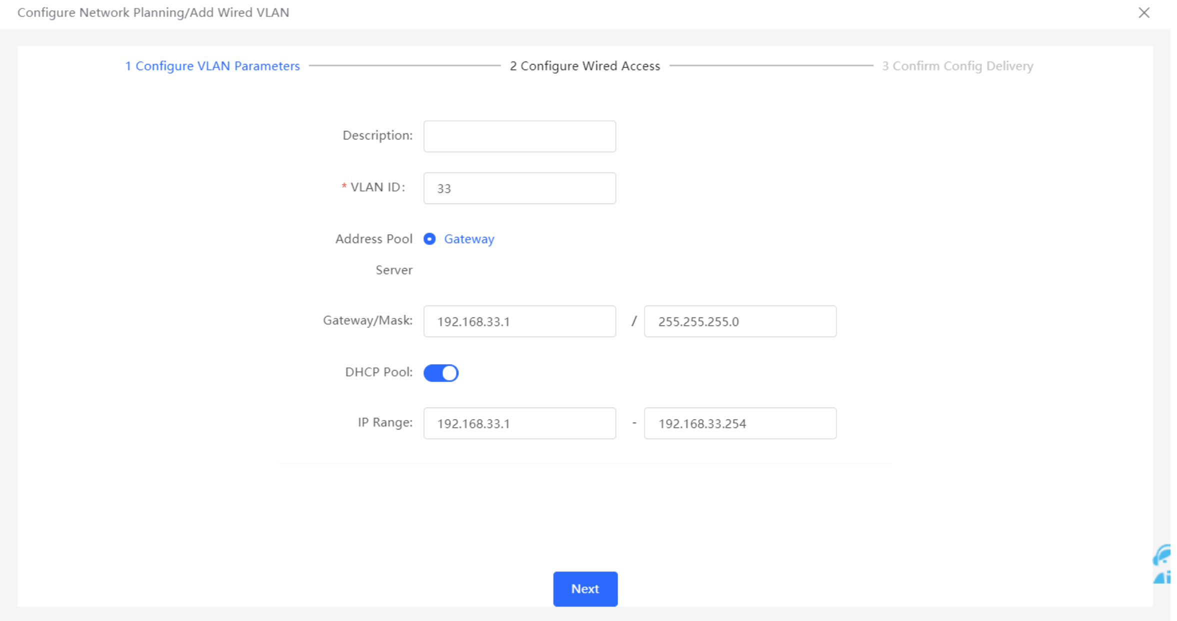
VLAN12 Wired VLAN
VLAN0012

VLAN22 Wi-Fi VLAN
22

VLAN33 Wired VLAN
33

SVI Address: (Gateway)
192.168.33.1

(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**.



Configure Network Planning/Add Wired VLAN

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

Description:

* VLAN ID: 33

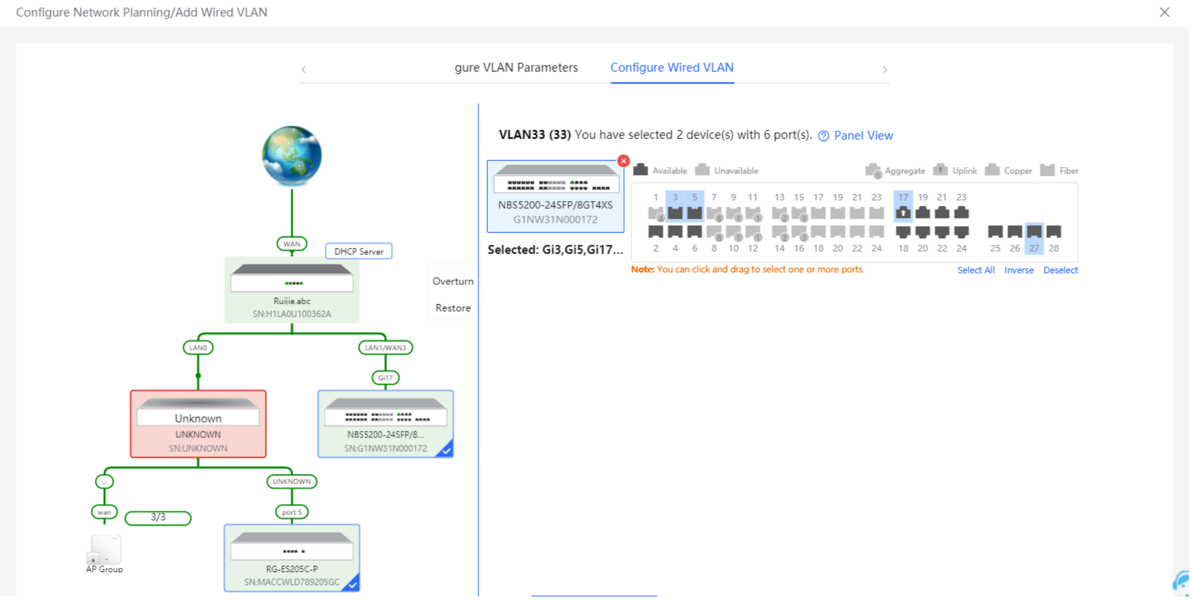
Address Pool Server: ● Gateway

Gateway/Mask: 192.168.33.1 / 255.255.255.0

DHCP Pool: ●

IP Range: 192.168.33.1 - 192.168.33.254

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



Configure Network Planning/Add Wired VLAN

gure VLAN Parameters | Configure Wired VLAN

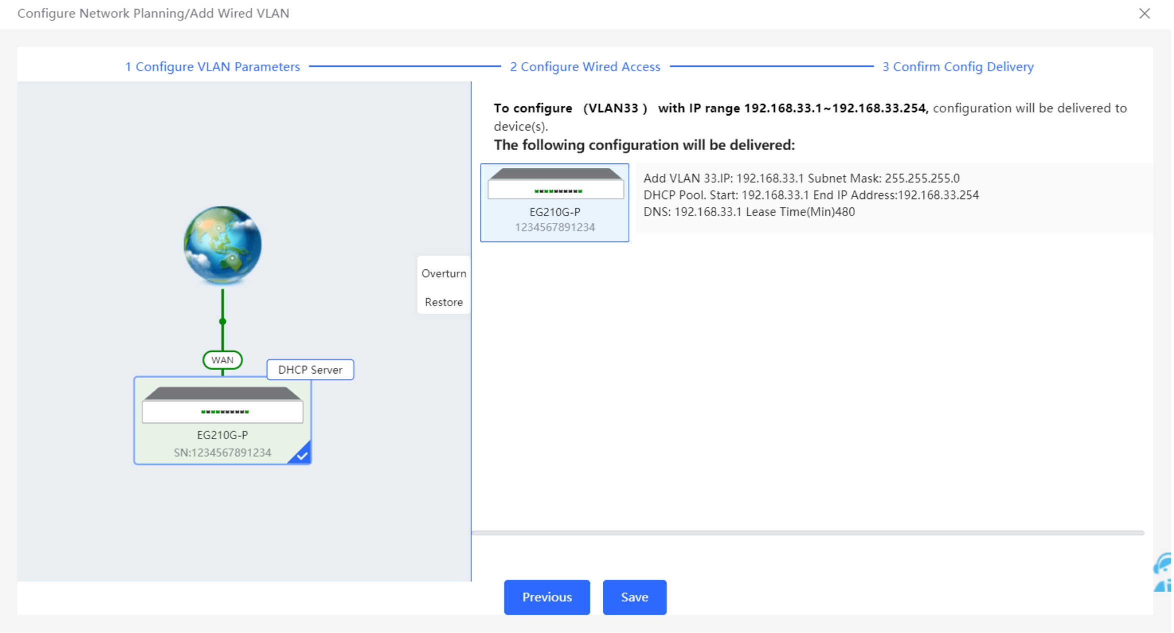
VLAN33 (33) You have selected 2 device(s) with 6 port(s). Panel View

NBS5200-24SFP/8GT4XS
G1NW31N000172

Selected: Gi3,Gi5,Gi17...

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

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



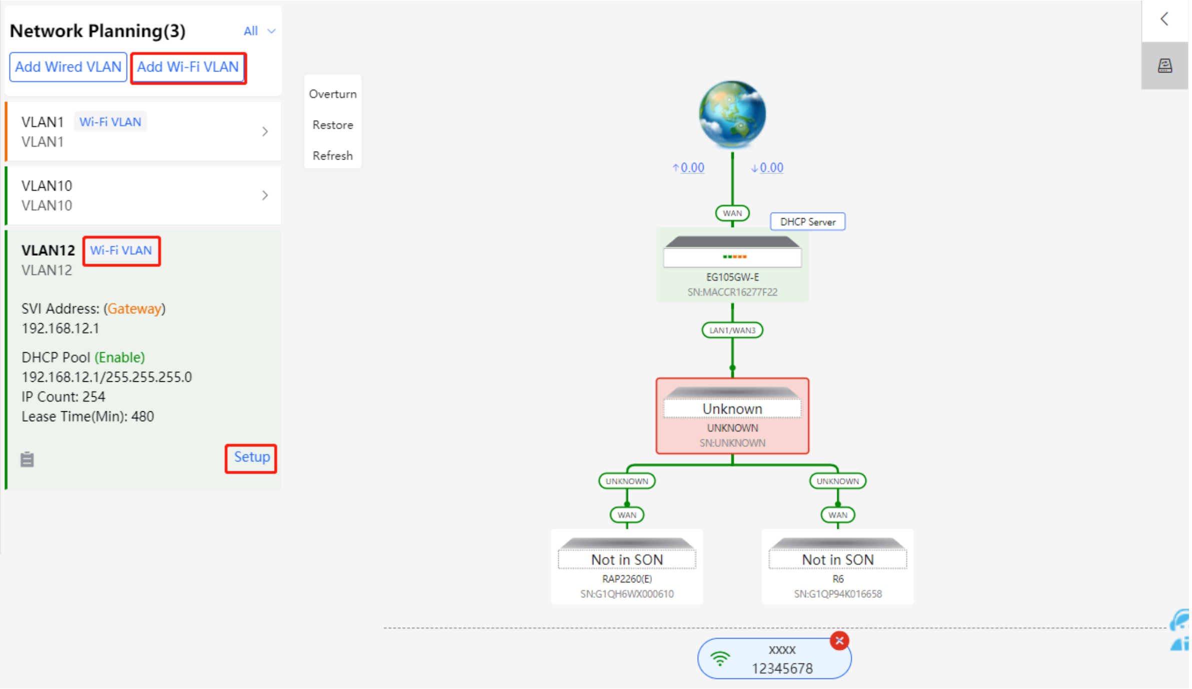
To configure （VLAN33） with IP range 192.168.33.1~192.168.33.254, configuration will be delivered to device(s).

The following configuration will be delivered:

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

2.3.2 Configuring the Wireless Network

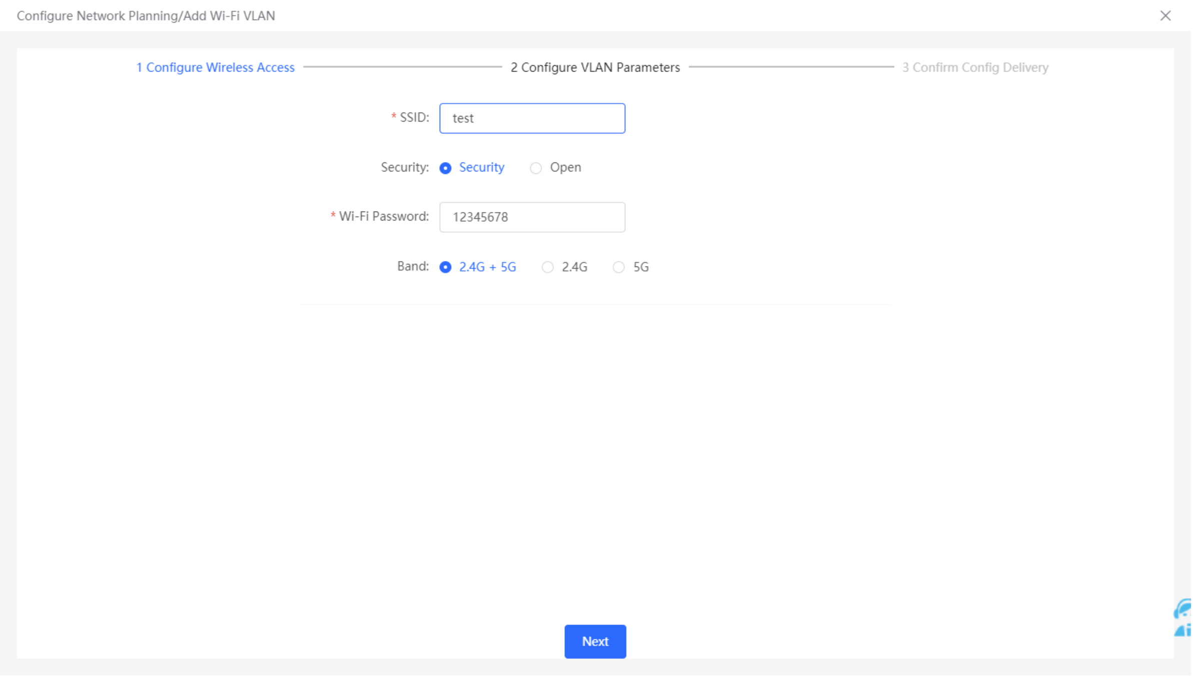
(1) Click **Add Wi-Fi VLAN** to add wireless network configuration, or select an existing Wi-Fi VLAN and click **Setup** to modify its configuration.



SVI Address: (Gateway)
192.168.12.1

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

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



Configure Network Planning/Add Wi-Fi VLAN

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

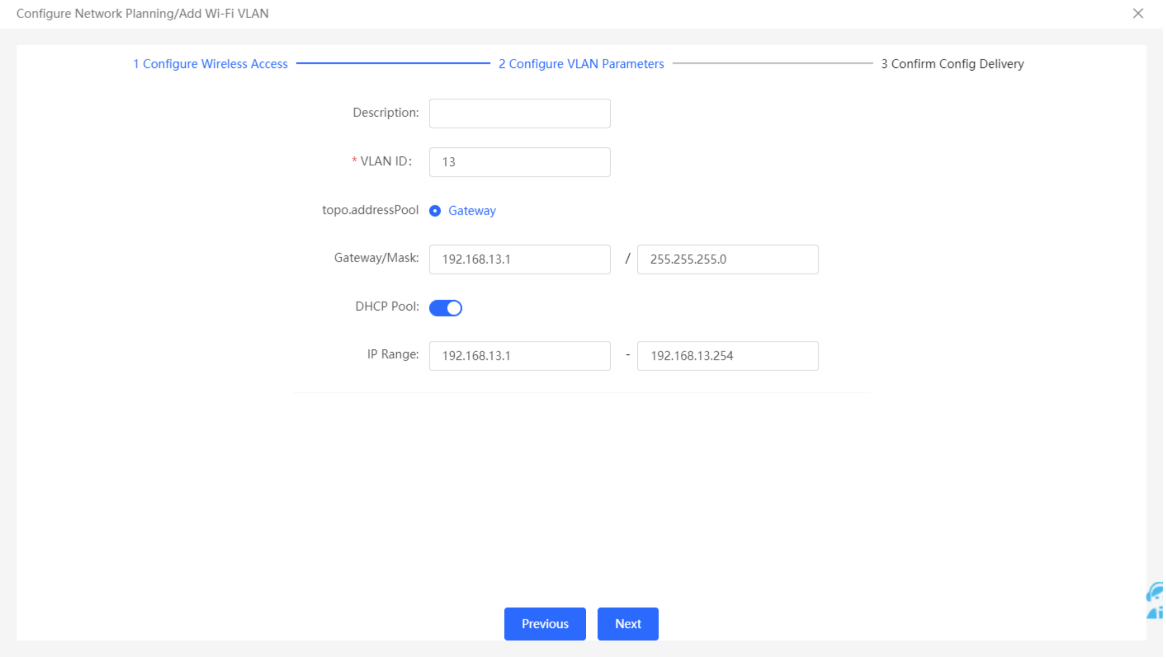
* SSID: test

Security: ● Security ○ Open

* Wi-Fi Password: 12345678

Band: ● 2.4G + 5G ○ 2.4G ○ 5G

(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**.



Configure Network Planning/Add Wi-Fi VLAN

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

Description:

* VLAN ID: 13

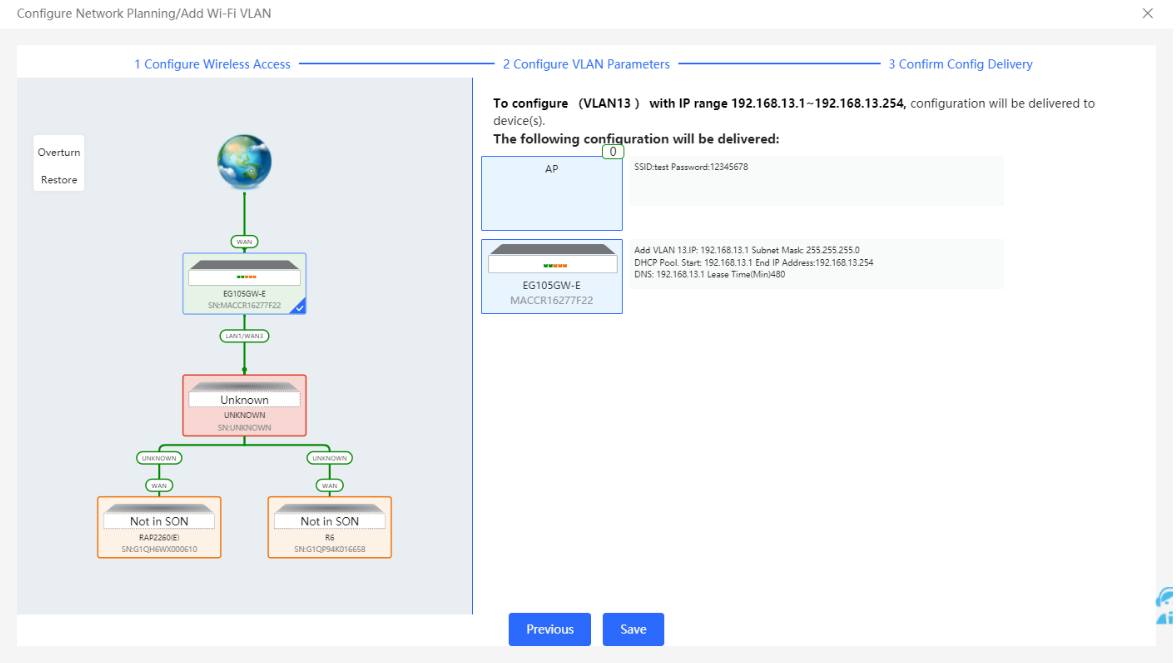
topo.addressPool ● Gateway

Gateway/Mask: 192.168.13.1 / 255.255.255.0

DHCP Pool: On

IP Range: 192.168.13.1 - 192.168.13.254

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


Configure Network Planning/Add Wi-Fi VLAN

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

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

The following configuration will be delivered:

AP	SSID:test Password:12345678
EG105GW-E MACCR16277F22	Add VLAN 13.IP: 192.168.13.1 Subnet Mask: 255.255.255.0 DHCP Pool. Start: 192.168.13.1 End IP Address:192.168.13.254 DNS: 192.168.13.1 Lease Time(Min)480

2.4 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.

2.4.1 Viewing Real-time Traffic

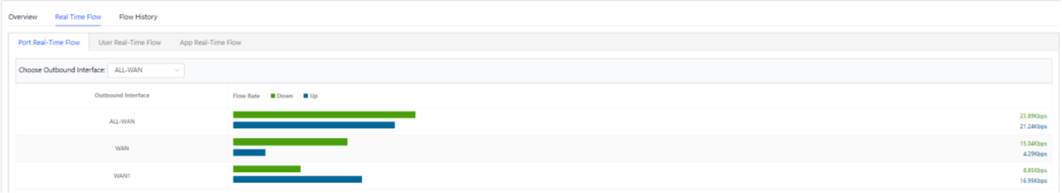
[**Local Device**] Choose **Overview** > **Real Time Flow**.

(1) View real-time traffic of a port.

a Click the **Port Real-Time Flow** tab.

b Set **Choose Outbound Interface**.

Set **Choose Outbound Interface** to a port or **ALL-WAN**. You can view the uplink or downlink traffic of a port or the system.

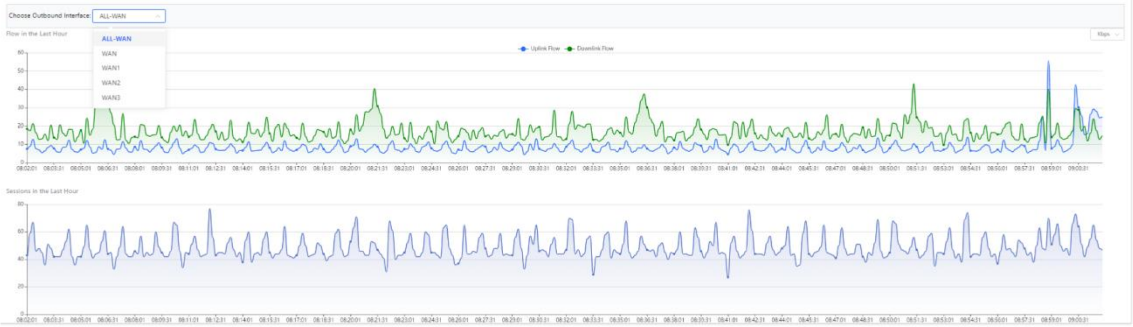


Choose Outbound Interface: ALL-WAN

Outbound Interface	Flow Rate 🟩 Down 🟦 Up
ALL-WAN	23.89Kbps 21.24Kbps
WAN	15.04Kbps 4.29Kbps
WAN1	8.85Kbps 16.95Kbps

c View traffic in the last one hour.

Choose a port or **ALL-WAN** from the **Choose Outbound Interface** drop-down list and view the traffic and sessions (including sessions of an original WAN port after LAN/WAN switching) in the last one hour.



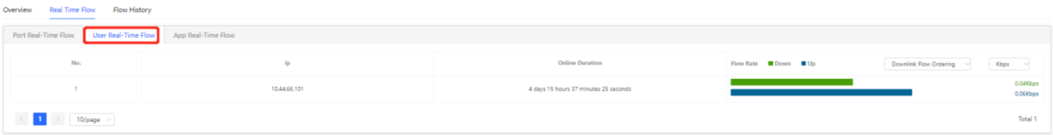
Choose Outbound Interface: ALL-WAN

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 real-time traffic of a user.

a Click the **User Real-Time Flow** tab.



No.	ip	Online Duration	Flow Rate 🟩 Down 🟦 Up
1	10.44.66.101	4 days 15 hours 37 minutes 25 seconds	0.04Kbps 0.06Kbps

Total 1

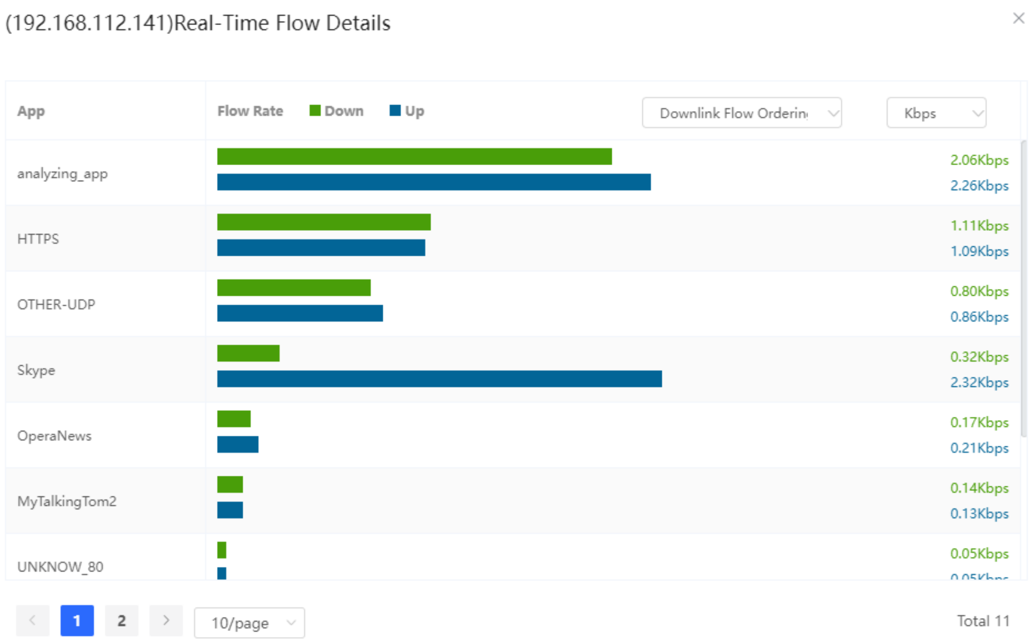
b The system displays real-time traffic of users.

You can view the IP address, online duration, uplink traffic, and downlink traffic of each user.

If there are multiple users, 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.

c View traffic details of a user.

Click **Detailed**. The pop-up page displays the uplink traffic and downlink traffic of each app used by the current user. You can set the sorting mode (by downlink traffic or uplink traffic), unit, and other parameters based on service requirements.



(192.168.112.141)Real-Time Flow Details

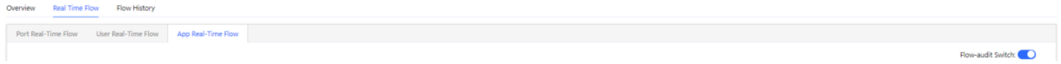
App	Flow Rate 🟩 Down 🟦 Up
analyzing_app	2.06Kbps 2.26Kbps
HTTPS	1.11Kbps 1.09Kbps
OTHER-UDP	0.80Kbps 0.86Kbps
Skype	0.32Kbps 2.32Kbps
OperaNews	0.17Kbps 0.21Kbps
MyTalkingTom2	0.14Kbps 0.13Kbps
UNKNOW_80	0.05Kbps 0.05Kbps

Total 11

(3) View real-time traffic of an app.

a Click the **App Real-Time Flow** tab.

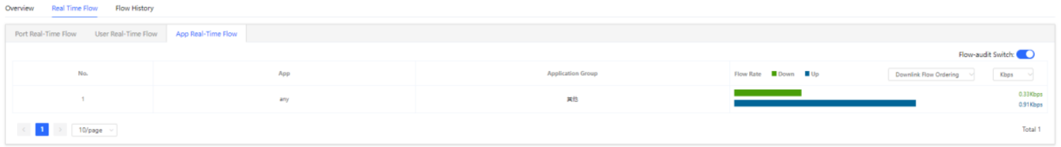
b Turn on **Flow-audit Switch**.



c The system displays real-time traffic of apps.

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.

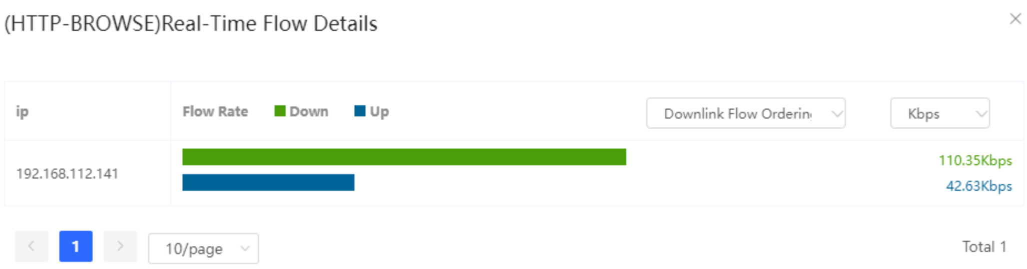


No.	App	Application Group	Flow Rate 🟩 Down 🟦 Up
1	any	其他	0.33Kbps 0.91Kbps

Total 1

d View traffic details of an app.

Click **Detailed**. The pop-up page displays details about the traffic of each user who uses the current app. You can set the sorting mode (by downlink traffic or uplink traffic), unit, and other parameters based on service requirements.



(HTTP-BROWSE)Real-Time Flow Details

ip	Flow Rate 🟩 Down 🟦 Up Downlink Flow Orderin Kbps
192.168.112.141	110.35Kbps 42.63Kbps

1 10/page Total 1

2.4.2 Viewing Historical Traffic

[**Local Device**] Choose **Overview** > **Flow History**.

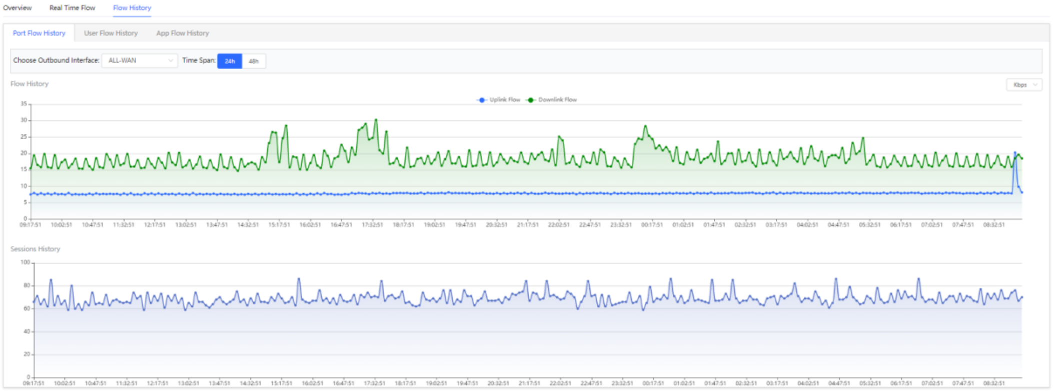
(4) View historical traffic of a port.

a Click the **Port Flow History** tab.

b Set **Choose Outbound Interface** and **Time Span**.

Set **Choose Outbound Interface** to a port or **ALL-WAN**. You can view the uplink or downlink traffic of a port or the system.

The system allows you to view historical data of 24 hours or 48 hours. Set **Time Span** and **Choose Outbound Interface**. The system displays historical data of a port or all ports in the current time span.



Overview Real Time Flow Flow History

Port Flow History User Flow History App Flow History

Choose Outbound Interface: ALL-WAN Time Span: 24h 48h

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.

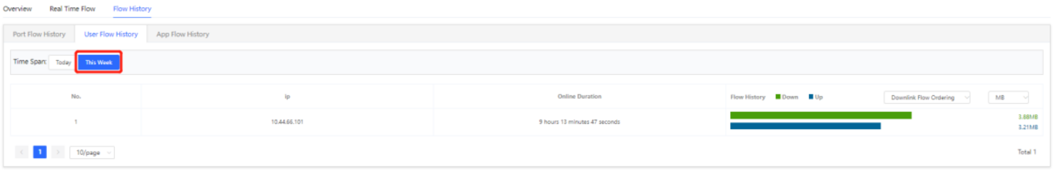
(5) View historical traffic of a user.

a Click the **User Flow History** tab.

b Set **Time Span**.

On the **User Flow History** tab page, you can view today's or this week's historical traffic data of a user.

For example, you can click **This Week** to switch to this week's data statistics display page, as shown in the figure below.



Overview Real Time Flow Flow History

Port Flow History User Flow History App Flow History

Time Span: Today This Week

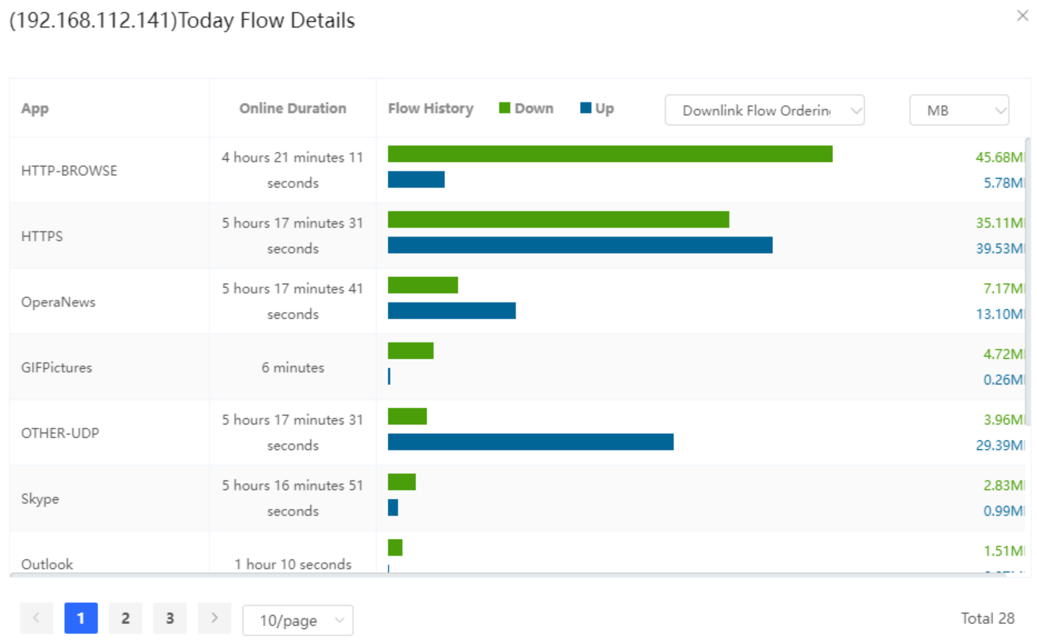
No.	ip	Online Duration	Flow History 🟩 Down 🟦 Up Downlink Flow Ordering MB
1	10.44.66.101	9 hours 13 minutes 47 seconds	3.88MB 3.21MB

1 10/page Total 1

If there are multiple users, the system displays traffic data by downlink traffic in descending order by default. You can view the online duration, uplink traffic, and downlink traffic of each user 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.

c View traffic details of apps used by a user.

Click **Detailed**. The pop-up page displays the traffic and online duration of each app used by the current user. You can set the sorting mode (by downlink traffic or uplink traffic), unit, and other parameters based on service requirements.



(192.168.112.141)Today Flow Details

App	Online Duration	Flow History 🟩 Down 🟦 Up	Downlink Flow Orderin MB
HTTP-BROWSE	4 hours 21 minutes 11 seconds		45.68M 5.78M
HTTPS	5 hours 17 minutes 31 seconds		35.11M 39.53M
OperaNews	5 hours 17 minutes 41 seconds		7.17M 13.10M
GIFPictures	6 minutes		4.72M 0.26M
OTHER-UDP	5 hours 17 minutes 31 seconds		3.96M 29.39M
Skype	5 hours 16 minutes 51 seconds		2.83M 0.99M
Outlook	1 hour 10 seconds		1.51M

Total 28

(6) View historical traffic of an app.

a Click the **App Flow History** tab.

b Turn on **Flow-audit Switch**.

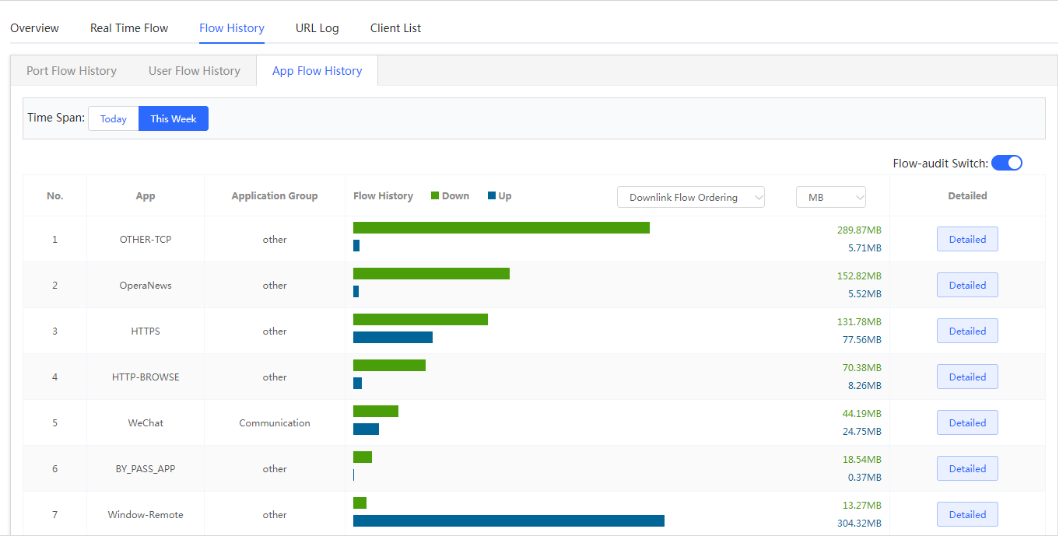
Note

The status of **Flow-audit Switch** is consistent with that of **Flow-audit Switch** on the **App Real-Time Flow** page. After it is turned on, the app real-time flow function and app flow history function are enabled.

c Set the time span.

On the **App Flow History** tab page, you can view today's or this week's historical user data.

For example, you can click **This Week** to switch to this week's data statistics display page, as shown in the figure below.



Overview | Real Time Flow | Flow History | URL Log | Client List

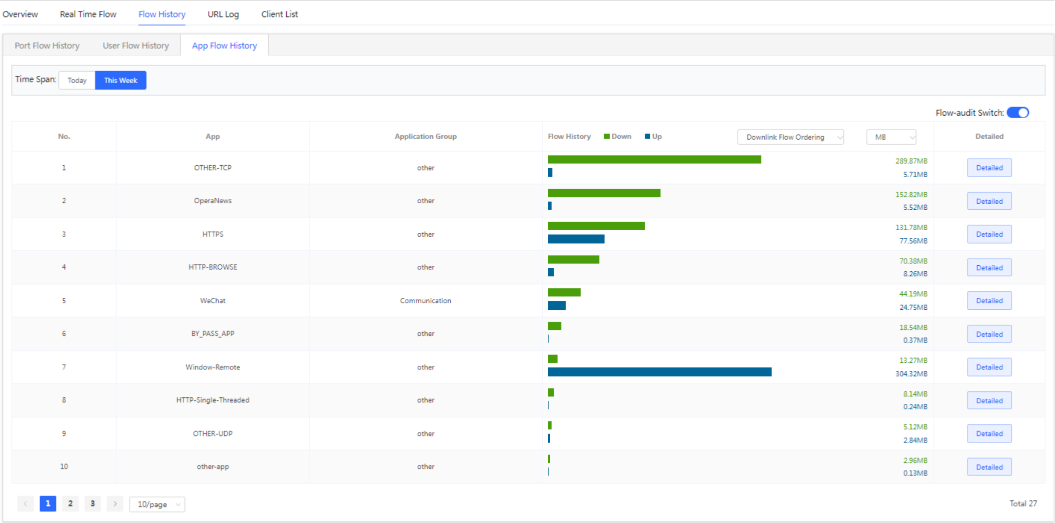
Port Flow History | User Flow History | App Flow History

Time Span: Today | This Week

Flow-audit Switch:

No.	App	Application Group	Flow History 🟩 Down 🟦 Up · Downlink Flow Ordering · MB	Detailed
1	OTHER-TCP	other	289.87MB 5.71MB	Detailed
2	OperaNews	other	152.82MB 5.52MB	Detailed
3	HTTPS	other	131.78MB 77.56MB	Detailed
4	HTTP-BROWSE	other	70.38MB 8.26MB	Detailed
5	WeChat	Communication	44.19MB 24.75MB	Detailed
6	BY_PASS_APP	other	18.54MB 0.37MB	Detailed
7	Window-Remote	other	13.27MB 304.32MB	Detailed

If there are multiple apps, 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 app 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.



Overview | Real Time Flow | Flow History | URL Log | Client List

Port Flow History | User Flow History | App Flow History

Time Span: Today | This Week

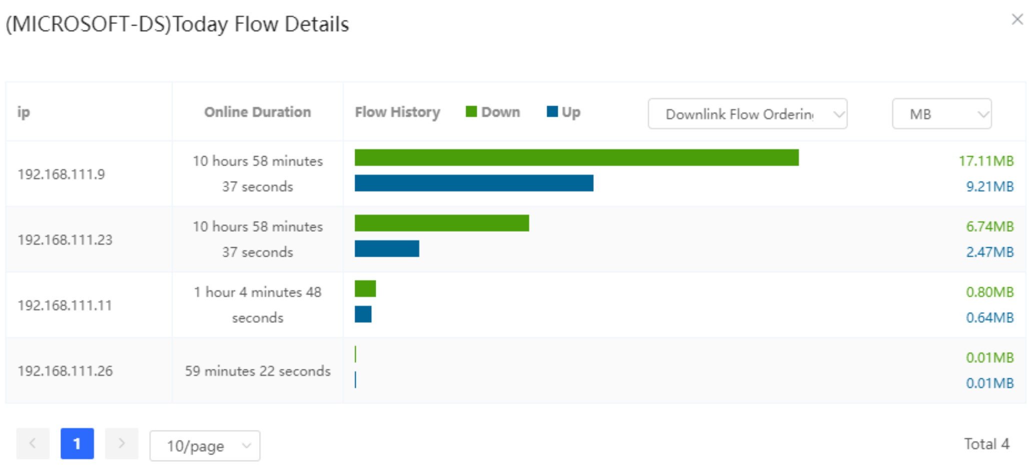
Flow-audit Switch:

No.	App	Application Group	Flow History 🟩 Down 🟦 Up · Downlink Flow Ordering · MB	Detailed
1	OTHER-TCP	other	289.87MB 5.71MB	Detailed
2	OperaNews	other	152.82MB 5.52MB	Detailed
3	HTTPS	other	131.78MB 77.56MB	Detailed
4	HTTP-BROWSE	other	70.38MB 8.26MB	Detailed
5	WeChat	Communication	44.19MB 24.75MB	Detailed
6	BY_PASS_APP	other	18.54MB 0.37MB	Detailed
7	Window-Remote	other	13.27MB 304.32MB	Detailed
8	HTTP-Single-Threaded	other	8.14MB 0.24MB	Detailed
9	OTHER-UDP	other	5.12MB 2.84MB	Detailed
10	other-app	other	2.96MB 0.13MB	Detailed

< 1 2 3 > 10/page Total 27

d View traffic details of an app.

Click **Detailed**. The pop-up page displays details about the traffic of each user who uses the current app. You can set the sorting mode (by downlink traffic or uplink traffic), unit, and other parameters based on service requirements.

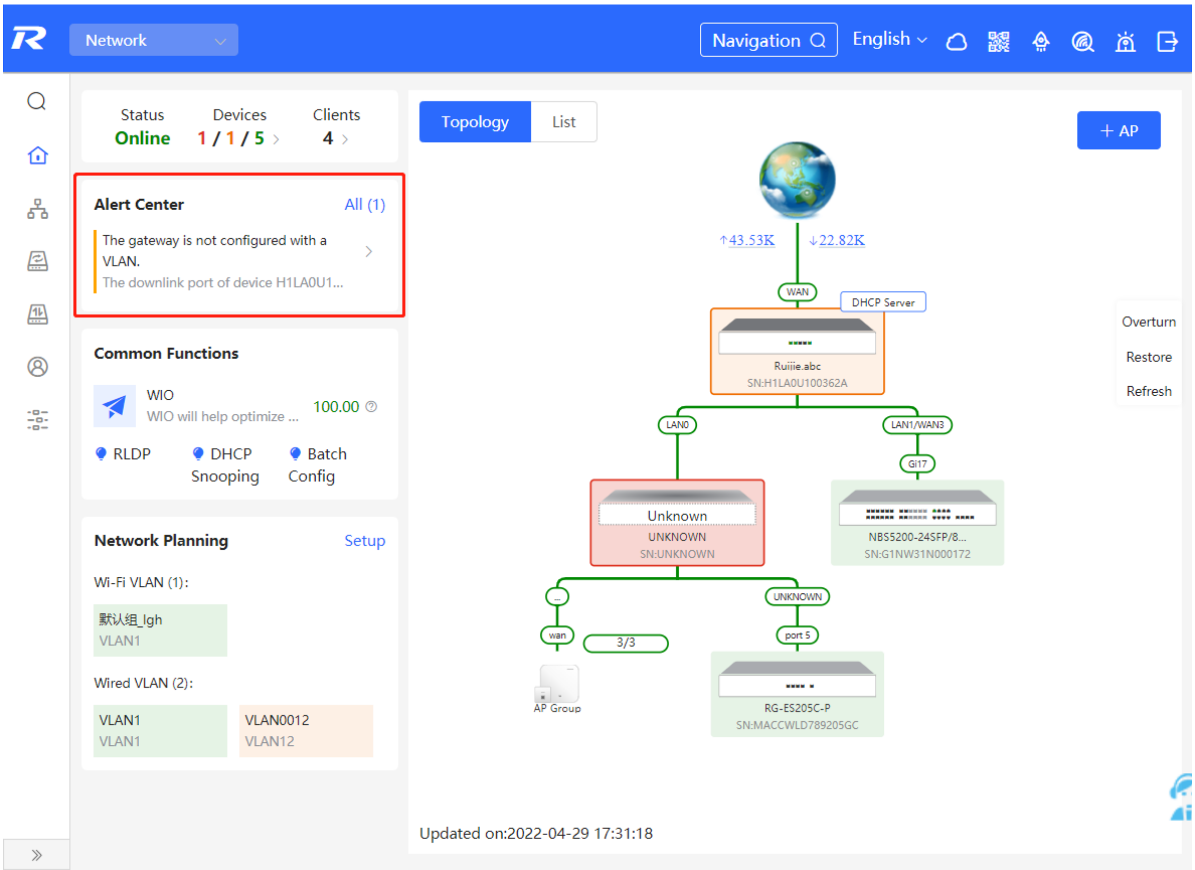


(MICROSOFT-DS)Today Flow Details

ip	Online Duration	Flow History 🟩 Down	🟦 Up
192.168.111.9	10 hours 58 minutes 37 seconds	17.11MB	9.21MB
192.168.111.23	10 hours 58 minutes 37 seconds	6.74MB	2.47MB
192.168.111.11	1 hour 4 minutes 48 seconds	0.80MB	0.64MB
192.168.111.26	59 minutes 22 seconds	0.01MB	0.01MB

2.5 Processing Alerts

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

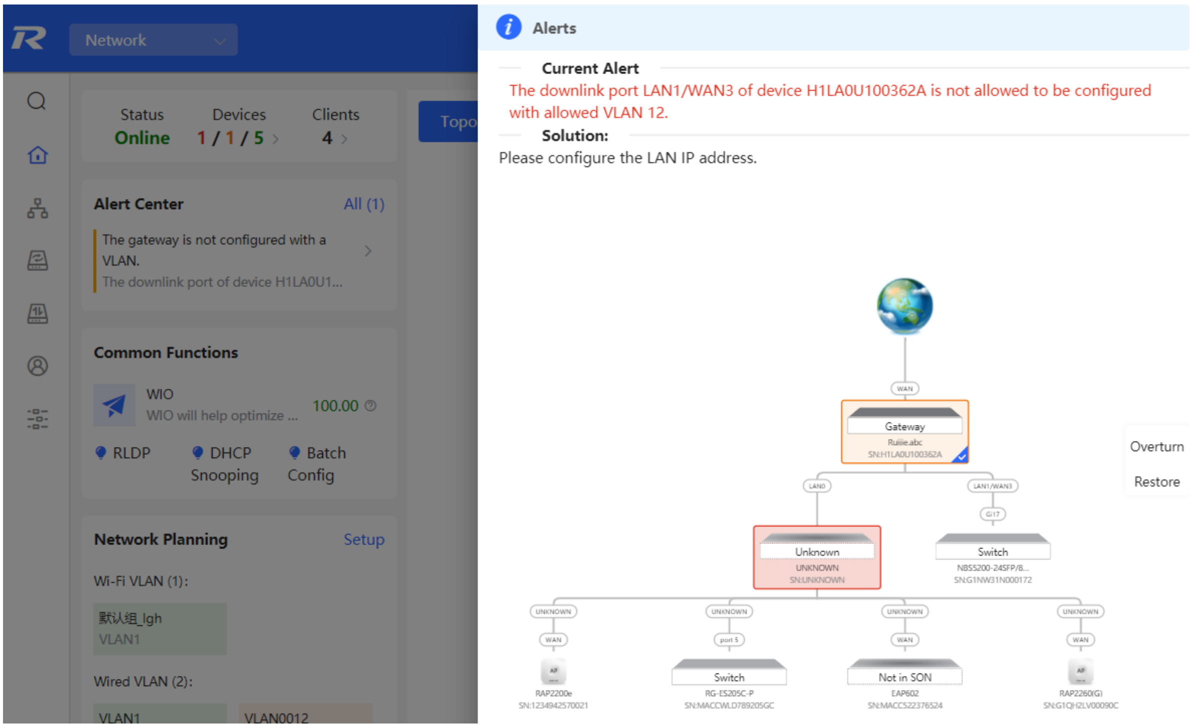


Alert Center All (1)

The gateway is not configured with a VLAN.
The downlink port of device H1LA0U1...

Status: Online
Devices: 1 / 1 / 5
Clients: 4

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



Alerts

Current Alert

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

Solution:

Please configure the LAN IP address.

Alert Center All (1)

The gateway is not configured with a VLAN.

The downlink port of device H1LA0U1...

3 Network Settings

3.1 Switching the Work Mode

3.1.1 Work Mode

For details, see Work Mode.

3.1.2 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 1.8 .) Find the configuration entry for this function according to the instructions in Configuration Steps below.

3.1.3 Configuration Steps

Note

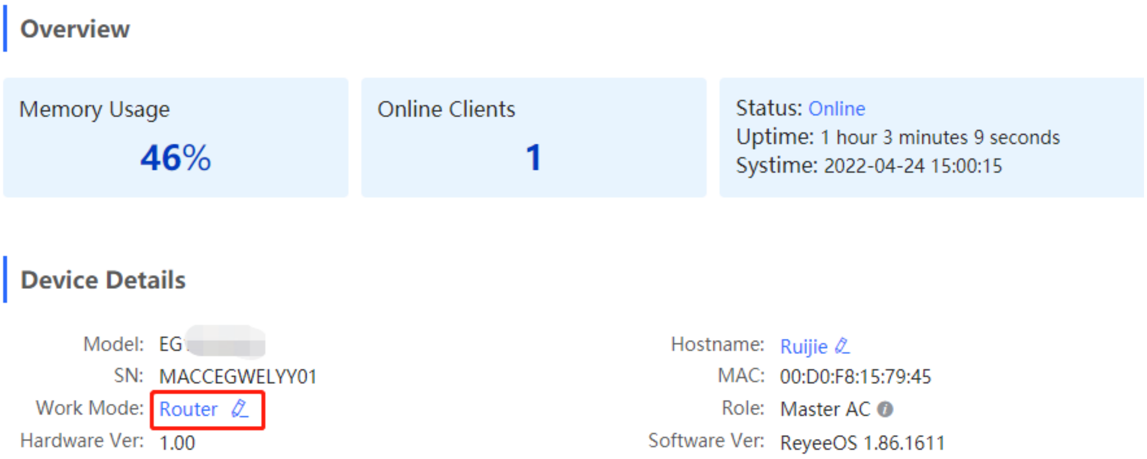
To modify the work mode to wireless repeater, see 错误!未找到引用源。.

Choose **Local Device** > **Overview** > **Device Details**.

Click the current work mode to change the work mode.

Caution

After you switch the work mode, the device will restore factory settings and the device IP address may change. You need to access the Web system again using the new IP address. Exercise caution when performing this operation.



Overview

Memory Usage
46%

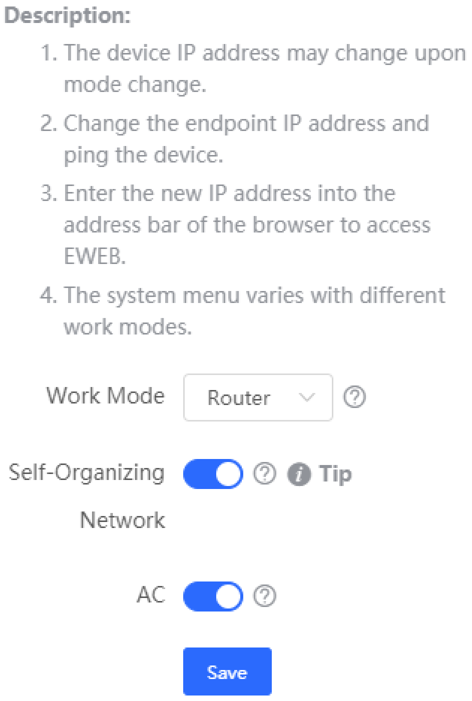
Online Clients
1

Status: Online
Uptime: 1 hour 3 minutes 9 seconds
Systime: 2022-04-24 15:00:15

Device Details

Model: EG[redacted]
SN: MACCEGWELYY01
Work Mode: Router
Hardware Ver: 1.00
Hostname: Ruijie
MAC: 00:D0:F8:15:79:45
Role: Master AC
Software Ver: ReyeeOS 1.86.1611

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.



Description:

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

Work Mode: Router

Self-Organizing Network: ON

AC: ON

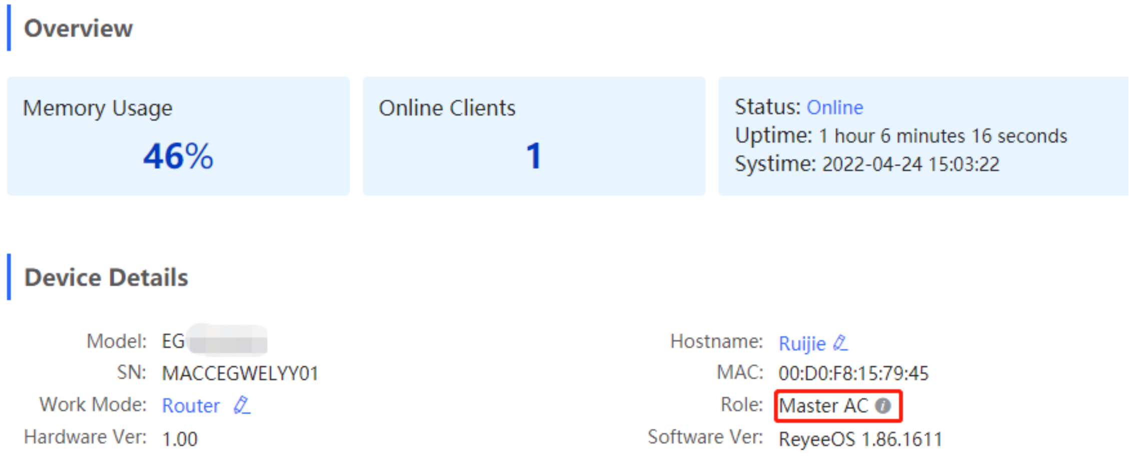
3.1.4 Viewing the Self-Organizing Role

Choose **Local Device** > **Overview** > **Device Details**.

After the self-organizing network discovery function is enabled, you can view the self-organizing role of the device on the **Device Details** page.

Master AP/AC: The device functions as an AC to manage downlink devices.

Slave AP: The device connects to the AC in self-organizing mode and is managed by the AC. Slave APs are uniformly managed by the master AP/AC. Some wireless network configurations cannot be modified separately in local mode, and must be delivered by the master AP/AC.



Overview

Memory Usage
46%

Online Clients
1

Status: Online
Uptime: 1 hour 6 minutes 16 seconds
Systime: 2022-04-24 15:03:22

Device Details

Model: EG[redacted]
SN: MACCEGWELYY01
Work Mode: Router
Hardware Ver: 1.00

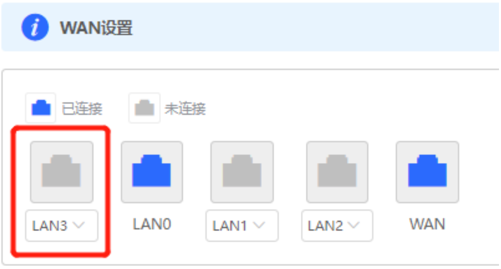
Hostname: Ruijie
MAC: 00:D0:F8:15:79:45
Role: Master AC
Software Ver: ReyeeOS 1.86.1611

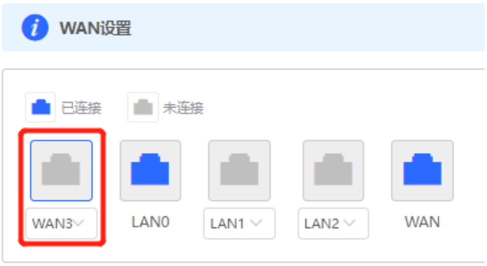
3.2 Configuring the WAN Ports

Choose **Local Device** > **Basics** > **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 ports.

- The number of lines supported varies with the product. The actual configuration prevails.
- If the LAN/WAN switchover can be configured, click the port to switch between the LAN and WAN modes.





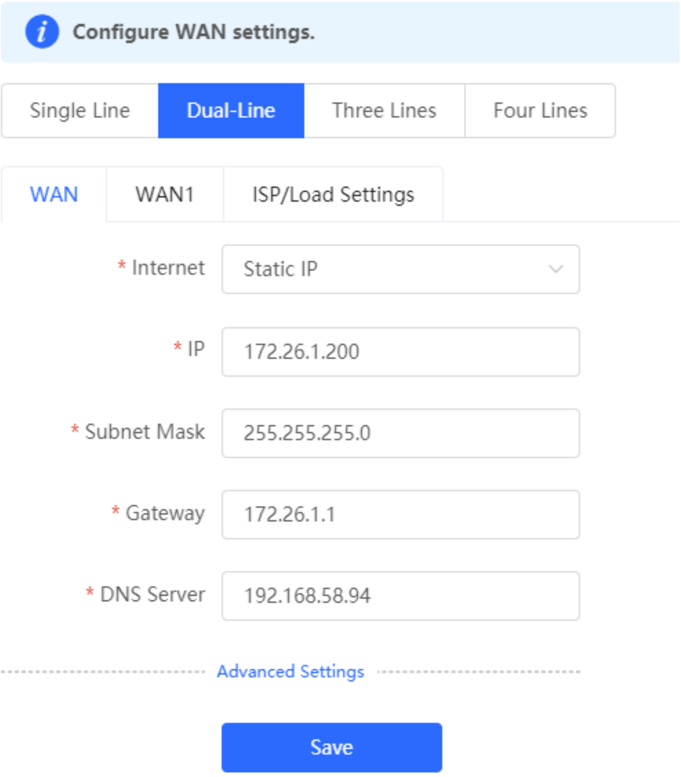
The number of the WAN ports and lines will change through LAN/WAN switchover. The actual number prevails,

3.2.1 Configuring the Internet Access Mode

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 Creating a Network Project.

Choose **Local Device** > **Basics** > **WAN**

Select the target WAN port and configure **Internet** by selecting PPPoE, DHCP or Static IP from the drop-down list box.



Configure WAN settings.

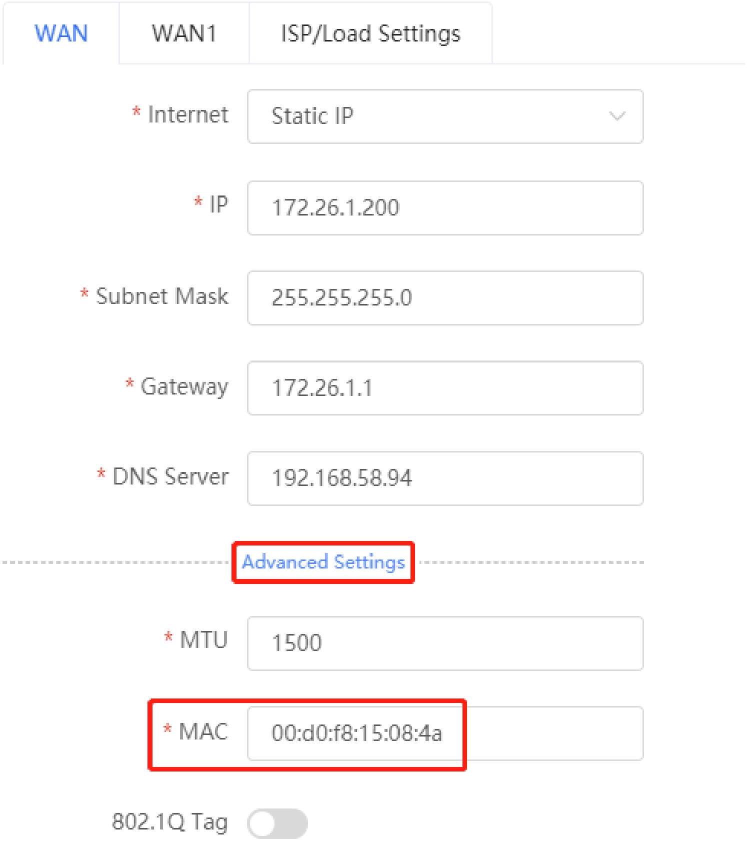
* Internet: Static IP
* IP: 172.26.1.200
* Subnet Mask: 255.255.255.0
* Gateway: 172.26.1.1
* DNS Server: 192.168.58.94

3.2.2 Modifying the MAC Address

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 ports to valid MAC addresses.

Choose **Local Device** > **Basics** > **WAN**

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



* Internet: Static IP

* IP: 172.26.1.200

* Subnet Mask: 255.255.255.0

* Gateway: 172.26.1.1

* DNS Server: 192.168.58.94

* MTU: 1500

* MAC: 00:d0:f8:15:08:4a

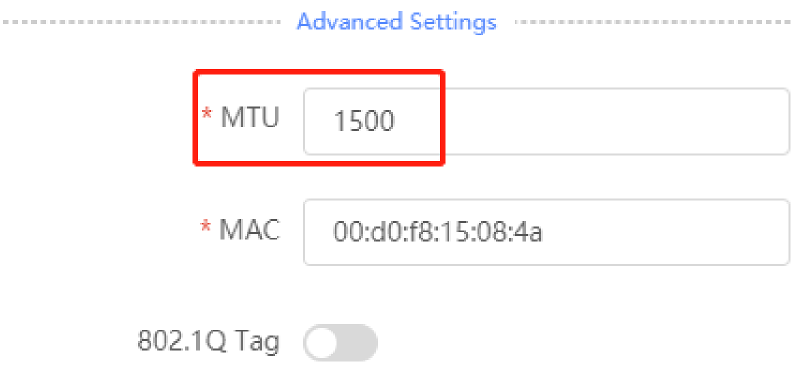
802.1Q Tag

3.2.3 Modifying the MTU

MTU specifies the maximum transmission unit allowed to pass a WAN port. By default, the MTU of a WAN port 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 set the MTU to a smaller value.

Choose **Local Device** > **Basics** > **WAN**

Select the target WAN port. Click **Advanced Settings**, enter a MTU value, and click **Save**.



* MTU: 1500

* MAC: 00:d0:f8:15:08:4a

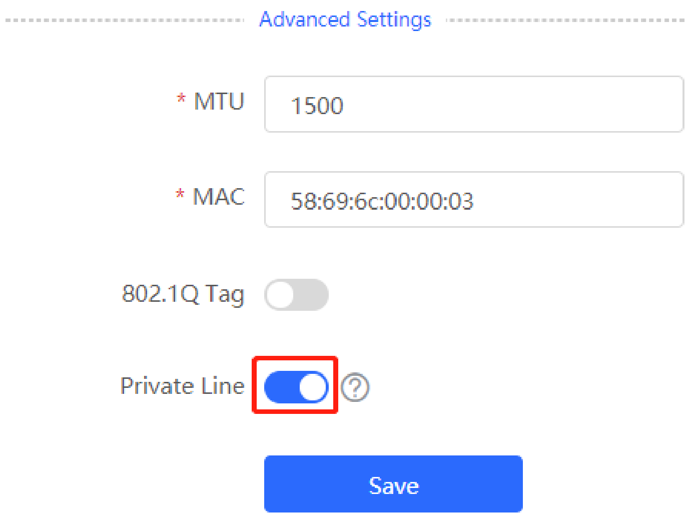
802.1Q Tag

3.2.4 Configuring the Private Line

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.

Choose **Local Device** > **Basics** > **WAN**

Select the target WAN port. Click **Advanced Settings**, enable **Private Line**, and click **Save**.



Advanced Settings

* MTU 1500

* MAC 58:69:6c:00:00:03

802.1Q Tag

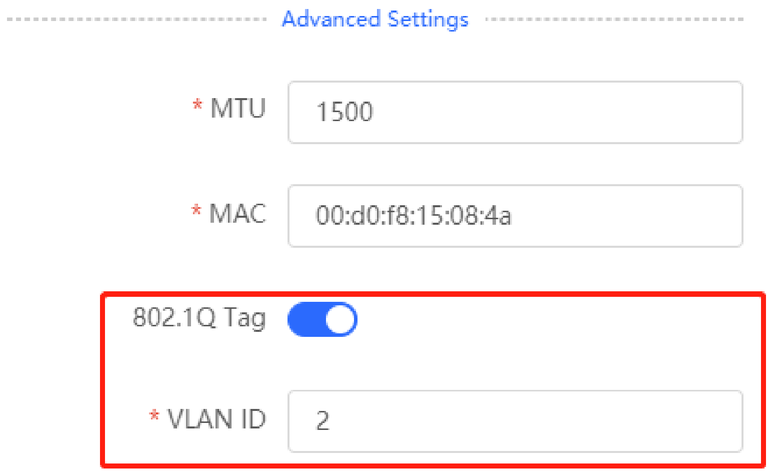
Private Line

3.2.5 Configuring the VLAN Tag

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

Choose **Local Device** > **Basics** > **WAN**

Select the target WAN port. Click **Advanced Settings**, enable **802.1Q Tag**, and click **Save**.



Advanced Settings

* MTU 1500

* MAC 00:d0:f8:15:08:4a

802.1Q Tag

* VLAN ID 2

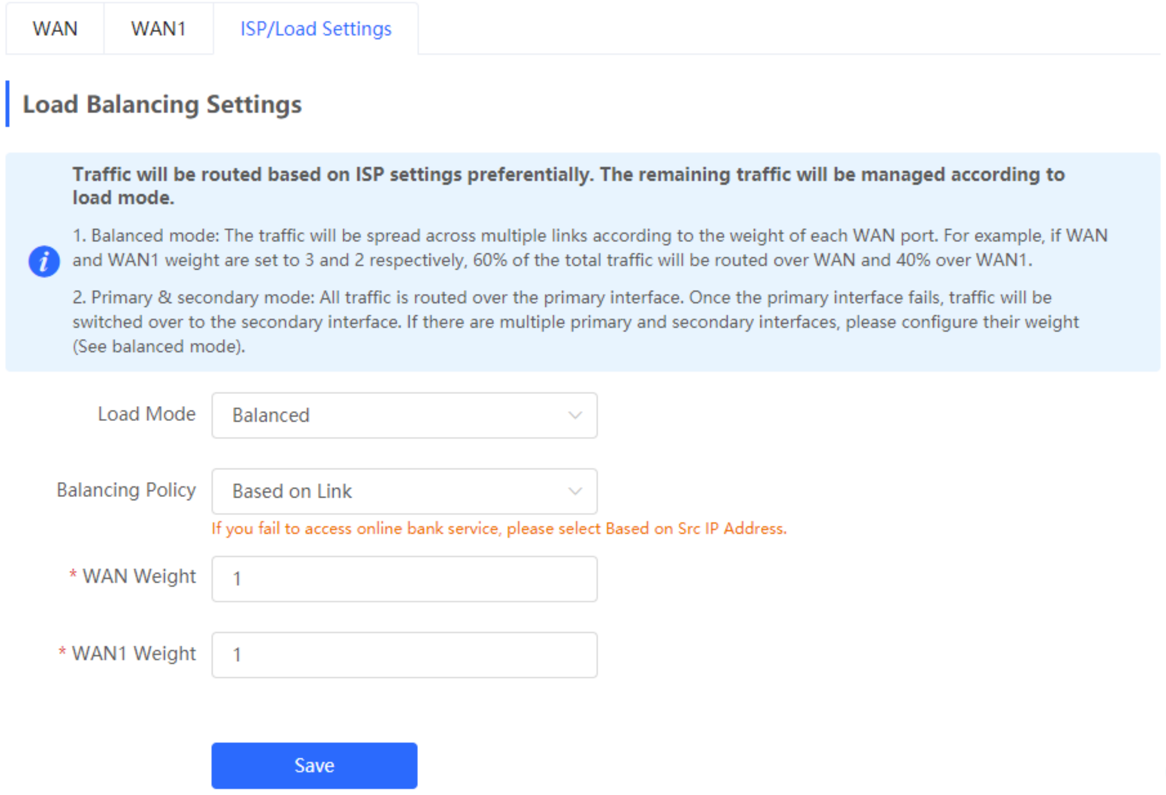
3.2.6 Configuring the Multi-Line Load Balancing Mode

Choose **Local Device** > **Basics** > **WAN** > **Single Line/Dual-Line/Three Lines/Four Lines** > **ISP/Load Settings** > **Load Balancing Settings**.

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

Table 3-1 Load balancing modes

Load Balancing Mode	Description
Balanced	The traffic will be spread across multiple links according to the weight of each WAN port. Larger traffic will be distributed to the WAN port with a higher weight. When you select this mode, you must specify the weight of each WAN port. For example, if WAN and WAN 1 weight are set to 3 and 2 respectively, 60% of the total traffic will be routed over WAN and 40% over WAN 1.
Primary & 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, please configure their wight. (See balanced mode.)



Load Balancing Settings

Traffic will be routed based on ISP settings preferentially. The remaining traffic will be managed according to load mode.

1. Balanced mode: The traffic will be spread across multiple links according to the weight of each WAN port. For example, if WAN and WAN1 weight are set to 3 and 2 respectively, 60% of the total traffic will be routed over WAN and 40% over WAN1.

2. Primary & secondary mode: 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 and secondary interfaces, please configure their weight (See balanced mode).

Load Mode: Balanced

Balancing Policy: Based on Link

If you fail to access online bank service, please select Based on Src IP Address.

* WAN Weight: 1

* WAN1 Weight: 1

After you set the load balancing mode to balanced, you can configure load balancing policies.

Table 3-2 Load balancing policies

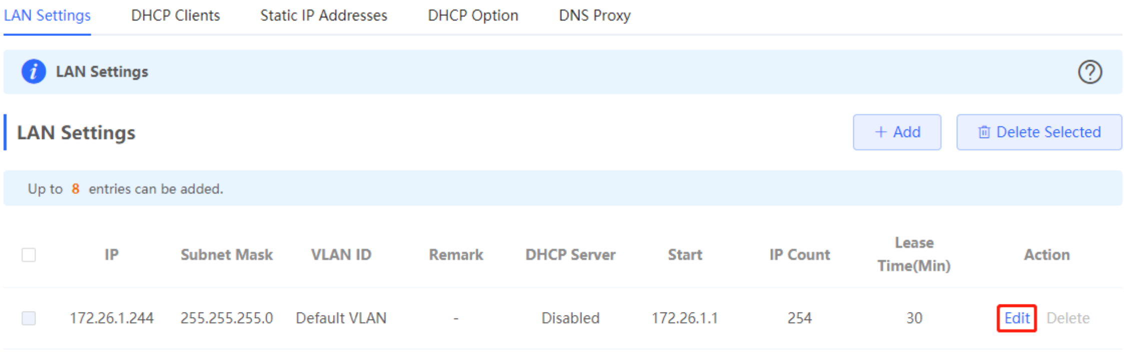
Load Balancing Policy	Description
Based on Link	After you enable this policy, the traffic is routed over multiple links based on the links. Packets with the same source IP address, destination IP address, source port, destination port, and protocol are routed over the same link.
Based on Src IP Address	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 outbound 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 outbound 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.

3.3 Configuring the LAN Ports

3.3.1 Modifying the LAN Port IP Address

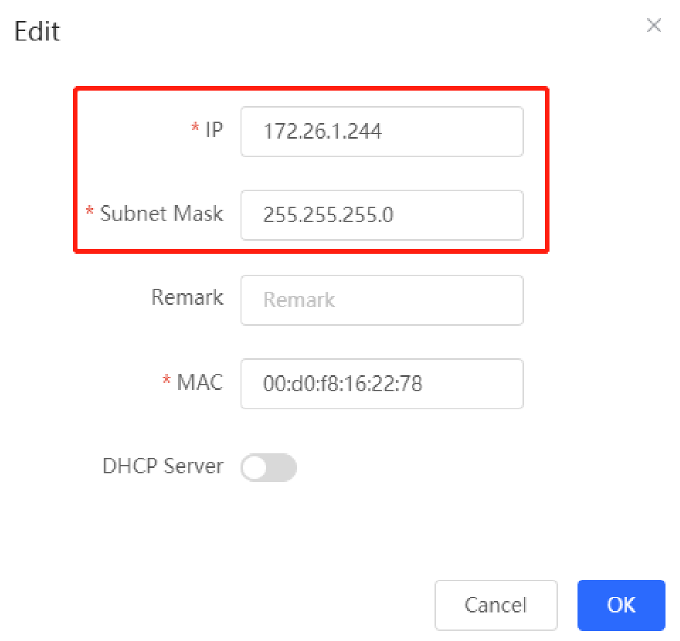
Choose **Local Device** > **Basics** > **LAN** > **LAN Settings**.

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.



Up to 8 entries can be added.

□	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
□	172.26.1.244	255.255.255.0	Default VLAN	-	Disabled	172.26.1.1	254	30	Edit Delete


Edit

* IP: 172.26.1.244

* Subnet Mask: 255.255.255.0

Remark: Remark

* MAC: 00:d0:f8:16:22:78

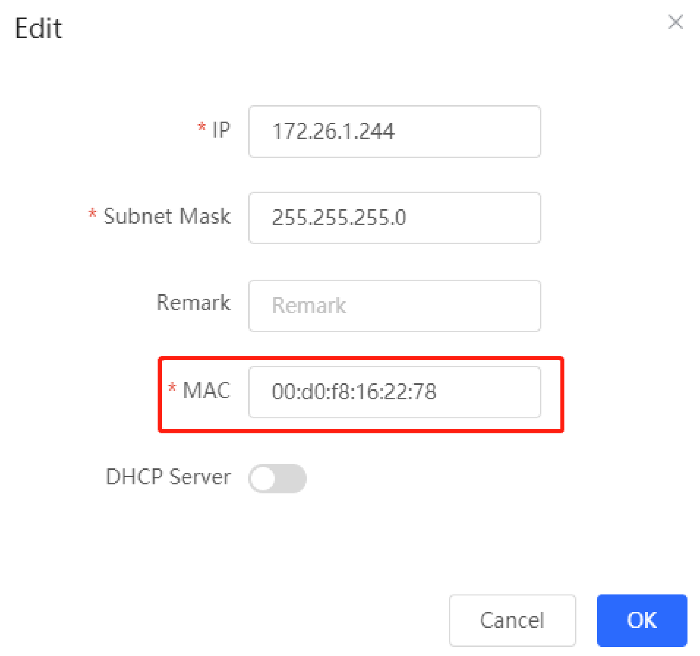
DHCP Server: ○

3.3.2 Modifying the MAC Address

Choose **Local Device** > **Basics** > **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.


Edit

* IP: 172.26.1.244

* Subnet Mask: 255.255.255.0

Remark: Remark

* MAC: 00:d0:f8:16:22:78

DHCP Server: ○

3.4 Configuring VLAN

3.4.1 VLAN Overview

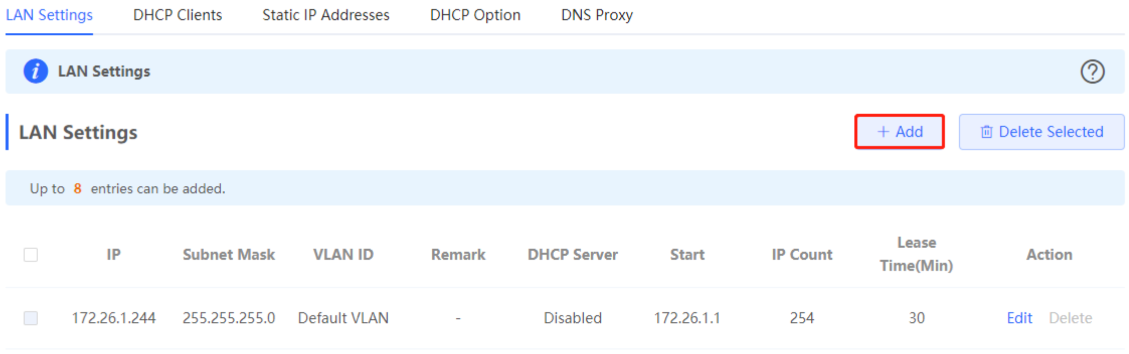
Virtual Local Area Network (VLAN) is a communication technology that divides a physical LAN into multiple logical broadcast domains. Each VLAN has independent broadcast domains. Hosts in the same VLAN can directly communicate with each other, while hosts in different VLANs cannot as they are isolated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

3.4.2 Creating a VLAN

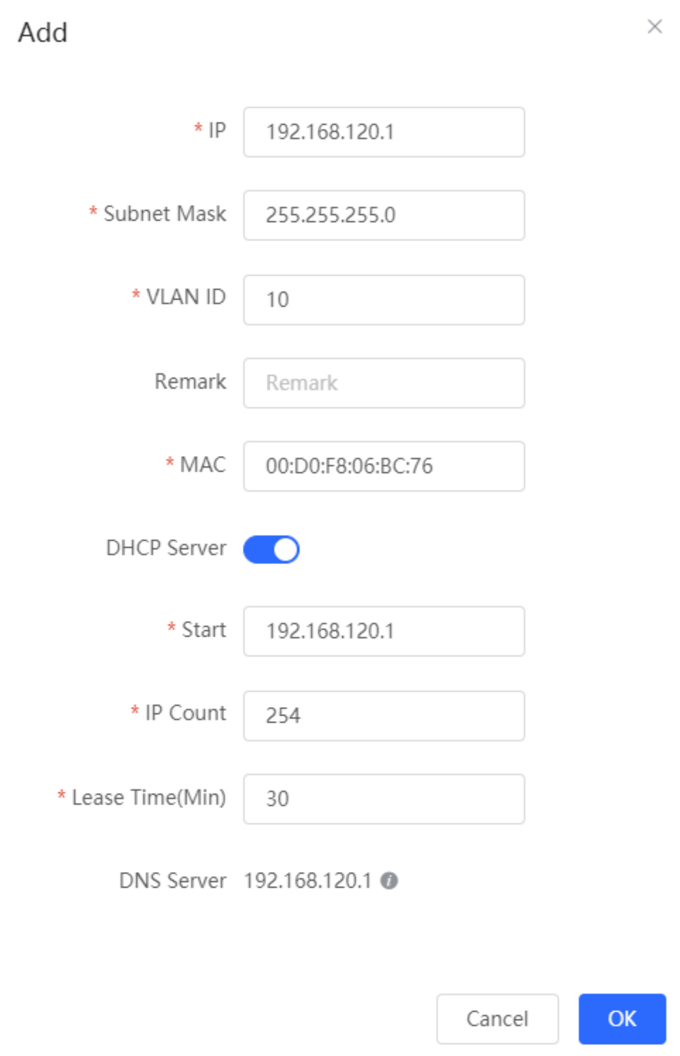
Choose **Local Device** > **Basics** > **LAN** > **LAN Settings**.

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



Up to 8 entries can be added.

□	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
□	172.26.1.244	255.255.255.0	Default VLAN	-	Disabled	172.26.1.1	254	30	Edit Delete



Add

* IP	192.168.120.1
* Subnet Mask	255.255.255.0
* VLAN ID	10
Remark	Remark
* MAC	00:D0:F8:06:BC:76
DHCP Server	●
* Start	192.168.120.1
* IP Count	254
* Lease Time(Min)	30
DNS Server	192.168.120.1

Table 3-3 VLAN configuration

Parameter	Description
IP	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.
Remark	Enter the VLAN description.
MAC	Configure an MAC address for the VLAN interface.

Parameter	Description
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 3.8.3 Configuring the DHCP.

⚠ **Caution**

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

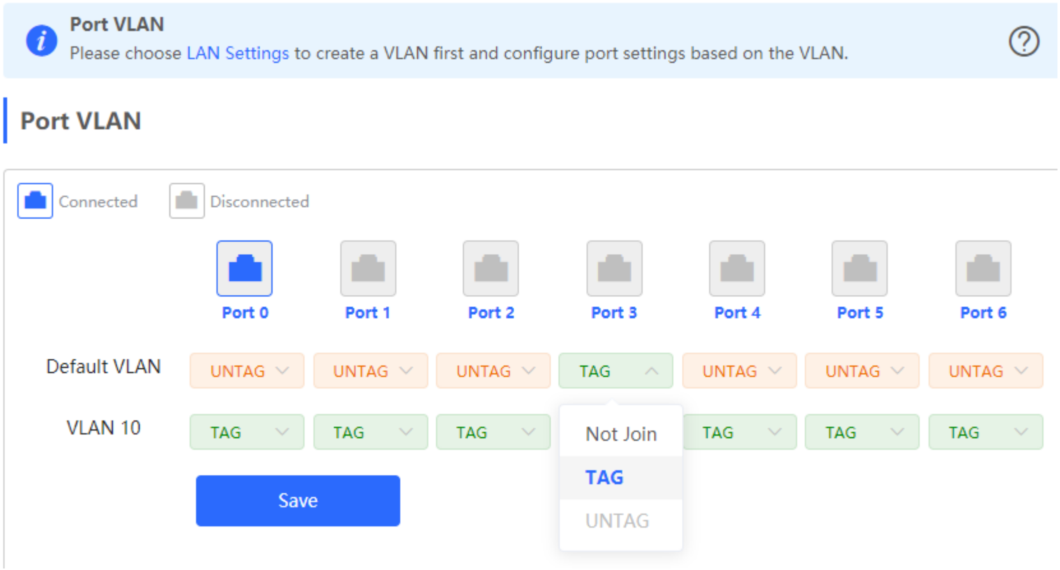
3.4.3 Configuring a Port VLAN

Choose **Local Device** > **Basics** > **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 3.4.2 Creating a VLAN.

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

- **UNTAG**: 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 UNTAG.
- **TAG**: 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.
- **Not Join**: Configure the port to deny packets with this VLAN ID to pass. For example, if you set VLAN 10 and VLAN 20 to **Not Join** for port 2, port 2 will not receive packets from VLAN 10 and VLAN 20.



Port VLAN
Please choose LAN Settings to create a VLAN first and configure port settings based on the VLAN.

Port VLAN

Connected Disconnected

	Port 0	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6
Default VLAN	UNTAG	UNTAG	UNTAG	TAG	UNTAG	UNTAG	UNTAG
VLAN 10	TAG	TAG	TAG		TAG	TAG	TAG

3.5 Configuring Repeater Mode

3.5.1 Wired Repeater

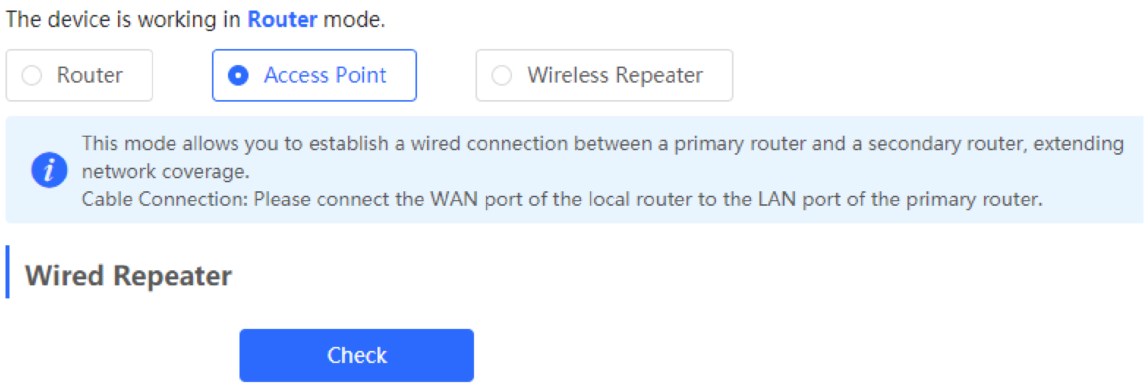
Choose **Local Device** > **Basics** > **Repeater Mode**.

Connect a network cable from the WAN port (uplink LAN port) of the device to the upper-layer device.

Select **Access Point**, click **Check**, confirm the Wi-Fi settings of the AP, and then click **Save** to expand the network coverage.

Caution

After the configuration is saved, connected clients will be disconnected from the network for a short period of time. You can reconnect the clients to the Wi-Fi network for restoration.



The device is working in **Router** mode.

○ Router ● Access Point ○ Wireless Repeater

This mode allows you to establish a wired connection between a primary router and a secondary router, extending network coverage.
Cable Connection: Please connect the WAN port of the local router to the LAN port of the primary router.

3.5.2 Wireless Repeater

The wireless repeater mode extends the Wi-Fi coverage range of the primary device. The device supports the dual-link wireless repeater mode and can extend both 2.4 GHz and 5 GHz signals of the primary device.

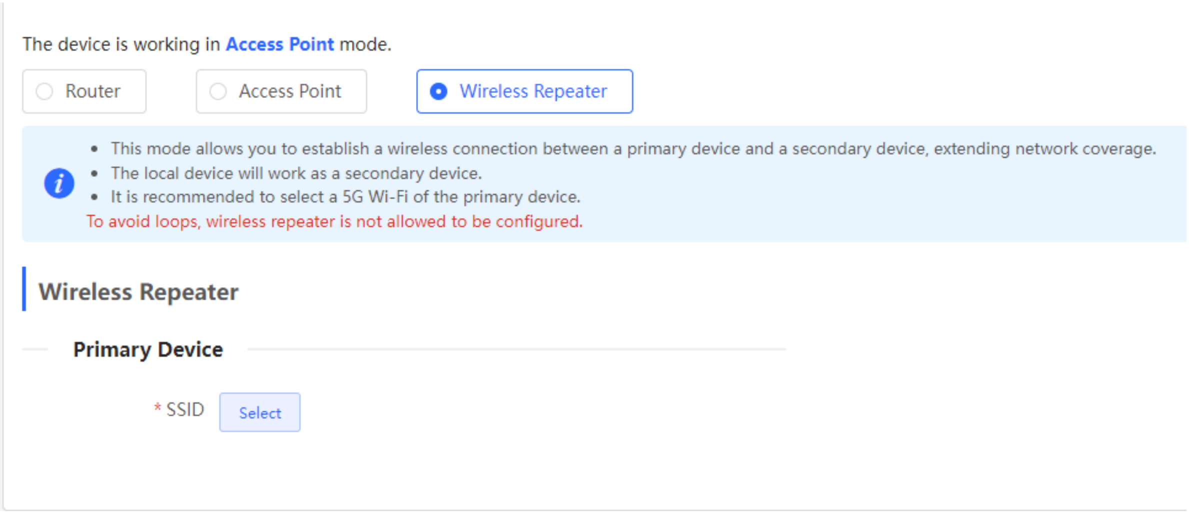
Note

To avoid loops in wireless repeater mode, remove the network cable from the WAN port.

Obtain the SSID and Wi-Fi password of the upper-layer router.

Choose **Local Device** > **Basics** > **Repeater Mode**.

(1) Click **Wireless Repeater** and then click **Select**. A list of surrounding Wi-Fi signals pops up. A list of nearby 5 GHz Wi-Fi networks is displayed by default. You can switch from 5 GHz to 2.4 GHz band by selecting **2.4G** from the drop-down list box. You are advised to select a strong 5 GHz Wi-Fi network signal.



The device is working in **Access Point** mode.

○ Router ○ Access Point ● Wireless Repeater

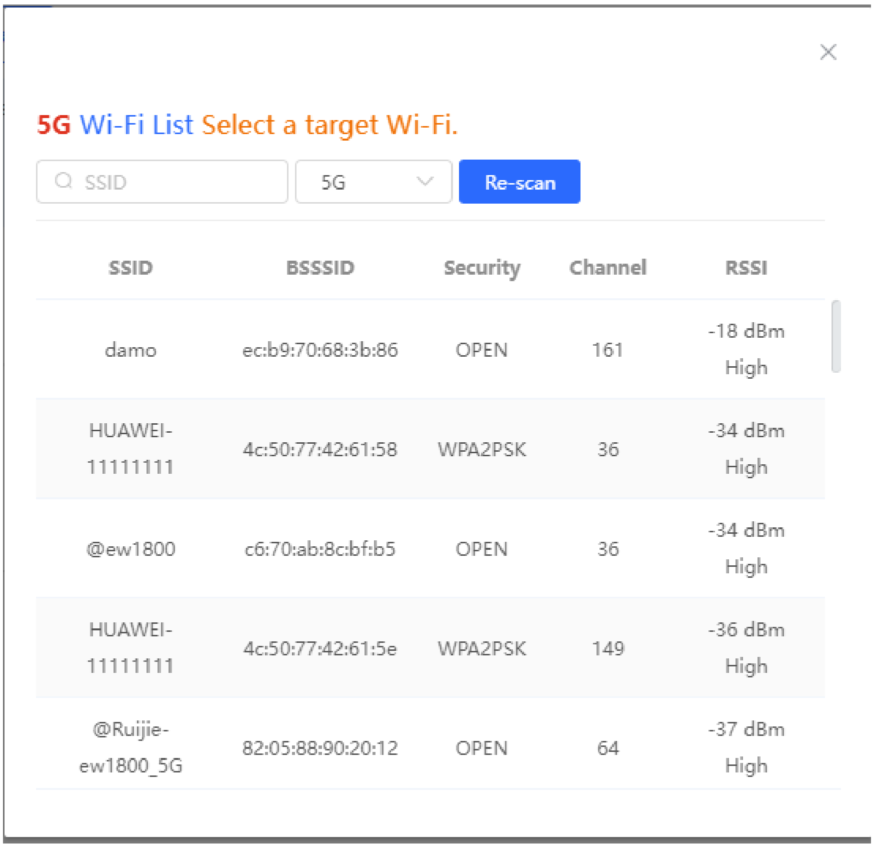
- This mode allows you to establish a wireless connection between a primary device and a secondary device, extending network coverage.
- The local device will work as a secondary device.
- It is recommended to select a 5G Wi-Fi of the primary device.

To avoid loops, wireless repeater is not allowed to be configured.

Wireless Repeater

Primary Device

* SSID



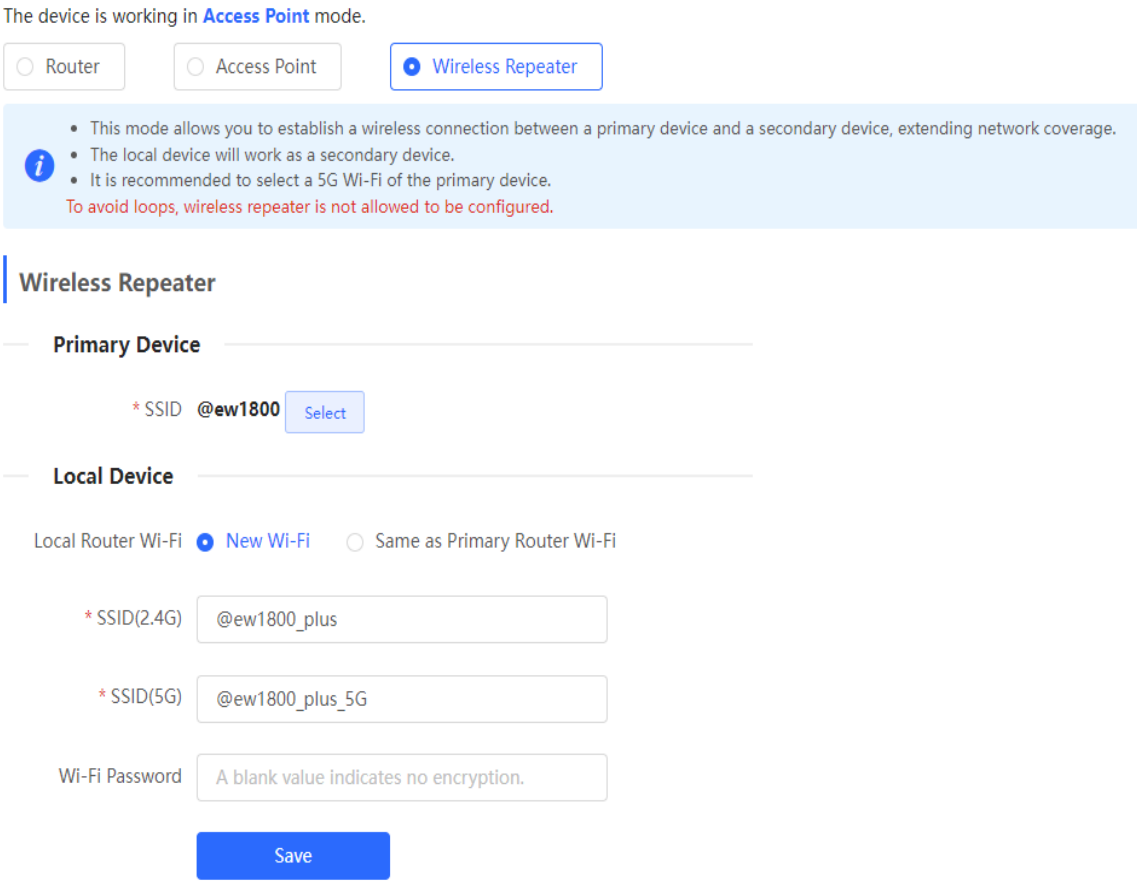
5G Wi-Fi List Select a target Wi-Fi.

SSID	BSSSID	Security	Channel	RSSI
damo	ec:b9:70:68:3b:86	OPEN	161	-18 dBm High
HUAWEI-11111111	4c:50:77:42:61:58	WPA2PSK	36	-34 dBm High
@ew1800	c6:70:ab:8c:bf:b5	OPEN	36	-34 dBm High
HUAWEI-11111111	4c:50:77:42:61:5e	WPA2PSK	149	-36 dBm High
@Ruijie-ew1800_5G	82:05:88:90:20:12	OPEN	64	-37 dBm High

(2) Select the Wi-Fi signal of the primary router that you want to extend. The configuration items of the local device are displayed. If the signal of the upper-layer device is encrypted, enter the Wi-Fi password of the upper-layer device.

(3) Configure **Local Router Wi-Fi**. You can select **New Wi-Fi** or **Same as Primary Router Wi-Fi**.

- If you select **Same as Primary Router Wi-Fi**, the Wi-Fi settings of the router are automatically synchronized with those on the primary router. Generally, clients merge Wi-Fi signals with the same name into one Wi-Fi signal, and they can search out only the Wi-Fi signal of the primary router.
- If **New Wi-Fi** is selected, you can set a local SSID and password. Clients will search out different Wi-Fi signals.



The device is working in **Access Point** mode.

○ Router ○ Access Point ● Wireless Repeater

- This mode allows you to establish a wireless connection between a primary device and a secondary device, extending network coverage.
- The local device will work as a secondary device.
- It is recommended to select a 5G Wi-Fi of the primary device.

To avoid loops, wireless repeater is not allowed to be configured.

Wireless Repeater

Primary Device

* SSID **@ew1800** Select

Local Device

Local Router Wi-Fi ● New Wi-Fi ○ Same as Primary Router Wi-Fi

* SSID(2.4G) @ew1800_plus

* SSID(5G) @ew1800_plus_5G

Wi-Fi Password A blank value indicates no encryption.

Save

Caution

After the configuration is saved, the AP will be disconnected from the Wi-Fi network and needs to connect to the new Wi-Fi network. Exercise caution when performing this operation. Record the new SSID and password.

You are advised to install the AP in a position where the RSSI is greater than two bars of signal to prevent signal loss. If the signal at the installation position is too weak, the Wi-Fi extension may fail or the quality of the extended signal may be poor.

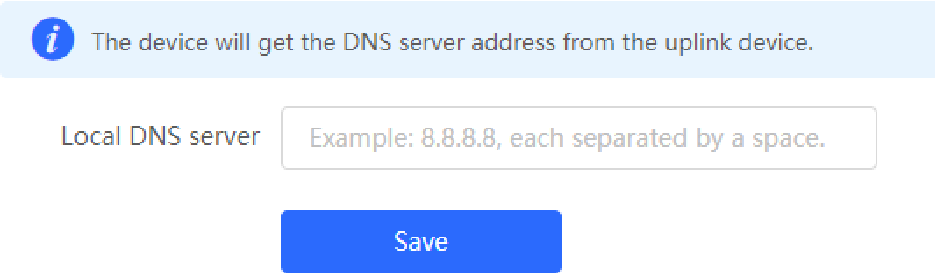
3.6 Configuring DNS

3.6.1 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.

Choose **Local Device** > **Advanced** > **Local DNS**.

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



The device will get the DNS server address from the uplink device.

Local DNS server: Example: 8.8.8.8, each separated by a space.

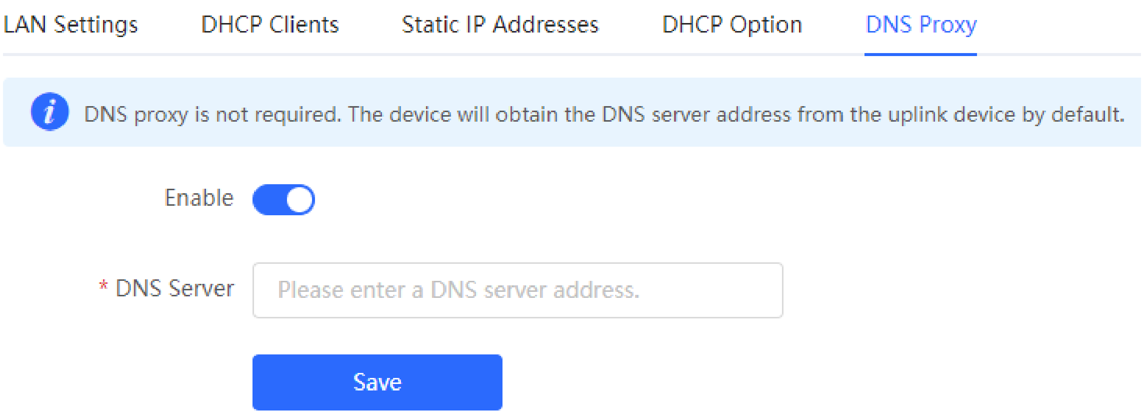
3.6.2 DNS Proxy

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

Choose **Local Device** > **Basics** > **LAN** > **LAN Settings**.

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.



DNS proxy is not required. The device will obtain the DNS server address from the uplink device by default.

Enable: ●

* DNS Server: Please enter a DNS server address.

3.7 Configuring IPv6

3.7.1 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.

3.7.2 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.

3.7.3 IPv6 Address Allocation Modes

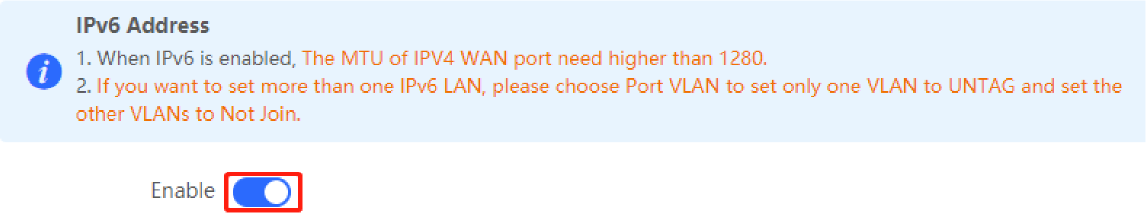
- Manual configuration: IPv6 addresses, prefixes, and other network parameters are configured manually.
- Stateless Address Autoconfiguration (SLAAC): The link-local address is generated based on the interface ID, and the IPv6 address is automatically allocated based on the prefix information in the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

3.7.4 Enabling the IPv6 Function

Choose **Local Device** > **Basics** > **IPv6 Address**.

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



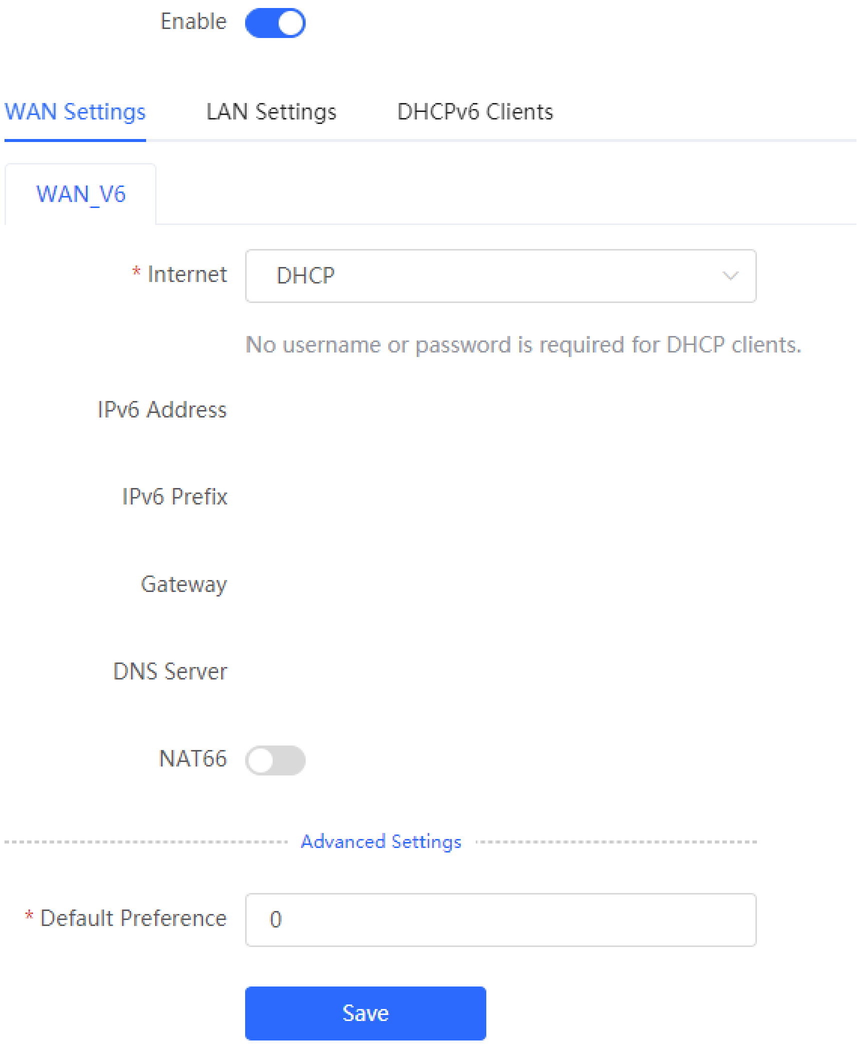
IPv6 Address

1. When IPv6 is enabled, The MTU of IPV4 WAN port need higher than 1280.
2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to UNTAG and set the other VLANs to Not Join.

3.7.5 Configuring an IPv6 Address for the WAN Port

Choose **Local Device** > **Basics** > **IPv6 Address** > **WAN Settings**.

After you enable the IPv6 function, you can set related parameters on the **WAN Settings** tab. The number of **WAN_V6** tabs indicates the number of WAN ports on the current device.



Enable

WAN Settings | LAN Settings | DHCPv6 Clients

WAN_V6

* Internet: DHCP

No username or password is required for DHCP clients.

IPv6 Address

IPv6 Prefix

Gateway

DNS Server

NAT66

Advanced Settings

* Default Preference: 0

Table 3-4 IPv6 address configuration for WAN port

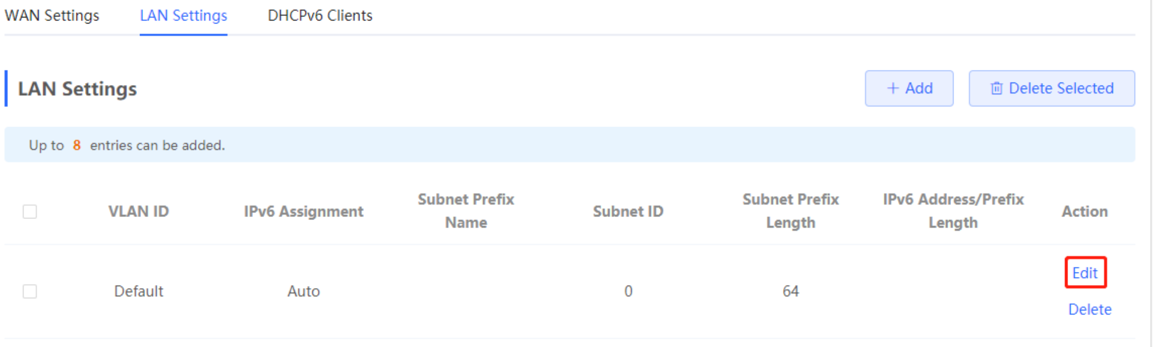
Parameter	Description
Internet	Configure a method for the WAN port to obtain an IPv6 address. **DHCP**: The current device functions as the DHCPv6 client, and it applies for an IPv6 address and prefix from the uplink network device. **Static IP**: You need to manually configure a static IPv6 address, gateway address, and DNS server. **Null**: The IPv6 function is disabled on the WAN port.
IPv6 Address	When **Internet** is set to **DHCP**, 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,** the IPv6 address prefix automatically obtained by the current device is displayed.

Parameter	Description
Gateway	When **Internet** is set to **DHCP**, 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**, 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 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.

3.7.6 Configuring an IPv6 Address for the LAN Port

Choose **Local Device** > **Basics** > **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 3.7.5 Configuring an IPv6 Address for the WAN Port.



LAN Settings

Up to 8 entries can be added.

□	VLAN ID	IPv6 Assignment	Subnet Prefix Name	Subnet ID	Subnet Prefix Length	IPv6 Address/Prefix Length	Action
□	Default	Auto		0	64		Edit Delete

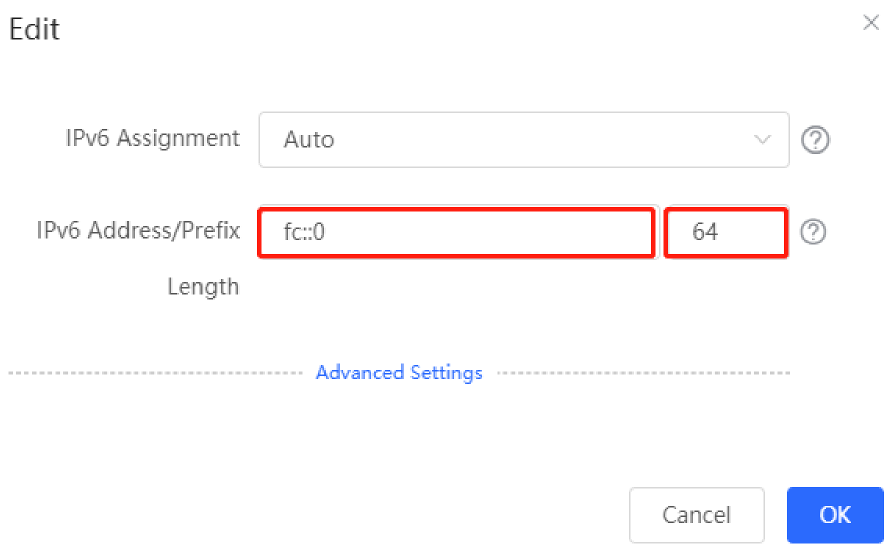
Click **Edit** next to the default VLAN, and set **IPv6 Address/Prefix Length** to a local address with no more than 64 bits. This address is also used as the IPv6 address prefix.

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**.

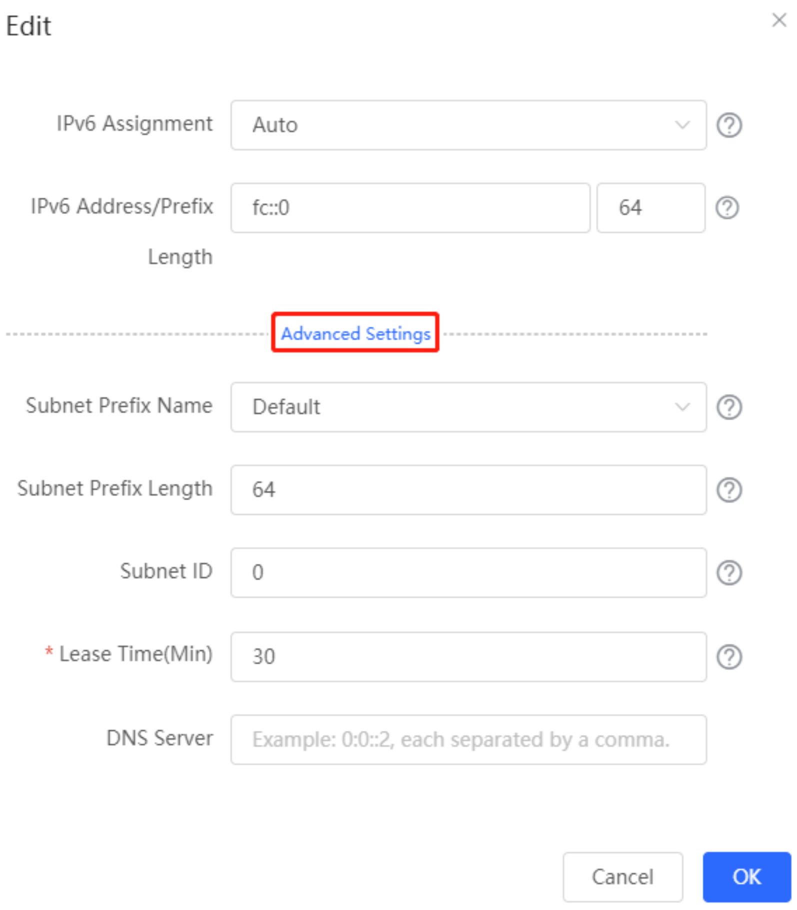


Edit

IPv6 Assignment: Auto

IPv6 Address/Prefix Length: fc::0 / 64

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



Edit

IPv6 Assignment: Auto

IPv6 Address/Prefix Length: fc::0 / 64

Subnet Prefix Name: Default

Subnet Prefix Length: 64

Subnet ID: 0

* Lease Time(Min): 30

DNS Server: Example: 0:0::2, each separated by a comma.

Table 3-5 IPv6 address configuration for LAN port

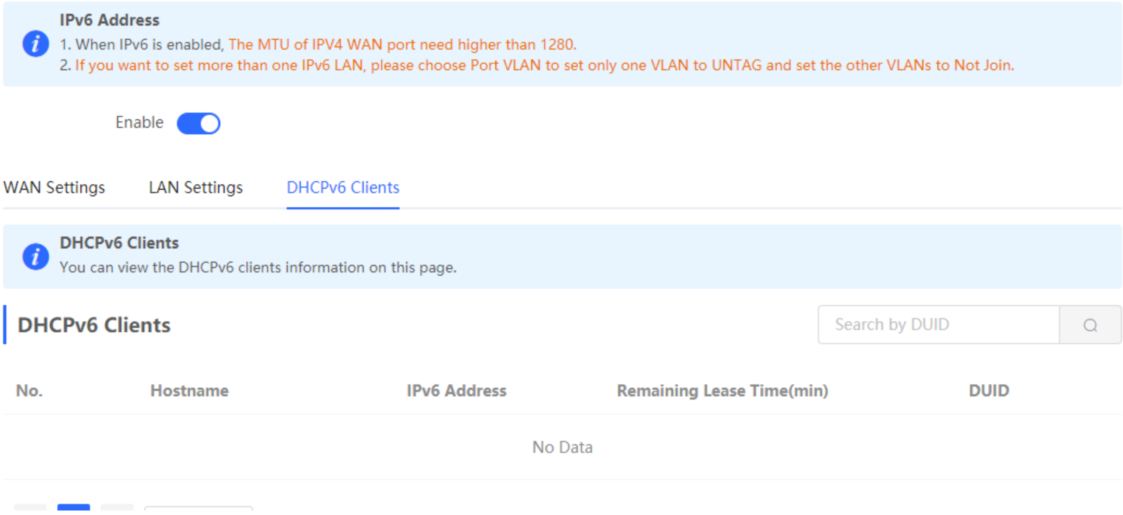
Parameter	Description
Subnet Prefix Name	Specify the interface from which the prefix is obtained, such as **WAN_V6** or **WAN1_V6**. By default, the device obtains prefixes from all interfaces.
Subnet Prefix Length	Specify the length of the subnet prefix. The value is in the range of 48 to 64.
Subnet 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.

3.7.7 Viewing the DHCPv6 Client

Choose **Local Device** > **Basics** > **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.



IPv6 Address

1. When IPv6 is enabled, The MTU of IPV4 WAN port need higher than 1280.
2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to UNTAG and set the other VLANs to Not Join.

Enable ●

WAN Settings | LAN Settings | DHCPv6 Clients

DHCPv6 Clients

You can view the DHCPv6 clients information on this page.

DHCPv6 Clients Search by DUID 🔍

No.	Hostname	IPv6 Address	Remaining Lease Time(min)	DUID
No Data				

3.8 Configuring a DHCP Server

3.8.1 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 3.7.6 Configuring an IPv6 Address for the LAN Port for more information about the DHCPv6 server function.

3.8.2 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 allocatable, the client will fail to obtain an IP address.

3.8.3 Configuring the DHCP Server

1. Configuring Basic Parameters

Choose **Local Device** > **Basics** > **LAN** > **LAN Settings**.

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.

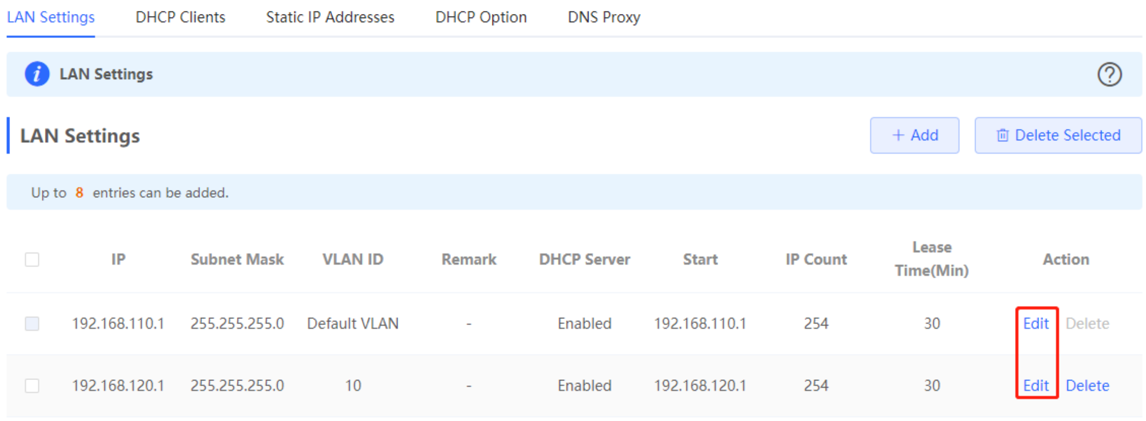
Caution

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: 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.

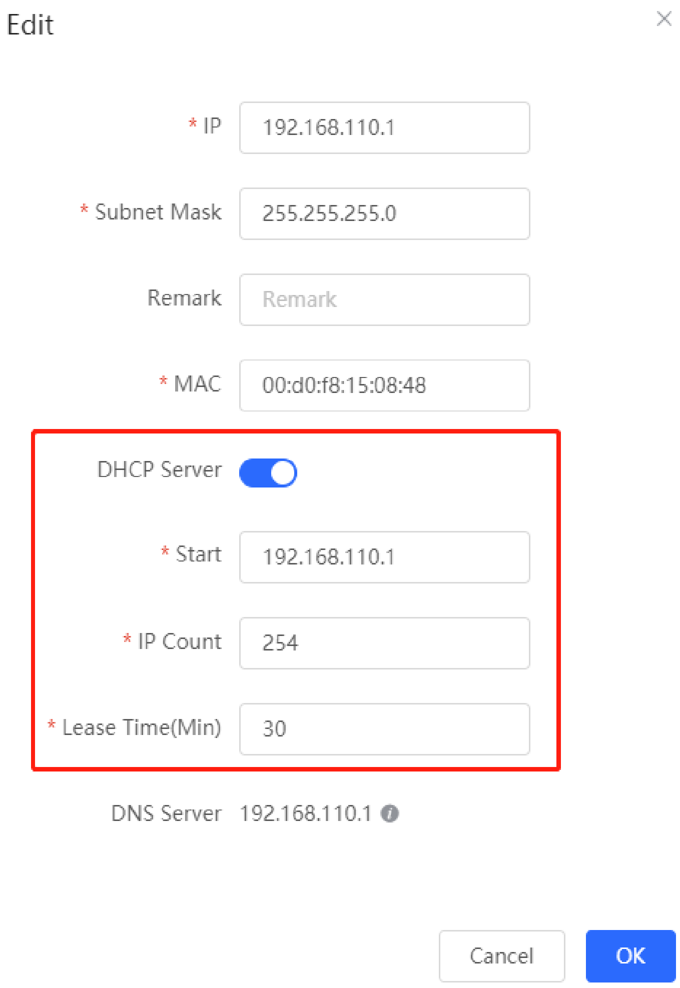
IP Count: Enter the number of IP addresses in the address pool.

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.



Up to 8 entries can be added.

□	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
□	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	254	30	Edit Delete
□	192.168.120.1	255.255.255.0	10	-	Enabled	192.168.120.1	254	30	Edit Delete



Edit

* IP: 192.168.110.1

* Subnet Mask: 255.255.255.0

Remark: Remark

* MAC: 00:d0:f8:15:08:48

DHCP Server: enabled

* Start: 192.168.110.1

* IP Count: 254

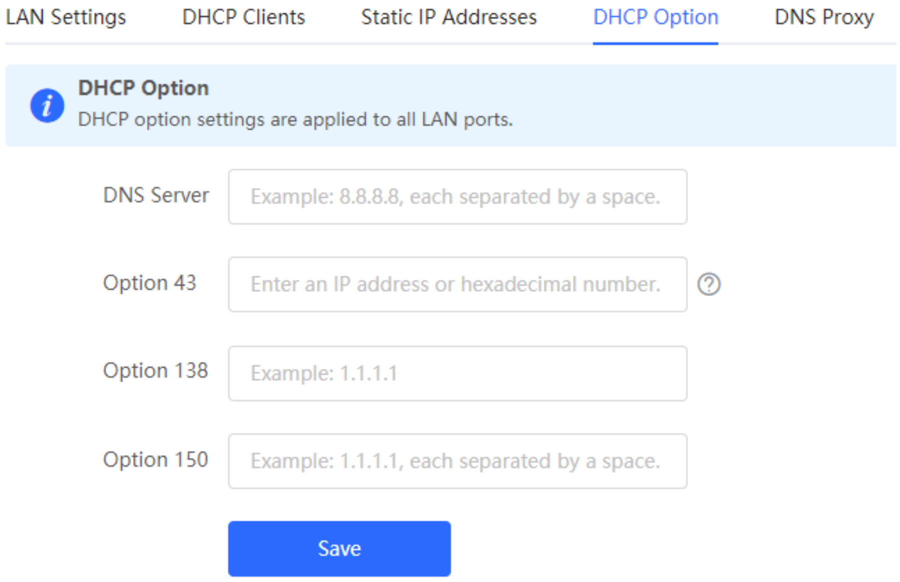
* Lease Time(Min): 30

DNS Server: 192.168.110.1

1. Configuring DHCP Option

Choose **Local Device** > **Basics** > **LAN** > **DHCP**.

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



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

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

Option 43: Enter an IP address or hexadecimal number.

Option 138: Example: 1.1.1.1

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

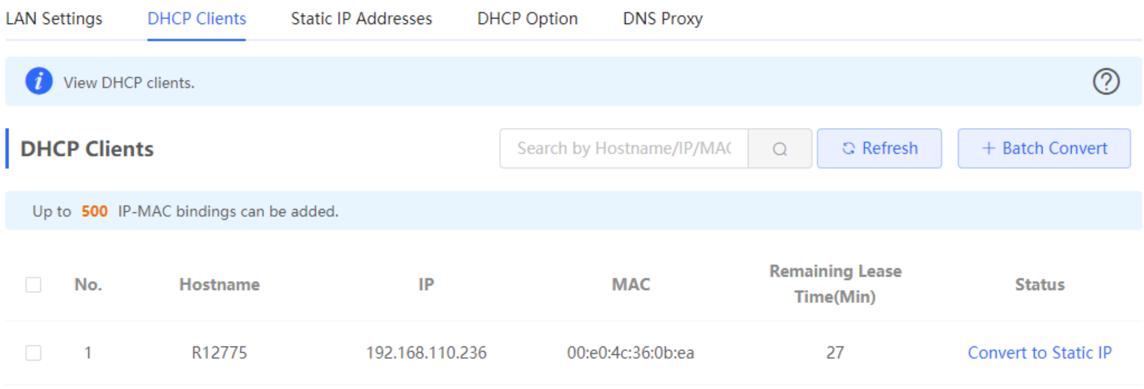
Table 3-6 DHCP Option configuration

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.

3.8.4 Viewing the DHCP Client

Choose **Local Device** > **Basics** > **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 Convert**. The dynamic address allocation relationship is added to the static address allocation list, so that the host can obtain the bound IP address for each connection. For details on how to view the static address allocation list, see Section **错误!未找到引用源。**.



View DHCP clients.

DHCP Clients

Up to 500 IP-MAC bindings can be added.

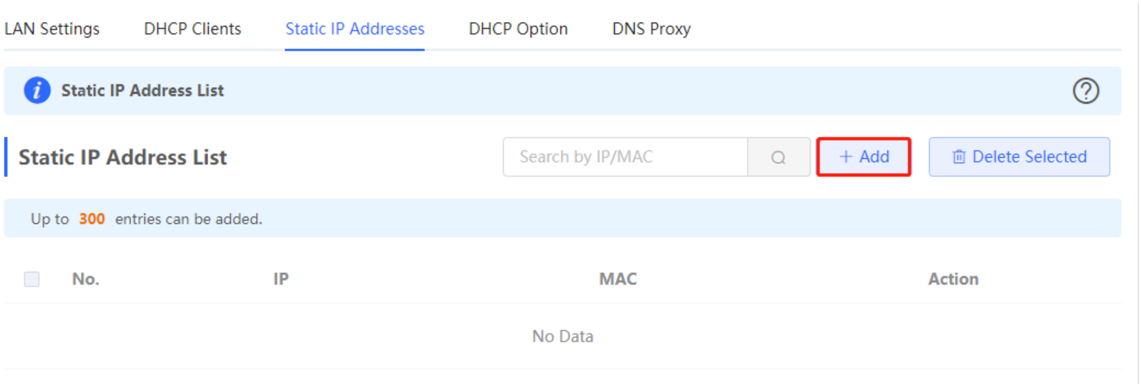
□	No.	Hostname	IP	MAC	Remaining Lease Time(Min)	Status
□	1	R12775	192.168.110.236	00:e0:4c:36:0b:ea	27	Convert to Static IP

3.8.5 Configuring Static IP Addresses

Choose **Local Device** > **Basics** > **LAN Static IP Addresses**.

The page displays all configured static IP addresses.

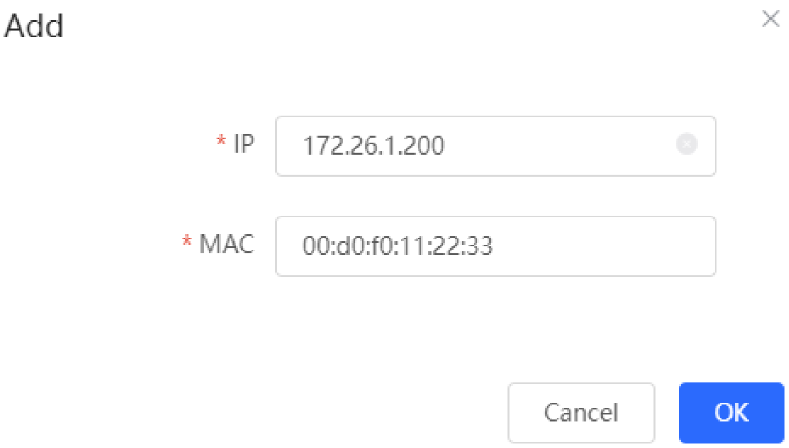
Click **Add**. In the pop-up window, enter the MAC address and IP address of the client to be bound, and click **OK**. After a static IP address is bound, the bound IP address will be obtained each time the client connects to the network.



Up to 300 entries can be added.

□	No.	IP	MAC	Action

No Data



* IP: 172.26.1.200

* MAC: 00:d0:f0:11:22:33

3.9 Static Routes

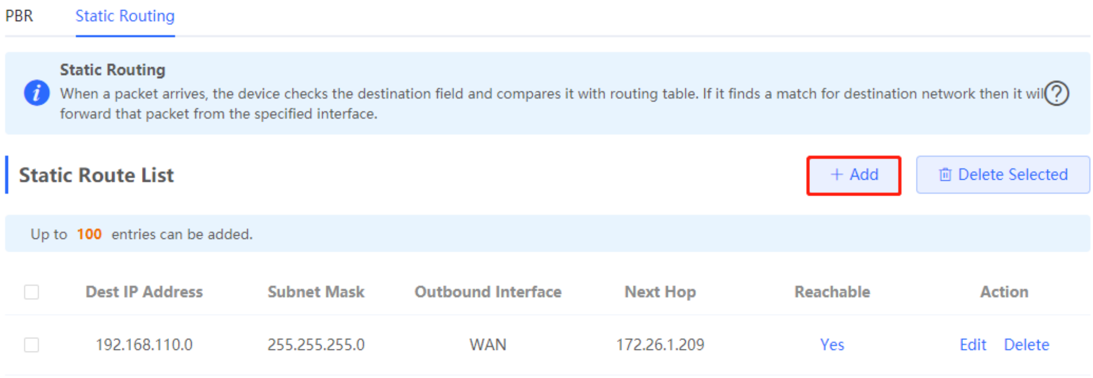
Choose **Local Device** > **Advanced** > **Routing** > **Static Routing**.

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

Caution

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

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

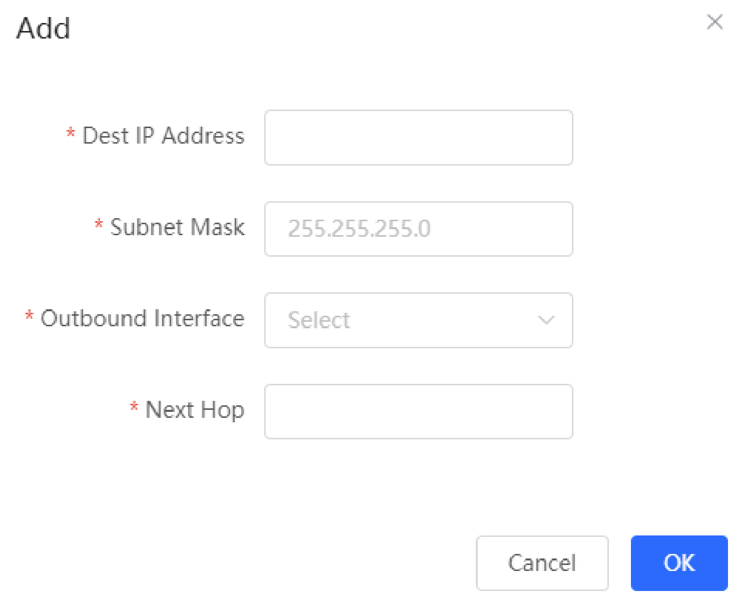


Static Routing

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

Up to 100 entries can be added.

□	Dest IP Address	Subnet Mask	Outbound Interface	Next Hop	Reachable	Action
□	192.168.110.0	255.255.255.0	WAN	172.26.1.209	Yes	Edit Delete



Add

* Dest IP Address

* Subnet Mask 255.255.255.0

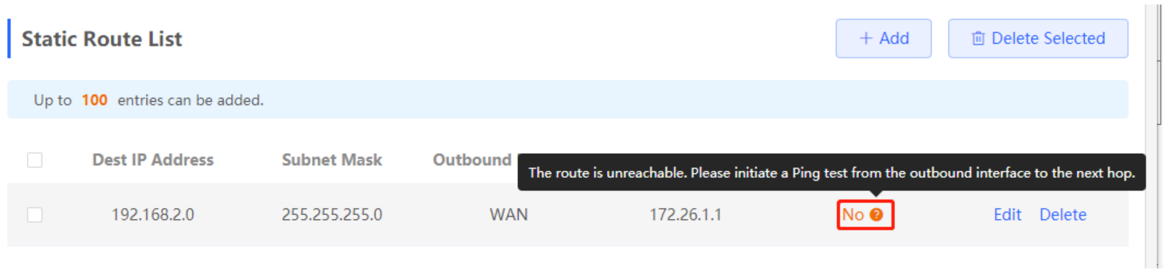
* Outbound Interface Select

* Next Hop

Table 3-7 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.



Static Route List

Up to 100 entries can be added.

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

□	Dest IP Address	Subnet Mask	Outbound			
□	192.168.2.0	255.255.255.0	WAN	172.26.1.1	No	Edit Delete

3.10 PBR

3.10.1 Overview

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.

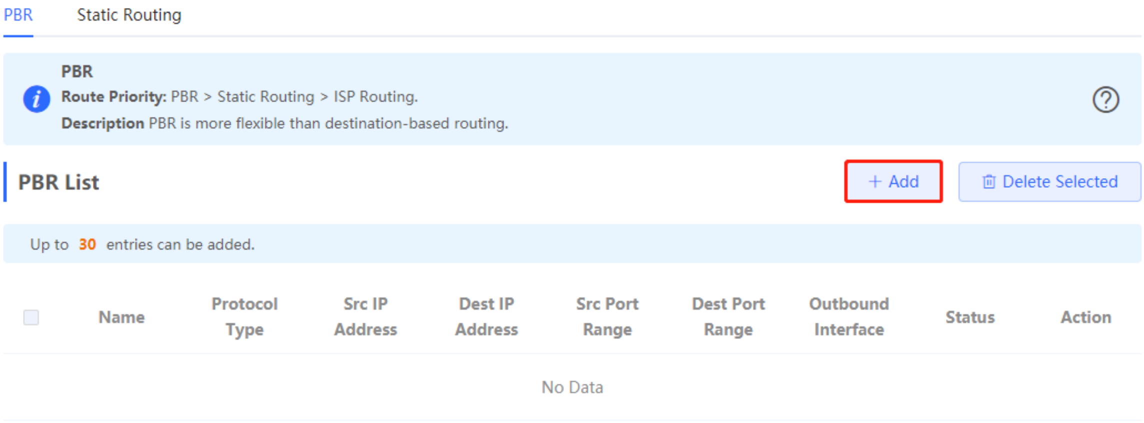
In a multi-line scenario, if the device is connected to the Internet and the internal network through different lines, the traffic will be evenly routed over the lines if no routing settings are available. In this case, access data to the internal network may be sent to the external network, or access 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 **错误!未找到引用源。**.

3.10.2 Configuration Steps

Choose **Local Device** > **Advanced** > **Routing** > **PBR**.

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

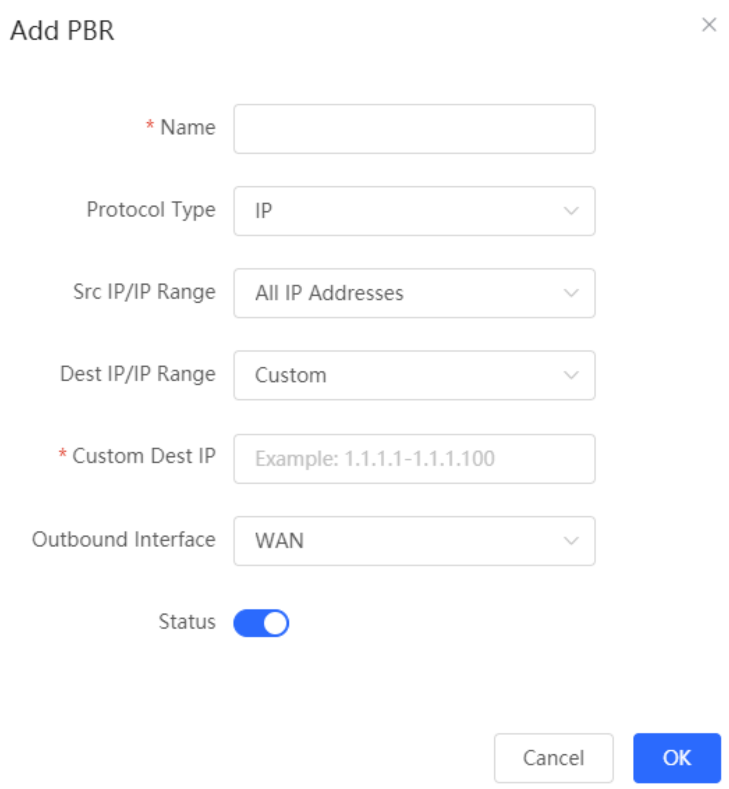


PBR
Route Priority: PBR > Static Routing > ISP Routing.
Description PBR is more flexible than destination-based routing.

PBR List

Up to 30 entries can be added.

□	Name	Protocol Type	Src IP Address	Dest IP Address	Src Port Range	Dest Port Range	Outbound Interface	Status	Action
No Data									



Add PBR

* Name

Protocol Type: IP

Src IP/IP Range: All IP Addresses

Dest IP/IP Range: Custom

* Custom Dest IP: Example: 1.1.1.1-1.1.1.100

Outbound Interface: WAN

Status

Table 3-8 PBR configuration

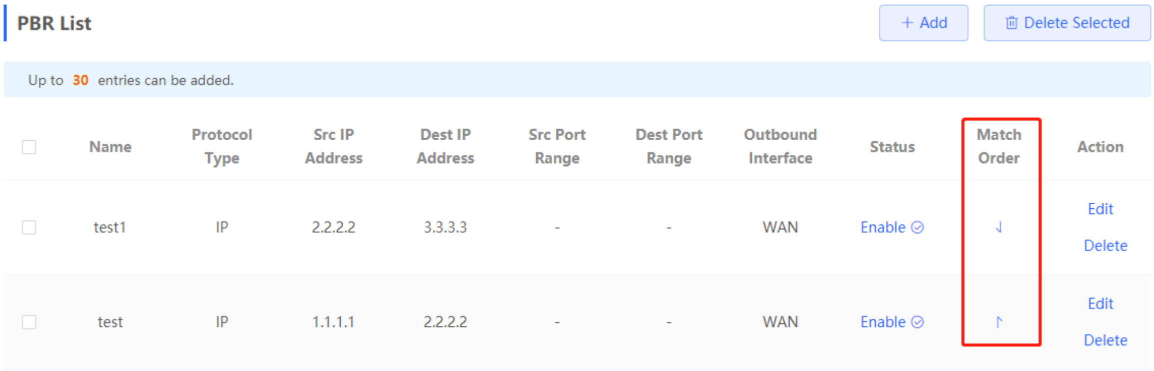
Parameter	Description
Name	Specify the name of the PBR rule, which uniquely identifies a PBR rule. The name must be unique for each rule.
Protocol Type	Specify the protocol to which the PBR rule is effective. You can set this parameter to **IP**, **ICMP**, **UDP**, **TCP**, or **Custom**.
Protocol Number	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.
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.

Parameter	Description
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.
Status	Turn on Status to specify whether to enable the PBR rule. If Status 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 port in the private line network. For details on how to set the private line network, see Section 3.2.4 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.



PBR List

Up to 30 entries can be added.

□	Name	Protocol Type	Src IP Address	Dest IP Address	Src Port Range	Dest Port Range	Outbound Interface	Status	Match Order	Action
□	test1	IP	2.2.2.2	3.3.3.3	-	-	WAN	Enable ✓	↓	Edit Delete
□	test	IP	1.1.1.1	2.2.2.2	-	-	WAN	Enable ✓	↑	Edit Delete

3.10.3 Typical Configuration Example

1. 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.

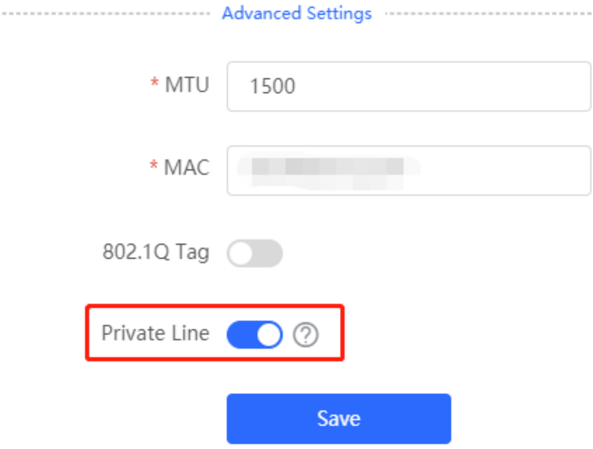
2. Configuration Roadmap

- 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.

3. 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 3.2.4 .


Advanced Settings

* MTU: 1500

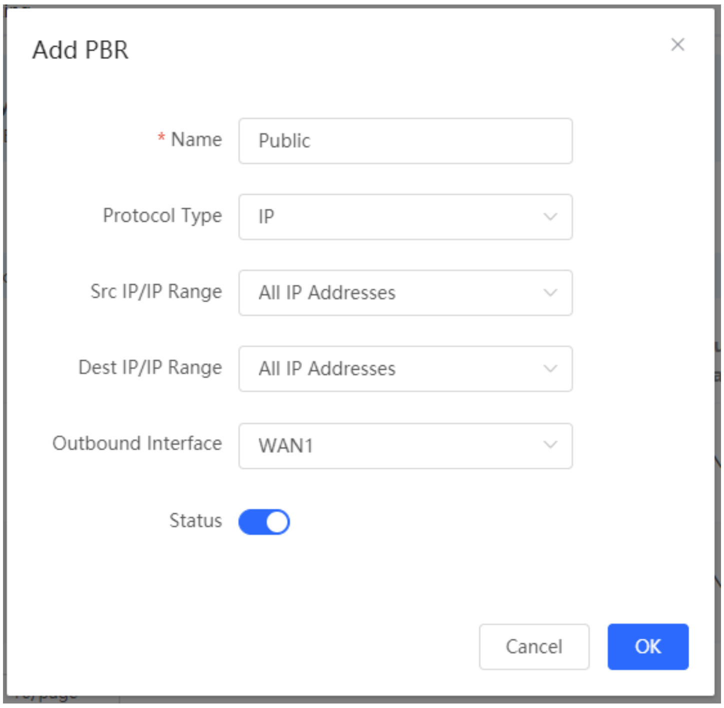
* MAC: [redacted]

802.1Q Tag: Off

Private Line: On

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

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


Add PBR

* Name: Public

Protocol Type: IP

Src IP/IP Range: All IP Addresses

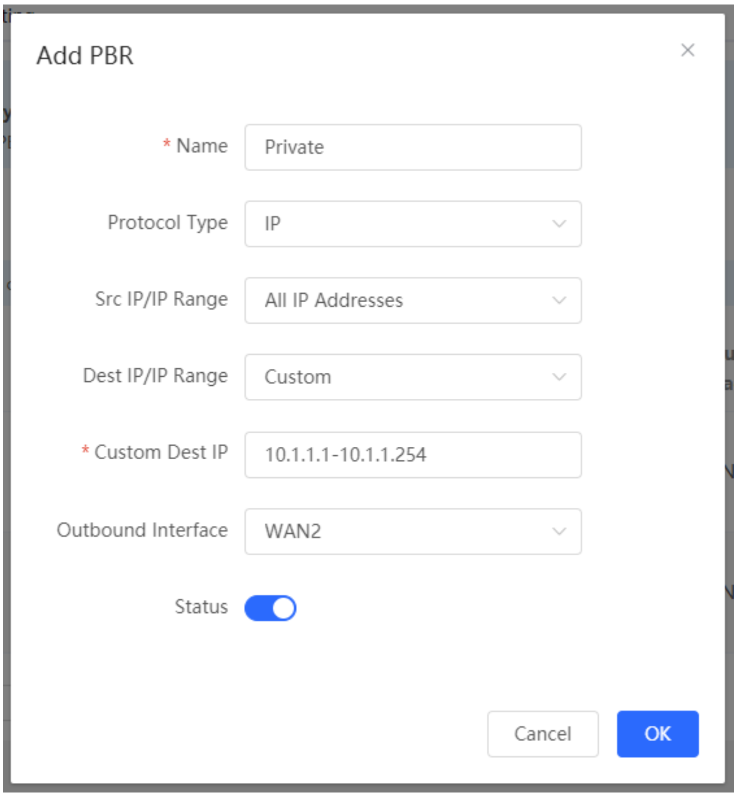
Dest IP/IP Range: All IP Addresses

Outbound Interface: WAN1

Status: On

(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.

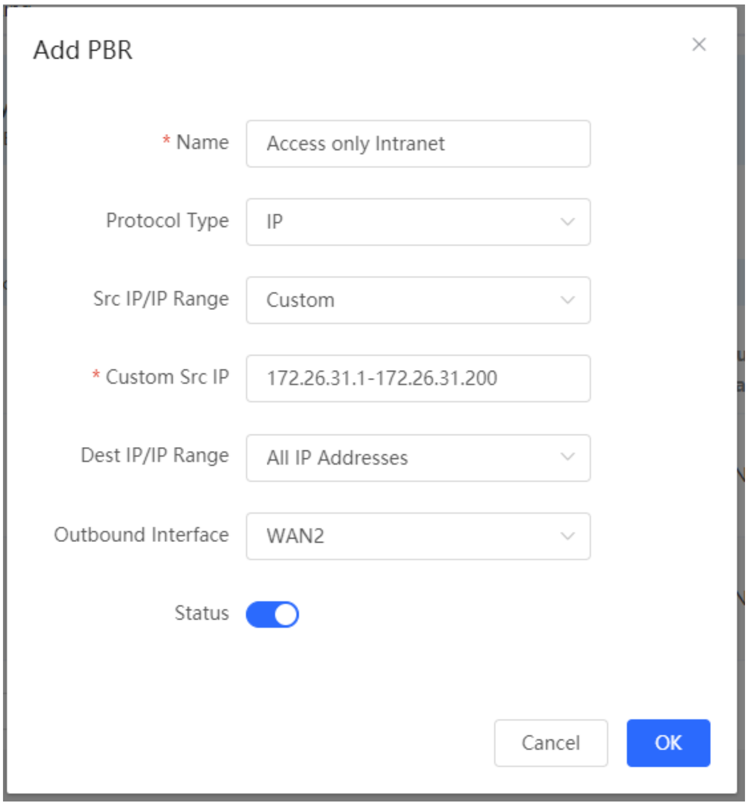


Add PBR

* Name	Private
Protocol Type	IP
Src IP/IP Range	All IP Addresses
Dest IP/IP Range	Custom
* Custom Dest IP	10.1.1.1-10.1.1.254
Outbound Interface	WAN2
Status	●

(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.



Add PBR

* Name: Access only Intranet

Protocol Type: IP

Src IP/IP Range: Custom

* Custom Src IP: 172.26.31.1-172.26.31.200

Dest IP/IP Range: All IP Addresses

Outbound Interface: WAN2

Status: on

3.11 Configuring ARP Binding and ARP Guard

3.11.1 Overview

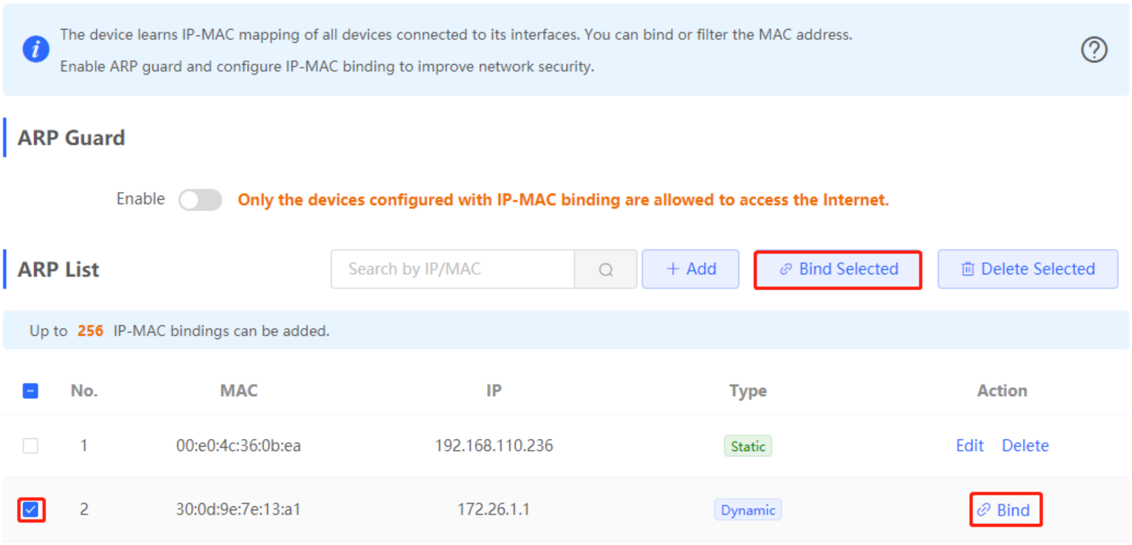
The device learns the IP address and MAC address of the network devices connected to its interfaces and generates the corresponding ARP entries. You can enable ARP guard and configure IP-MAC binding to restrict Internet access of LAN hosts and improve network security.

3.11.2 Configuring ARP Binding

Choose **Local Device** > **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.



The device learns IP-MAC mapping of all devices connected to its interfaces. You can bind or filter the MAC address.
Enable ARP guard and configure IP-MAC binding to improve network security.

ARP Guard

Enable Only the devices configured with IP-MAC binding are allowed to access the Internet.

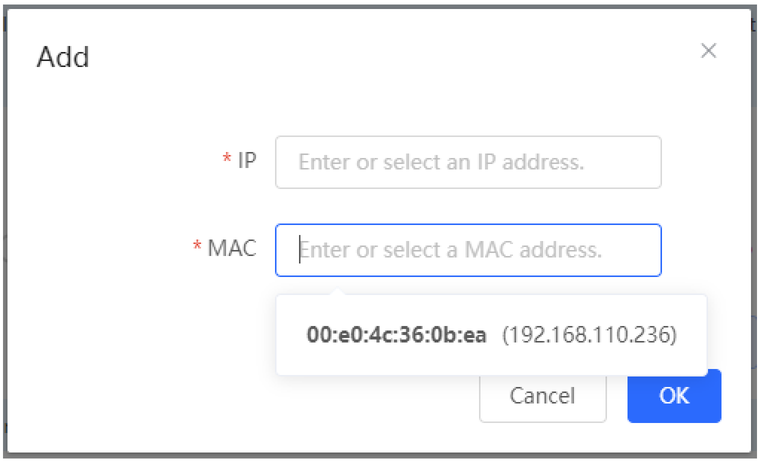
ARP List

Search by IP/MAC | + Add | Bind Selected | Delete Selected

Up to 256 IP-MAC bindings can be added.

☑	No.	MAC	IP	Type	Action
□	1	00:e0:4c:36:0b:ea	192.168.110.236	Static	Edit Delete
☑	2	30:0d:9e:7e:13:a1	172.26.1.1	Dynamic	Bind

(2) Click **Add**, enter the 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.



Add

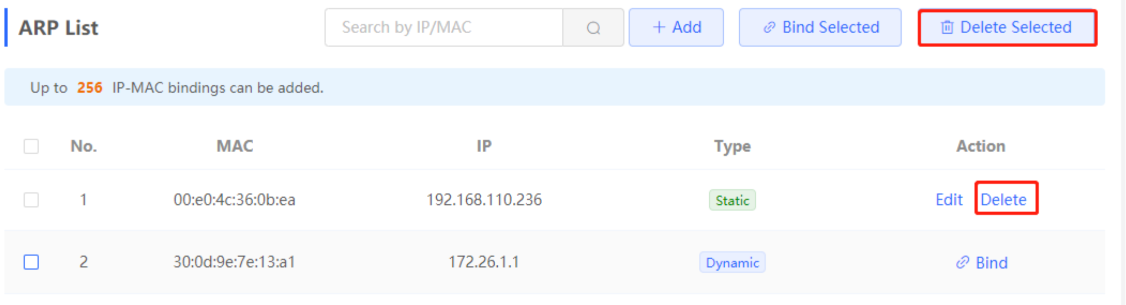
* IP: Enter or select an IP address.

* MAC: Enter or select a MAC address.

00:e0:4c:36:0b:ea (192.168.110.236)

Cancel | OK

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



ARP List

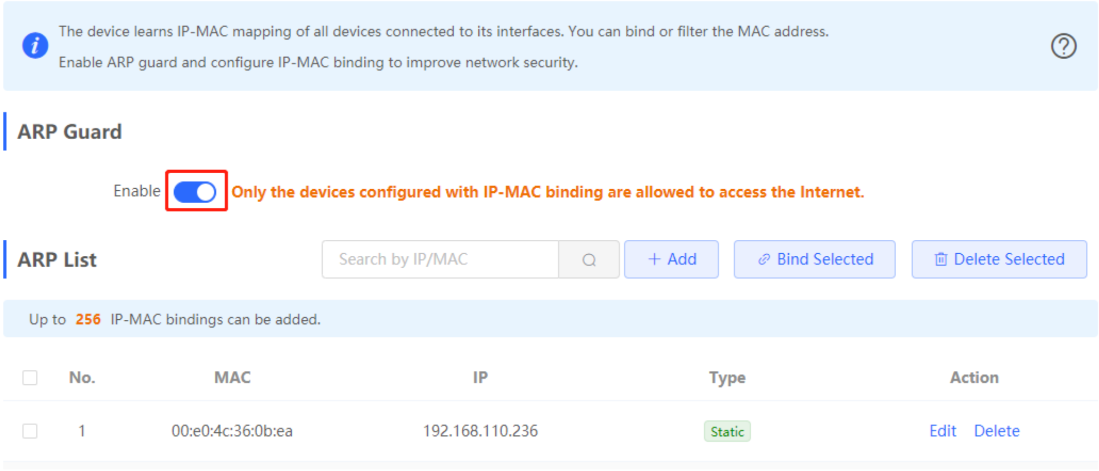
Search by IP/MAC | + Add | Bind Selected | Delete Selected

Up to 256 IP-MAC bindings can be added.

□	No.	MAC	IP	Type	Action
□	1	00:e0:4c:36:0b:ea	192.168.110.236	Static	Edit Delete
□	2	30:0d:9e:7e:13:a1	172.26.1.1	Dynamic	Bind

3.11.3 Configuring ARP Guard

Turn on **Enable** in the **ARP Guard** section to enable 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 3.11.2 Configuring ARP Binding.



The device learns IP-MAC mapping of all devices connected to its interfaces. You can bind or filter the MAC address.
Enable ARP guard and configure IP-MAC binding to improve network security.

ARP Guard

Enable Only the devices configured with IP-MAC binding are allowed to access the Internet.

ARP List

Up to 256 IP-MAC bindings can be added.

□	No.	MAC	IP	Type	Action
□	1	00:e0:4c:36:0b:ea	192.168.110.236	Static	Edit Delete

3.12 Configuring MAC Address Filtering

3.12.1 Overview

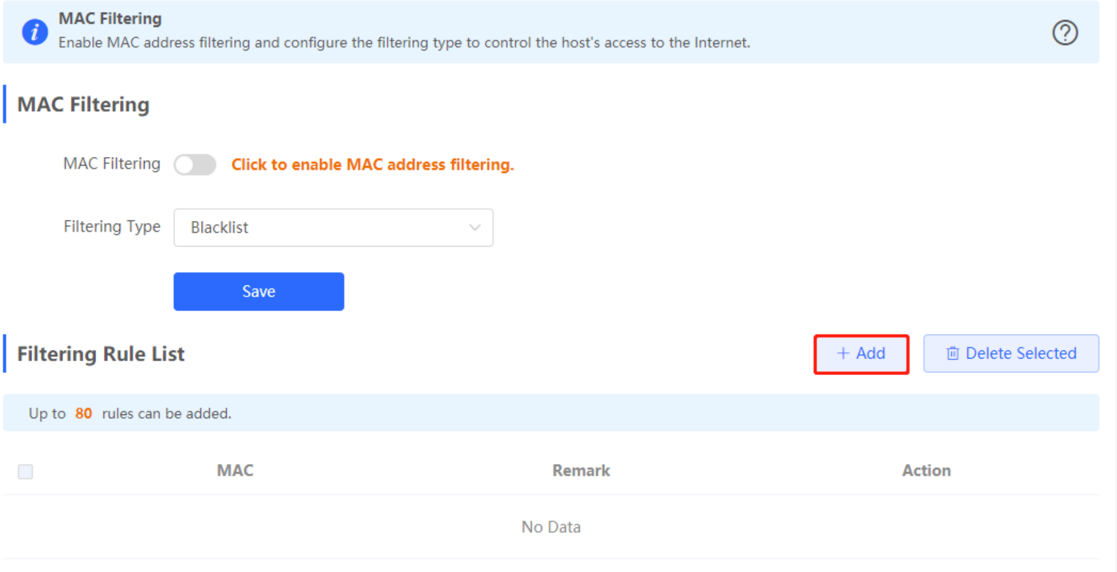
You can enable MAC address filtering and configure a whitelist or blacklist to effectively control Internet access from LAN hosts.

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

3.12.2 Configuration Steps

Choose **Local Device** > **Security** > **MAC Filtering**.

(1) 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.



MAC Filtering
Enable MAC address filtering and configure the filtering type to control the host's access to the Internet.

MAC Filtering

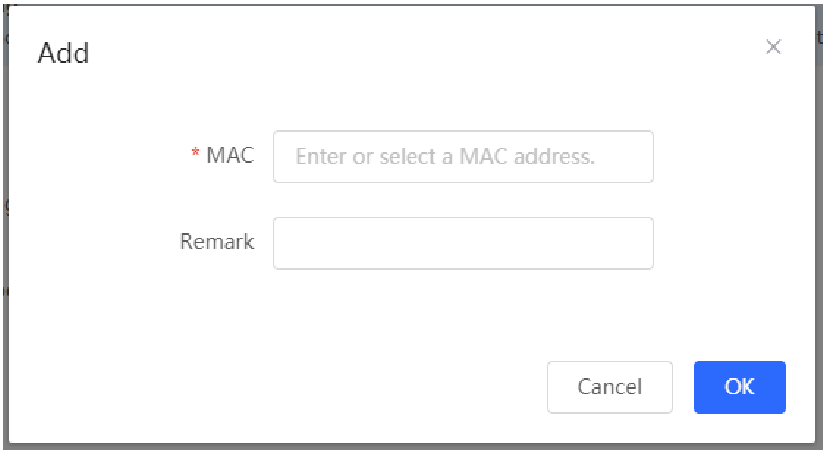
MAC Filtering Click to enable MAC address filtering.

Filtering Type: Blacklist

Filtering Rule List

Up to 80 rules can be added.

□	MAC	Remark	Action
		No Data	

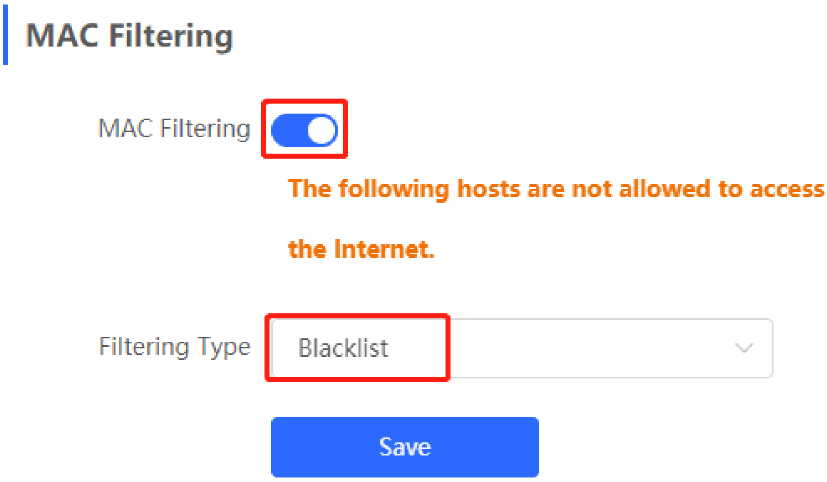


Add

* MAC Enter or select a MAC address.

Remark

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



MAC Filtering

MAC Filtering

The following hosts are not allowed to access the Internet.

Filtering Type Blacklist

3.13 Configuring the PPPoE Server

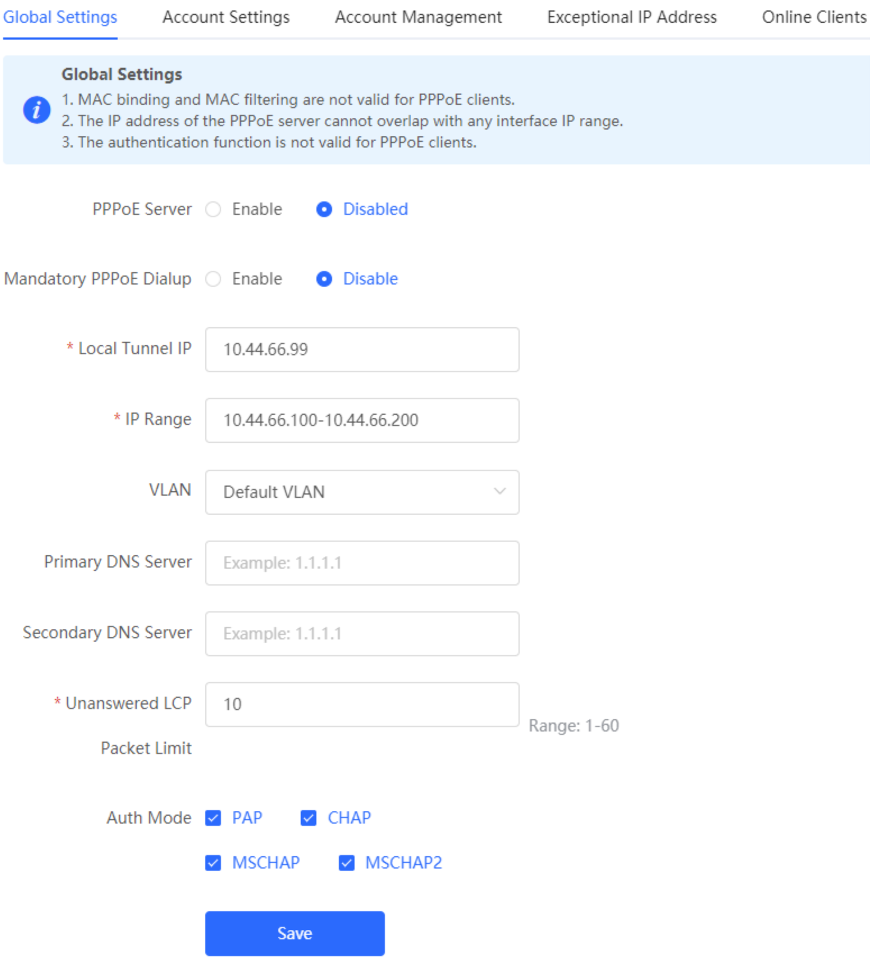
3.13.1 Overview

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.

3.13.2 Global Settings

Choose **Local Device** > **Advanced** > **PPPoE Server** > **Global Settings**.

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



Global Settings

1. MAC binding and MAC filtering are not valid for PPPoE clients.
2. The IP address of the PPPoE server cannot overlap with any interface IP range.
3. The authentication function is not valid for PPPoE clients.

PPPoE Server ○ Enable ● Disabled

Mandatory PPPoE Dialup ○ Enable ● Disable

* Local Tunnel IP: 10.44.66.99

* IP Range: 10.44.66.100-10.44.66.200

VLAN: Default VLAN

Primary DNS Server: Example: 1.1.1.1

Secondary DNS Server: Example: 1.1.1.1

* Unanswered LCP Packet Limit: 10 Range: 1-60

Auth Mode ☑ PAP ☑ CHAP ☑ MSCHAP ☑ MSCHAP2

Table 3-9 PPPoE server configuration

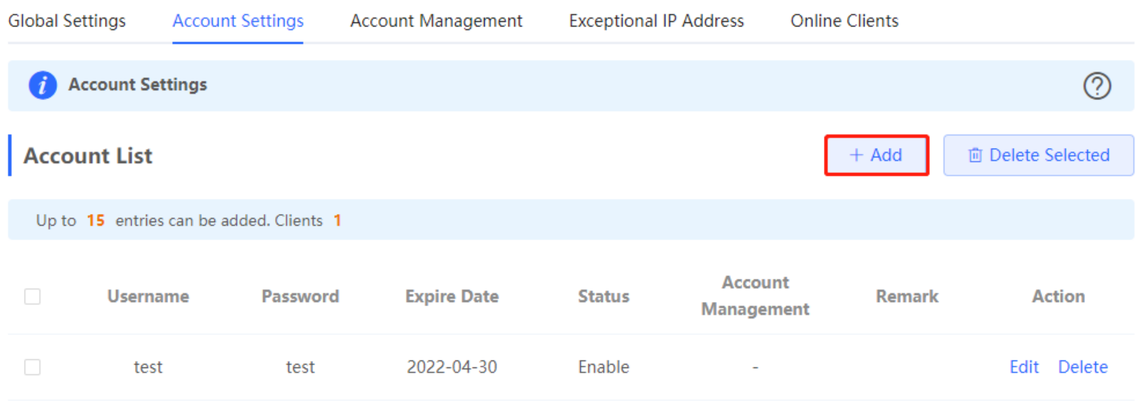
Parameter	Description
PPPoE Server	Specify whether to enable the PPPoE server function.
Mandatory PPPoE Dialup	Specify whether LAN users must access the Internet through dialing.
Local Tunnel IP	Set the point-to-point address of the PPPoE server.
IP Range	Specify the IP address range that can be allocated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

Parameter	Description
Auth Mode	Select at least one authentication mode from the following: PAP, CHAP, MSCHAP, and MSCHAP2.

3.13.3 Configuring a PPPoE User Account

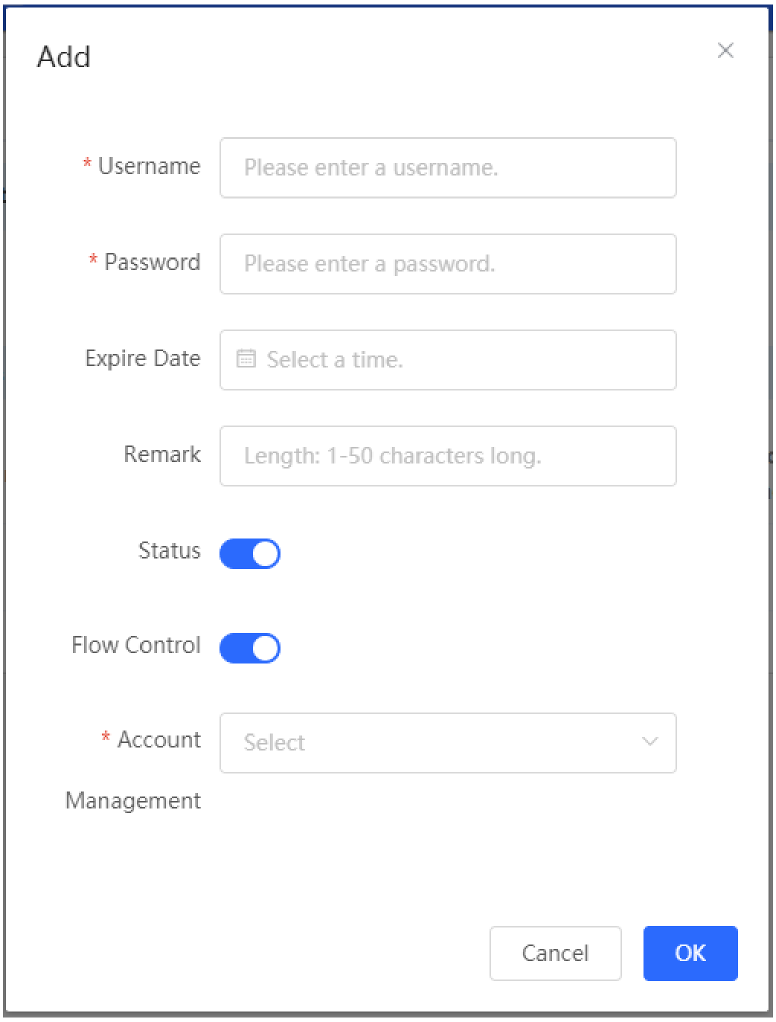
Choose **Local Device** > **Advanced** > **PPPoE Server** > **Account Settings**.

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.



Up to 15 entries can be added. Clients 1

□	Username	Password	Expire Date	Status	Account Management	Remark	Action
□	test	test	2022-04-30	Enable	-		Edit Delete



* Username: Please enter a username.

* Password: Please enter a password.

Expire Date: Select a time.

Remark: Length: 1-50 characters long.

Status: ●

Flow Control: ●

* Account Management: Select

Table 3-10 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.

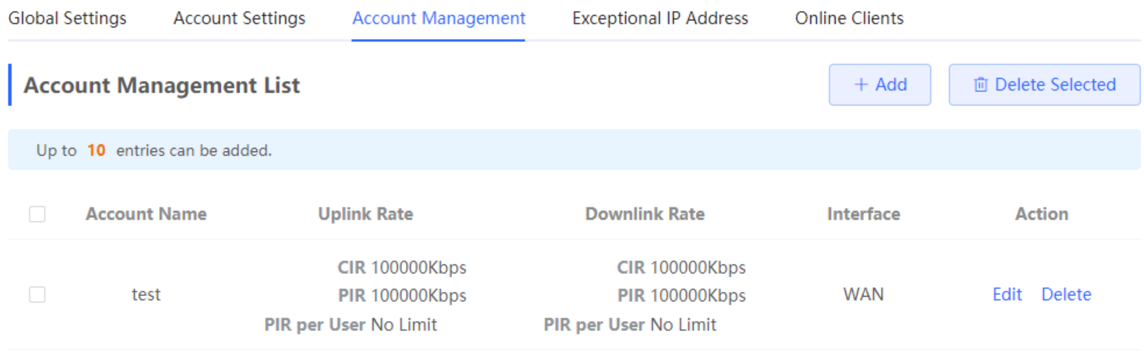
Parameter	Description
Flow Control	Specify whether to apply flow control on the account. If flow control is enabled, you need to configure flow control policies for the PPPoE authentication user. If smart flow control is disabled, **Flow Control** must be turned off. To turn on **Flow Control**, enable smart flow control first. For details on how to configure smart flow control, see Section 6.7.2 Intelligence Flow Control.
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 3.13.4 Configuring a Flow Control Package.

3.13.4 Configuring a Flow Control Package

Choose **Local Device** > **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 6.7.2 Intelligence 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.



Account Management List

Up to 10 entries can be added.

□	Account Name	Uplink Rate	Downlink Rate	Interface	Action
□	test	CIR 100000Kbps PIR 100000Kbps PIR per User No Limit	CIR 100000Kbps PIR 100000Kbps PIR per User No Limit	WAN	Edit Delete

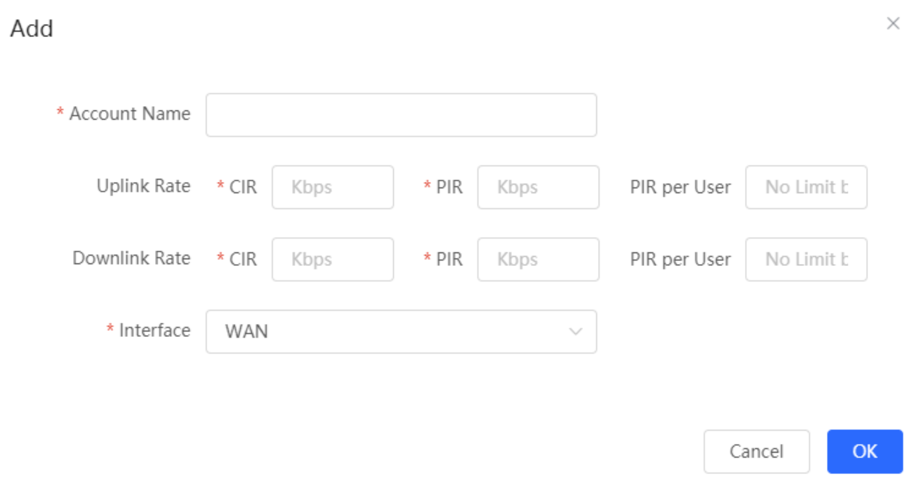


Table 3-11 PPPoE user flow control package configuration

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/Downlink CIR	Specify the committed information rate (CIR) for the authentication account when the bandwidth is insufficient.
Uplink/Downlink PIR	Specify the peak information rate (PIR) that can be used by the authentication account when the bandwidth is sufficient.
Uplink/Downlink PIR per User	Specify the PIR that can be consumed by each user. This parameter is optional. By default, the PIR per user is not limited.
Interface	Specify the interface to which the flow control package applies.

3.13.5 Configuring Exceptional IP Addresses

Choose **Local Device** > **Advanced** > **PPPoE Server** > **Exceptional IP Address**.

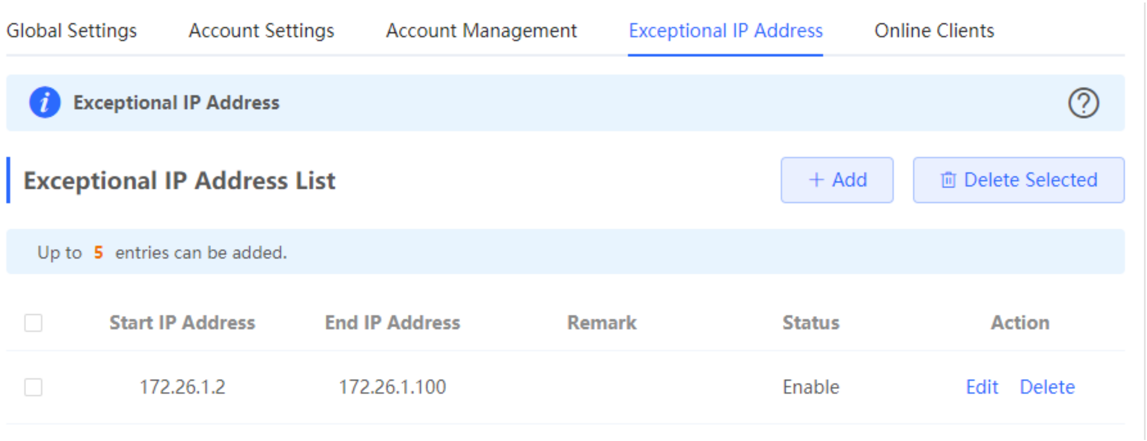
When the PPPoE server is enabled, if you want to allow some IP addresses in a specific VLAN to access the Internet without passing account and password authentication, you can configure these IP addresses as exceptional IP addresses.

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.

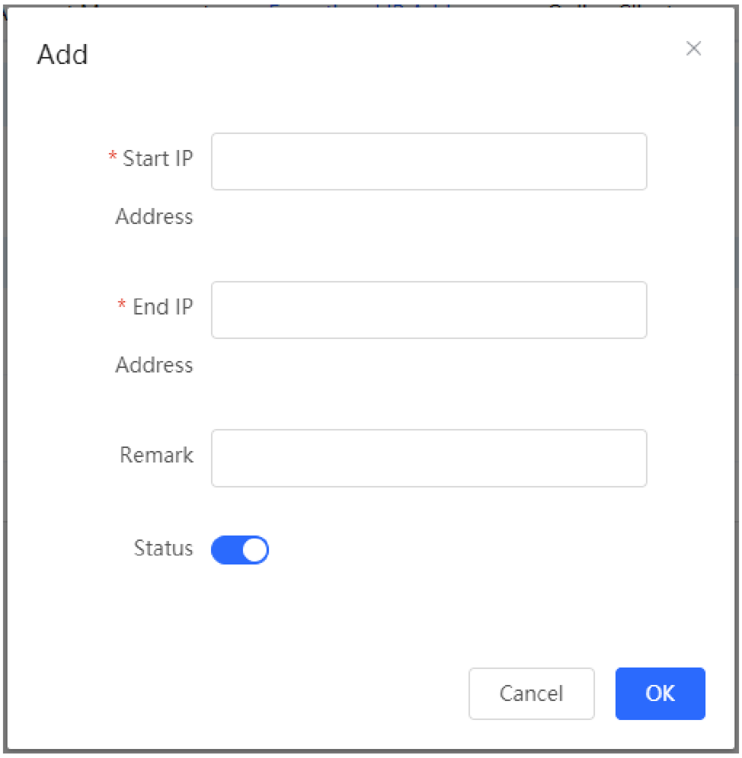
Remark: Description of an exceptional IP address.

Status: Whether the exceptional IP address is effective.



Up to 5 entries can be added.

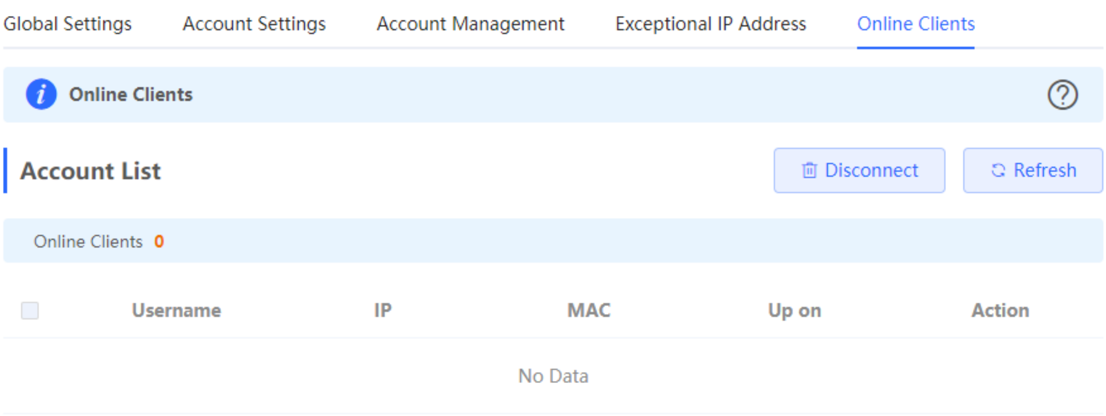
□	Start IP Address	End IP Address	Remark	Status	Action
□	172.26.1.2	172.26.1.100		Enable	Edit Delete



3.13.6 Viewing Online Users

Choose **Local Device** > **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.



Online Clients

Account List

Online Clients 0

□	Username	IP	MAC	Up on	Action
No Data					

Table 3-12 PPPoE online user information

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

3.14 Port Mapping

3.14.1 Overview

1. Port Mapping

The port mapping function can establish a mapping relationship between the IP address and port number of a WAN port 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 port 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 port.

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.

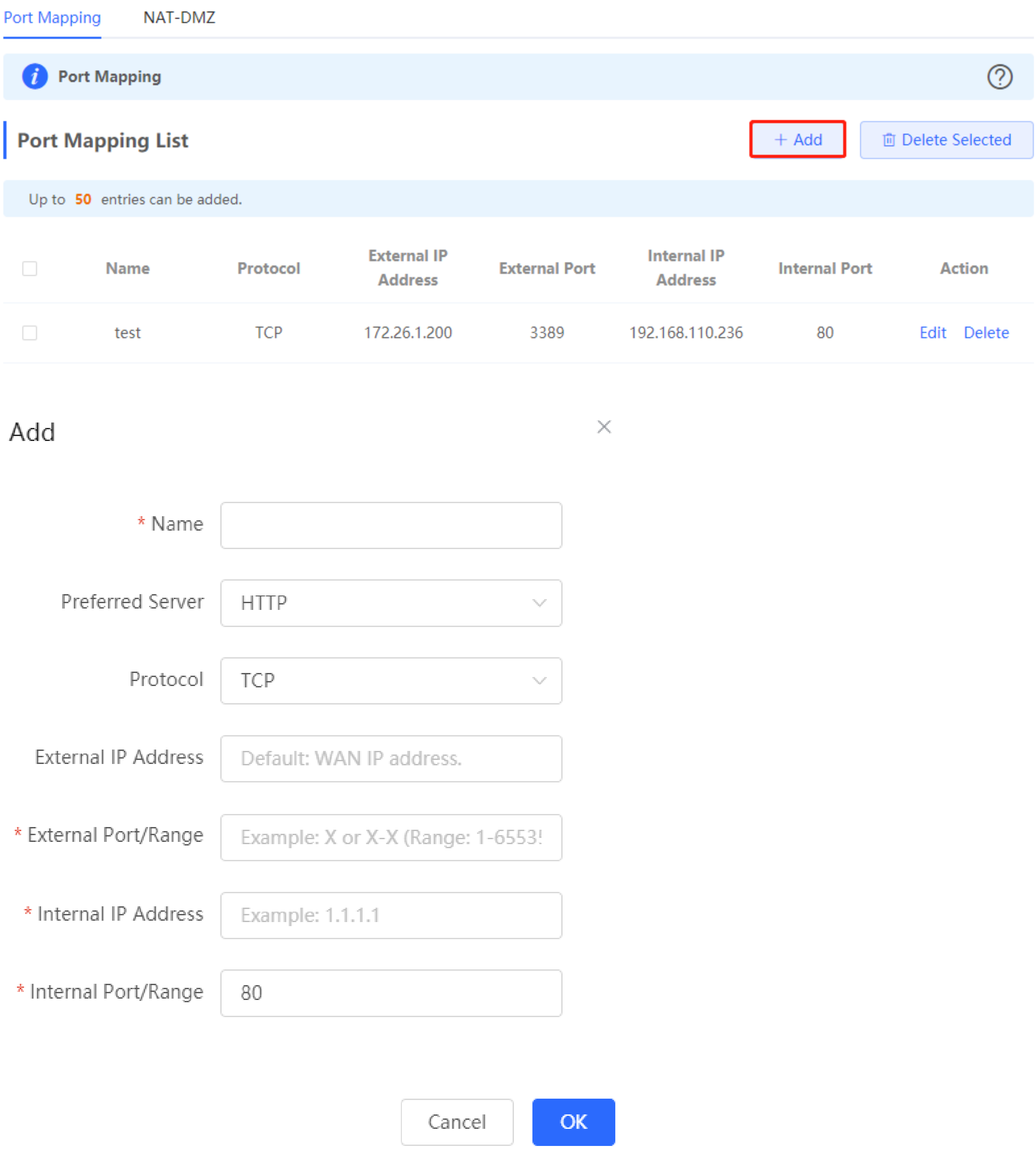
3.14.2 Getting Started

- 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.

3.14.3 Configuration Steps

Choose **Local Device** > **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.



Up to 50 entries can be added.

□	Name	Protocol	External IP Address	External Port	Internal IP Address	Internal Port	Action
□	test	TCP	172.26.1.200	3389	192.168.110.236	80	Edit Delete

* Name	
Preferred Server	HTTP
Protocol	TCP
External IP Address	Default: WAN IP address.
* External Port/Range	Example: X or X-X (Range: 1-6553!
* Internal IP Address	Example: 1.1.1.1
* Internal Port/Range	80

Table 3-13 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 Internet access. The default value is the IP address of the WAN port.
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 port, 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 port, 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**.

3.14.4 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.

3.14.5 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.

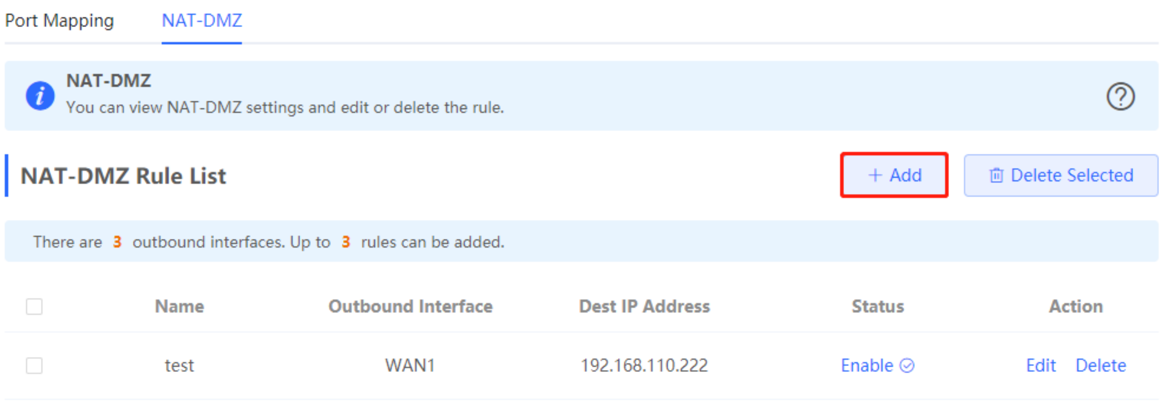
(2) Enable the remote access permission on the server. The possible cause is that remote access is displayed on the server, resulting in normal internal access but abnormal access across network segments.

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

3.14.6 Configuration Steps (DMZ)

Choose **Local Device** > **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.

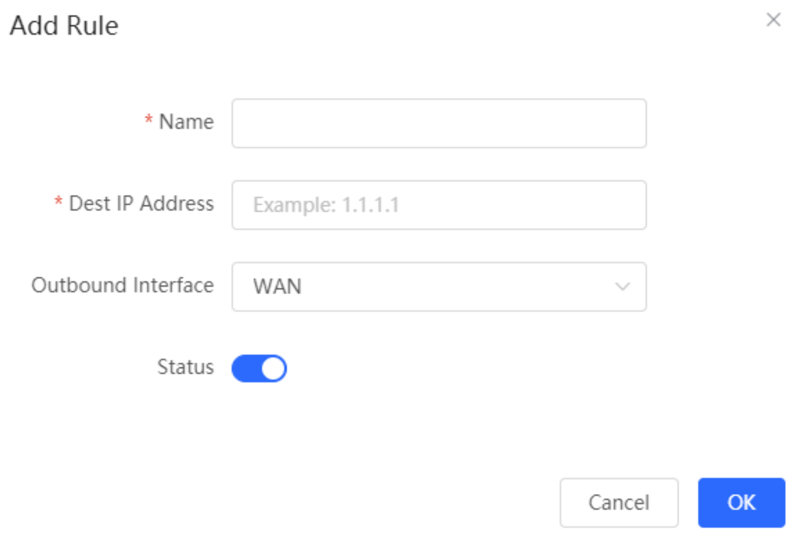


NAT-DMZ
You can view NAT-DMZ settings and edit or delete the rule.

NAT-DMZ Rule List

There are 3 outbound interfaces. Up to 3 rules can be added.

□	Name	Outbound Interface	Dest IP Address	Status	Action
□	test	WAN1	192.168.110.222	Enable ✓	Edit Delete



Add Rule

* Name:

* Dest IP Address: Example: 1.1.1.1

Outbound Interface: WAN

Status: ●

Table 3-14 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 port in the DMZ rule. You can configure only one rule for a WAN port.
Status	Specify whether the rule is effective. The rule is effective after you turn on **Status**.

3.15 UPnP

3.15.1 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:

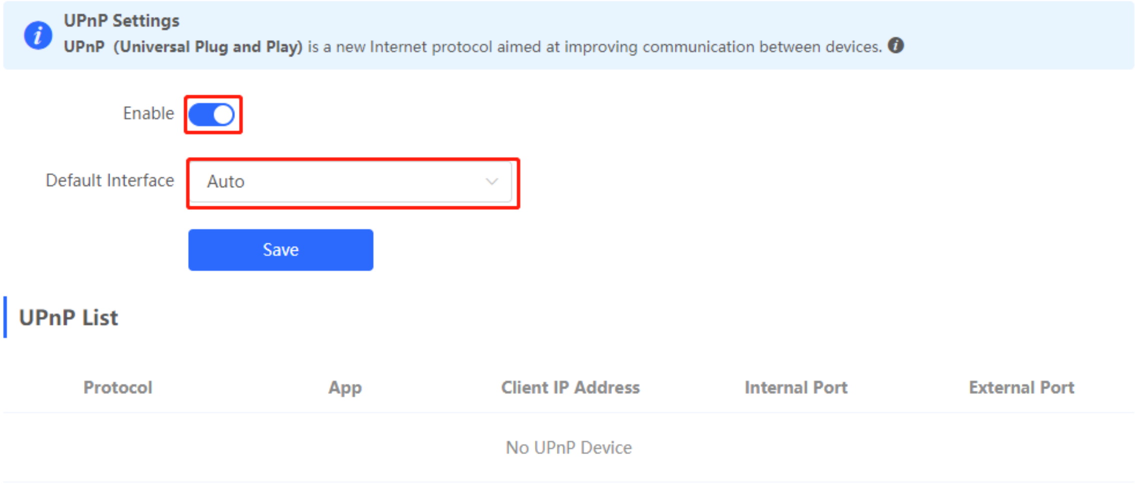
- UPnP is enabled on the device.
- The operating system of the LAN host supports UPnP and has UPnP enabled.
- The programs support UPnP and have UPnP enabled.

3.15.2 Configuring UPnP

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

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.



UPnP Settings

UPnP (Universal Plug and Play) is a new Internet protocol aimed at improving communication between devices.

Enable: on

Default Interface: Auto

Save

UPnP List

Protocol	App	Client IP Address	Internal Port	External Port
No UPnP Device				

Table 3-15 UPnP configuration

Parameter	Description
Enable	Specify whether to enable UPnP. By default, UPnP is disabled.

Default Interface	Specify the WAN port address bound to the UPnP service. By default, the default interface is a WAN port. On the device with multiple WAN ports, you can manually select the WAN port to bind or set this parameter to **Auto** to allow the device to select a WAN port automatically.

3.15.3 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.

3.16 DDNS

3.16.1 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 port 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 DynDNS and No-IP DNS.

3.16.2 Getting Started

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

3.16.3 Configuring DDNS

1. Configuration Steps

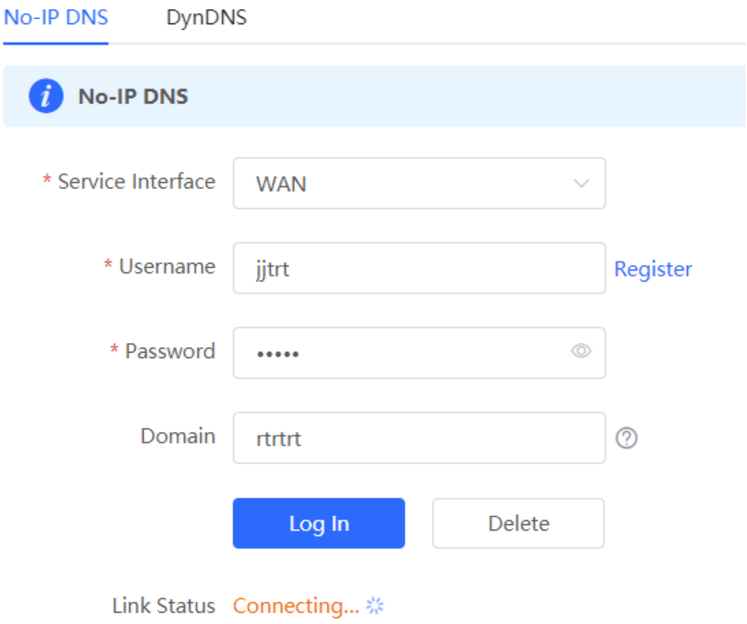
The device supports No-IP DNS and DynDNS. DynDNS can be used by International users only, and No-IP DNS can be used by both Chinese and International users.

Choose **Local Device** > **Advanced** > **Dynamic DNS** > **No-IP DNS/DynDNS**.

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 port 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 port IP address.



* Service Interface: WAN

* Username: jjtrt

* Password: •••••

Domain: rtrtrt

Link Status: Connecting...

Table 3-16 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 port bound to the domain name when multiple WAN ports are available. By default, the service interface is a WAN port.
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 port IP address. If no domain name is specified, all the domain names of the current account are parsed to the WAN port IP address. This parameter is optional for DynDNS, and the value is provided by the DynDNS service provider.

2. 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 port IP address.

3.17 Connecting to IPTV

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 错误!未找到引用源。.

IPTV is a network television service provided by the ISP.

3.17.1 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.

3.17.2 Configuration Steps (VLAN Type)

Choose **Local Device** > **Basics** > **IPTV** > **IPTV/VLAN**.

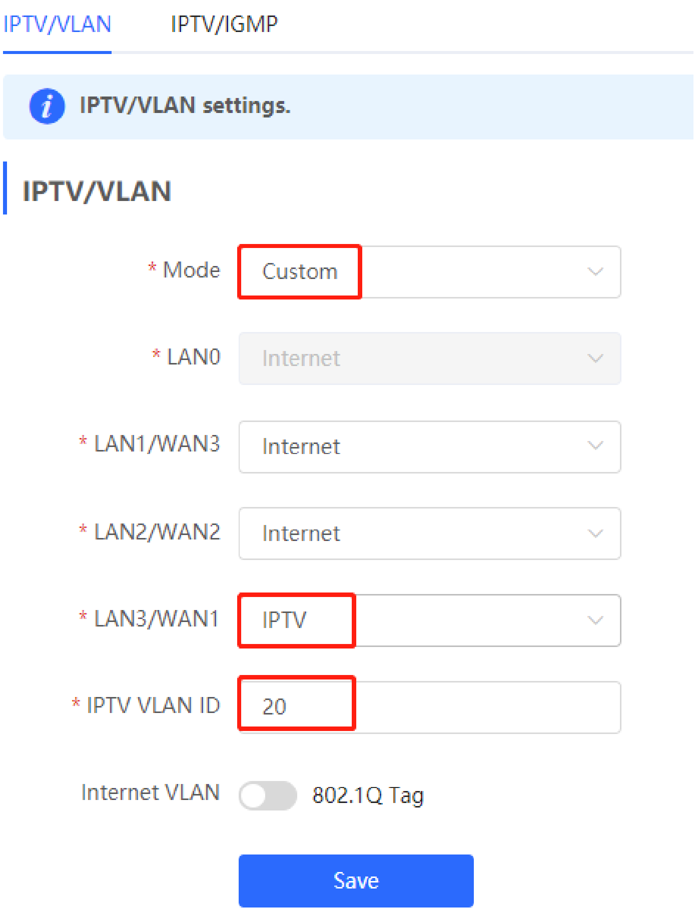
Select a proper mode based on your region, click the drop-down list box next to the interface to connect and select **IPTV**, and enter the VLAN ID provided by the ISP. For example, when you want to connect the IPTV set top box to LAN 3 port of the device and the VLAN ID is 20, the configuration UI is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



IPTV/VLAN settings.

IPTV/VLAN

* Mode: Custom

* LAN0: Internet

* LAN1/WAN3: Internet

* LAN2/WAN2: Internet

* LAN3/WAN1: IPTV

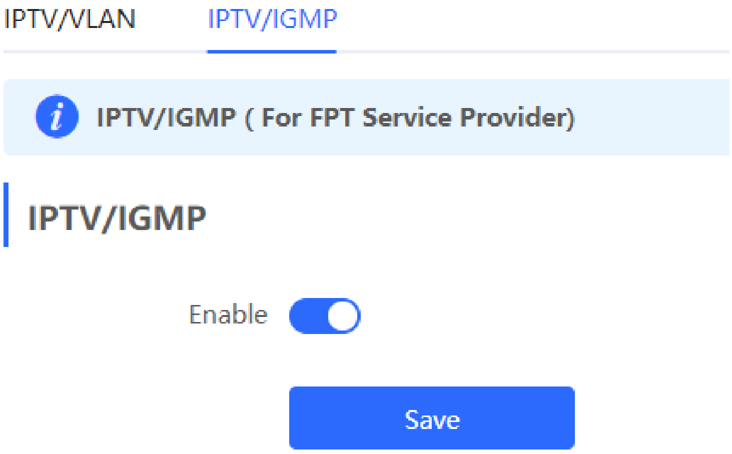
* IPTV VLAN ID: 20

Internet VLAN: 802.1Q Tag

3.17.3 Configuration Steps (IGMP Type)

Choose **Local Device** > **Basics** > **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.



IPTV/IGMP (For FPT Service Provider)

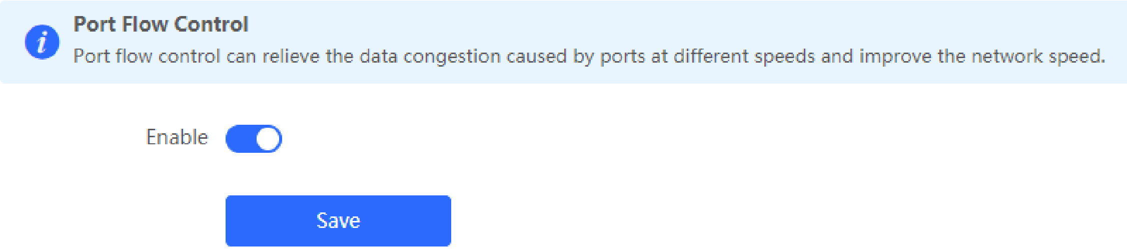
IPTV/IGMP

Enable

3.18 Port Flow Control

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

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.



Port Flow Control

Port flow control can relieve the data congestion caused by ports at different speeds and improve the network speed.

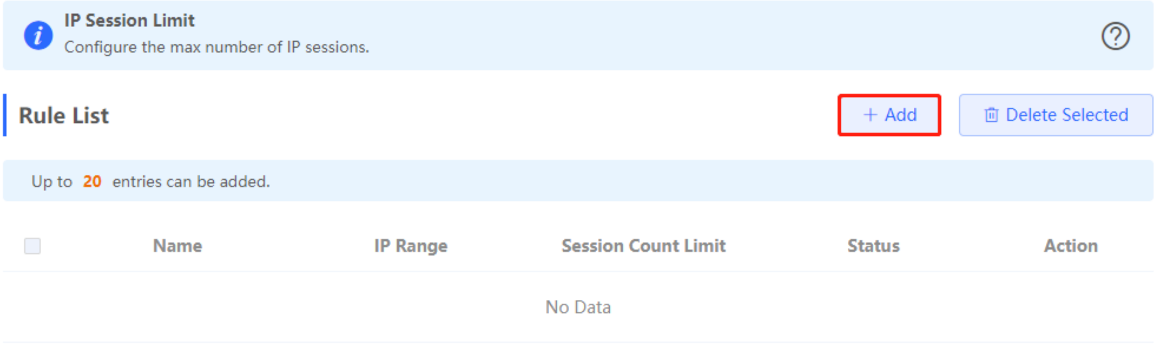
Enable: on

3.19 Limiting the Number of Connections

Choose **Local Device** > **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.

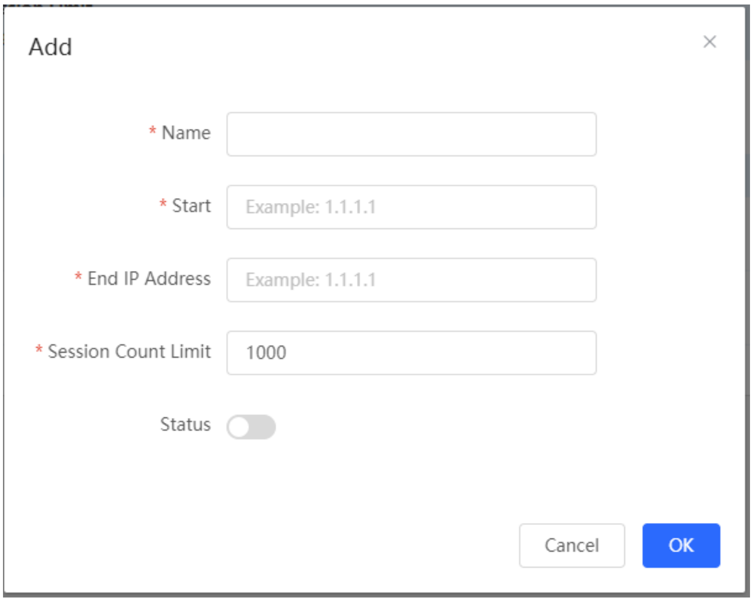


IP Session Limit

Configure the max number of IP sessions.

Up to 20 entries can be added.

□	Name	IP Range	Session Count Limit	Status	Action
		No Data			



Add

- * Name:
- * Start: Example: 1.1.1.1
- * End IP Address: Example: 1.1.1.1
- * Session Count Limit: 1000
- Status: off

Table 3-17 IP session limit rule information

Parameter	Description
Name	Enter the name of the IP session limit rule.

Parameter	Description
Start	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.
Session Count Limit	Specify the maximum number of session connections for an IP address matching the rule.
Status	Specify whether the rule is effective. The rule takes effect after you turn on this parameter.

3.20 Configuring Device Security

3.20.1 Overview

Prohibit Ping: This function identifies and directly discards the ping packets in the traffic sent to the device, so as to prohibit the ping operation on the device. Only admin IP addresses can ping through the device.

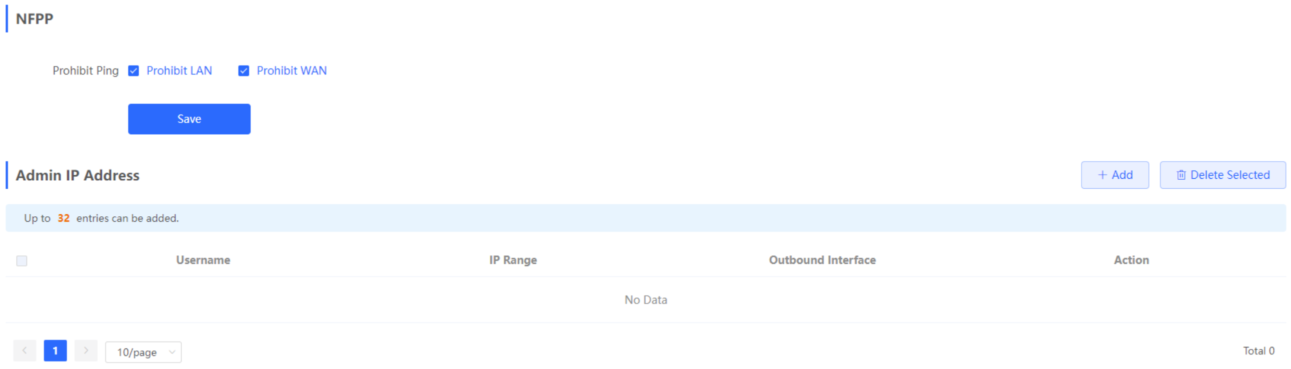
Admin IP Address: Admin IP addresses are exempt from the ping prohibition function. Packets sent from admin IP addresses can pass through and will not be discarded.

3.20.2 Enabling the Ping Prohibition Function

[**Local Device**] Choose **Security** > **Local Safety**.

The ping prohibition function includes the following:

- If you select **Prohibit LAN**, ping packets sent from all clients on the LAN to the device will be discarded.
- If you select **Prohibit WAN**, ping packets sent from all clients on the WANs to the device will be discarded. Ping packets sent from a client to the device will be responded only after the IP address of the client is contained in **Admin IP Address** list. For the configuration of admin IP addresses, see Configuring an Admin IP Address.



NFPP

Prohibit Ping ☑ Prohibit LAN ☑ Prohibit WAN

Admin IP Address

Up to 32 entries can be added.

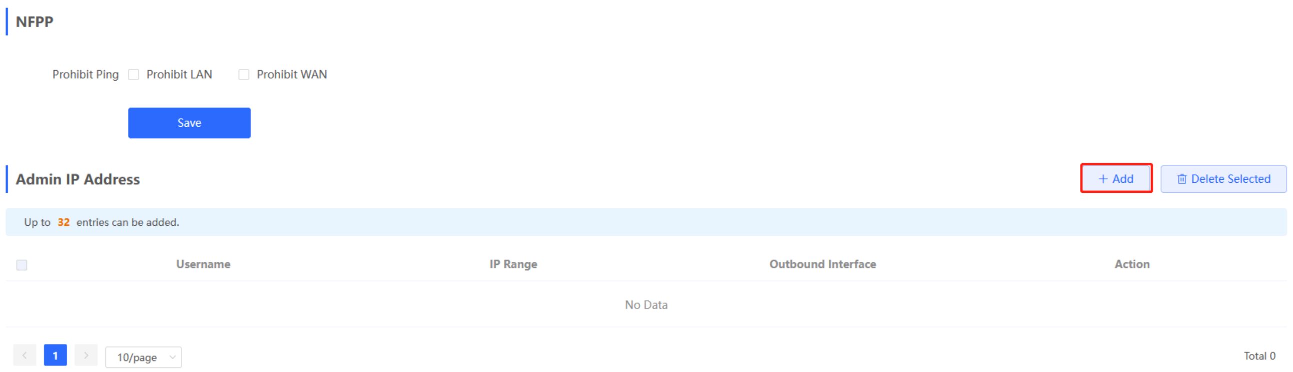
☐	Username	IP Range	Outbound Interface	Action
		No Data		

Total 0

3.20.3 Configuring an Admin IP Address

[**Local Device**] Choose **Security** > **Local Safety**.

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



NFPP

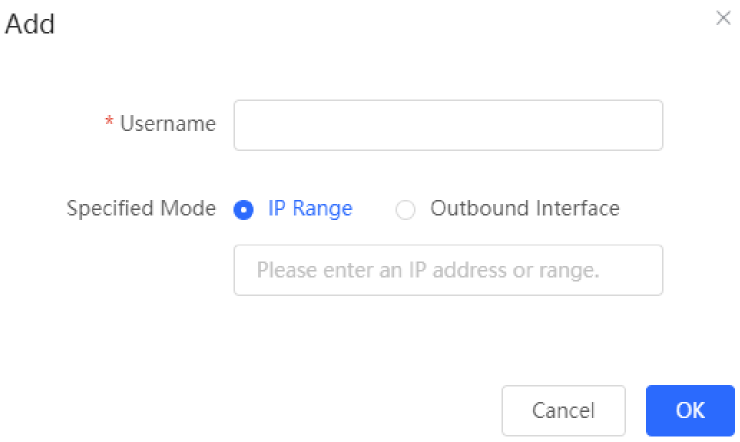
Prohibit Ping □ Prohibit LAN □ Prohibit WAN

Admin IP Address

Up to 32 entries can be added.

□	Username	IP Range	Outbound Interface	Action
No Data				

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



Add

* Username

Specified Mode ● IP Range ○ Outbound Interface

Please enter an IP address or range.

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

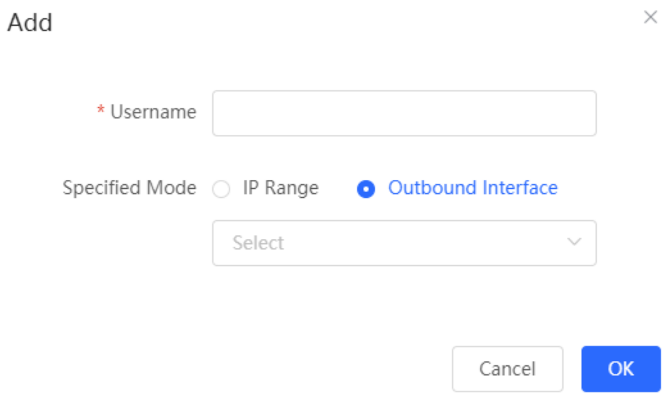
The name is a string of 1–32 characters.

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

(3) Configure an IP address.

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

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



Add

* Username

Specified Mode ○ IP Range ● Outbound Interface

Select

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

The name is a string of 1–32 characters.

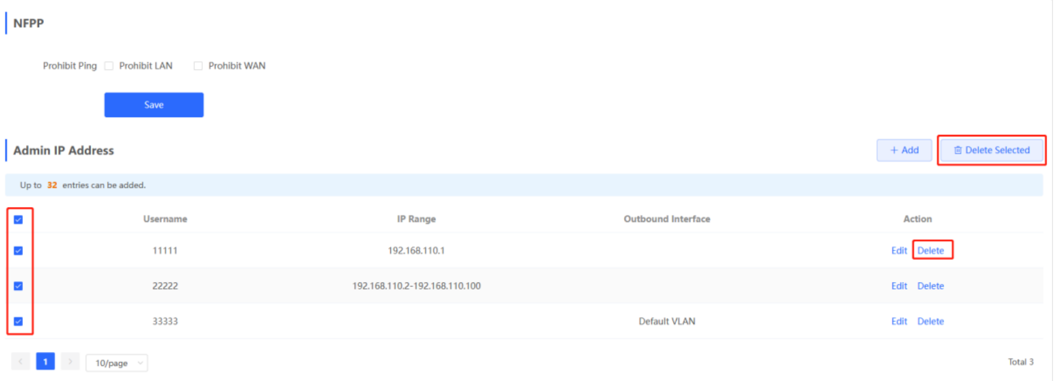
(2) Set **Specific Mode** to **Outbound Interface**.

(3) Specify the port.

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



NFPP

Prohibit Ping □ Prohibit LAN □ Prohibit WAN

Admin IP Address

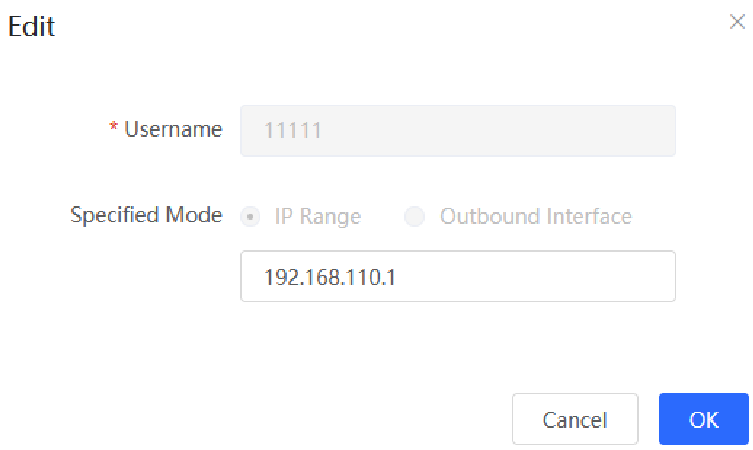
Up to 32 entries can be added.

☑	Username	IP Range	Outbound Interface	Action
☑	11111	192.168.110.1		Edit Delete
☑	22222	192.168.110.2-192.168.110.100		Edit Delete
☑	33333		Default VLAN	Edit Delete

Total 3

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.

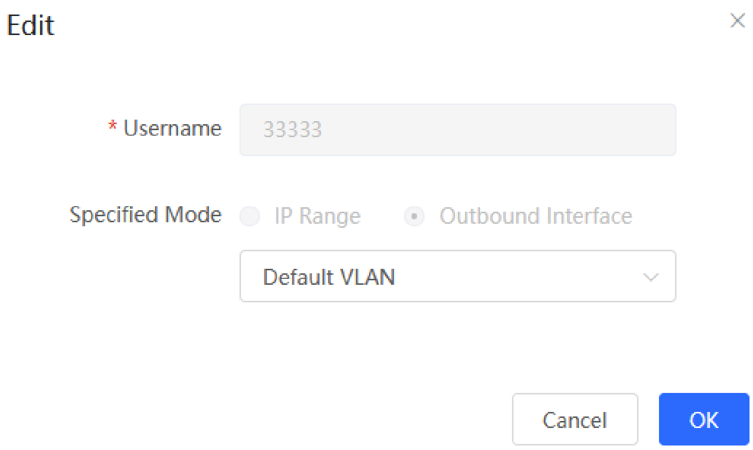


Edit

* Username: 11111

Specified Mode: ● IP Range ○ Outbound Interface

192.168.110.1



Edit

* Username: 33333

Specified Mode: ○ IP Range ● Outbound Interface

Default VLAN

3.21 Configuring TTL Rules

3.21.1 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.

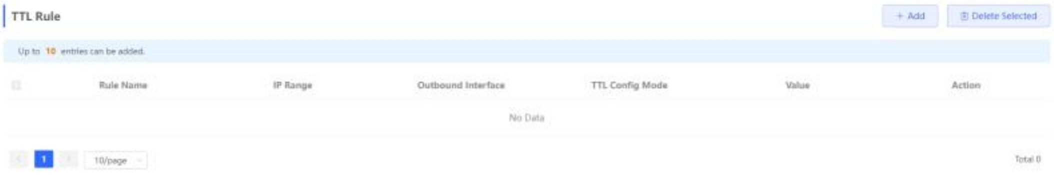
Note

- 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.

3.21.2 Configuring TTL Rules

[**Local Device**] Choose **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.

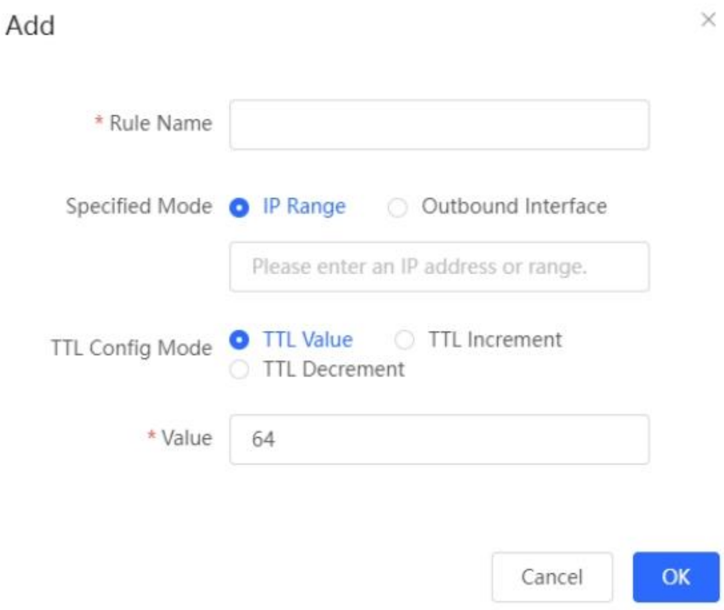


TTL Rule

Up to 10 entries can be added.

□	Rule Name	IP Range	Outbound Interface	TTL Config Mode	Value	Action
No Data						

1. Configuring a TTL Rule



Add

* Rule Name:

Specified Mode: ● IP Range ○ Outbound Interface

Please enter an IP address or range.

TTL Config Mode: ● TTL Value ○ TTL Increment ○ TTL Decrement

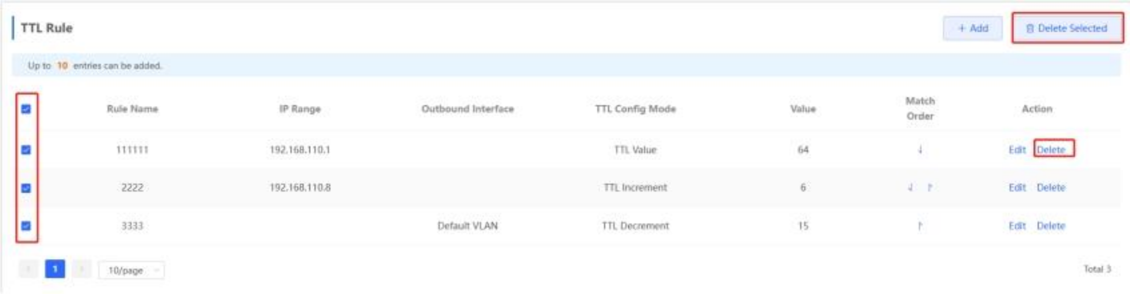
* Value: 64

Table 3-18 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: **IP Range**: Indicates that the TTL rule takes effect on a specified IP address 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.



TTL Rule

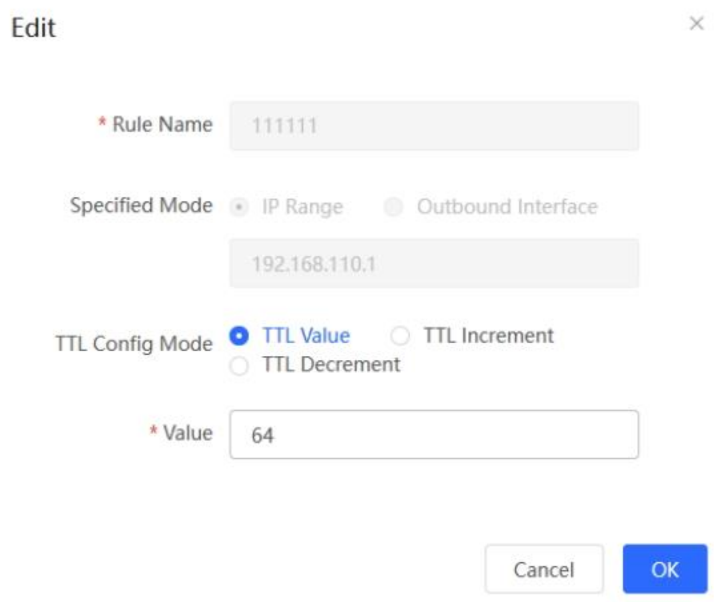
Up to 10 entries can be added.

☑	Rule Name	IP Range	Outbound Interface	TTL Config Mode	Value	Match Order	Action
☑	111111	192.168.110.1		TTL Value	64	↓	Edit Delete
☑	2222	192.168.110.8		TTL Increment	6	↓ ↑	Edit Delete
☑	3333		Default VLAN	TTL Decrement	15	↑	Edit Delete

Total 3

3. Editing a TTL Rule

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



Edit

* Rule Name: 111111

Specified Mode: ● IP Range ○ Outbound Interface

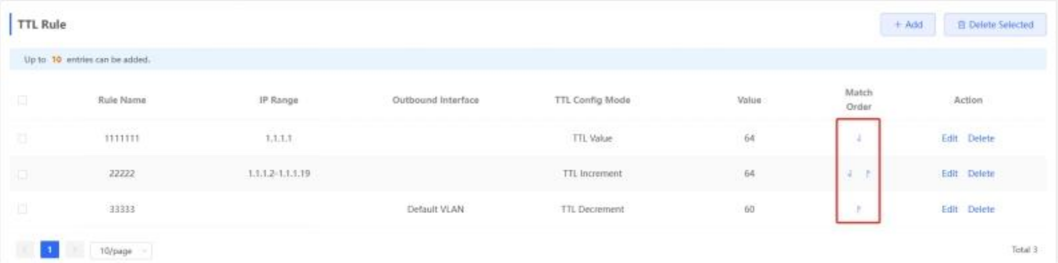
192.168.110.1

TTL Config Mode: ● TTL Value ○ TTL Increment ○ TTL Decrement

* Value: 64

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.



TTL Rule

Up to 10 entries can be added.

□	Rule Name	IP Range	Outbound Interface	TTL Config Mode	Value	Match Order	Action
□	1111111	1.1.1.1		TTL Value	64	↓	Edit Delete
□	22222	1.1.1.2-1.1.1.19		TTL Increment	64	↓ ↑	Edit Delete
□	33333		Default VLAN	TTL Decrement	60	↑	Edit Delete

3.22 Other Settings

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

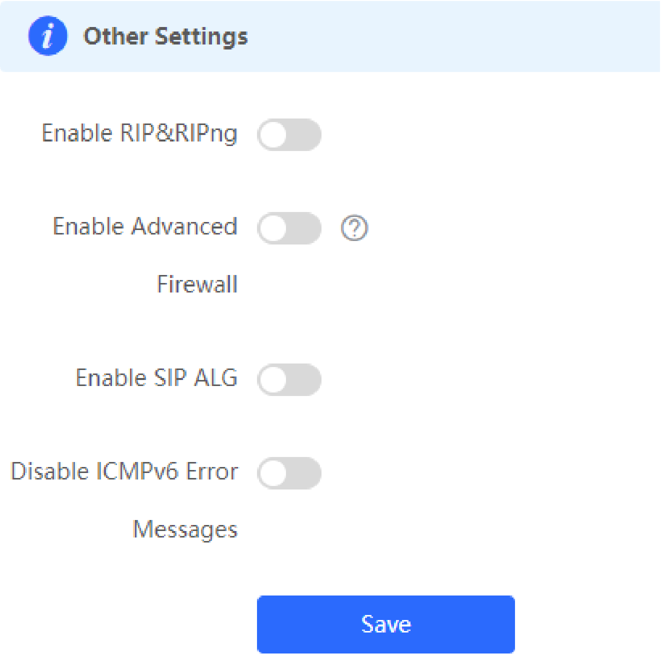
You can set some functions not frequently used on the Other Settings page. By default, all the functions on this page are disabled.

Enable RIP&RIPng: After this function is enabled, LAN and WAN ports 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 Advanced Firewall: After this function is enabled, enhanced attack defense and packet protocol check will degrade the forwarding performance of the device.

Enable SIP ALG: Some voice communication uses the Session Initiation Protocol (SIP) protocol. If the server is connected to a WAN port, 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.

Disable ICMPv6 Error Messages: In normal cases, when the device receives an ICMPv6 anomaly packet, it sends an ICMPv6 error packet to the packet source. If you do not want the device to send these packets due to security considerations, enable this function.



Other Settings

Enable RIP&RIPng ○

Enable Advanced Firewall ○

Enable SIP ALG ○

Disable ICMPv6 Error Messages ○

4 Wireless Management

Note

Wireless management includes wireless function settings of the device and management of downlink wireless devices of the device. When self-organizing network discovery is enabled, the wireless settings are synchronized to all wireless devices in the network. You can configure groups to limit the device scope under wireless management. For details, see Section 4.1 .

4.1 Configuring AP Groups

4.1.1 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.

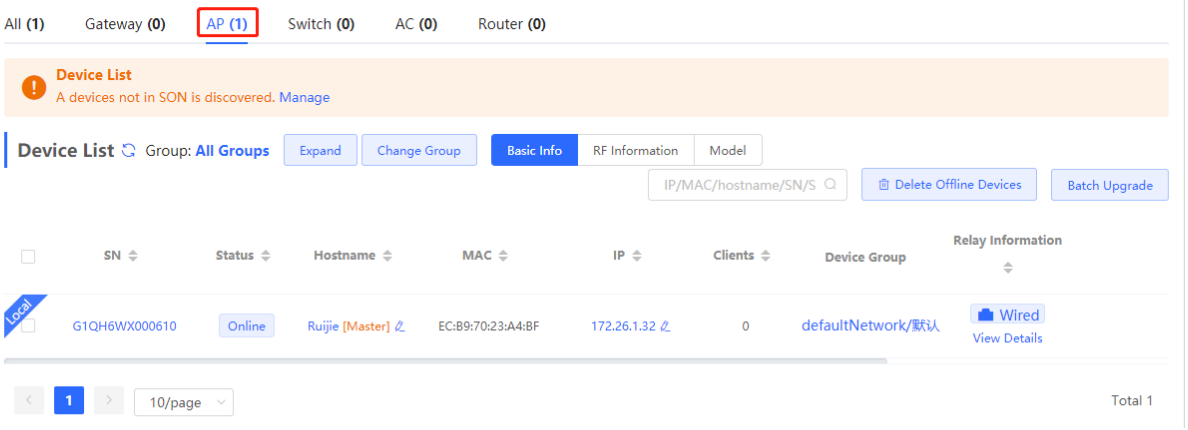
Note

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

4.1.2 Configuration Steps

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

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



All (1) Gateway (0) AP (1) Switch (0) AC (0) Router (0)

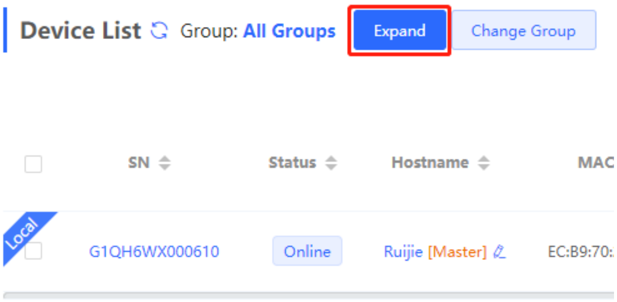
Device List
A devices not in SON is discovered. Manage

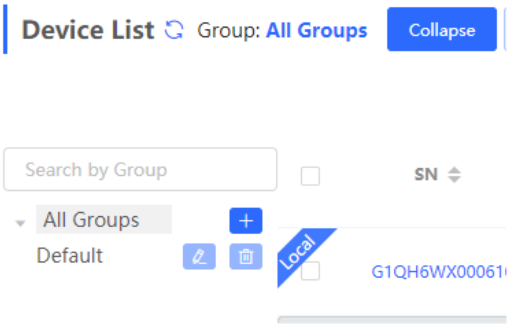
Device List Group: All Groups Expand Change Group Basic Info RF Information Model

IP/MAC/hostname/SN/S Delete Offline Devices Batch Upgrade

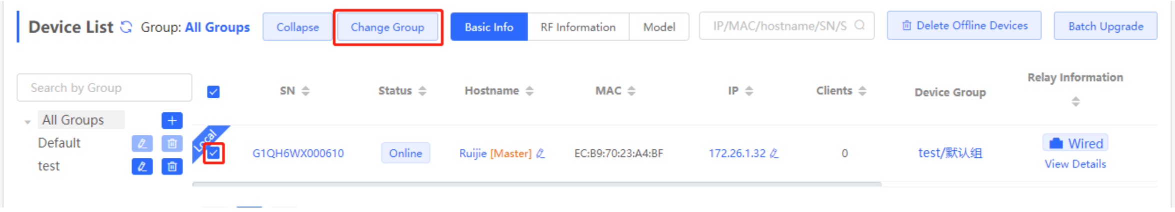
□	SN	Status	Hostname	MAC	IP	Clients	Device Group	Relay Information
□	G1QH6WX000610	Online	Ruijie [Master]	EC:B9:70:23:A4:BF	172.26.1.32	0	defaultNetwork/默认	Wired View Details

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

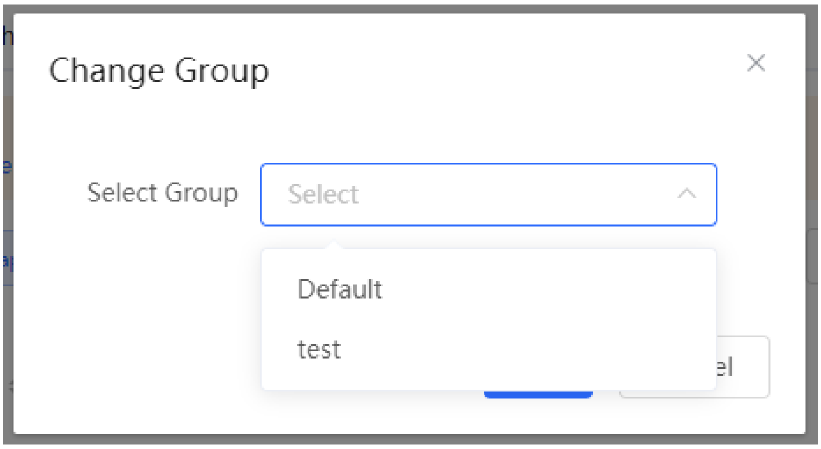




(3) Click a group name in the left. All devices in the group are displayed. One device can belong to only one group. By default, all devices belong to the default group. Select a record in the device list and click **Change Group** to migrate the selected device to the specified group. After a device 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.



☑	SN	Status	Hostname	MAC	IP	Clients	Device Group	Relay Information
☑	G1QH6WX000610	Online	Ruijie [Master]	EC:B9:70:23:A4:BF	172.26.1.32	0	test/默认组	Wired View Details



4.2 Configuring Wi-Fi

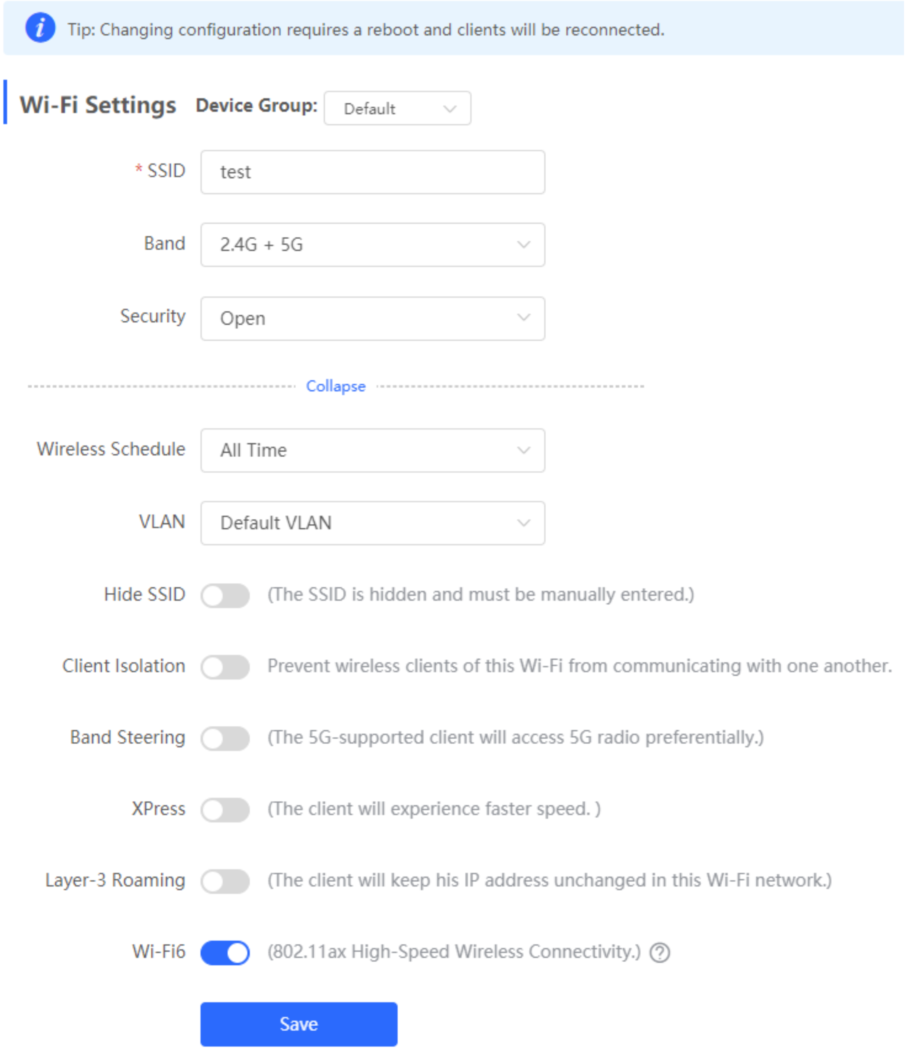
Choose **Network (WLAN)** > **Wi-Fi** > **Wi-Fi Settings**.

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

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

Caution

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



Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi Settings Device Group: Default

- * SSID: test
- Band: 2.4G + 5G
- Security: Open

- Wireless Schedule: All Time
- VLAN: Default VLAN
- Hide SSID: off (The SSID is hidden and must be manually entered.)
- Client Isolation: off Prevent wireless clients of this Wi-Fi from communicating with one another.
- Band Steering: off (The 5G-supported client will access 5G radio preferentially.)
- XPress: off (The client will experience faster speed.)
- Layer-3 Roaming: off (The client will keep his IP address unchanged in this Wi-Fi network.)
- Wi-Fi6: on (802.11ax High-Speed Wireless Connectivity.)

Table 4-1 Wireless network configuration

Parameter	Description
SSID	Enter the name displayed when a wireless client searches for a wireless network.
SSID Encoding	If the SSID does not contain Chinese, this item will be hidden. If the SSID contains Chinese, this item will be displayed. You can select UTF-8 or GBK.
Band	Set the band used by the Wi-Fi signal. The options are 2.4 GHz and 5 GHz. The 5 GHz band provides faster network transmission rate and less interference than the 2.4 GHz band, but is inferior to the 2.4 GHz band in terms of signal coverage range and wall penetration performance. Select a proper band based on actual needs. The default value is **2.4G + 5G**, indicating that the device provides signals at both 2.4 GHz and 5 GHz bands.

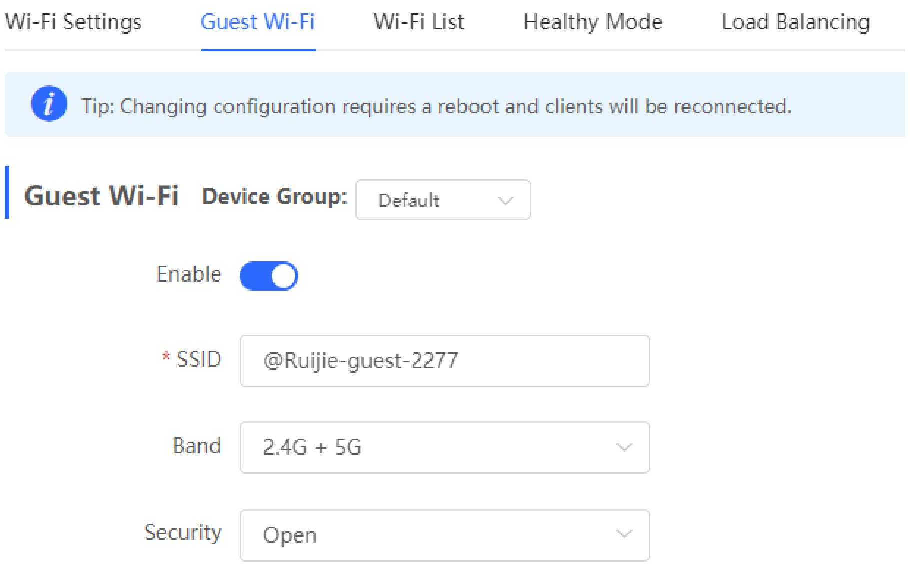
Parameter	Description
Security	Select an encryption mode for the wireless network connection. The options are as follows: Open: The device can associate with Wi-Fi without a password. WPA-PSK/WPA2-PSK: Wi-Fi Protected Access (WPA) or WPA2 is used for encryption. WPA_WPA2-PSK (recommended): WPA2-PSK or WPA-PSK is used for encryption.
Wi-Fi Password	Specify the password for connection to the wireless network. The password is a string of 8 to 16 characters.
Wireless Schedule	Specify the time periods during which Wi-Fi is enabled. After you set this parameter, users cannot connect to Wi-Fi in other periods.
VLAN	Set the VLAN to which the Wi-Fi signal belongs.
Hide SSID	Enabling the hide SSID function can prevent unauthorized user access to Wi-Fi, improving security. However, mobile phones or computers cannot find the 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	After you enable this parameter, clients associated with the Wi-Fi are isolated from one other, and end users connected to the same AP (in the same network segment) cannot access each other. This improves security.
Band Steering	After this function is enabled, 5G-capable clients select 5G Wi-Fi preferentially. You can enable this function only when **Band** is set to **2.4G + 5G**.
XPress	After this function is enabled, the device sends game packets preferentially, providing more stable wireless network for games.
Layer-3 Roaming	After this function is enabled, clients keep their IP addresses unchanged when associating with the same Wi-Fi. This function improves the roaming experience of users in the cross-VLAN scenario.
Wi-Fi6	After this function is enabled, wireless users can have faster network access speed and optimized network access experience. This function is valid only on APs and routers supporting 802.11ax. Clients must also support 802.11ax to experience high-speed network access empowered by Wi-Fi 6. If clients do not support Wi-Fi 6, disable this function.

4.3 Configuring Guest Wi-Fi

Choose **Network (WLAN)** > **Wi-Fi** > **Guest Wi-Fi**.

Guest Wi-Fi is a wireless network provided for guests, and is disabled by default. **Client Isolation** is enabled for guest Wi-Fi by default, and it cannot be disabled. In this case, users associating with guest Wi-Fi are mutually isolated, and they can only access the Internet through Wi-Fi. This improves network access security. You can configure a wireless schedule for the guest network. After the specified schedule expires, the guest network will become unreachable.

Turn on the guest Wi-Fi and set the guest SSID and password. Click **Advanced Settings** to configure the wireless schedule of the guest Wi-Fi and more Wi-Fi parameters. (For details, see Section 4.2 .) Click **Save**. Guests can access the Internet through Wi-Fi after entering the SSID and password.



Tip: Changing configuration requires a reboot and clients will be reconnected.

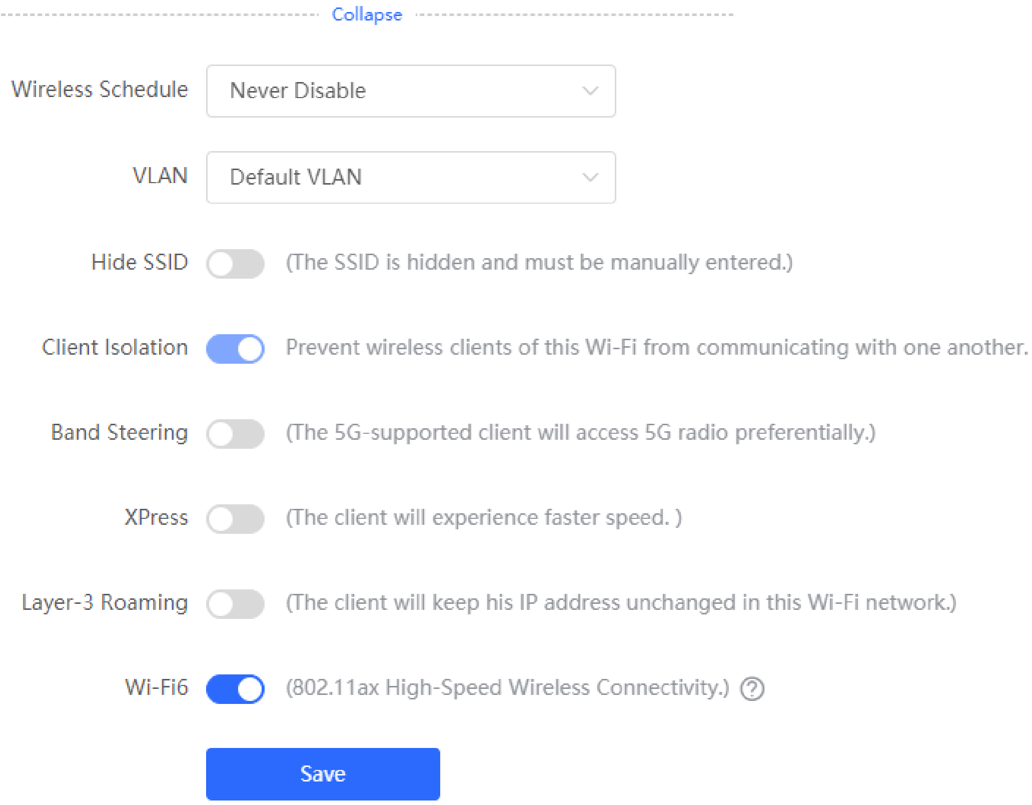
Guest Wi-Fi Device Group: Default

Enable

* SSID: @Ruijie-guest-2277

Band: 2.4G + 5G

Security: Open



Collapse

Wireless Schedule: Never Disable

VLAN: Default VLAN

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

Client Isolation: Prevent wireless clients of this Wi-Fi from communicating with one another.

Band Steering: (The 5G-supported client will access 5G radio preferentially.)

XPress: (The client will experience faster speed.)

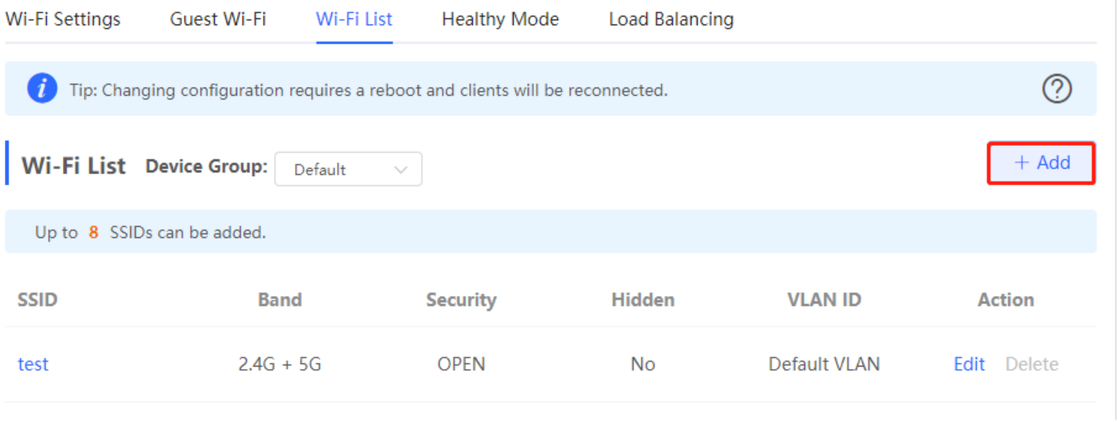
Layer-3 Roaming: (The client will keep his IP address unchanged in this Wi-Fi network.)

Wi-Fi6: (802.11ax High-Speed Wireless Connectivity.)

4.4 Adding a Wi-Fi

Choose **Network (WLAN)** > **Wi-Fi** > **Wi-Fi List**.

Click **Add**, enter the SSID and password, and click **OK** to create a Wi-Fi. Click **Advanced Settings** to configure more Wi-Fi parameters. For details, see Section 4.2 . After a Wi-Fi is added, clients can find this Wi-Fi, and the Wi-Fi information is displayed in the Wi-Fi list.

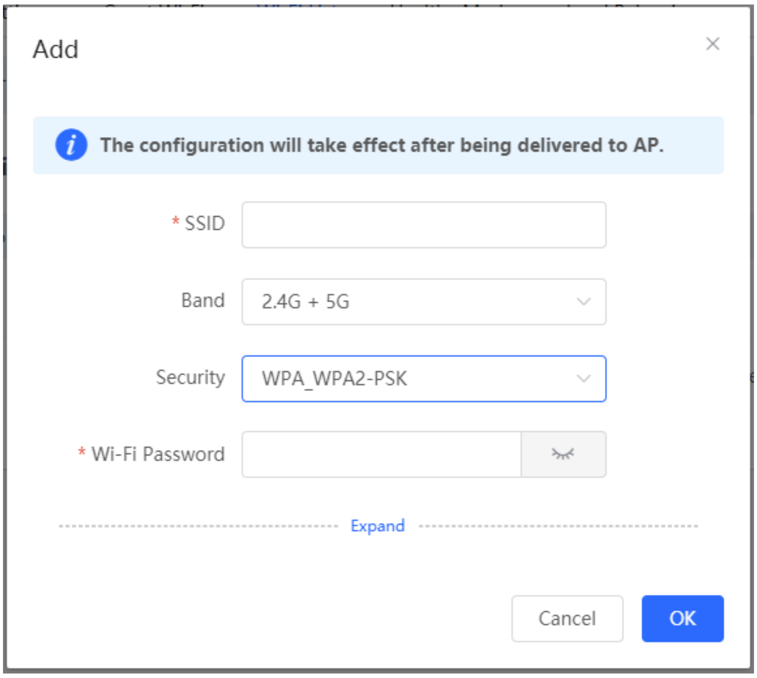


Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi List Device Group: Default

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
test	2.4G + 5G	OPEN	No	Default VLAN	Edit Delete



Add

The configuration will take effect after being delivered to AP.

* SSID:

Band: 2.4G + 5G

Security: WPA_WPA2-PSK

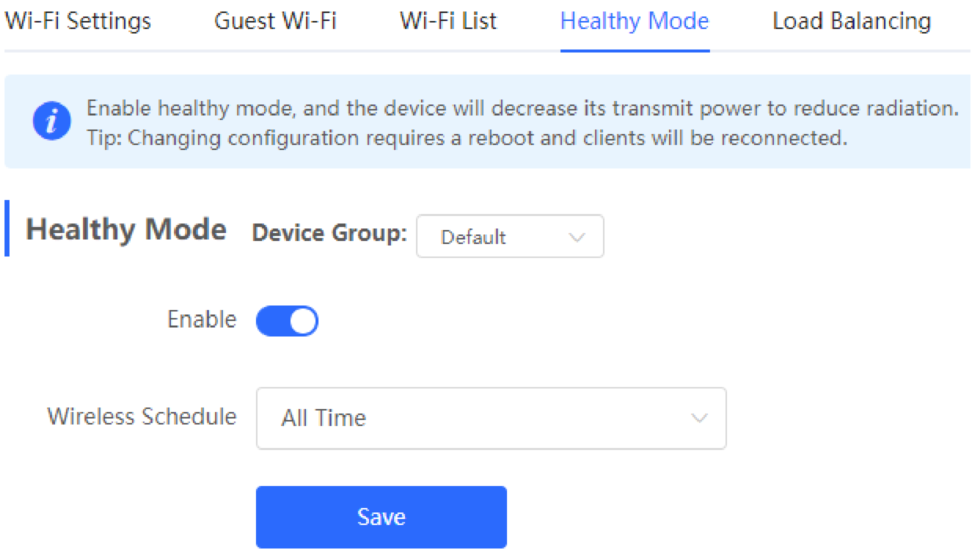
* Wi-Fi Password:

4.5 Healthy Mode

Choose **Network (WLAN)** > **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.



Enable healthy mode, and the device will decrease its transmit power to reduce radiation.
Tip: Changing configuration requires a reboot and clients will be reconnected.

Healthy Mode

Device Group: Default

Enable: On

Wireless Schedule: All Time

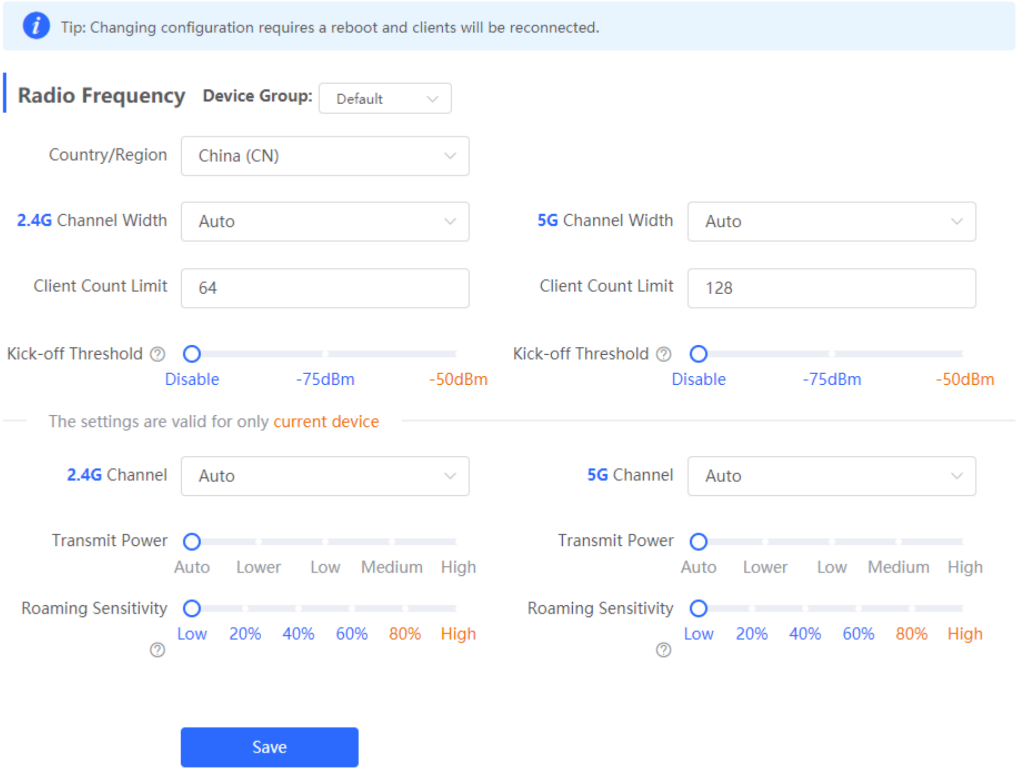
4.6 RF Settings

Choose **Network (WLAN)** > **Radio Frequency**.

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.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Radio Frequency Device Group: Default

Country/Region: China (CN)

2.4G Channel Width: Auto

5G Channel Width: Auto

Client Count Limit: 64

Client Count Limit: 128

Kick-off Threshold: Disable

Kick-off Threshold: Disable

The settings are valid for only current device

2.4G Channel: Auto

5G Channel: Auto

Transmit Power: Auto

Transmit Power: Auto

Roaming Sensitivity: Low

Roaming Sensitivity: Low

Table 4-2 RF configuration

Parameter	Description
Country/Region	The Wi-Fi channels stipulated by each country may be different. To ensure that clients can find the Wi-Fi signal, select the country or region where the device is located.
2.4G/5G Channel Width	A lower bandwidth indicates more stable network, and a higher bandwidth indicates easier interference. In case of severe interference, select a relatively low bandwidth to prevent network freezing to certain extent. The 2.4 GHz band supports the 20 MHz and 40 MHz bandwidths. The 5 GHz band supports the 20 MHz, 40 MHz, and 80 MHz bandwidths. By default, the value is **Auto**, indicating that the bandwidth is selected automatically based on the environment.

Parameter	Description
Client Count Limit	If a large number of users access the AP or router, the wireless network performance of the AP or router may be degraded, affecting users' Internet access experience. After you set this parameter, new user access is prohibited when the number of access users reaches the specified value. If the clients require high bandwidth, you can adjust this parameter to a smaller value. You are advised to keep the default value unless otherwise specified.
Kick-off Threshold	When multiple Wi-Fi signals are available, you can set this parameter to optimize the wireless signal quality to some extent. When a client is far away from the wireless device, the Wi-Fi connection is disconnected when the wireless signal strength of the end user is lower than the kick-off threshold. In this case, the client has to select a nearer wireless signal. The client is prone to be kicked off if the kick-off threshold is high. To ensure that the client can normally access the Internet, you are advised to set this parameter to **Disable** or a value smaller than -75 dBm.
2.4G/5G Channel	Before you set the channel, install WiFi Moho or another app with the Wi-Fi scan function on your mobile phone to view the interference analysis result and find the optimal channel. Select the optimal channel according to the analysis result. More wireless devices in the channel indicate larger interference.
Transmit Power	Larger transmit power indicates stronger wireless signal strength, wider coverage range, and larger interference to the surrounding wireless network. When a large number of APs or routers are deployed, you can appropriately adjust the transmit power to a lower value. By default, the wireless transmit power is automatically adjusted according to the environment. You are advised to retain the default configuration.
Roaming Sensitivity	Roaming sensitivity specifies the speed at which a moving wireless client connects to the optimal wireless signal. A high roaming sensitivity indicates a narrow coverage range of the wireless signal. When the client is moving and multiple Wi-Fi signals are available, you can increase the roaming sensitivity to improve the wireless signal quality. You are advised to retain the default configuration.

Note

Wireless channels available for your selection are determined by the country code. Select the country code based on the country or region of your device.

Channel, transmit power, and roaming sensitivity cannot be set globally, and the configuration is valid only on the current device. To modify related configuration for other devices, configure these devices separately.

4.7 Configuring Wi-Fi Blacklist or Whitelist

4.7.1 Overview

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

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

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

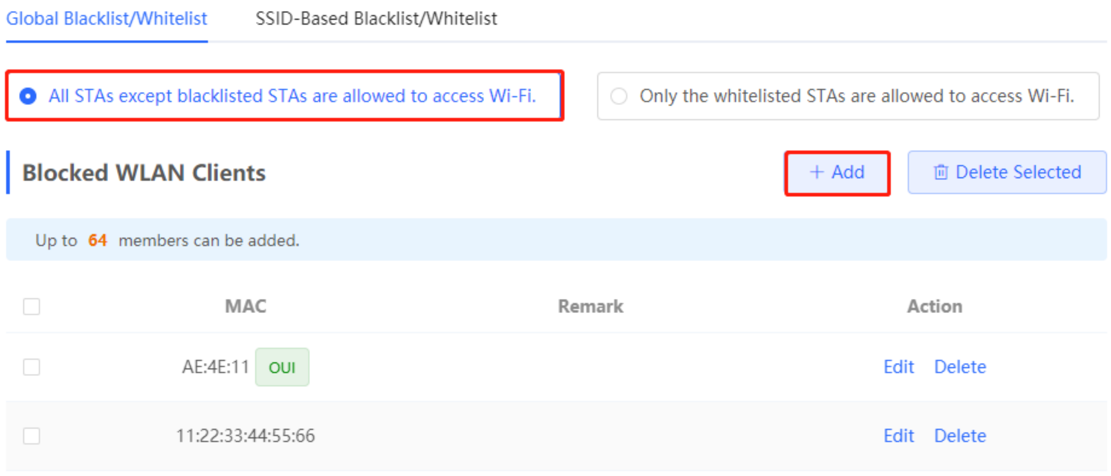
⚠ **Caution**

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

4.7.2 Configuring a Global Blacklist/Whitelist

Choose **Clients (WLAN)** > **Blacklist/Whitelist** > **Global Blacklist/Whitelist**.

Select the blacklist or whitelist mode and click **Add** to configure a blacklist or whitelist client. In the **Add** dialog box, enter the MAC address and remark 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 blacklist will be forced offline and not allowed to access the Wi-Fi network. The global blacklist and whitelist settings take effect on all Wi-Fi networks of the router.

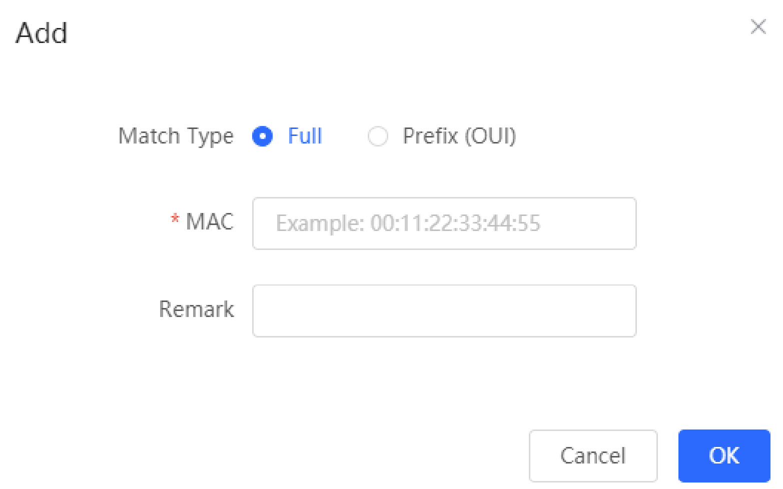


● All STAs except blacklisted STAs are allowed to access Wi-Fi.
○ Only the whitelisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients

Up to 64 members can be added.

	MAC	Remark	Action
□	AE:4E:11 OUI		Edit Delete
□	11:22:33:44:55:66		Edit Delete

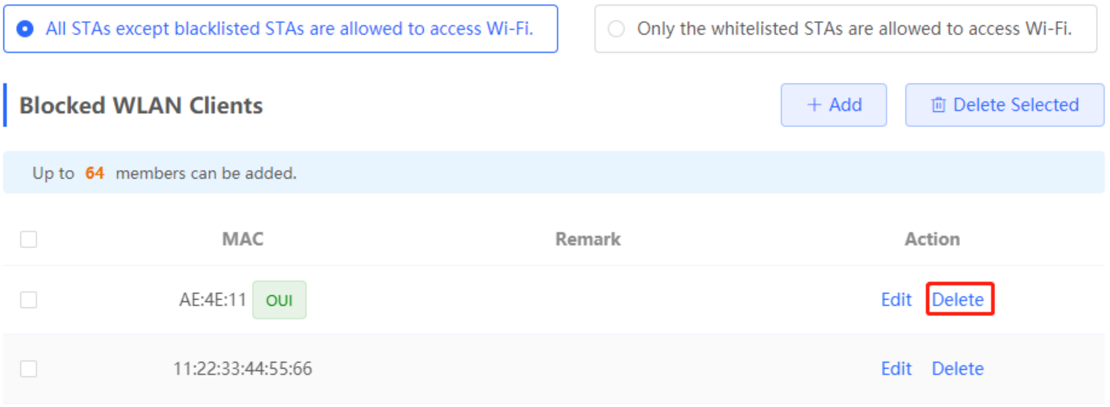


Match Type ● Full ○ Prefix (OUI)

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

Remark

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



● All STAs except blacklisted STAs are allowed to access Wi-Fi.　○ Only the whitelisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients

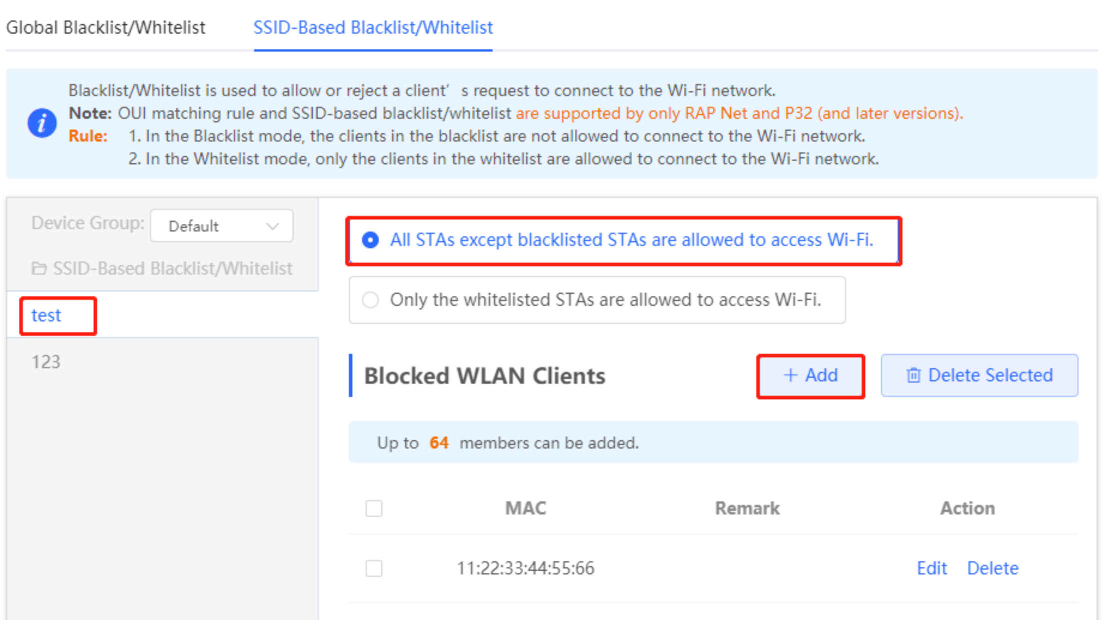
Up to 64 members can be added.

□	MAC	Remark	Action
□	AE:4E:11 OUI		Edit Delete
□	11:22:33:44:55:66		Edit Delete

4.7.3 Configuring an SSID-based Blacklist/Whitelist

Choose **Clients (** **WLAN)** > **Blacklist/Whitelist** > **SSID-Based Blacklist/Whitelist**.

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



Blacklist/Whitelist is used to allow or reject a client' s request to connect to the Wi-Fi network.

Note: OUI matching rule and SSID-based blacklist/whitelist are supported by only RAP Net and P32 (and later versions).

Rule: 1. In the Blacklist mode, the clients in the blacklist are not allowed to connect to the Wi-Fi network.
2. In the Whitelist mode, only the clients in the whitelist are allowed to connect to the Wi-Fi network.

Device Group: Default

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

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

Blocked WLAN Clients

Up to 64 members can be added.

□	MAC	Remark	Action
□	11:22:33:44:55:66		Edit Delete

4.8 Configuring AP Load Balancing

4.8.1 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.

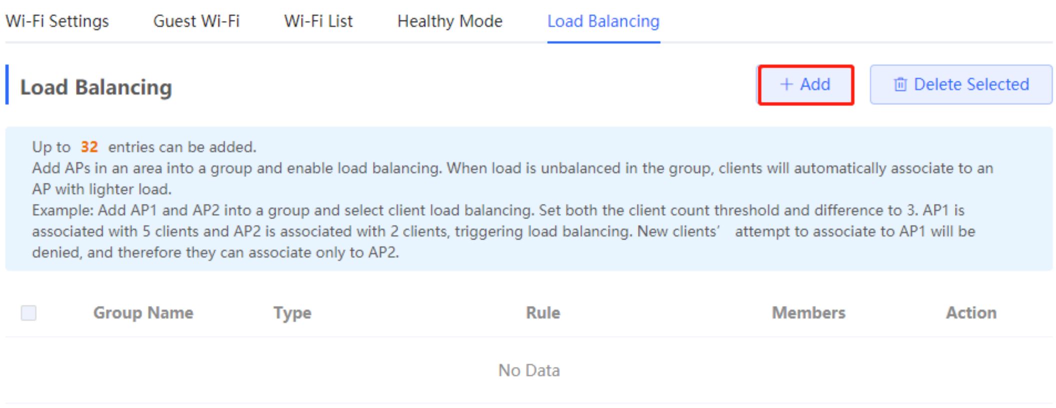
Example: Add AP1 and AP2 into a group and select client load balancing. Set both the client count threshold and difference to 3. AP1 is associated with 5 clients and AP2 is associated with 2 clients, triggering load balancing. New clients' attempt to associate to AP1 will be denied, and therefore they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

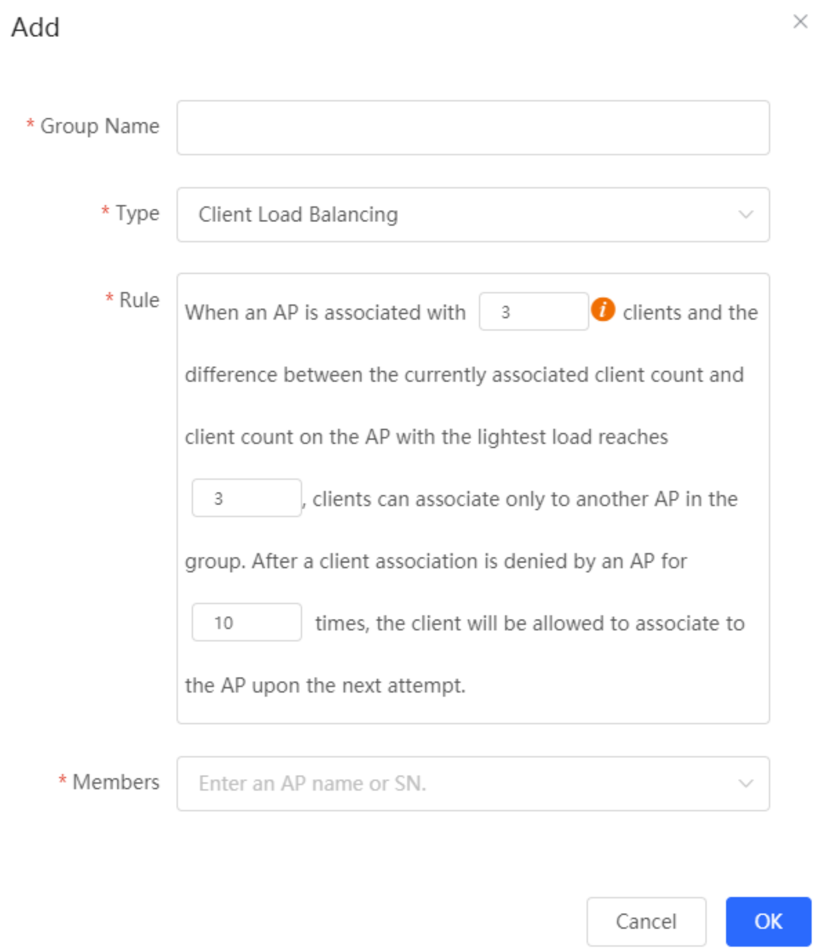
4.8.2 Configuring Client Load Balancing

Choose **Network (WLAN)** > **Wi-Fi** > **Load Balancing**.

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



Up to 32 entries can be added.
Add APs in an area into a group and enable load balancing. When load is unbalanced in the group, clients will automatically associate to an AP with lighter load.
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 to AP2.



* Group Name:

* Type: Client Load Balancing

* Rule: 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: Enter an AP name or SN.

Table 4-3 Client load balancing configuration

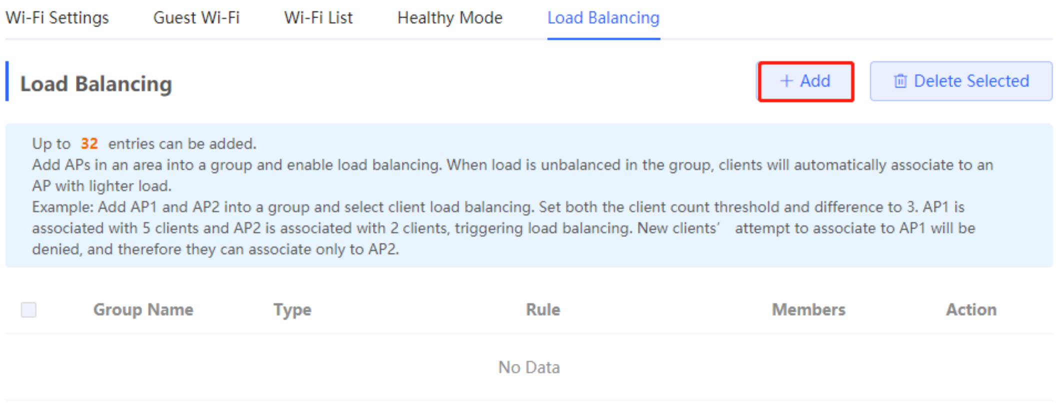
Parameter	Description
Group Name	Enter the name of the AP load balancing group.
Type	Select **Client Load Balancing**.

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.

4.8.3 Configuring Traffic Load Balancing

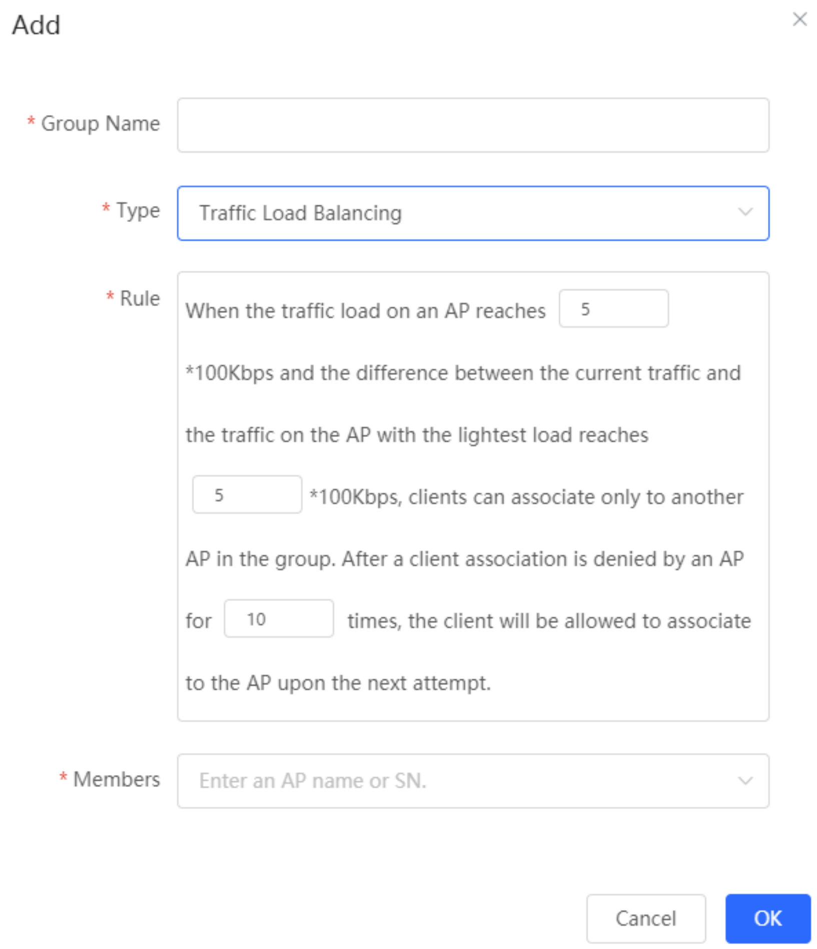
Choose **Network (WLAN)** > **Wi-Fi** > **Load Balancing**.

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



Up to 32 entries can be added.
Add APs in an area into a group and enable load balancing. When load is unbalanced in the group, clients will automatically associate to an AP with lighter load.
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 to AP2.

□	Group Name	Type	Rule	Members	Action
No Data					



* Group Name

* Type: Traffic Load Balancing

* Rule: When the traffic load on an AP reaches 5 *100Kbps and the difference between the current traffic and the traffic on the AP with the lightest load reaches 5 *100Kbps, 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: Enter an AP name or SN.

Table 4-4 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 Kbit/s, 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.

4.9 Wireless Network Optimization

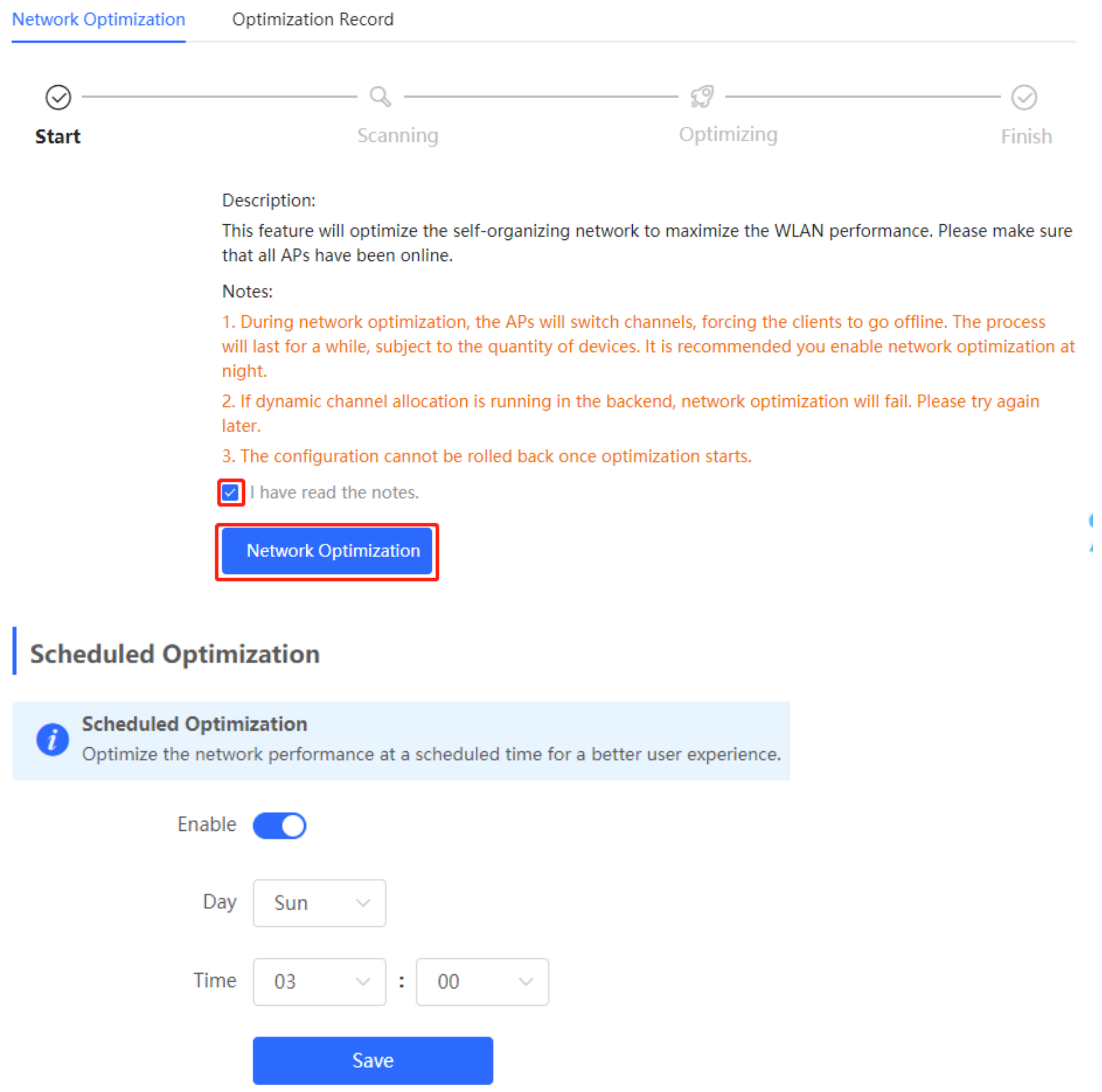
4.9.1 Wireless Network Optimization with One Click

Choose **Network** > **WIO**.

On the **Network Optimization** tab, select **I have read the notes** and click **Network Optimization** to perform automatic wireless network optimization in the networking environment. You can configure scheduled optimization to optimize the network at the specified time. You are advised to set the scheduled optimization time to daybreak or the idle periods.

Caution

Clients may be kicked offline during optimization and the configuration cannot be rolled back after optimization starts. Exercise caution when performing this operation.



Description:
This feature will optimize the self-organizing network to maximize the WLAN performance. Please make sure that all APs have been online.

Notes:

1. During network optimization, the APs will switch channels, forcing the clients to go offline. The process will last for a while, subject to the quantity of devices. It is recommended you enable network optimization at night.
2. If dynamic channel allocation is running in the backend, network optimization will fail. Please try again later.
3. The configuration cannot be rolled back once optimization starts.

☑ I have read the notes.

Network Optimization

Scheduled Optimization

Scheduled Optimization
Optimize the network performance at a scheduled time for a better user experience.

Enable: On

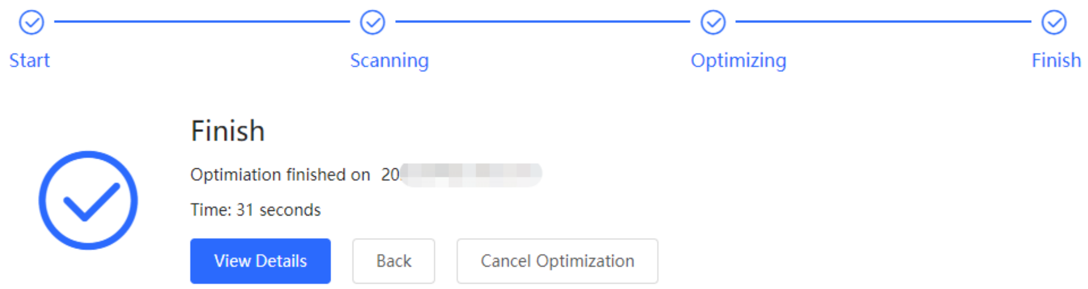
Day: Sun

Time: 03 : 00

Save

After optimization starts, please wait patiently until optimization is complete. After optimization ends, click **Cancel Optimization** to restore optimized RF parameters to default values.

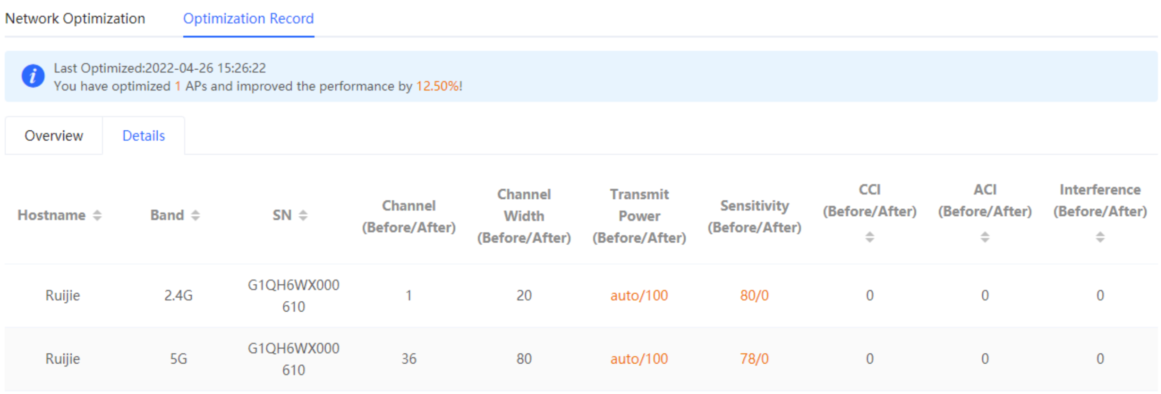
Click **View Details** or the **Optimization Record** tab to view the latest optimization record details.



Finish

Optimiation finished on 20[redacted]

Time: 31 seconds



Last Optimized:2022-04-26 15:26:22
You have optimized 1 APs and improved the performance by 12.50%!

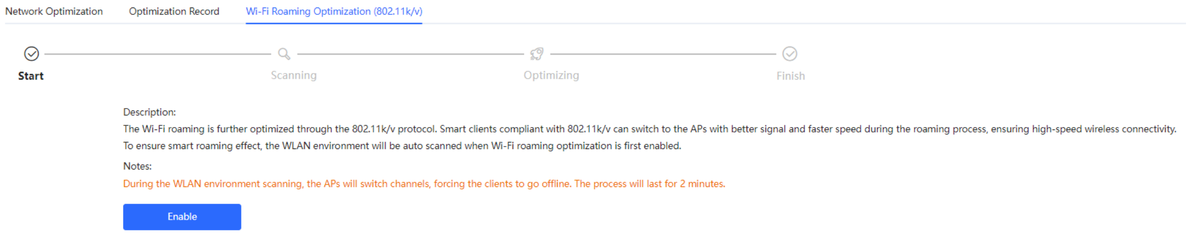
Hostname	Band	SN	Channel (Before/After)	Channel Width (Before/After)	Transmit Power (Before/After)	Sensitivity (Before/After)	CCI (Before/After)	ACI (Before/After)	Interference (Before/After)
Ruijie	2.4G	G1QH6WX000610	1	20	auto/100	80/0	0	0	0
Ruijie	5G	G1QH6WX000610	36	80	auto/100	78/0	0	0	0

4.9.2 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** > **WIO** > **Wi-Fi Roaming Optimization (802.11k/v)**.



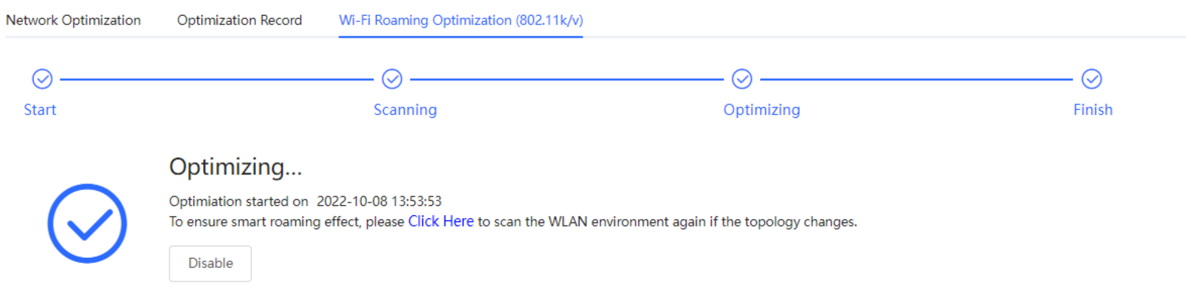
Description:
The Wi-Fi roaming is further optimized through the 802.11k/v protocol. Smart clients compliant with 802.11k/v can switch to the APs with better signal and faster speed during the roaming process, ensuring high-speed wireless connectivity.
To ensure smart roaming effect, the WLAN environment will be auto scanned when Wi-Fi roaming optimization is first enabled.

Notes:
During the WLAN environment scanning, the APs will switch channels, forcing the clients to go offline. The process will last for 2 minutes.

Caution

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

Click **Enable** and the optimization starts.



Optimizing...

Optimiation started on 2022-10-08 13:53:53

To ensure smart roaming effect, please Click Here to scan the WLAN environment again if the topology changes.

4.10 Wi-Fi Authentication

4.10.1 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 or following the WeChat official accounts. 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.

4.10.2 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. Encryption may lead to exceptions during Connect Wi-Fi via WeChat authentication.

(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 4.10.9 Authentication-Free.

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

4.10.3 WeChat Authentication

1. Overview

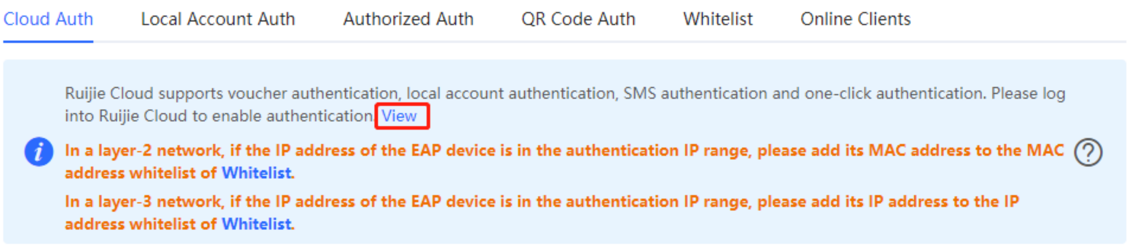
The EG device is connected to the MACC authentication server on the cloud. After Wi-Fi users connect to Wi-Fi, a Portal page pops up. The users need to jump to WeChat and follow the WeChat official account before they can access the Internet. WeChat authentication is applicable to the shopping mall scenario, where merchants guide customers to follow their WeChat official accounts through WeChat authentication.

2. Getting Started

(1) Connect Wi-Fi via WeChat 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 WeChat Official Account platform and NOC MACC platform before you enable the authentication function on the device. Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication, and one-click authentication. Please log into Ruijie Cloud to enable authentication.



Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication and one-click authentication. Please log into Ruijie Cloud to enable authentication. View

In a layer-2 network, if the IP address of the EAP device is in the authentication IP range, please add its MAC address to the MAC address whitelist of Whitelist.

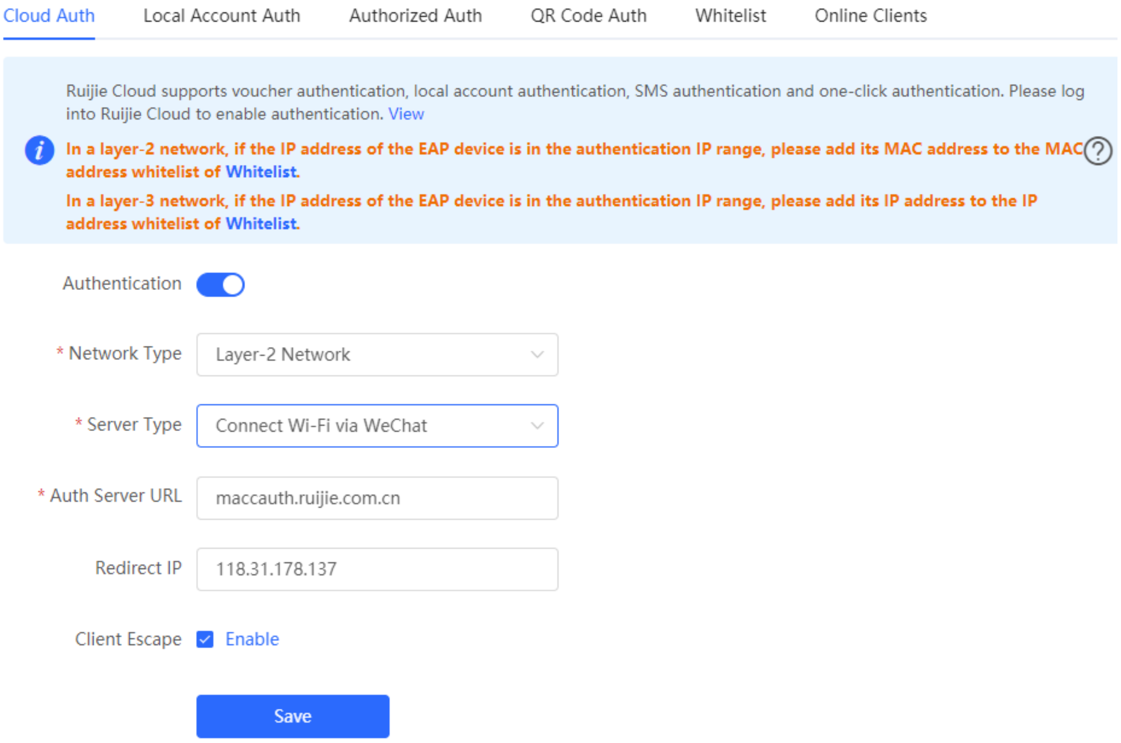
In a layer-3 network, if the IP address of the EAP device is in the authentication IP range, please add its IP address to the IP address whitelist of Whitelist.

3. Configuration Steps

Choose **Local Device** > **Advanced** > **Authentication** > **Cloud Auth**.

(1) Enable WeChat authentication for Internet access.

Turn on **Authentication**, set **Server Type** to **Connect Wi-Fi via WeChat**, configure **Network Type**, **Auth Server URL**, **Redirect IP**, and **Client Escape**, and click **Save**.



Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication and one-click authentication. Please log into Ruijie Cloud to enable authentication. View

In a layer-2 network, if the IP address of the EAP device is in the authentication IP range, please add its MAC address to the MAC address whitelist of Whitelist.

In a layer-3 network, if the IP address of the EAP device is in the authentication IP range, please add its IP address to the IP address whitelist of Whitelist.

Authentication: On

* Network Type: Layer-2 Network

* Server Type: Connect Wi-Fi via WeChat

* Auth Server URL: maccauth.ruijie.com.cn

Redirect IP: 118.31.178.137

Client Escape: ☑ Enable

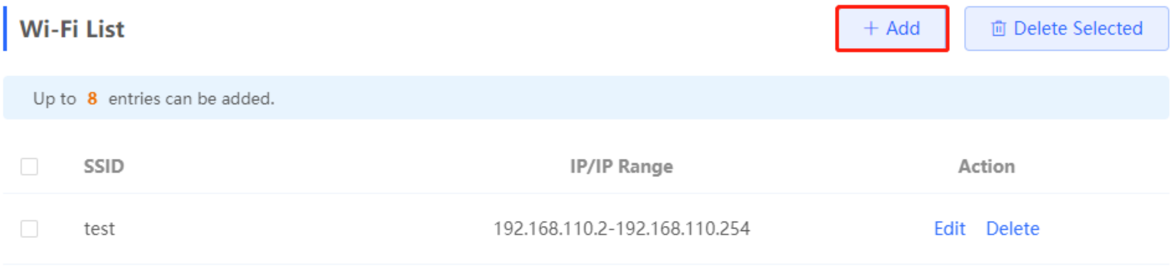
Table 4-5 WeChat authentication configuration

Parameter	Description
Network Type	The default value is **Layer-2 Network**. Select a network type based on the actual network environment. As Connect Wi-Fi via WeChat is a Layer 2 protocol, in a Layer 3 network environment, you need to connect downlink devices to the current authentication device through the DHCP relay and deploy the DHCP address pool for the authentication-engaged network segments in the authentication device. In this way, the authentication device can obtain MAC addresses of wireless users through DHCP. In this scenario, set this parameter to **Layer-3 Network**.
Server Type	Select **Connect Wi-Fi via WeChat**.
Auth Server URL	After you complete the MACC server configuration, the MACC server returns a URL. The device sends an authentication request to this URL.
Redirect IP	The redirect IP address corresponds to a menu or link address set in the official account. The default value is 118.31.178.137. Generally, you do not need to change the value. After the user is redirected to the WeChat official account, the user needs to visit this IP address before the subsequent authentication steps can continue. Change the value to an IP address in a not used LAN network segment, if required. For details, see Troubleshooting.
Client Escape	After this function is enabled, the authentication function is disabled on the device if the authentication server fails, so that all the users can directly access the Internet. After the server recovers, the authentication function is started automatically.

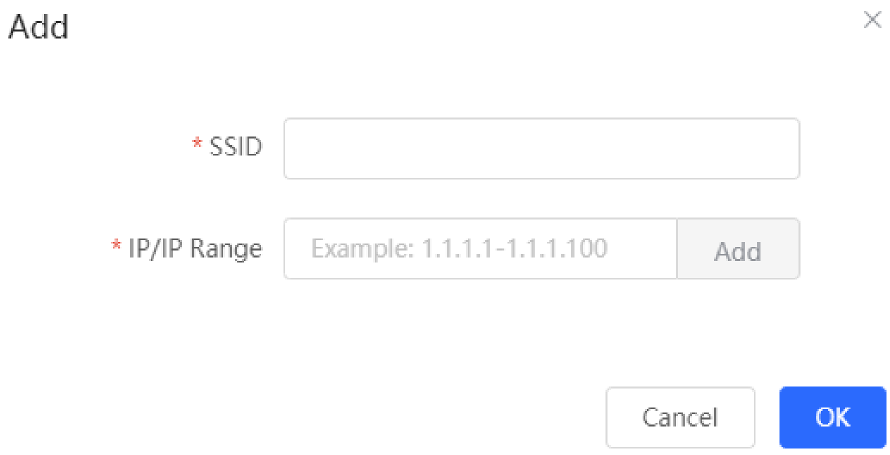
(2) Configure the authentication scope.

Click **Add** on the current page. In the dialog box that appears, enter the SSID and IP address range that needs authentication, and click **OK**.

For clients that do not need authentication, such as printers, computers, or some users, set **IP/IP Range** to authentication-free, so that these clients can directly access the Internet. For details, see Section 4.10.9 Authentication-Free.



□	SSID	IP/IP Range	Action
□	test	192.168.110.2-192.168.110.254	Edit Delete


Add

* SSID

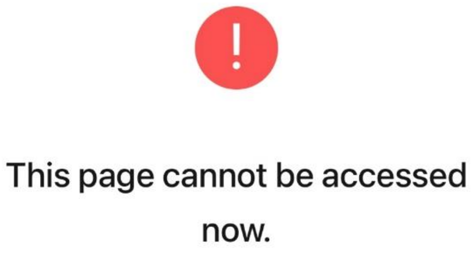
* IP/IP Range Example: 1.1.1.1-1.1.1.100

4. Verifying Configuration

When a mobile phone connects to the specific Wi-Fi, the Portal authentication page pops up automatically. The user visits the WeChat page under instructions on the Portal authentication page, follows the WeChat official account, clicks the menu or auto reply link to complete authentication. Then, the user can normally access the Internet. After successful user authentication, you can choose **Advanced** > **Authentication** > **Online Clients** to view information about this authenticated user. For details, see Section 4.10.10 Online Authenticated User Management.

5. Troubleshooting

- When the user clicks the authentication menu or link in the official account during WeChat authentication, the message **This page cannot be accessed now.** pops up, leading to authentication failure.

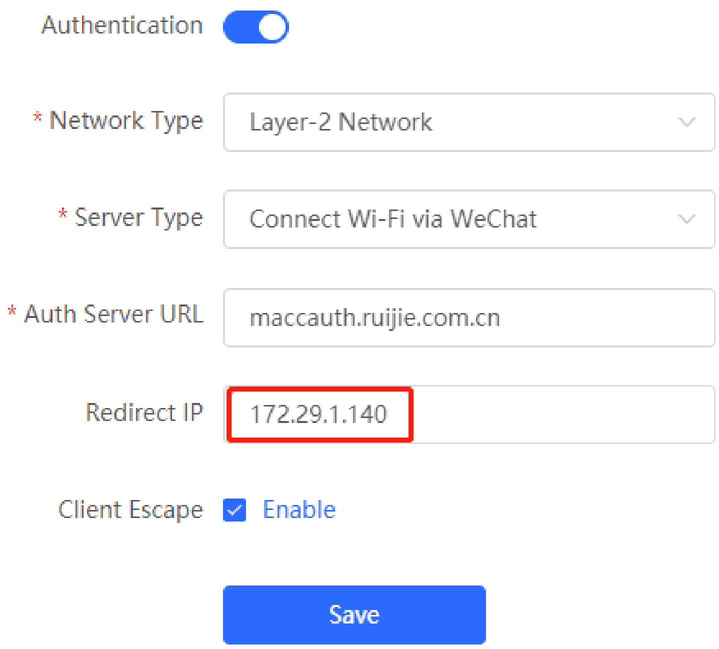

This page cannot be accessed now.

Cause: The link address set in the official account authentication entry in the Official Account Platform is regarded as insecure by Security Center of the WeChat client. When a client sends a request to this address, WeChat blocks this request.

Solution: Change the forced redirection address and the address in the official account authentication menu or link to an IP address not used in the LAN. For example, if the network segment 172.29.0.0 is not used in the LAN, set both the official account redirection IP address and the link address in the official account to 172.29.1.140.

⚠ **Caution**

If the official account redirection IP address is set to an IP address in a network segment used in the LAN, WeChat authentication will fail.



Authentication

* Network Type: Layer-2 Network

* Server Type: Connect Wi-Fi via WeChat

* Auth Server URL: maccauth.ruijie.com.cn

Redirect IP: 172.29.1.140

Client Escape: ☑ Enable

4.10.4 Enterprise WeChat Authentication

1. **Overview**

Similar to WeChat authentication, Wi-Fi users need to jump to the enterprise WeChat after connecting to Wi-Fi and complete applet authentication in the workspace before they can access the Internet. Enterprise WeChat authentication can be used to manage Internet access of employee clients and guest clients in the enterprise environment.

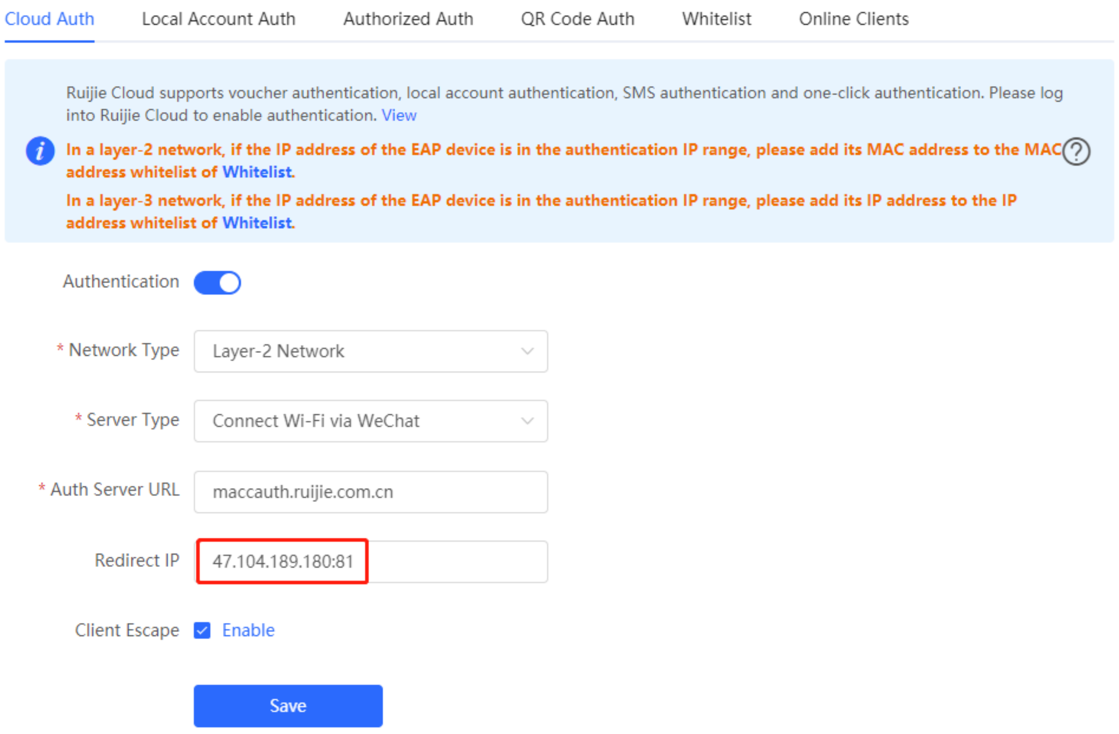
2. **Getting Started**

Same as those in Section 4.10.3 WeChat Authentication. Before you enable enterprise WeChat authentication, complete relevant configurations on the enterprise WeChat console and NOC MACC platform.

3. **Configuration Steps**

Choose **Local Device** > **Advanced** > **Authentication** > **Cloud Auth**.

The configuration steps are similar to those in WeChat authentication, with major difference in that the official account redirection IP address in enterprise WeChat authentication should be set to 47.104.189.180:81. For details, see Section 4.10.3 WeChat Authentication.



Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication and one-click authentication. Please log into Ruijie Cloud to enable authentication. View

In a layer-2 network, if the IP address of the EAP device is in the authentication IP range, please add its MAC address to the MAC address whitelist of Whitelist.

In a layer-3 network, if the IP address of the EAP device is in the authentication IP range, please add its IP address to the IP address whitelist of Whitelist.

Authentication: ●

* Network Type: Layer-2 Network

* Server Type: Connect Wi-Fi via WeChat

* Auth Server URL: maccauth.ruijie.com.cn

Redirect IP: 47.104.189.180:81

Client Escape: ☑ Enable

4. Employee Authentication

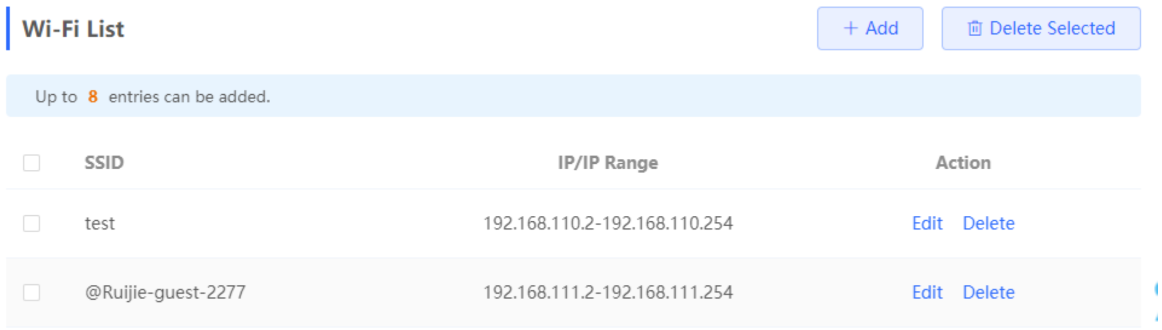
Make sure that the employee has joined the enterprise WeChat organization. When the employee connects the mobile phone to Wi-Fi, the employee is automatically redirected to the enterprise WeChat for authentication. After the employee opens the enterprise WeChat, employee needs to enter the **Workspace** menu of the enterprise WeChat and click the authentication app created by the administrator to obtain Internet access permission. After the authentication success message pops up, the employee can access the Internet normally.

The enterprise WeChat may not be started on the Portal authentication page on some mobile phones due to poor compatibility. If this occurs, users can manually open the enterprise WeChat and continue follow-up operations.

5. Guest Authentication

Guest access to the Internet via Wi-Fi should be authorized by the receptionist. After a guest connects to the guest Wi-Fi, the authentication QR code pops up. At this time, the authenticated employee scans the QR code using the enterprise WeChat on the mobile phone and enters the guest name. Then, the guest can pass authentication and access the Internet normally.

It should be noted that when configuring guest authentication, you need to configure at least two Wi-Fi SSIDs and corresponding network segments in the Wi-Fi list, which are used for employee connection and guest connection, respectively.



Up to 8 entries can be added.

□	SSID	IP/IP Range	Action
□	test	192.168.110.2-192.168.110.254	Edit Delete
□	@Ruijie-guest-2277	192.168.111.2-192.168.111.254	Edit Delete

4.10.5 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 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.

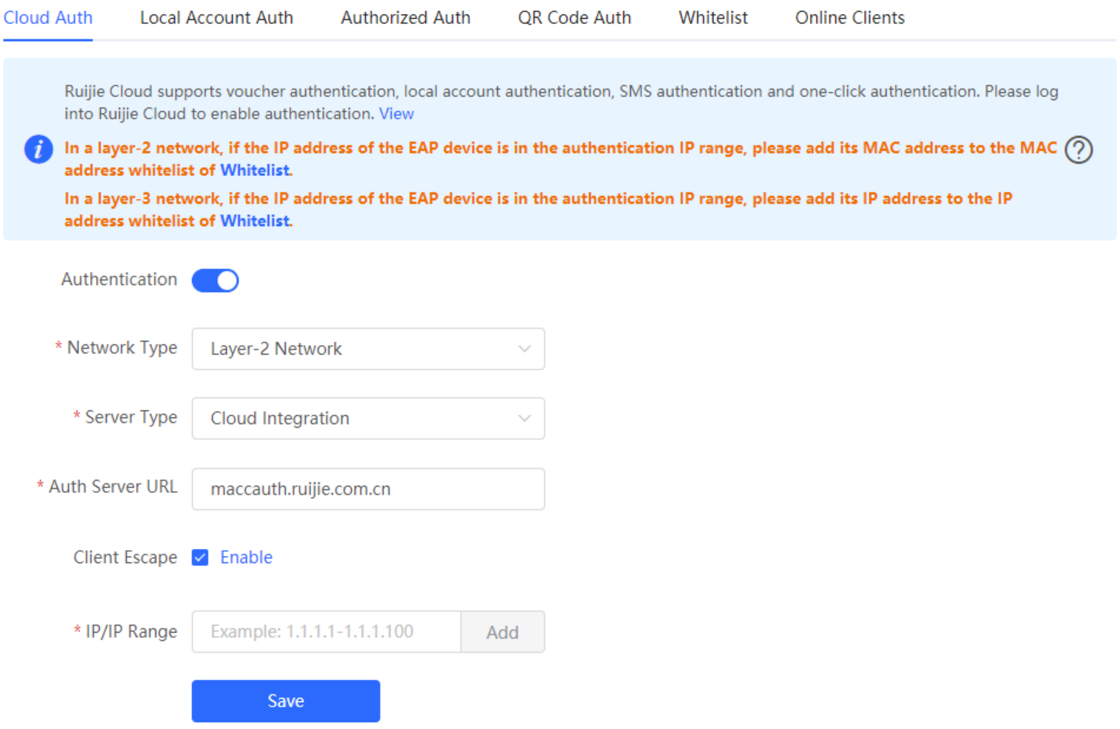
- The gateway address of the wireless users to be authenticated is deployed on the authentication device.
- If the gateway address is not deployed on the authentication device, the device functions as a DHCP server to allocate IP addresses to the wireless users and obtain MAC addresses of the wireless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

(2) Complete the corresponding configuration on the NOC MACC 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 **Local Device** > **Advanced** > **Authentication** > **Cloud Auth**.

Turn on **Authentication**, set **Server Type** to **Cloud Integration**, configure **Network Type**, **Auth Server URL**, **Client Escape**, and **IP/IP Range**, and click **Save**.



Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication and one-click authentication. Please log into Ruijie Cloud to enable authentication. View

In a layer-2 network, if the IP address of the EAP device is in the authentication IP range, please add its MAC address to the MAC address whitelist of Whitelist.

In a layer-3 network, if the IP address of the EAP device is in the authentication IP range, please add its IP address to the IP address whitelist of Whitelist.

Authentication: enabled

* Network Type: Layer-2 Network

* Server Type: Cloud Integration

* Auth Server URL: maccauth.ruijie.com.cn

Client Escape: ☑ Enable

* IP/IP Range: Example: 1.1.1.1-1.1.1.100

Table 4-6 WiFiDog authentication configuration

Parameter	Description
Network Type	The default value is **Layer-2 Network**. Select a network type based on the actual network environment.
Server Type	Select **Cloud Integration**.
Auth Server URL	After you complete the MACC server configuration, the MACC server returns a URL. The device sends an authentication request to this URL.
Client Escape	After this function is enabled, the authentication function is disabled on the device if the authentication server fails, so that all the users can directly access the Internet. After the server recovers, the authentication function is started automatically.
IP/IP Range	Specify the IP address range for authentication. The value can be 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 are supported.

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 MACC 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 MACC 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 MACC 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 **Advanced** > **Authentication** > **Online Clients** to view information about this authenticated user. For details, see Section 4.10.10 Online Authenticated User Management.

4.10.6 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

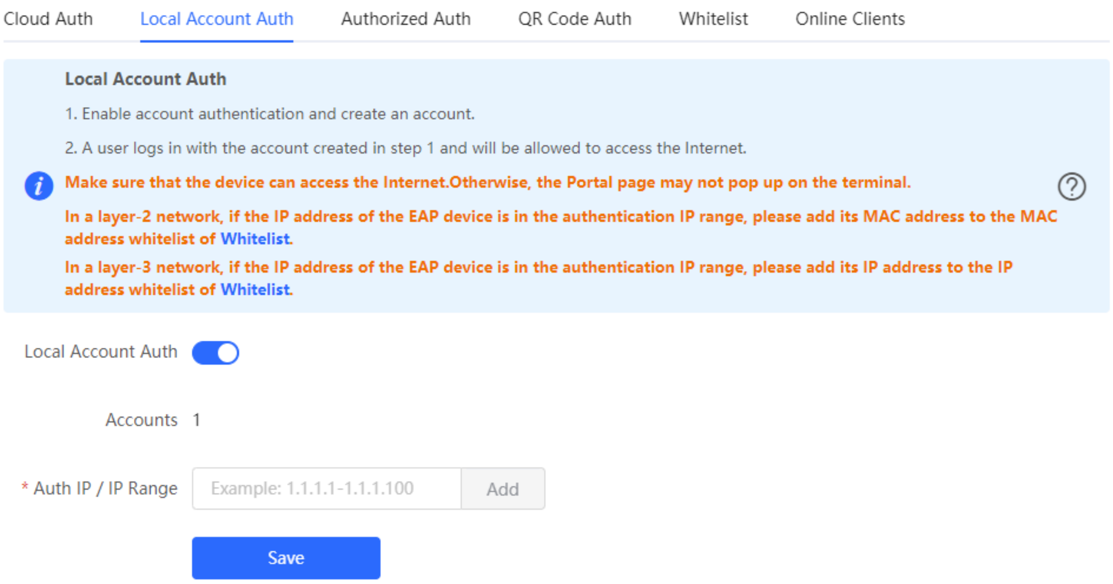
Ensure that the device with the authentication function enabled has been connected to the Internet. Otherwise, the authentication page does not pop up when a client associates with Wi-Fi.

3. Configuration Steps

Choose **Local Device** > **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.



Local Account Auth

1. Enable account authentication and create an account.

2. A user logs in with the account created in step 1 and will be allowed to access the Internet.

Make sure that the device can access the Internet.Otherwise, the Portal page may not pop up on the terminal.

In a layer-2 network, if the IP address of the EAP device is in the authentication IP range, please add its MAC address to the MAC address whitelist of Whitelist.

In a layer-3 network, if the IP address of the EAP device is in the authentication IP range, please add its IP address to the IP address whitelist of Whitelist.

Local Account Auth: On

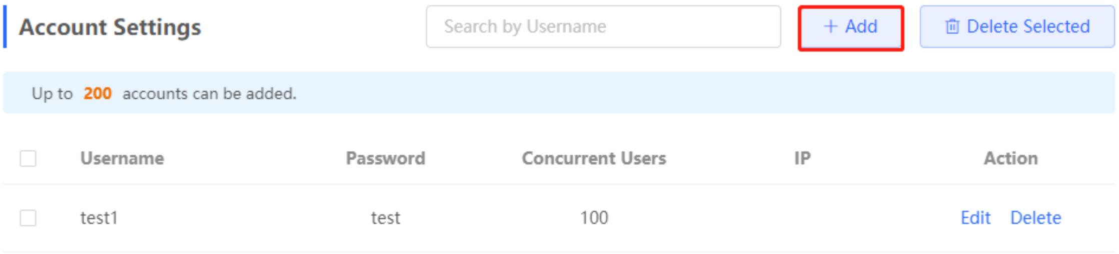
Accounts 1

* Auth IP / IP Range: Example: 1.1.1.1-1.1.1.100 Add

(2) Configure an authentication account.

Click **Add** to configure an authentication account for Internet access. Multiple clients can access the Internet using the same account and password. The **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 **IP** column next to the account. The account list records a maximum of five latest device IP addresses using the same account.



Account Settings

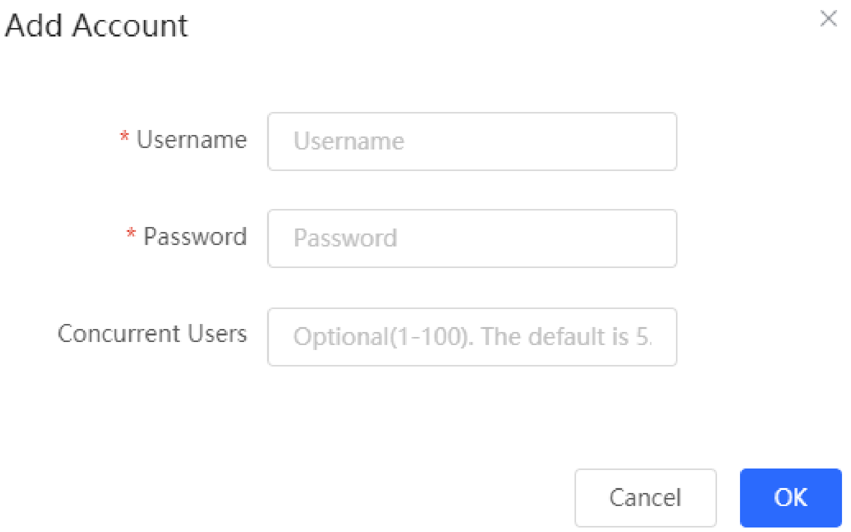
Search by Username

+ Add

Delete Selected

Up to 200 accounts can be added.

□	Username	Password	Concurrent Users	IP	Action
□	test1	test	100		Edit Delete



Add Account

* Username: Username

* Password: Password

Concurrent Users: Optional(1-100). The default is 5.

Cancel OK

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 **Advanced** > **Authentication** > **Online Clients** to view information about the successfully connected user. For details, see Section 4.10.10 Online Authenticated User Management.

4.10.7 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.

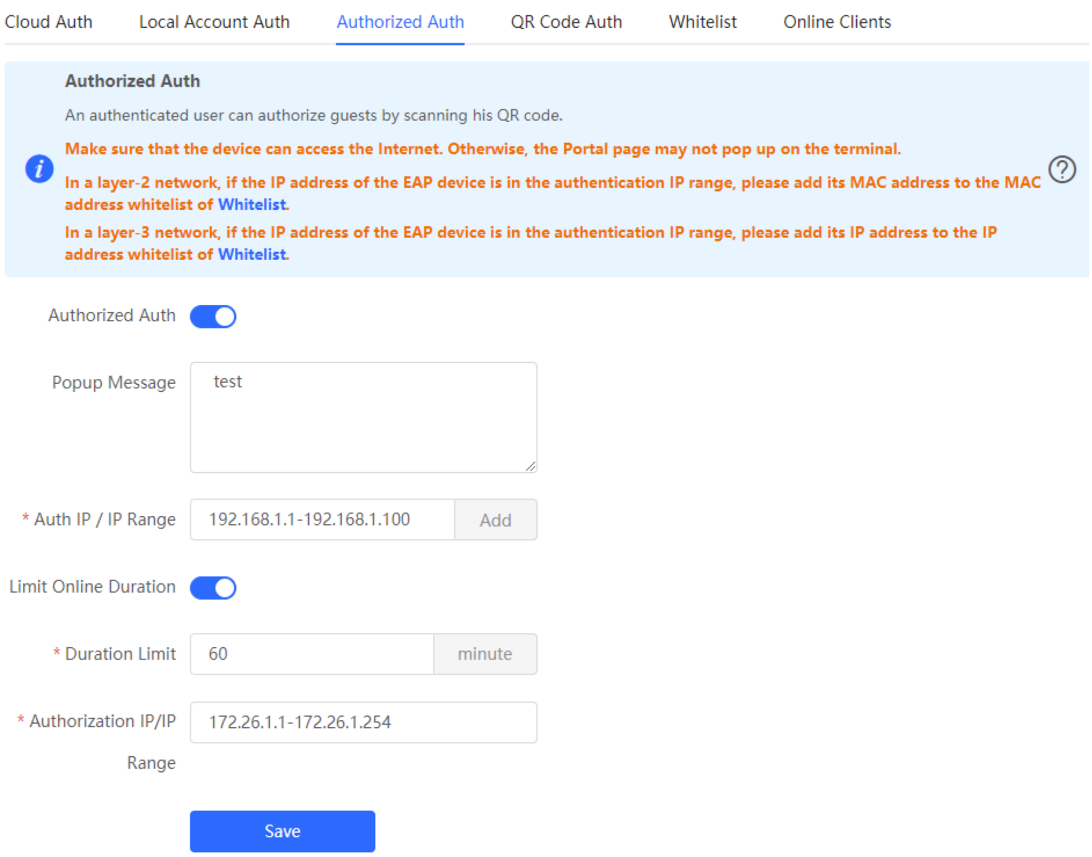
2. Getting Started

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 **Local Device** > **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**.



Authorized Auth

An authenticated user can authorize guests by scanning his QR code.

Make sure that the device can access the Internet. Otherwise, the Portal page may not pop up on the terminal.

In a layer-2 network, if the IP address of the EAP device is in the authentication IP range, please add its MAC address to the MAC address whitelist of Whitelist.

In a layer-3 network, if the IP address of the EAP device is in the authentication IP range, please add its IP address to the IP address whitelist of Whitelist.

Authorized Auth: on

Popup Message: test

* Auth IP / IP Range: 192.168.1.1-192.168.1.100 Add

Limit Online Duration: on

* Duration Limit: 60 minute

* Authorization IP/IP Range: 172.26.1.1-172.26.1.254

Table 4-7 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.

Parameter	Description
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 **Advanced** > **Authentication** > **Online Clients** to view information about the successfully connected user. For details, see Section 4.10.10 Online Authenticated User Management.

4.10.8 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.

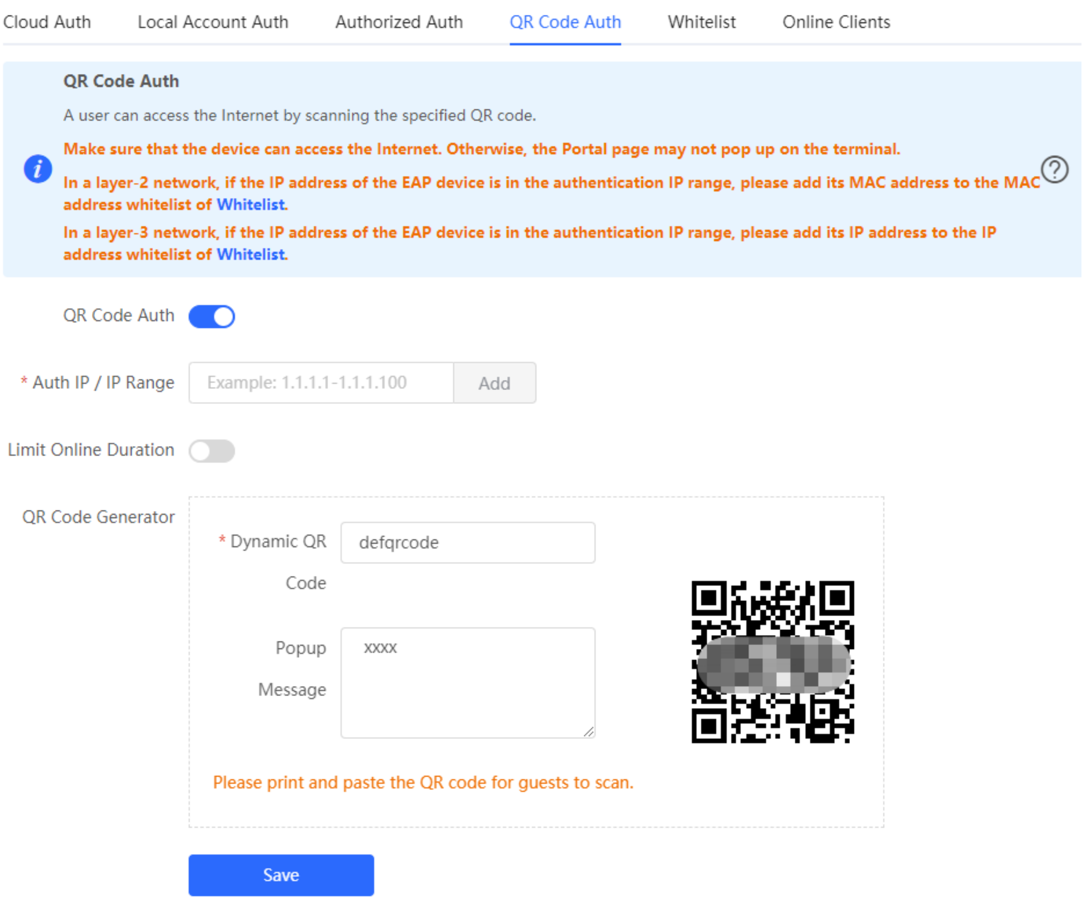
2. Getting Started

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 Local Device > 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**.



QR Code Auth

A user can access the Internet by scanning the specified QR code.

Make sure that the device can access the Internet. Otherwise, the Portal page may not pop up on the terminal.

In a layer-2 network, if the IP address of the EAP device is in the authentication IP range, please add its MAC address to the MAC address whitelist of Whitelist.

In a layer-3 network, if the IP address of the EAP device is in the authentication IP range, please add its IP address to the IP address whitelist of Whitelist.

QR Code Auth: ●

* Auth IP / IP Range: Example: 1.1.1.1-1.1.1.100

Limit Online Duration: ○

QR Code Generator:

* Dynamic QR Code: defqrcode

Popup Message: xxxx

Please print and paste the QR code for guests to scan.

Table 4-8 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.
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.

Parameter	Description
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 **Advanced** > **Authentication** > **Online Clients** to view information about the successfully connected user. For details, see Section 4.10.10 Online Authenticated User Management.

4.10.9 Authentication-Free

1. Overview

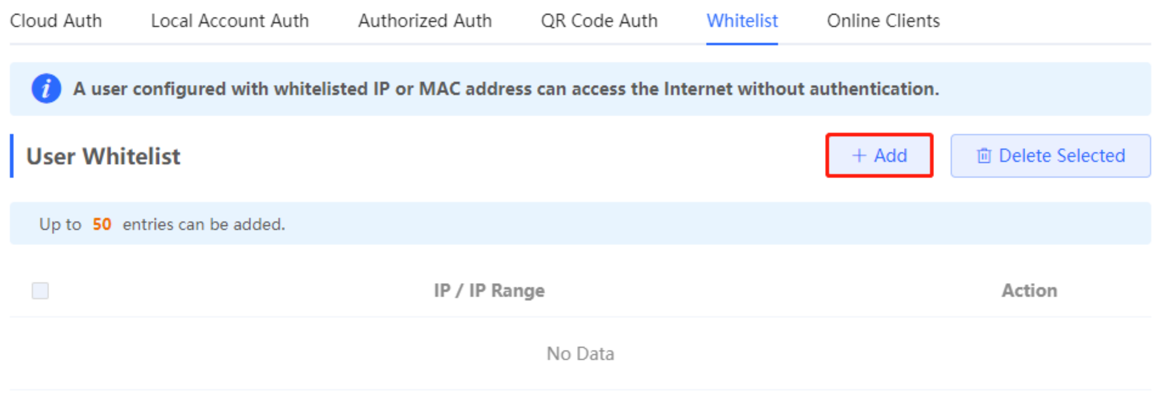
After IP addresses or MAC addresses are configured for authentication-free users, they can directly access the Internet without passing authentication. Traffic from all the users in the blacklist is blocked.

2. Configuring an Authentication-Free User

Choose **Local Device** > **Advanced** > **Authentication** > **Whitelist** > **User Whitelist**.

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.

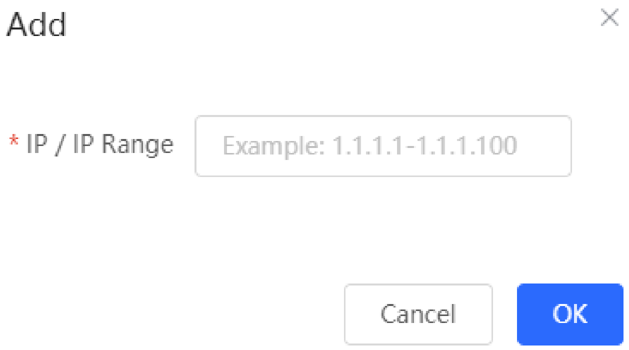


A user configured with whitelisted IP or MAC address can access the Internet without authentication.

User Whitelist

Up to 50 entries can be added.

□	IP / IP Range	Action
No Data		



Add

* IP / IP Range Example: 1.1.1.1-1.1.1.100

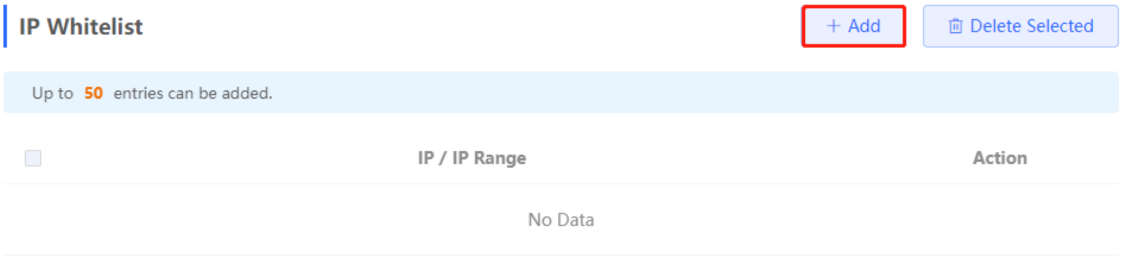
Cancel OK

3. Configuring Extranet IP Addresses for Authentication-Free

Choose **Local Device** > **Advanced** > **Authentication** > **Whitelist** > **IP Whitelist**.

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.

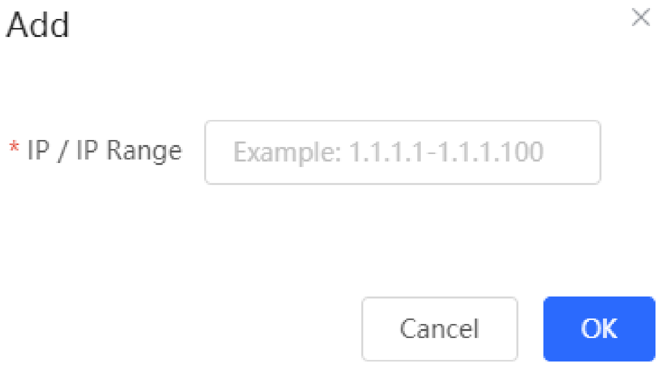


IP Whitelist

+ Add　Delete Selected

Up to 50 entries can be added.

□	IP / IP Range	Action
	No Data	



Add

* IP / IP Range Example: 1.1.1.1-1.1.1.100

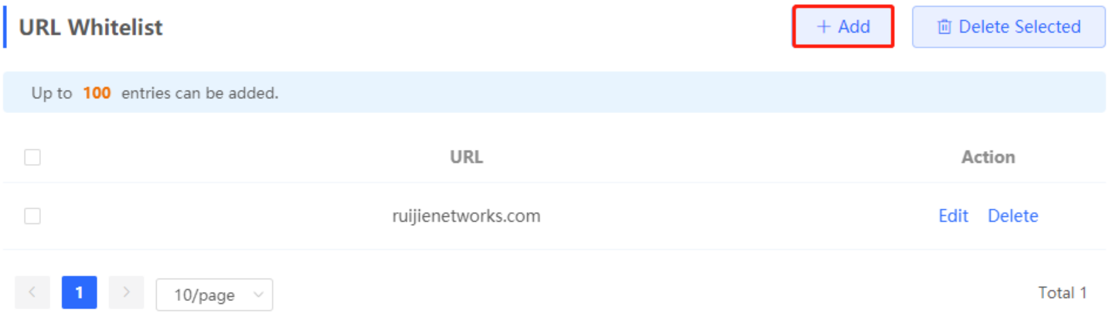
Cancel OK

4. Configuring a URL Whitelist

Choose **Local Device** > **Advanced** > **Authentication** > **Whitelist** > **URL Whitelist**.

URL Whitelist: Specify the URLs that can be accessed without authentication.

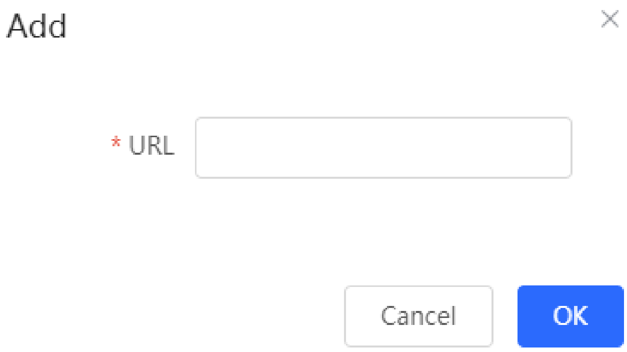
Click **Add**. In the dialog box that appears, enter the authentication-free URLs, and then click OK. When the destination URL of the user is in the URL whitelist, traffic from the user will be permitted directly, regardless of whether the user passes authentication. A maximum of 100 entries are supported.



Up to 100 entries can be added.

☐	URL	Action
☐	ruijienetworks.com	Edit Delete

Total 1



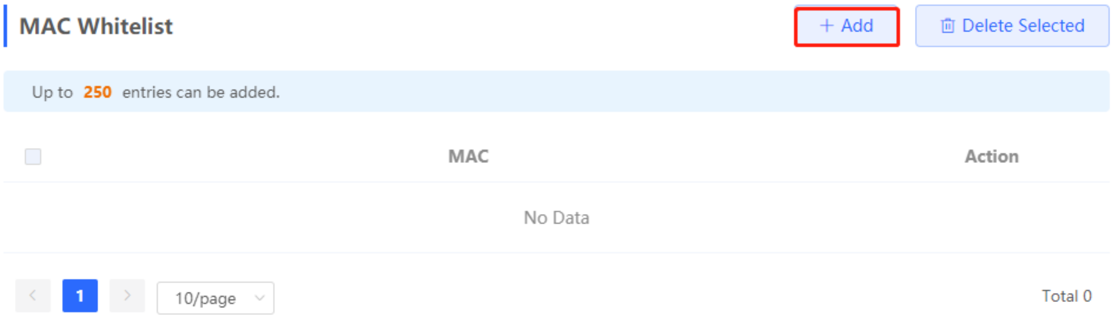
* URL

5. Configuring a User MAC Whitelist

Choose **Local Device** > **Advanced** > **Authentication** > **Whitelist** > **MAC Whitelist**.

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

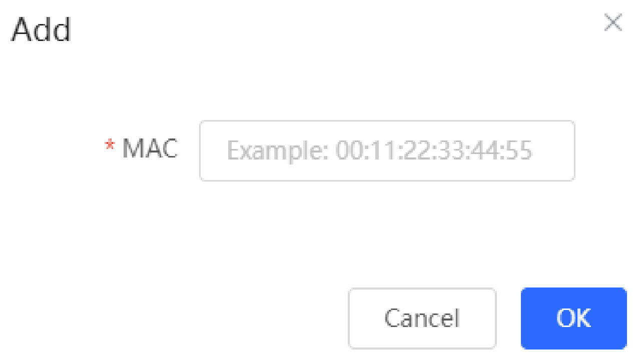
Click **Add**. In the dialog box that appears, enter the MAC addresses of authentication-free users, and then click **OK**. A maximum of 250 entries are supported.



Up to 250 entries can be added.

☐	MAC	Action
	No Data	

Total 0

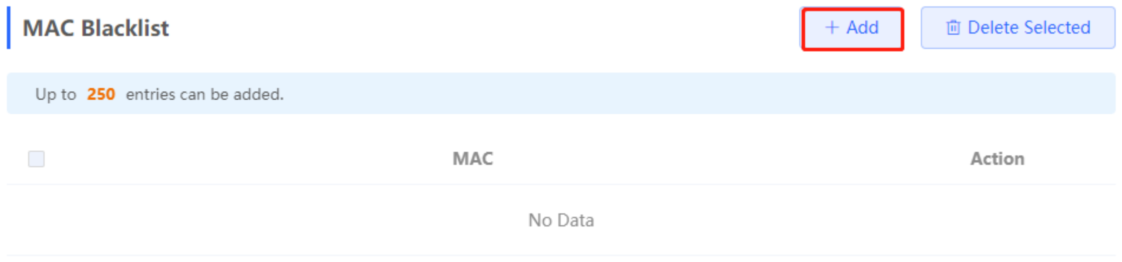


6. Configuring a User MAC Blacklist

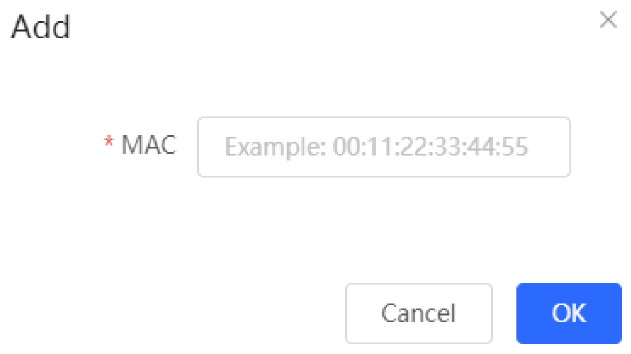
Choose **Local Device** > **Advanced** > **Authentication** > **Whitelist** > **MAC Blacklist**.

User MAC blacklist: Clients whose MAC addresses are in the blacklist are prohibited from accessing the Internet.

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



Up to 250 entries can be added.

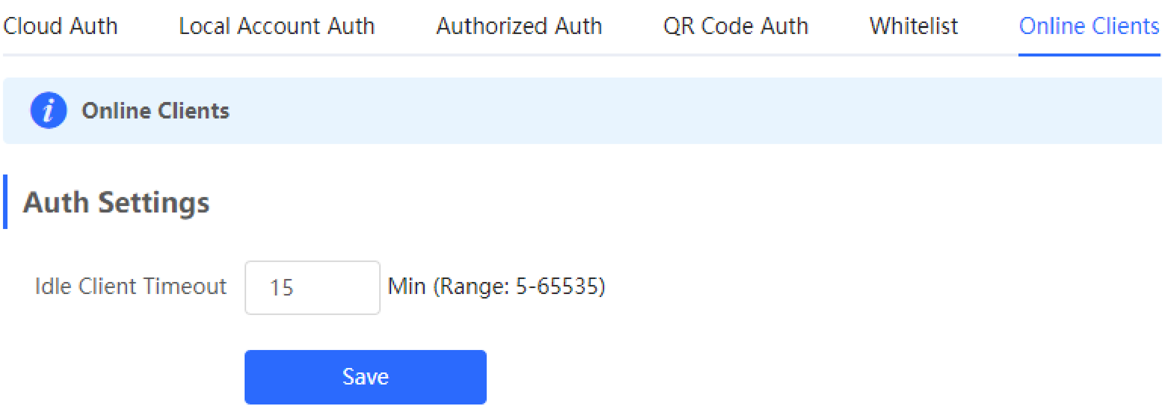


4.10.10 Online Authenticated User Management

1. Configuring the Idle Client Timeout Period

Choose **Local Device** > **Advanced** > **Authentication** > **Online Clients**.

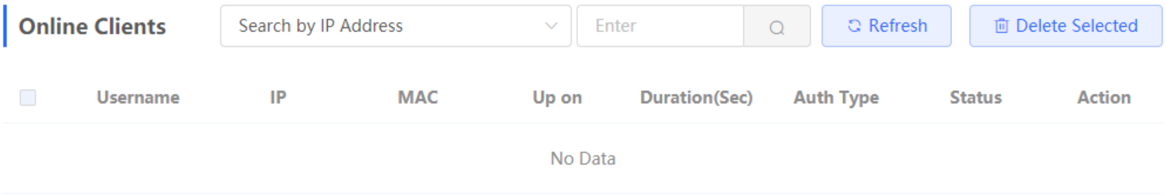
You can configure the idle client timeout period. The default value is 15 minutes. If no traffic from an online user passes through the device within the specified period, the device will force the user offline. The user can continue Internet access only after re-authentication.



Idle Client Timeout: 15 Min (Range: 5-65535)

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.



□	Username	IP	MAC	Up on	Duration(Sec)	Auth Type	Status	Action

No Data

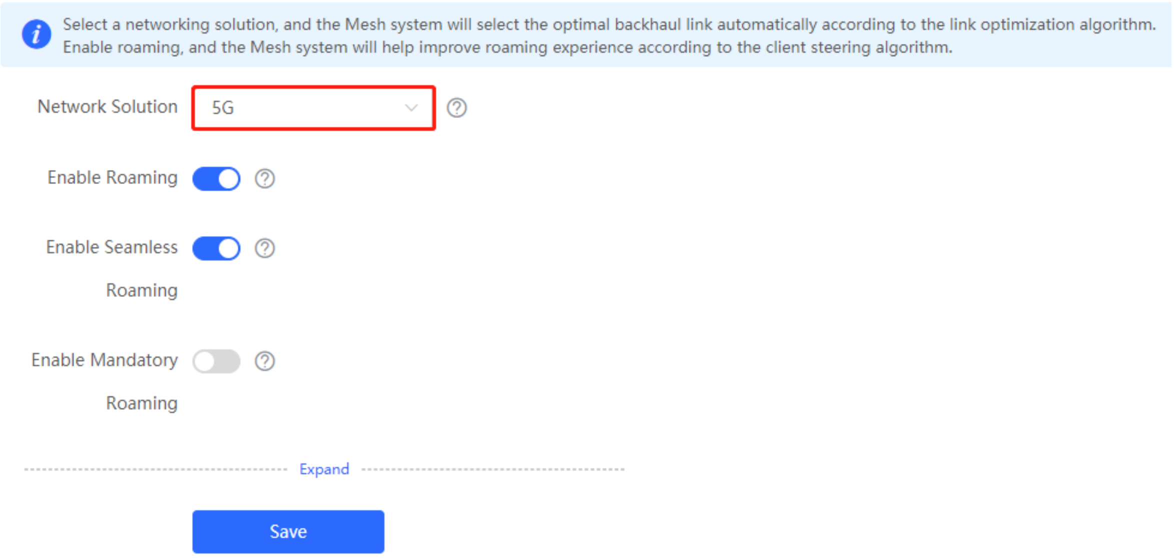
4.11 Reyee Mesh Settings

Choose **Network** > **Reyee Mesh**.

To enlarge the Wi-Fi coverage, routers can be connected through network cables or in wireless mode to form a wireless network that supports seamless roaming. The Reyee Mesh settings can help users form a mesh networking in an easier way, improving the wireless network experience.

4.11.1 Configuring a Networking Mode

After you set the networking mode to mesh, the mesh system intelligently selects the optimal backhaul link using the link optimization algorithm. Select a networking mode based on the wireless bands of the current networking environment.



Select a networking solution, and the Mesh system will select the optimal backhaul link automatically according to the link optimization algorithm. Enable roaming, and the Mesh system will help improve roaming experience according to the client steering algorithm.

Network Solution: 5G

Enable Roaming: on

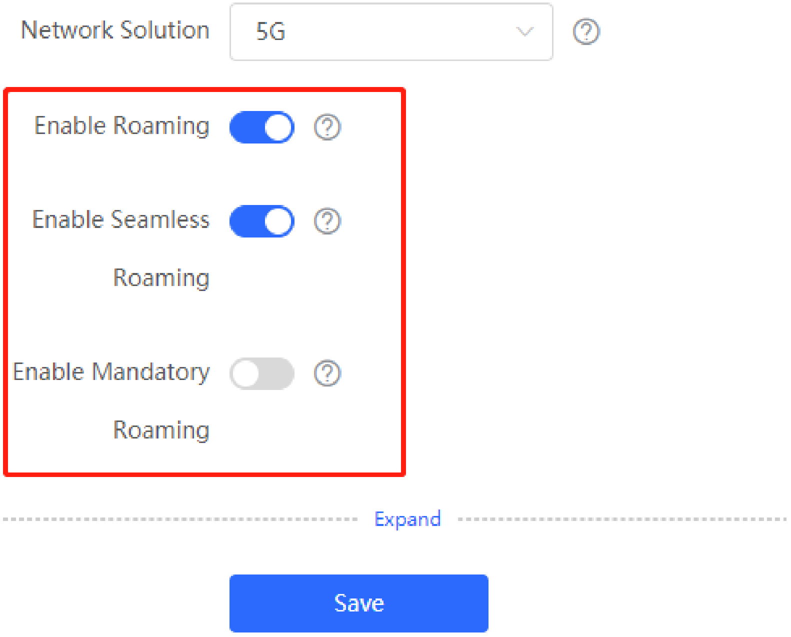
Enable Seamless Roaming: on

Enable Mandatory Roaming: off

4.11.2 Enabling Roaming

When the roaming function is enabled, the mesh system instructs the client to roam to the optimal access point with better WLAN experience using the client instruction algorithm. Seamless roaming implements more efficient switching between APs, avoids network delays or interruption, and effectively improves the wireless roaming experience. By default, the roaming function is enabled. You are advised to keep roaming enabled.

If clients do not support IEEE 802.11k or IEEE 802.11v, BSS Transition Management (BTM) cannot be used to instruct roaming. In this case, you need to enable mandatory roaming.



Network Solution: 5G

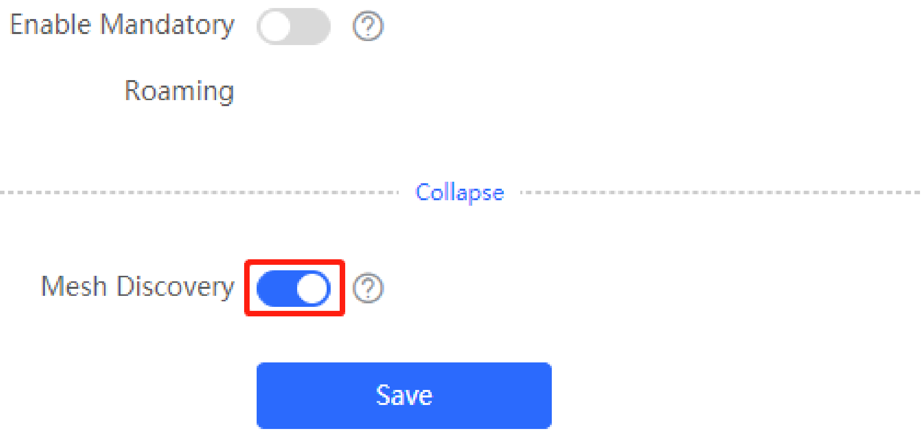
Enable Roaming: on

Enable Seamless Roaming: on

Enable Mandatory Roaming: off

4.11.3 Enabling Mesh Discovery

On the **Reyee Mesh Settings** page, click **Advanced Settings** and turn on or off **Mesh Discovery**. After mesh discovery is enabled, the LAN port on the router connected to the master device through a network cable will automatically join the mesh networking. You can also press the Mesh button to trigger Reyee Mesh pairing. After mesh discovery is disabled, the Mesh button will become invalid.



Note

After Reyee Mesh is disabled, the bridged slave router will still be connected.

4.12 Configuring the LAN Port of Downlink Access Point

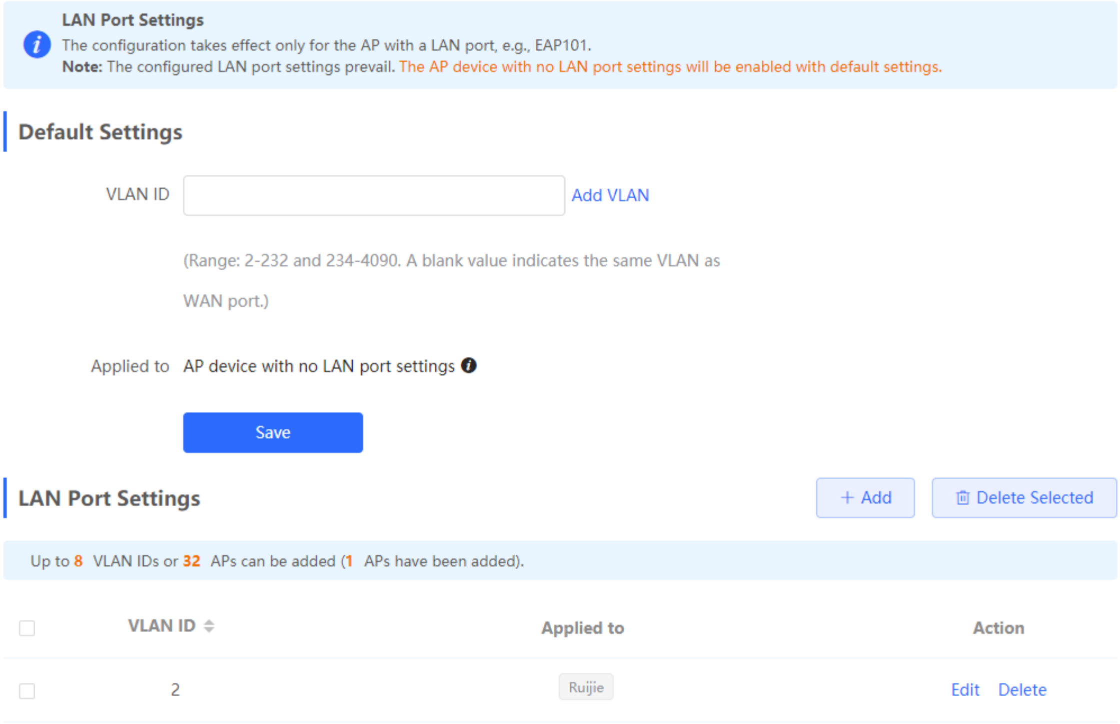
Caution

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

Choose **Network** > **LAN Ports**.

Enter the VLAN ID and click **Save** to configure the VLAN, to which the AP wired ports belong. If the VLAN ID is null, the wired ports and WAN port belong to the same VLAN.

In self-organizing network mode, the AP wired port configuration applies to all APs having wired LAN ports on the current network. The configuration applied to APs in **LAN Port Settings** takes effect preferentially. Click **Add** to add the AP wired port configuration. For APs, to which no configuration is applied in **LAN Port Settings**, the default configuration of the AP wired ports will take effect on them.



LAN Port Settings

The configuration takes effect only for the AP with a LAN port, e.g., EAP101.

Note: The configured LAN port settings prevail. The AP device with no LAN port settings will be enabled with default settings.

Default Settings

VLAN ID [ ] Add VLAN

(Range: 2-232 and 234-4090. A blank value indicates the same VLAN as WAN port.)

Applied to AP device with no LAN port settings

Save

LAN Port Settings

+ Add | Delete Selected

Up to 8 VLAN IDs or 32 APs can be added (1 APs have been added).

□	VLAN ID	Applied to	Action
□	2	Ruijie	Edit Delete

5 Switch Management

5.1 Configuring RLDP

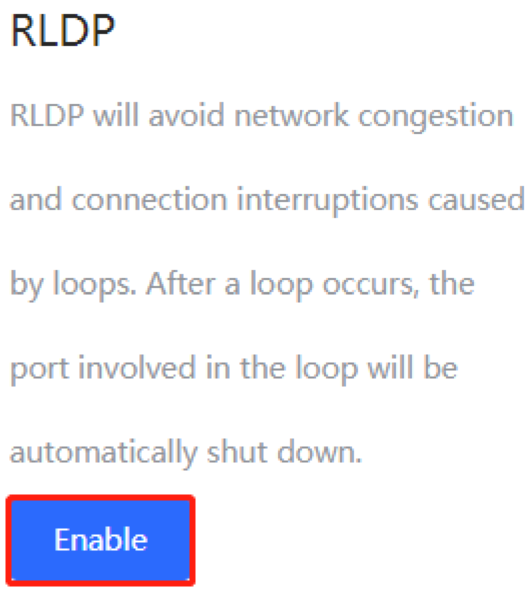
5.1.1 Overview

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.

5.1.2 Configuration Steps

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

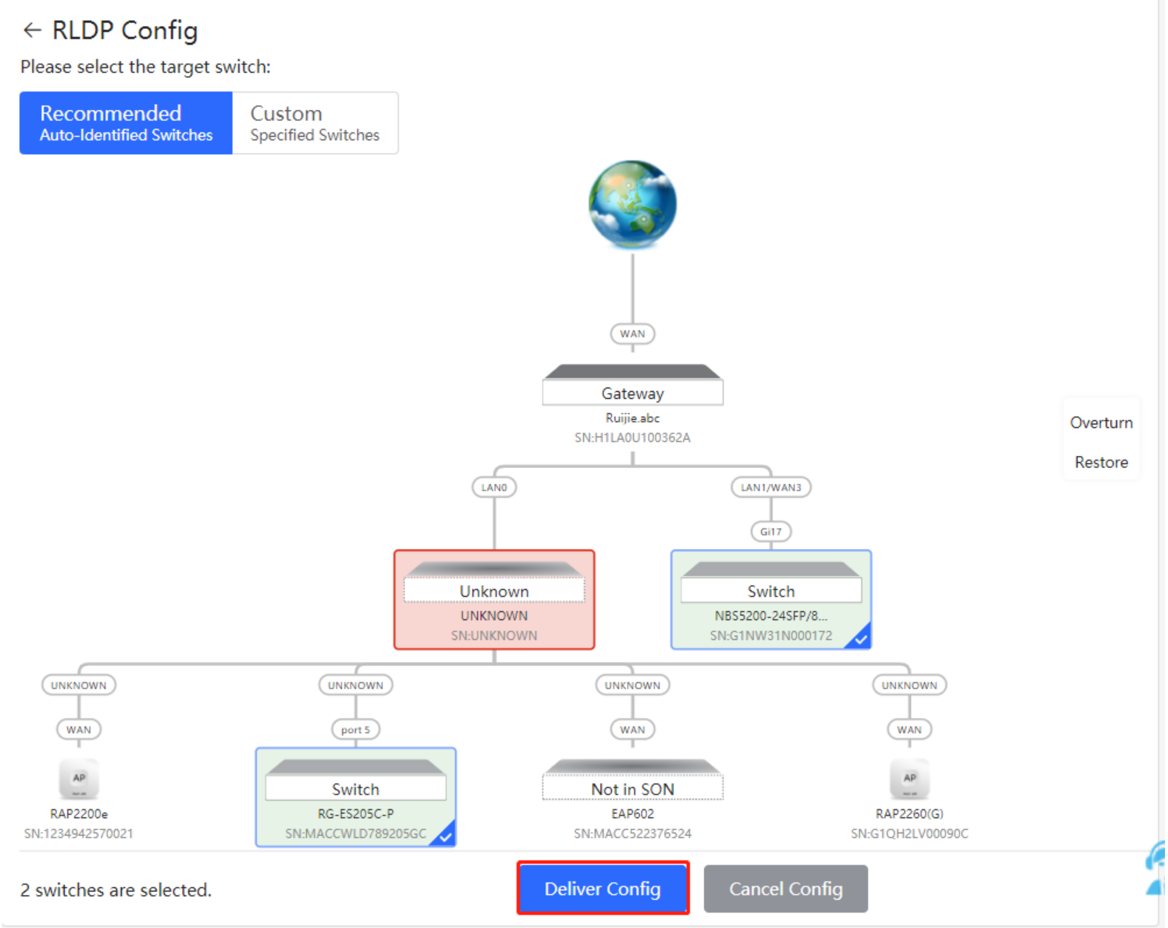
(1) Click **Enable** to access the **RLDP Config** page.



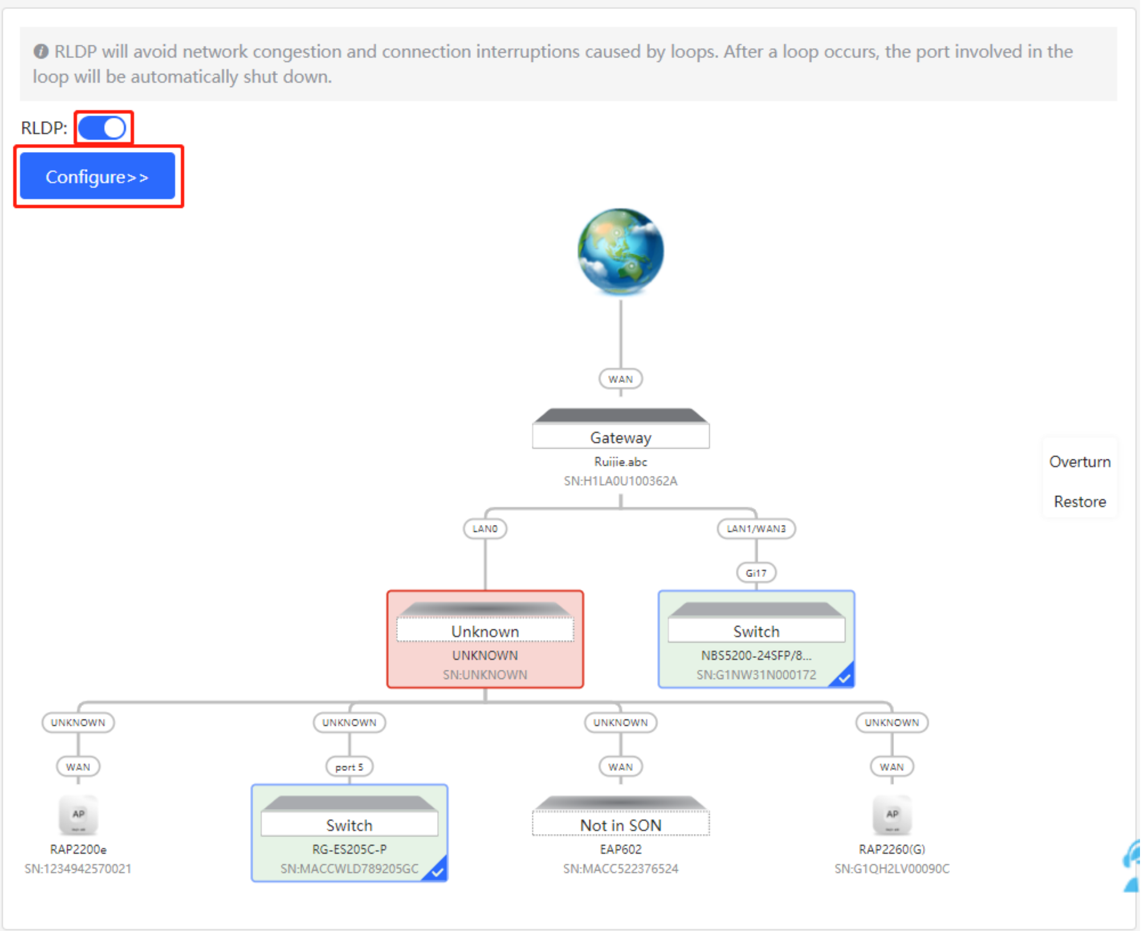
RLDP

RLDP will avoid network congestion and connection interruptions caused by loops. After a loop occurs, the port involved in the loop will be automatically shut down.

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



(3) After the configuration is delivered, if you want to modify the effective range of the RLDP function, click **Configure** to select desired switches in the topology again. Turn off **RLDP** to disable RLDP on all the switches with one click.



RLDP will avoid network congestion and connection interruptions caused by loops. After a loop occurs, the port involved in the loop will be automatically shut down.

RLDP: ●

5.2 Configuring DHCP Snooping

5.2.1 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.

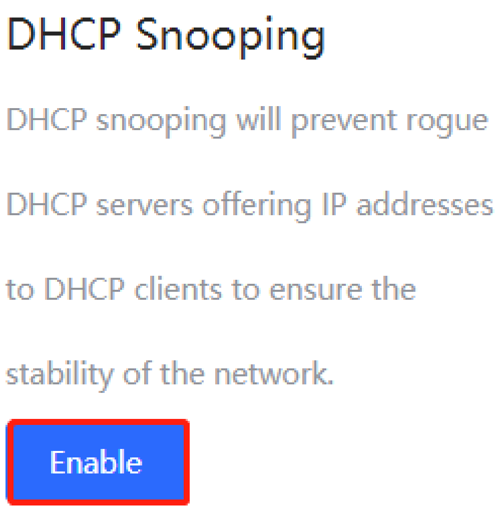
Caution

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 port for uplink connection.

5.2.2 Configuration Steps

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

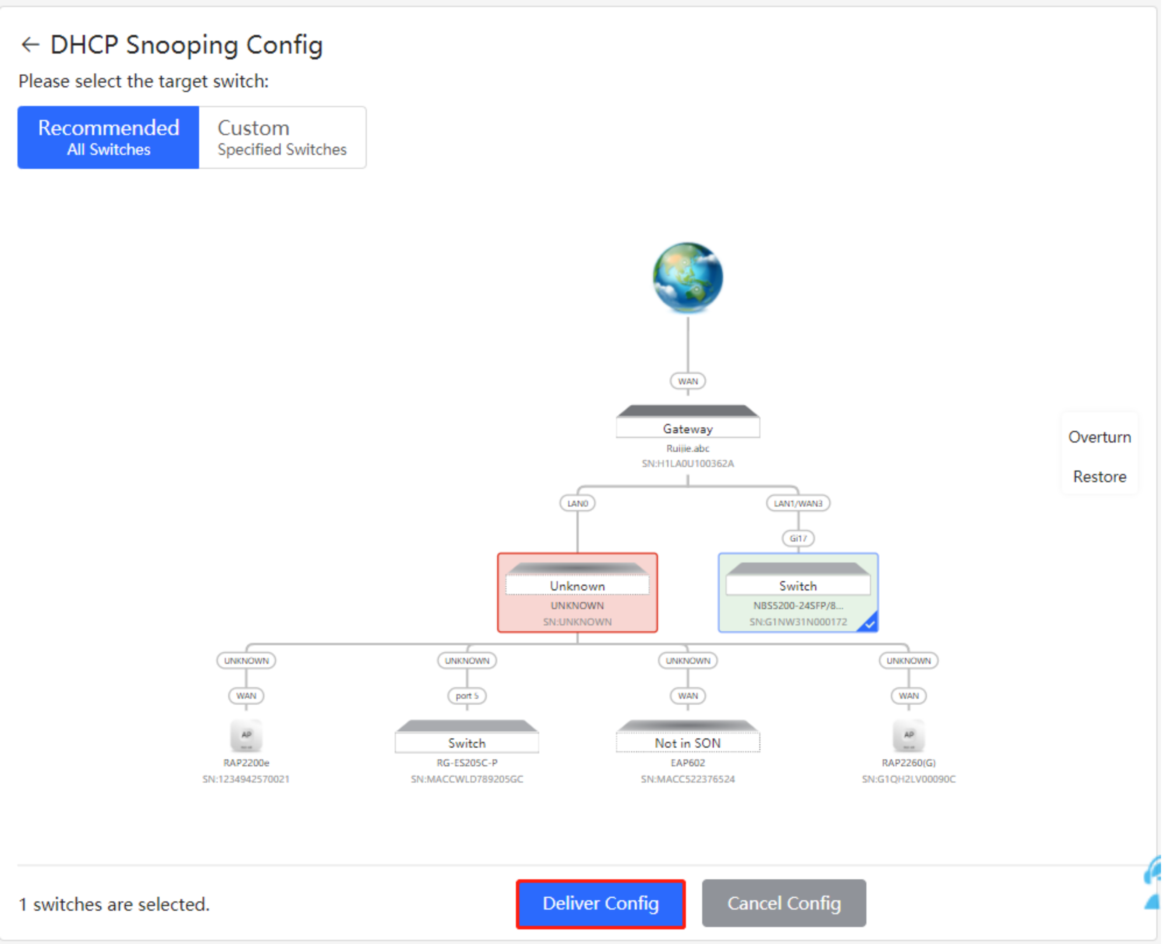
(1) Click **Enable** to access the **DHCP Snooping Config** page.



DHCP Snooping

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

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

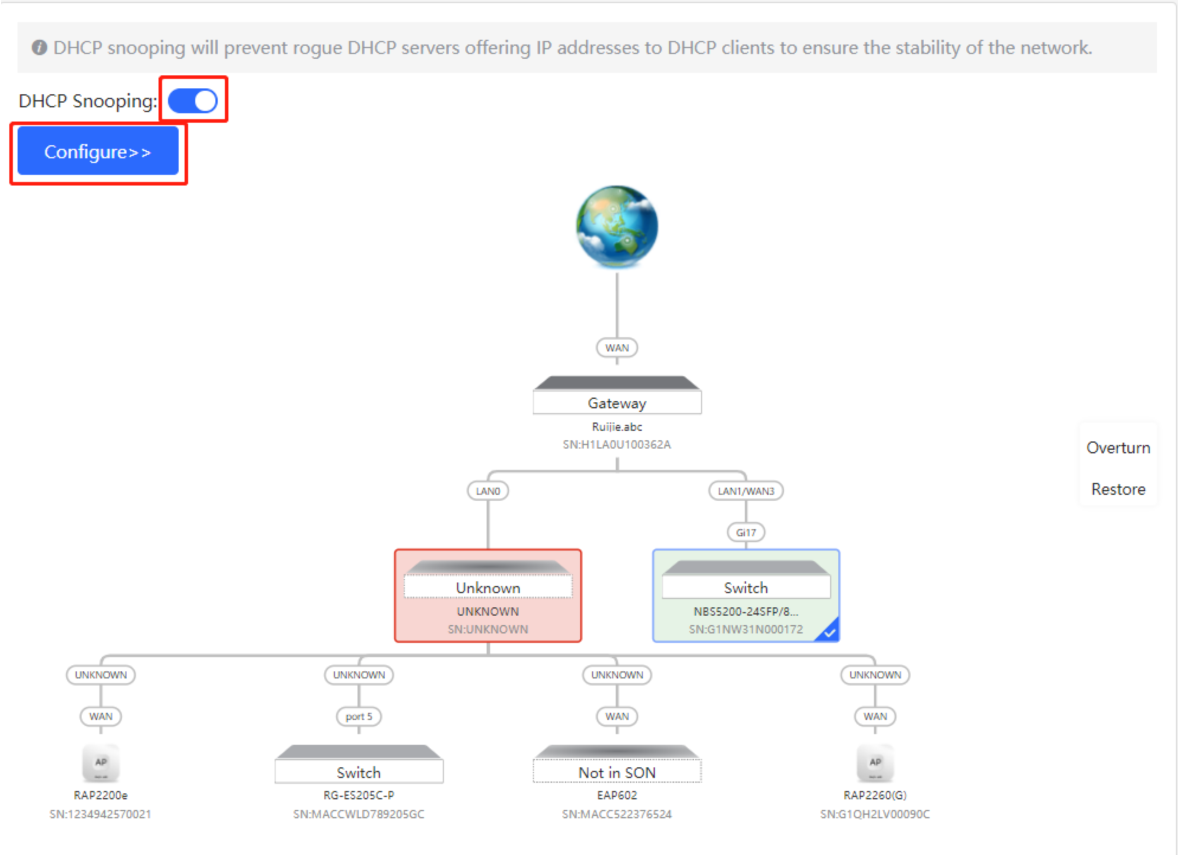


DHCP Snooping Config

Please select the target switch:

1 switches are selected.

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



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

DHCP Snooping: ●

5.3 Batch Configuring Switches

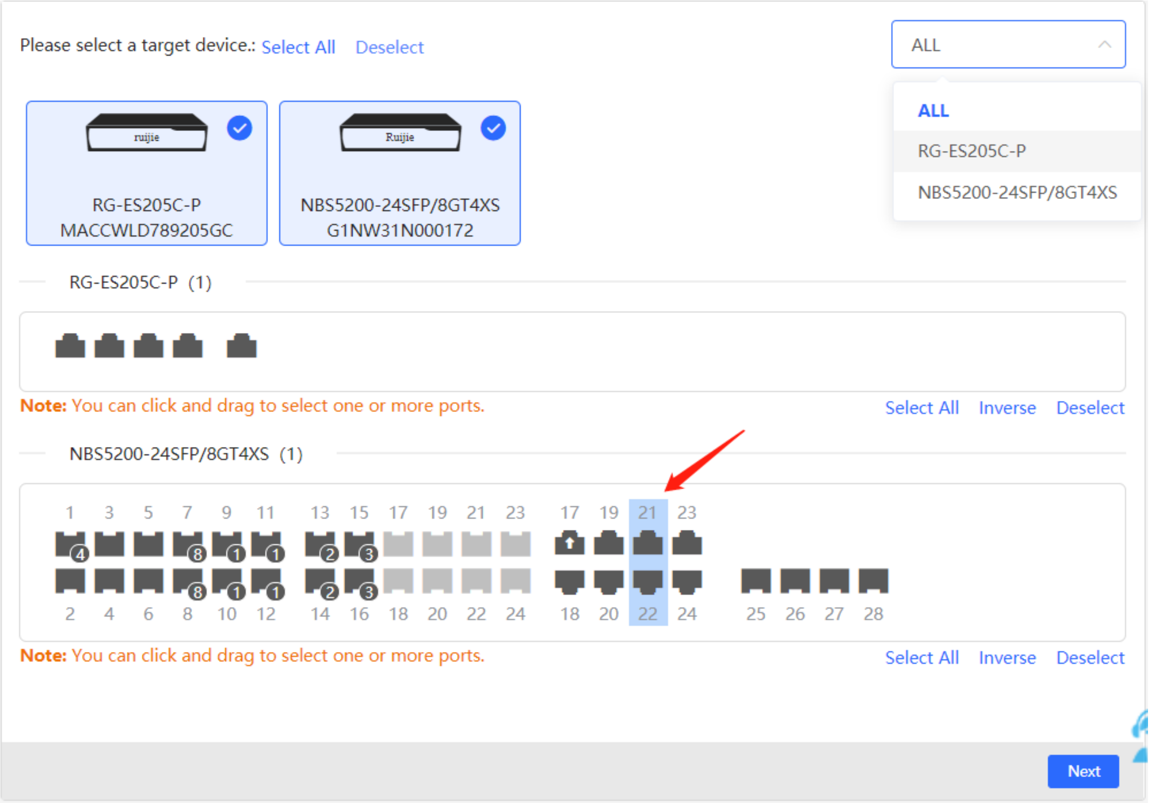
5.3.1 Overview

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

5.3.2 Configuration Steps

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

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



Please select a target device.: Select All Deselect

ALL

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

RG-ES205C-P
MACCWLD789205GC

NBS5200-24SFP/8GT4XS
G1NW31N000172

RG-ES205C-P (1)

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

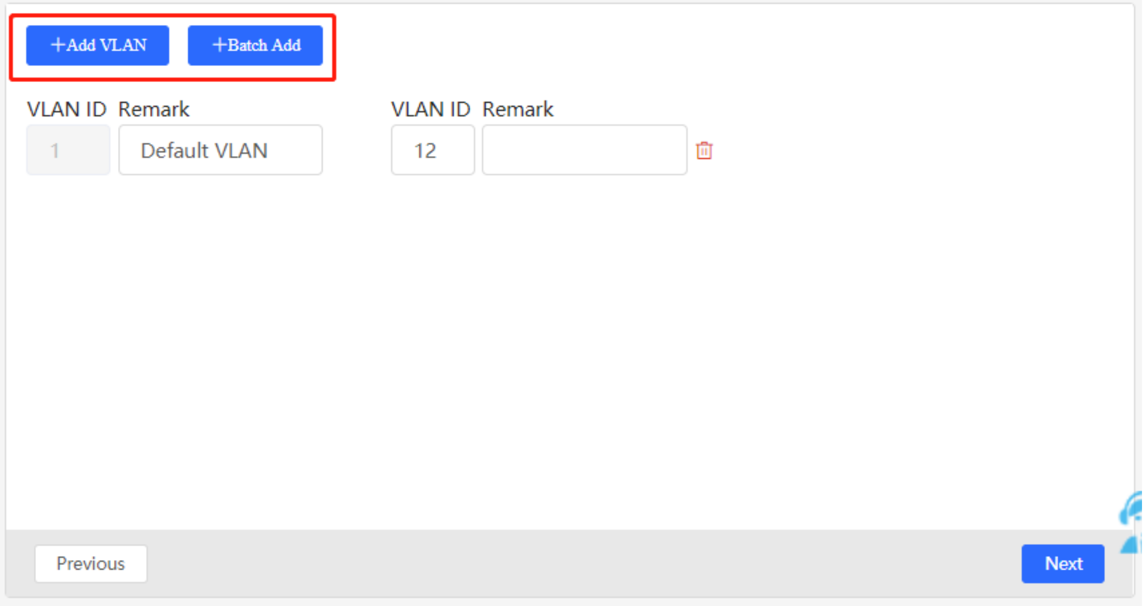
Select All Inverse Deselect

NBS5200-24SFP/8GT4XS (1)

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

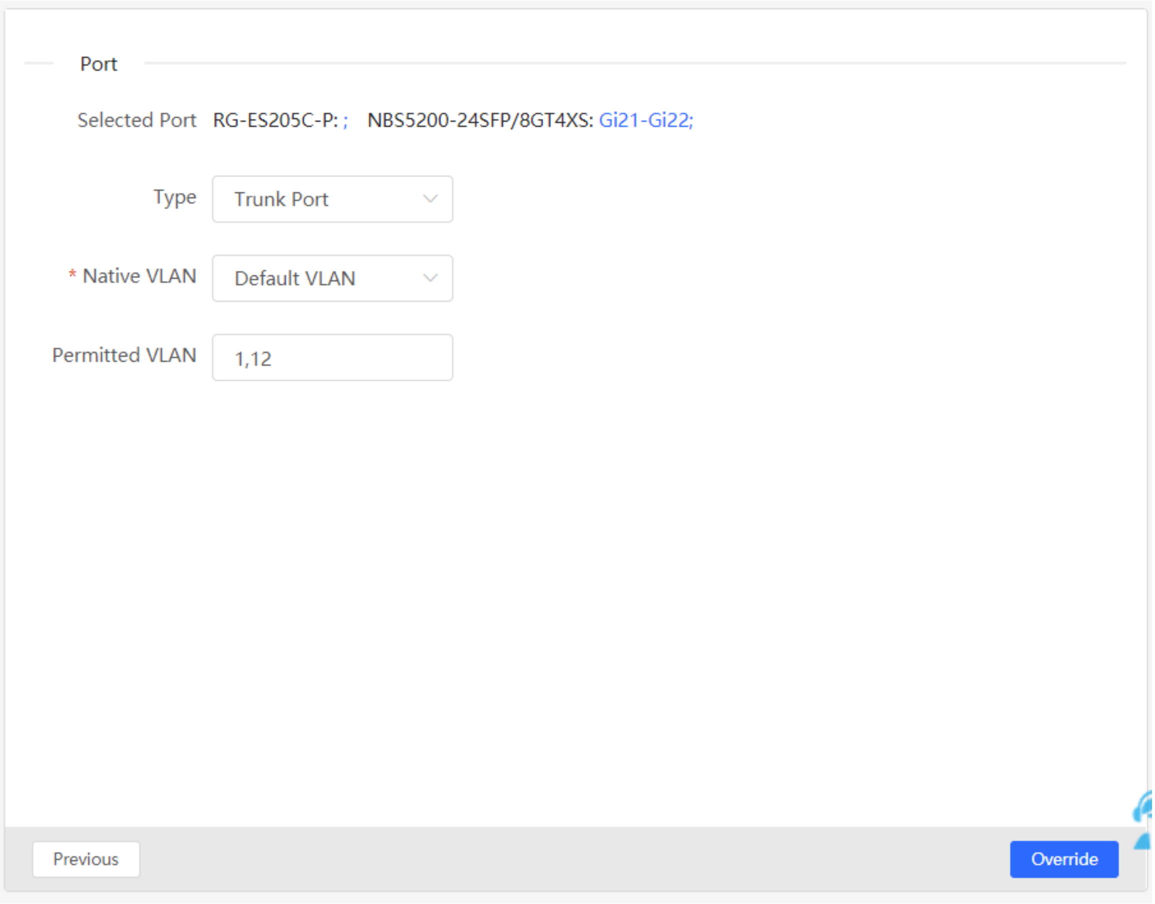
Select All Inverse Deselect

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



VLAN ID	Remark	VLAN ID	Remark
1	Default VLAN	12	

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



Port

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

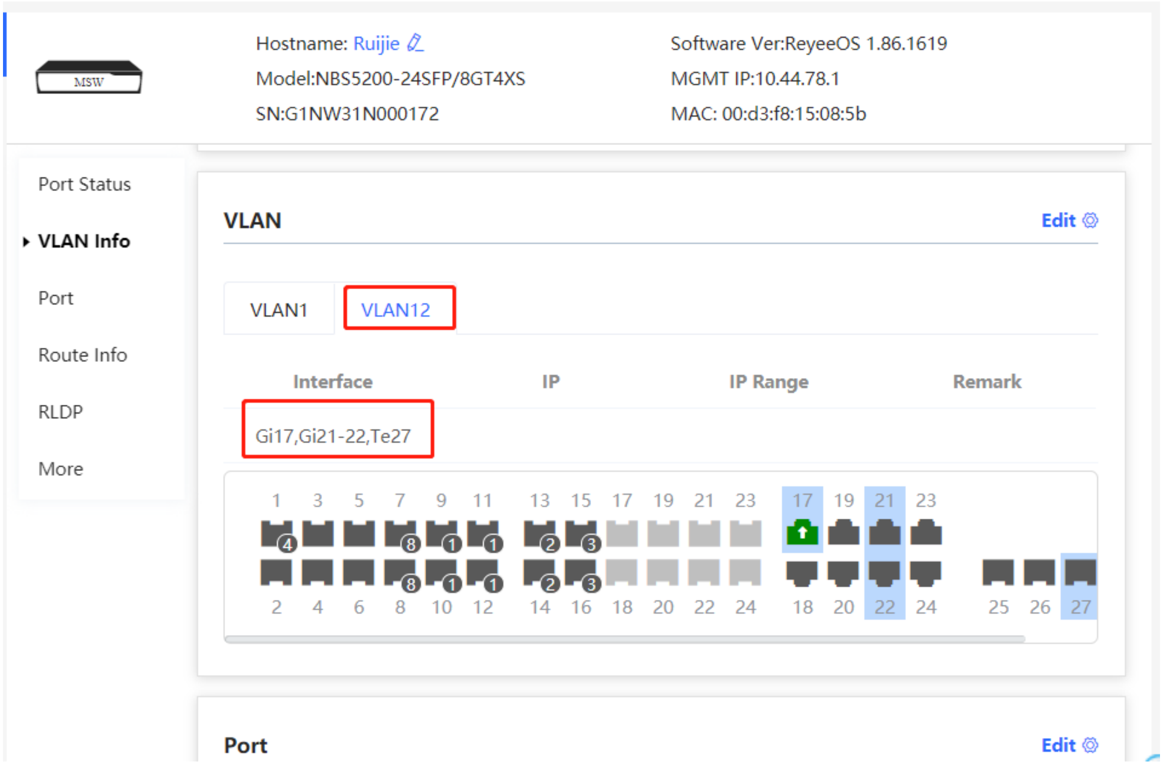
Type: Trunk Port

* Native VLAN: Default VLAN

Permitted VLAN: 1,12

5.3.3 Verifying Configuration

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



Hostname: Ruijie

Model:NBS5200-24SFP/8GT4XS

SN:G1NW31N000172

Software Ver:ReyeeOS 1.86.1619

MGMT IP:10.44.78.1

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

VLAN

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

Port

6 Online Behavior Management

6.1 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.

6.2 Address Management

Choose **Local Device** > **Behavior** > **Address Management**.

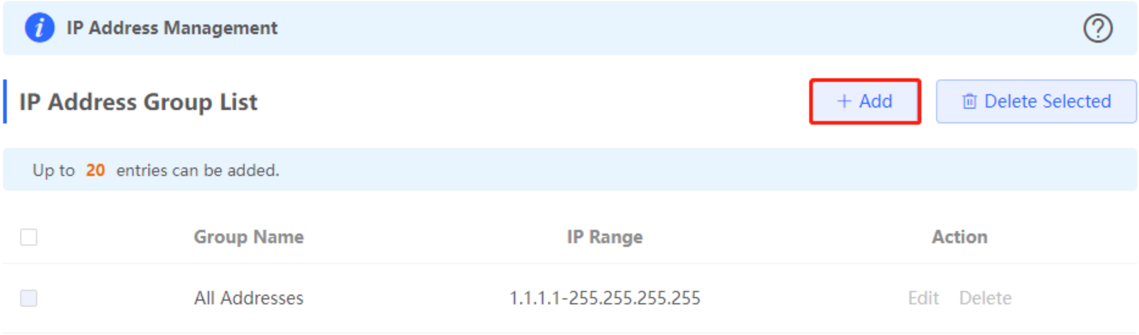
You can create address groups to classify IP addresses. A created address group can be used as a configuration item in a behavior management policy and is directly referenced by the address group name.

Click **Add**. In the dialog box that appears, enter the address group name and IP address range. You can click + to add multiple IP address ranges. Each address group can contain a maximum of five IP address ranges.

All the created address groups are displayed in the address group list. In the list, find the target address group and click **Edit** to modify the IP address range. Find the target address group and click **Delete** to delete it. By default, the address group named **All Addresses** is available and it cannot be modified or deleted.

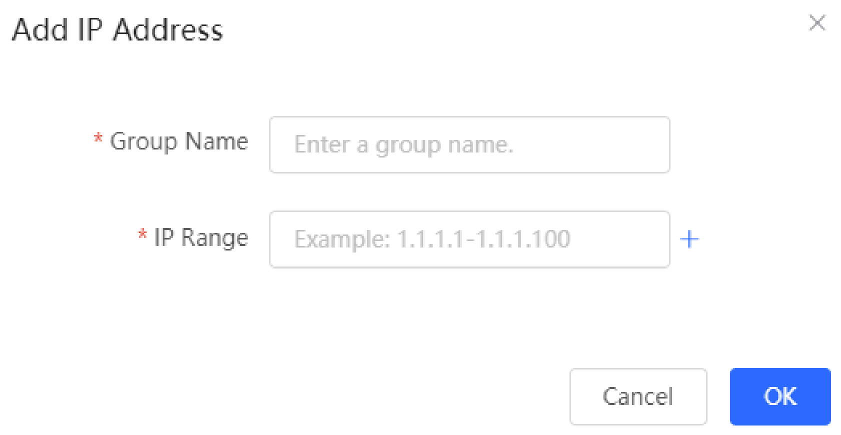
Caution

If an address group is referenced in any policy, it cannot be deleted on the **IP Address Management** page. To delete the address group, remove the reference relationship first.



Up to 20 entries can be added.

□	Group Name	IP Range	Action
□	All Addresses	1.1.1.1-255.255.255.255	Edit Delete



Add IP Address

* Group Name: Enter a group name.

* IP Range: Example: 1.1.1.1-1.1.1.100

6.3 Time Management

Choose **Local Device** > **Behavior** > **Time Management**.

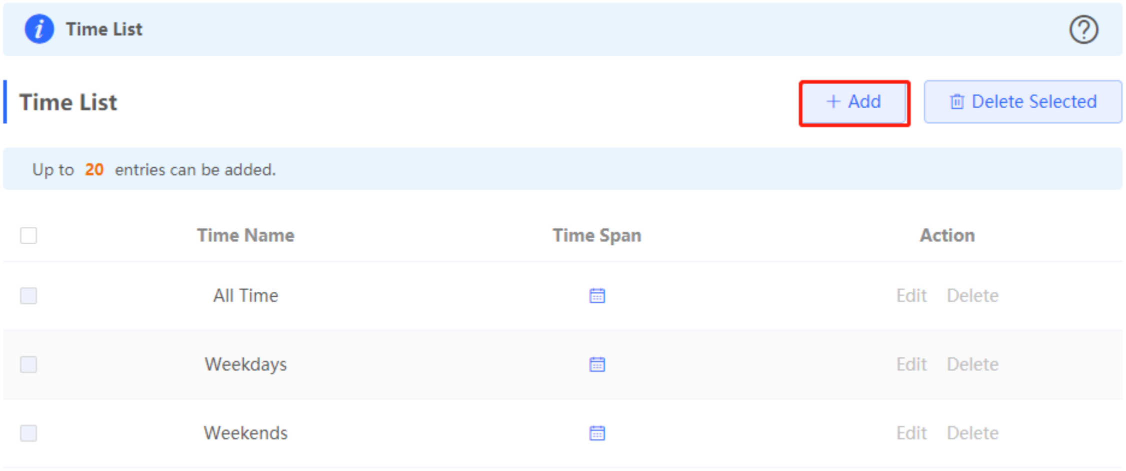
You can create time entries to classify time information. A created time entry can be used as a configuration item in a behavior management policy and is directly referenced by the time entry name.

Click **Add**. In the dialog box that appears, enter the time entry name and select the specific time to create a time entry.

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

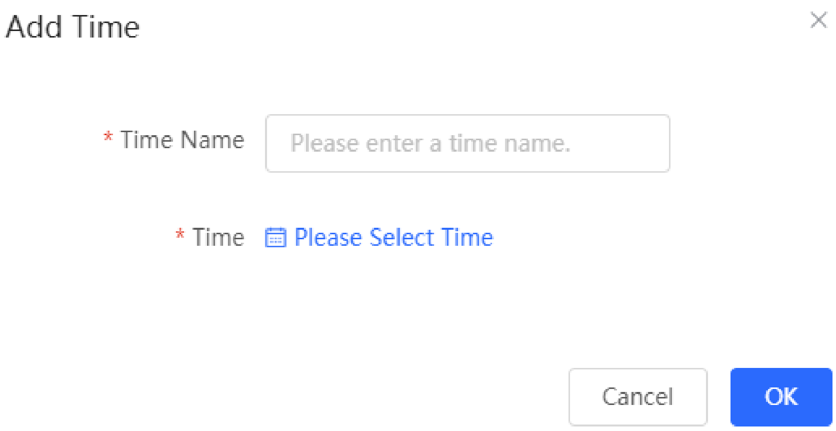
If a time entry is referenced in any policy, it cannot be deleted on the **Time Management** page. To delete the time entry, remove the reference relationship first.



Time List

Up to 20 entries can be added.

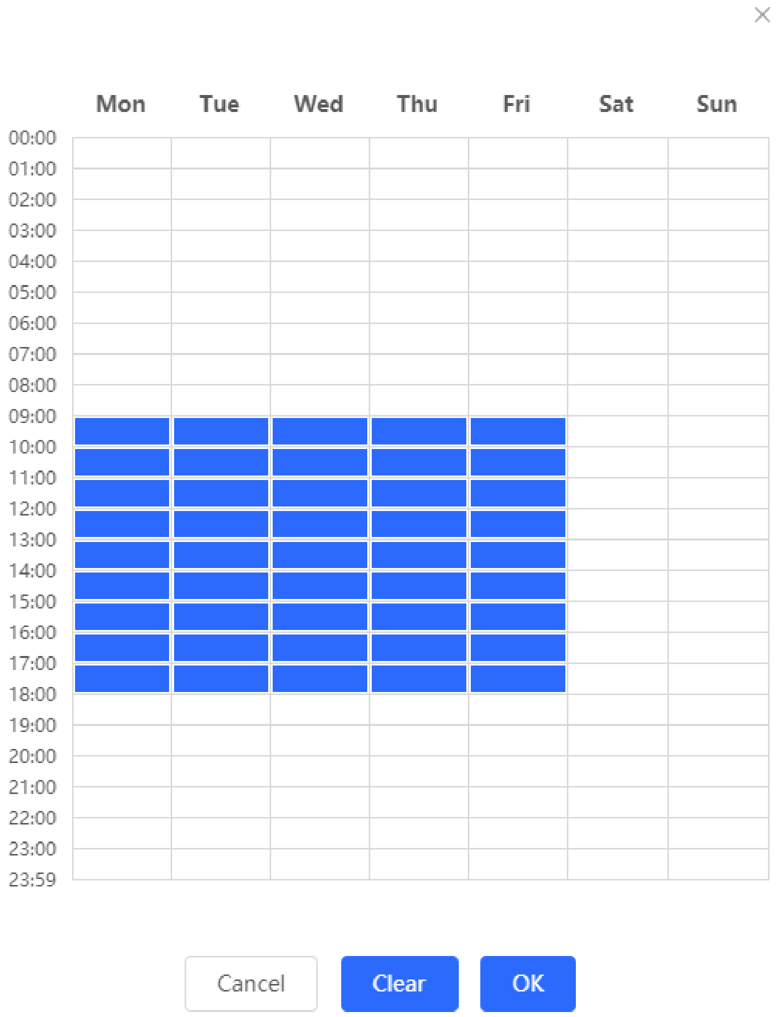
□	Time Name	Time Span	Action
□	All Time	📅	Edit Delete
□	Weekdays	📅	Edit Delete
□	Weekends	📅	Edit Delete



Add Time

* Time Name: Please enter a time name.

* Time: Please Select Time



6.4 App Control

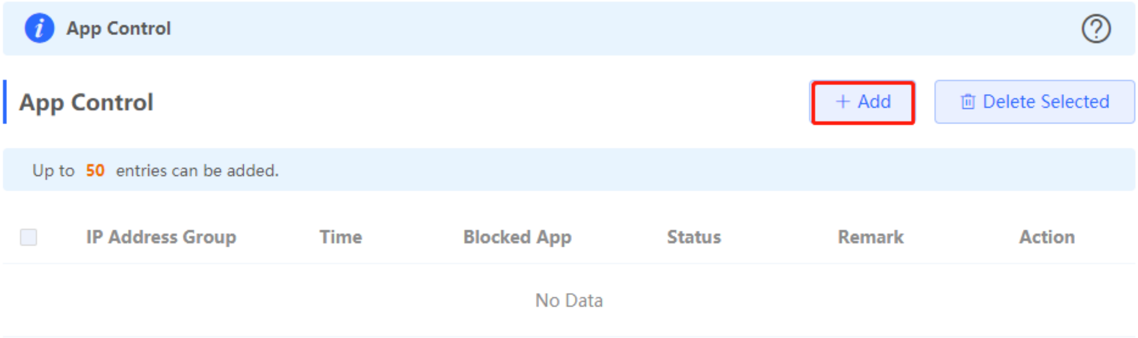
6.4.1 Overview

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 client IP address 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.

6.4.2 Configuration Steps

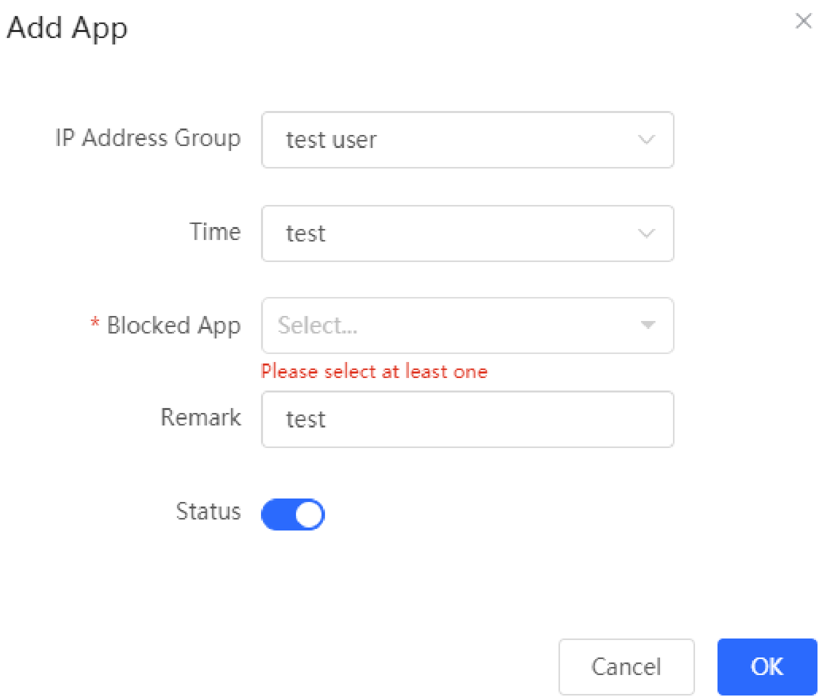
Choose **Local Device** > **Behavior** > **App Control**.

Click **Add** to create an app control policy.



Up to 50 entries can be added.

□	IP Address Group	Time	Blocked App	Status	Remark	Action
No Data						



IP Address Group: test user

Time: test

* Blocked App: Select...

Please select at least one

Remark: test

Status: ●

Table 6-1 App control policy configuration

Parameter	Description
IP Address Group	Specify the IP address range to which the app control policy applies. You can select an IP address group defined in Section 6.2 Address Management from the drop-down list box, or select **Custom** and manually enter the specific IP address range.

Parameter	Description
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 6.3 Time Management from the drop-down list box, or select **Custom** and manually enter the specific time range.
Blocked App	Specify the apps or app groups to block.
Remark	Enter the policy description.
Status	Specify whether to enable the app control policy.

6.5 Website Management

6.5.1 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 client IP address and time range. For example, employees in the office network are prohibited from accessing game websites during work periods to improve network security.

6.5.2 Configuration Steps

Choose Local Device > Behavior > Website Management.

1. **Configuring Website Groups**

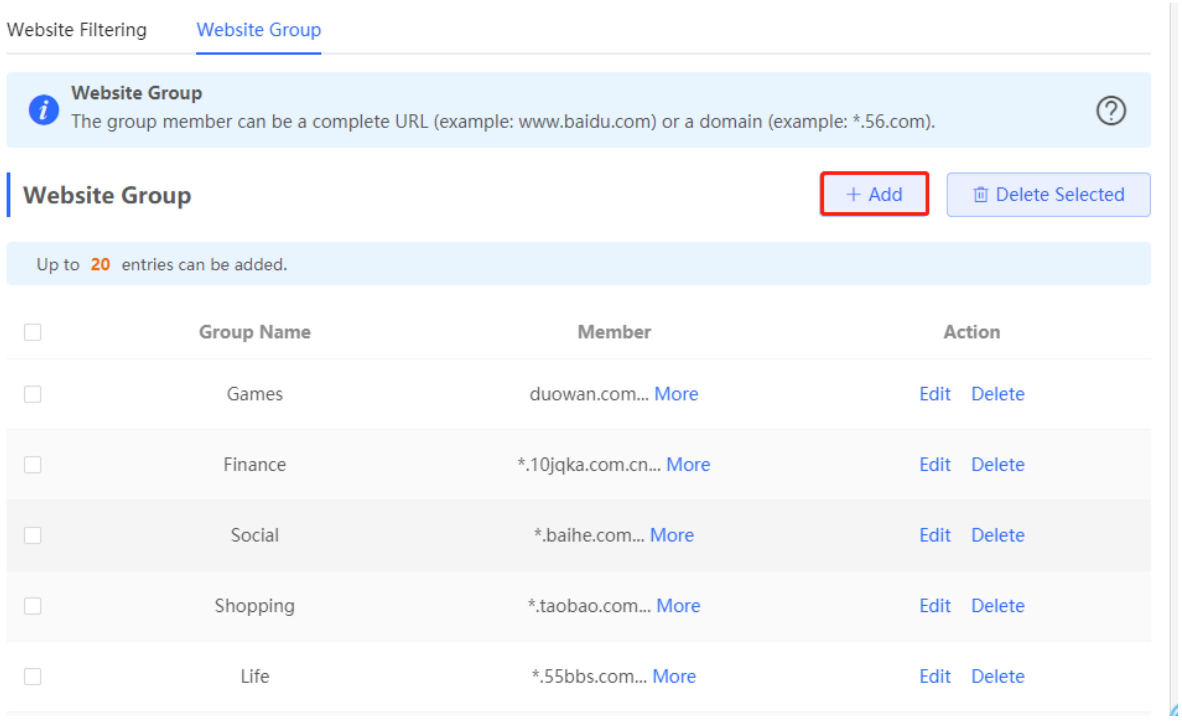
Choose **Local Device** > **Behavior** > **Website Management** > **Website Group**.

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.

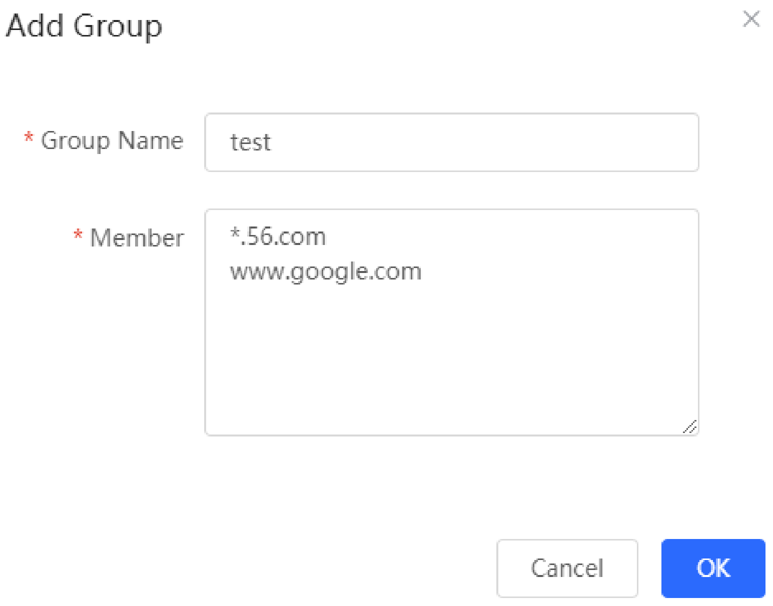


Website Group
The group member can be a complete URL (example: www.baidu.com) or a domain (example: *.56.com).

Website Group

Up to 20 entries can be added.

□	Group Name	Member	Action
□	Games	duowan.com... More	Edit Delete
□	Finance	*.10jqka.com.cn... More	Edit Delete
□	Social	*.baihe.com... More	Edit Delete
□	Shopping	*.taobao.com... More	Edit Delete
□	Life	*.55bbs.com... More	Edit Delete



Add Group

* Group Name: test

* Member:
*.56.com
www.google.com

Table 6-2 Website group configuration

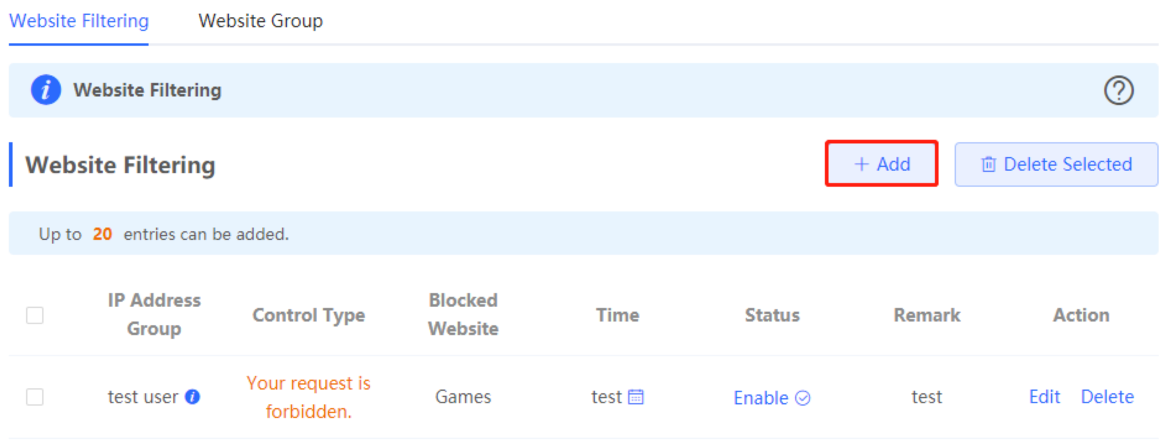
Parameter	Description
Group Name	Configure a unique name for the website group. The name can be a string of 1 to 64 characters.
Member	Specify members in the website group. You can enter multiple websites in a batch. The group member can be complete URL (such as www.baidu.com) or keywords in the URL (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 **Local Device** > **Behavior** > **Website Management** > **Website Filtering**.

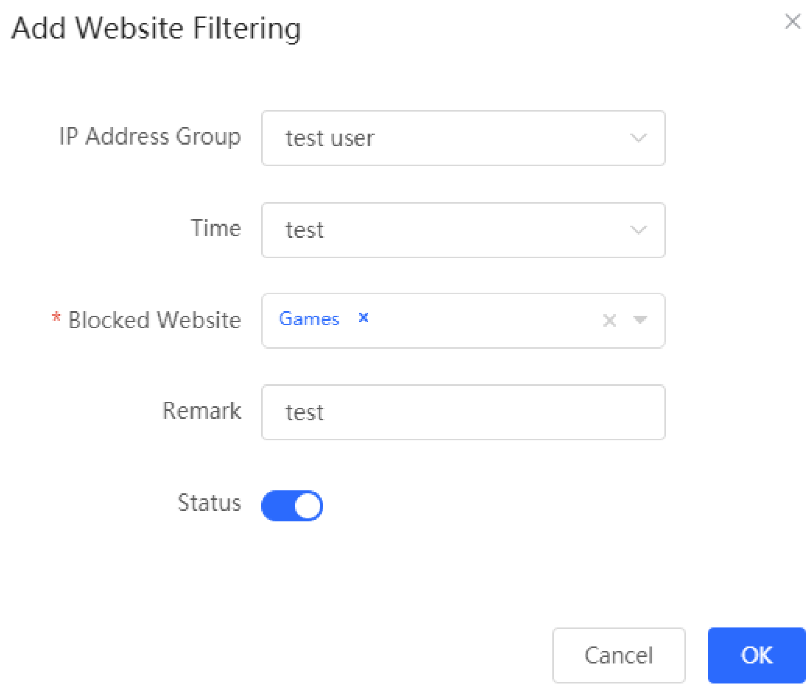
Click the **Website Filtering** tab. On the page that appears, all the created website filtering rules are displayed in the list. Click Edit to modify the rule information. Click Delete to delete the specific filtering rule.

Click **Add** to create a website filtering rule.



Up to 20 entries can be added.

□	IP Address Group	Control Type	Blocked Website	Time	Status	Remark	Action
□	test user	Your request is forbidden.	Games	test	Enable	test	Edit Delete



IP Address Group: test user

Time: test

* Blocked Website: Games

Remark: test

Status: ●

Table 6-3 Website filtering rule configuration

Parameter	Description
IP Address Group	Specify the IP address range to which the website filtering rule applies. You can select an IP address group defined in Section 6.2 Address Management from the drop-down list box, or select **Custom** and manually enter the specific IP address range.

Parameter	Description
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 6.3 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.
Remark	Enter the rule description.
Status	Specify whether to enable the website filtering rule.

6.6 QQ Management

6.6.1 Overview

The switch supports QQ blacklist and QQ whitelist. You can limit QQ account logins by using either of the following modes:

QQ blacklist mode: QQ accounts in the blacklist are prohibited from login and message receiving, and there are no limits on QQ accounts not in the blacklist. By default, the QQ blacklist is empty, indicating that all QQ accounts log in normally.

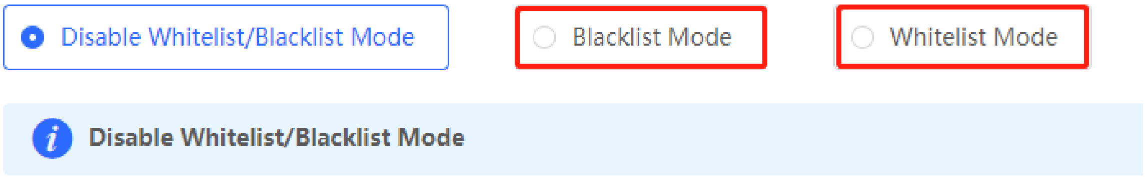
QQ whitelist mode: QQ accounts in the whitelist can log in normally, and QQ account not in the whitelist are prohibited from login and message receiving. By default, the QQ whitelist is empty, indicating that all QQ accounts are prohibited.

6.6.2 Configuration Steps

Choose **Local Device** > **Behavior** > **QQ Management**.

1. **Switching the QQ Management Mode**

By default, **Disable Whitelist/Blacklist Mode** is selected, indicating that all QQ accounts can log in and access the Internet normally. Select **Blacklist Mode** to switch to the QQ blacklist mode, or select **Whitelist Mode** to switch to the QQ whitelist mode.



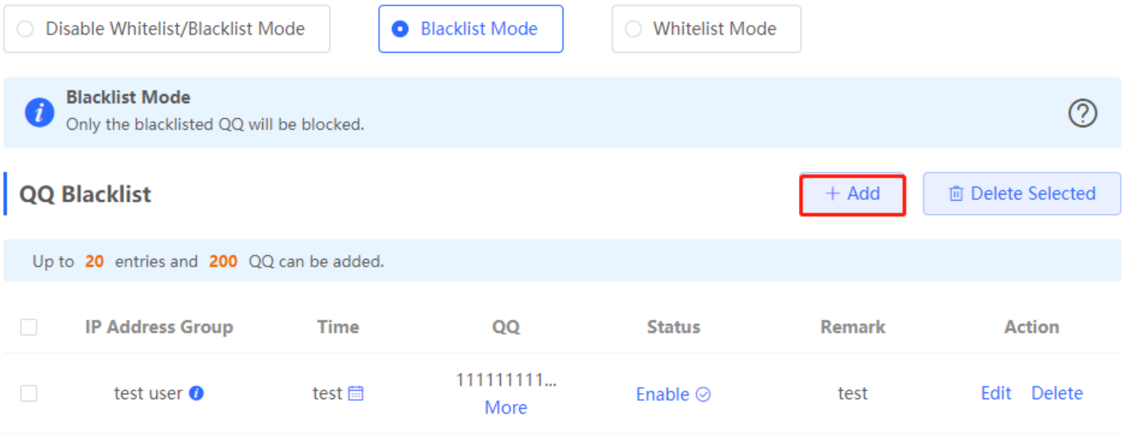
● Disable Whitelist/Blacklist Mode ○ Blacklist Mode ○ Whitelist Mode

Disable Whitelist/Blacklist Mode

2. Configuring QQ Blacklist/Whitelist

Choose **Local Device** > **Behavior** > **QQ Management** > **Whitelist/Blacklist Mode**.

After you switch to the QQ blacklist/whitelist mode, click **Add** to add entries to the blacklist/whitelist. The following describes how to configure a QQ blacklist. The configuration steps for a QQ whitelist are similar.



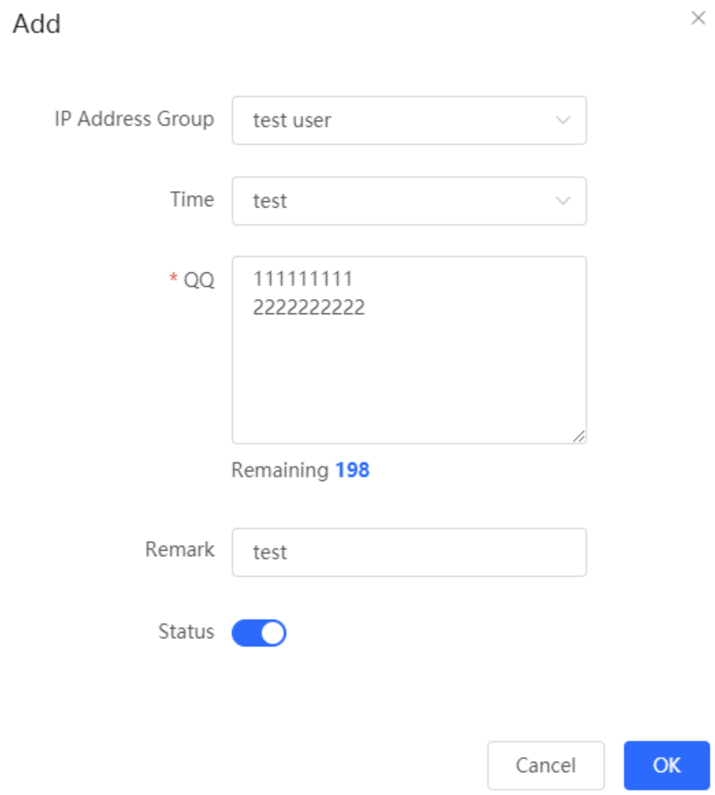
○ Disable Whitelist/Blacklist Mode ● Blacklist Mode ○ Whitelist Mode

Blacklist Mode
Only the blacklisted QQ will be blocked.

QQ Blacklist

Up to 20 entries and 200 QQ can be added.

□	IP Address Group	Time	QQ	Status	Remark	Action
□	test user	test	111111111... More	Enable	test	Edit Delete



Add

IP Address Group: test user

Time: test

* QQ: 111111111
2222222222

Remaining 198

Remark: test

Status: on

Table 6-4 QQ blacklist/whitelist configuration

Parameter	Description
IP Address Group	Specify the IP address range to which the QQ blacklist/whitelist applies. You can select an IP address group defined in Section 6.2 Address Management from the drop-down list box, or select **Custom** and manually enter the specific IP address range.

Parameter	Description
Time	Specify the time range under control of the QQ blacklist/whitelist. In the specified time range, managed clients cannot log in to the prohibited QQ accounts. You can select a time range defined in Section 6.3 Time Management from the drop-down list box, or select **Custom** and manually enter the specific time range.
QQ	In QQ blacklist mode, specify the QQ accounts to block. In the specified time range, managed clients cannot log in to the prohibited QQ accounts, and other QQ accounts can log in normally. In QQ whitelist mode, specify the QQ accounts to permit. In the specified time range, managed clients can log in these QQ accounts normally, but not other QQ accounts. You can enter multiple QQ accounts, separated by new lines.
Remark	Enter the rule description.
Status	Specify whether to enable the QQ management rule.

6.7 Flow Control

6.7.1 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.

6.7.2 Intelligence 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

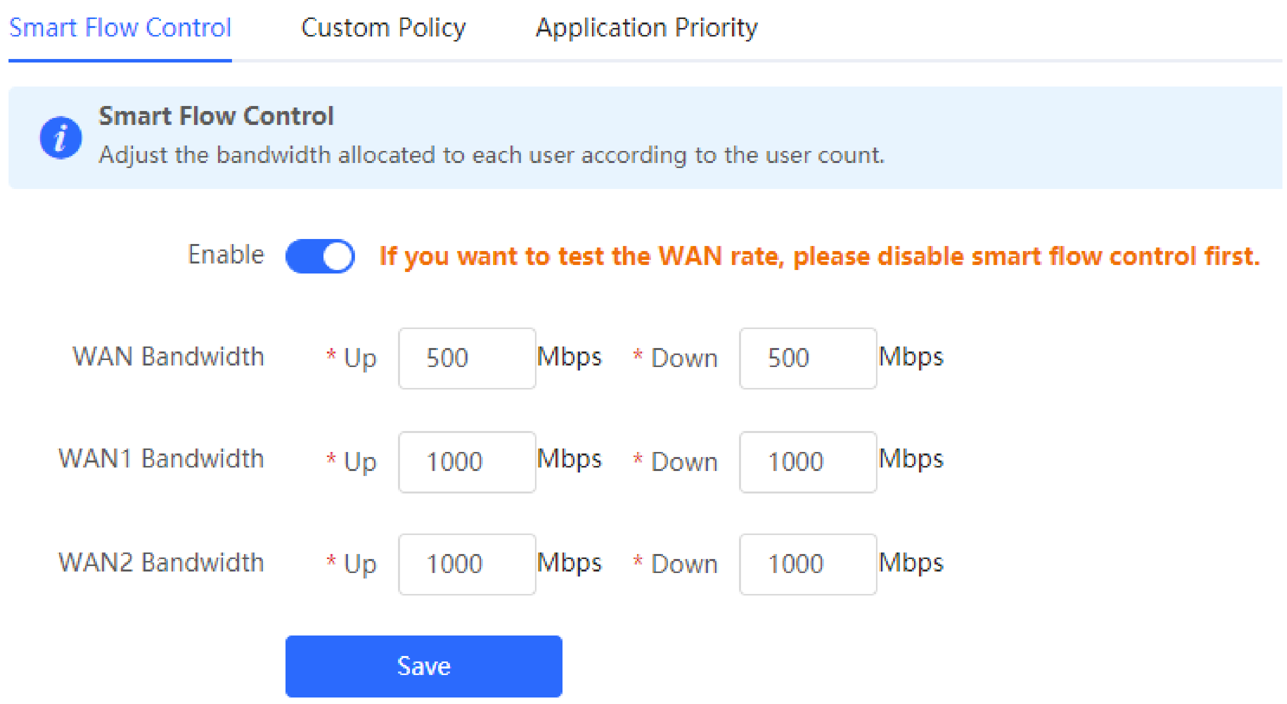
Choose **Local Device** > **Behavior** > **Flow Control** > **Smart Flow Control**.

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 ports separately. For details on the multi-line configuration, see Section 3.2 Configuring the WAN Ports.

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.



Smart Flow Control

Adjust the bandwidth allocated to each user according to the user count.

Enable: ● If you want to test the WAN rate, please disable smart flow control first.

WAN Bandwidth * Up 500 Mbps * Down 500 Mbps

WAN1 Bandwidth * Up 1000 Mbps * Down 1000 Mbps

WAN2 Bandwidth * Up 1000 Mbps * Down 1000 Mbps

Table 6-5 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 ports, 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.

6.7.3 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 IP address 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.

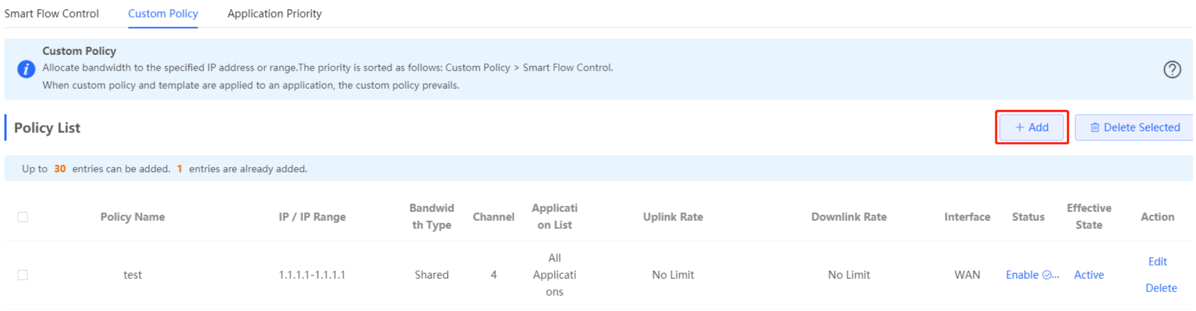
2. Getting Started

Before you configure a custom policy, enable smart flow control first. For details, see Section 6.7.2 Intelligence Flow Control.

3. Configuration Steps

Choose **Local Device** > **Behavior** > **Flow Control** > **Custom Policy**.

Click **Add** to create a custom flow control policy. You can create a maximum of 30 custom policies.

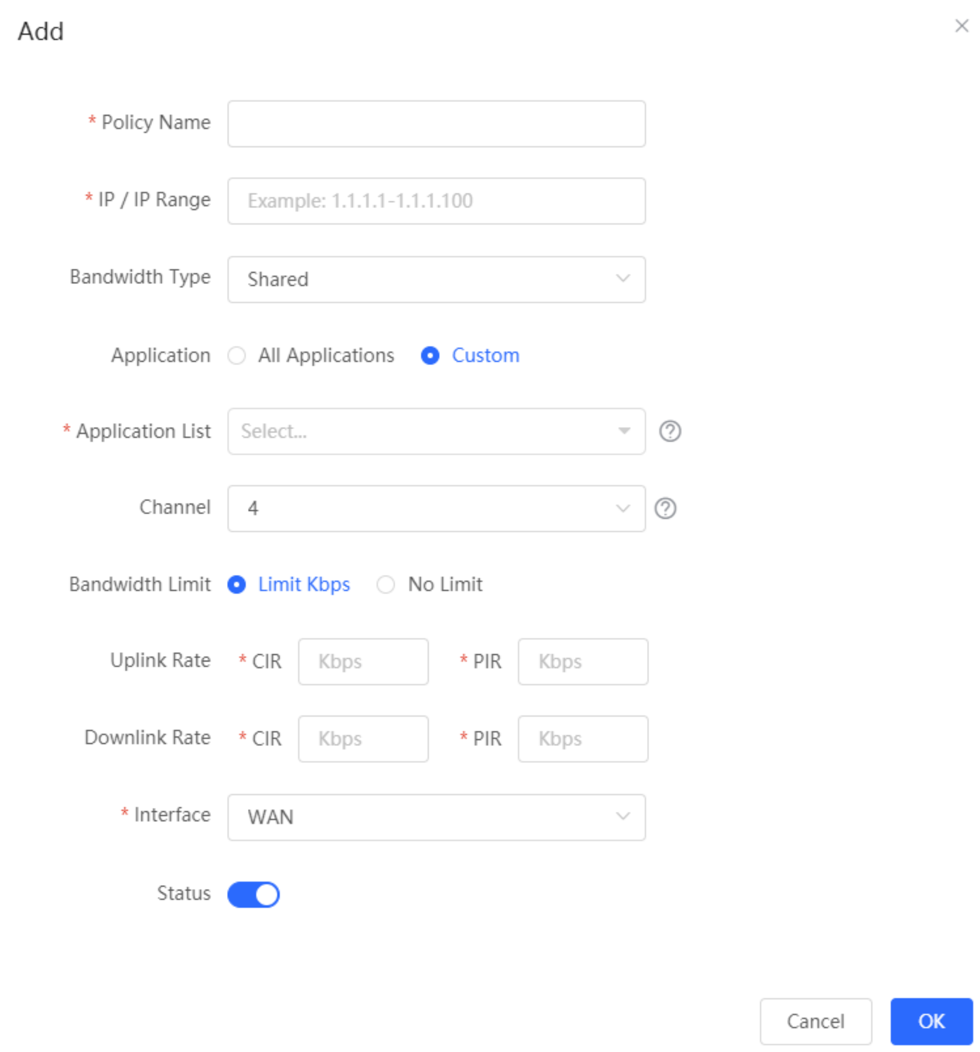


Custom Policy
Allocate bandwidth to the specified IP address or range.The priority is sorted as follows: Custom Policy > Smart Flow Control.
When custom policy and template are applied to an application, the custom policy prevails.

Policy List

Up to 30 entries can be added. 1 entries are already added.

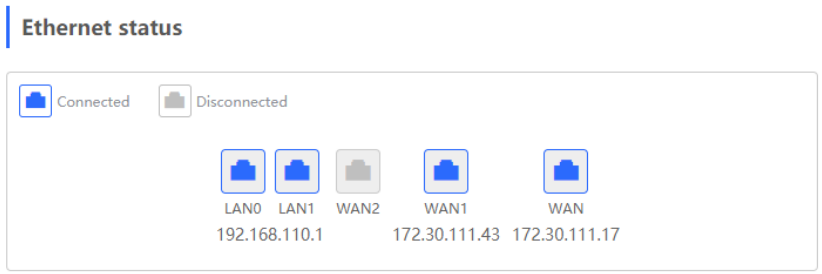
□	Policy Name	IP / IP Range	Bandwidth Type	Channel	Application List	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
□	test	1.1.1.1-1.1.1.1	Shared	4	All Applications	No Limit	No Limit	WAN	Enable ⊘...	Active	Edit Delete



Add

* Policy Name	
* IP / IP Range	Example: 1.1.1.1-1.1.1.100
Bandwidth Type	Shared
Application	○ All Applications ● Custom
* Application List	Select...
Channel	4
Bandwidth Limit	● Limit Kbps ○ No Limit
Uplink Rate	* CIR Kbps * PIR Kbps
Downlink Rate	* CIR Kbps * PIR Kbps
* Interface	WAN
Status	●

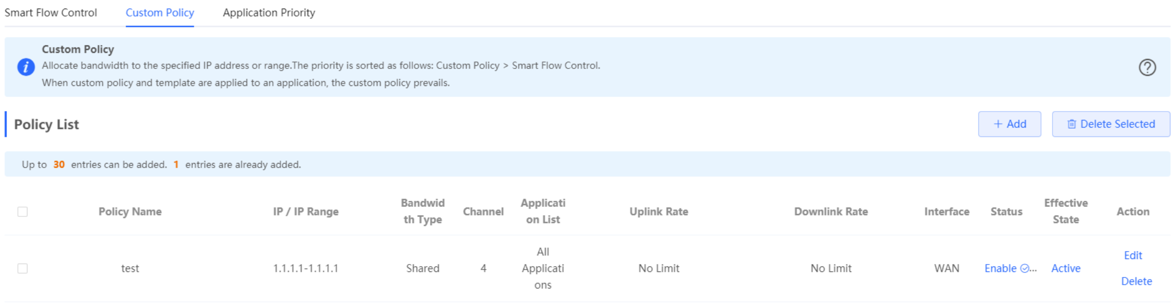
Table 6-6 Custom policy configuration

Parameter	Description
Policy Name	Specify the unique ID of the custom flow control policy. The policy name cannot be modified.
IP / IP Range	Specify the IP address range to which the custom policy applies. You can configure a single IP address or an IP address network segment. The IP address range must be in the LAN segment. You can choose **Overview** > **Ethernet status** to view the current LAN segments. For example, the LAN segment of the device in the following figure is 192.168.110.0/24.  Ethernet status Connected Disconnected LAN0 LAN1 WAN2 WAN1 WAN 192.168.110.1 172.30.111.43 172.30.111.17
Bandwidth Type	**Shared**: All the users (IP addresses) in the user group share the predefined uplink and downlink bandwidth, and the bandwidth of each user is not limited. **Independent**: All the users (IP addresses) in the user group share the predefined uplink and downlink bandwidth, and the maximum bandwidth of a single user can be limited.
Application	When **Bandwidth Type** is set to **Shared**, you can specify the application to which the flow control policy is valid. **All Applications**: The flow control policy is valid to all applications. **Custom**: The flow control policy is valid only to specific applications in the application list. When **Bandwidth Type** is set to **Independent**, you cannot specify the application to which the flow control policy is valid. By default, the policy is valid to all applications.
Application List	When **Application** is set to **Custom**, you need to specify the application to which the policy is valid. The traffic of the selected application is limited by the policy.
Channel	Specify the guarantee level of the traffic. The value is in the range of 0 to 7. A smaller value indicates a higher priority. The value 0 has the highest priority. The traffic priority value corresponds to the application group in the application priority template. The value 2 indicates key channel, the value 4 indicates common channel, and the value 6 indicates suppression channel. For details on the application group in the application priority template, see Section 6.7.4 .

Parameter	Description
Bandwidth Limit	Specify whether to limit the bandwidth. **Limit Kbps**: You can set the uplink and downlink bandwidth limits based on actual needs. **No Limit**: When the bandwidth is sufficient, the maximum bandwidth is not limited. When the bandwidth is insufficient, the minimum bandwidth is not guaranteed.
Uplink/ Downlink Rate	Specify the data transmission rates for upload and download, including the CIR, PIR, and PIR per user, in Kbps. **CIR**: Specify the minimum bandwidth that can be shared by all users when the bandwidth is insufficient. **PIR**: Specify the maximum bandwidth available for all the users when the bandwidth is sufficient. **PIR per User**: Specify the maximum bandwidth for a user when multiple users share the bandwidth. This parameter is optional and can be configured only when Bandwidth Type is set to Independent. By default, the uplink and downlink rates are not limited.
Interface	Specify the WAN port to which the policy applies. If you set this parameter to All WAN Ports, this policy applies to all the WAN ports.
Status	Specify whether to enable the custom flow control policy. If Status is turned off, this policy does not take effect.

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**.



Custom Policy
Allocate bandwidth to the specified IP address or range.The priority is sorted as follows: Custom Policy > Smart Flow Control.
When custom policy and template are applied to an application, the custom policy prevails.

Up to 30 entries can be added. 1 entries are already added.

□	Policy Name	IP / IP Range	Bandwidth Type	Channel	Application List	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
□	test	1.1.1.1-1.1.1.1	Shared	4	All Applications	No Limit	No Limit	WAN	Enable ⊘...	Active	Edit Delete

Table 6-7 Policy list information

Parameter	Description
Status	Indicate whether the current policy is enabled. You can click to modify the status.
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 port is online.

Parameter	Description
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.

6.7.4 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 6.7.2 Intelligence Flow Control.

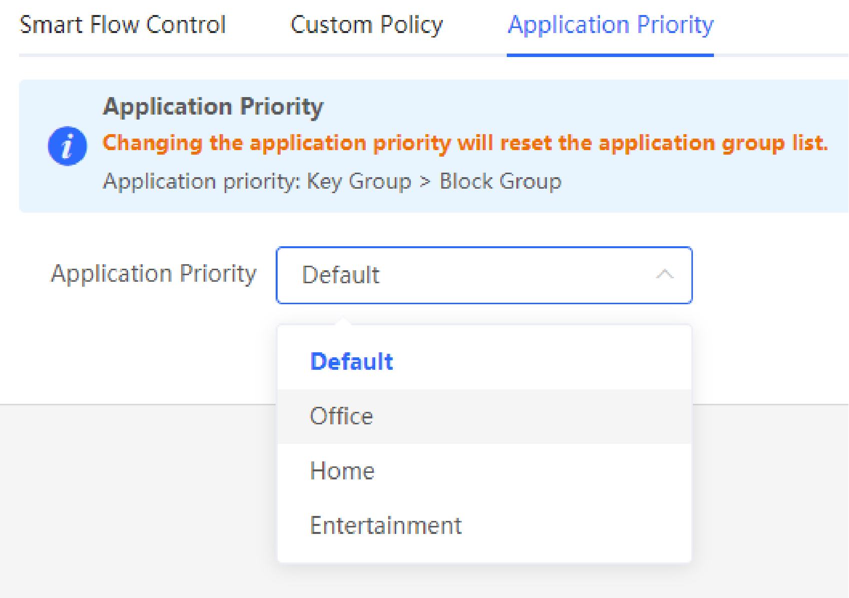
3. Configuration Steps

Choose **Local Device** > **Behavior** > **Flow Control** > **Application Priority**.

(1) Create an application priority template.

Select a template from the **Application Priority** drop-down list box.

Four application priority templates are predefined to meet the needs in different scenarios. You can switch among the templates based on actual needs.



Application Priority

Changing the application priority will reset the application group list.

Application priority: Key Group > Block Group

Application Priority: Default

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.

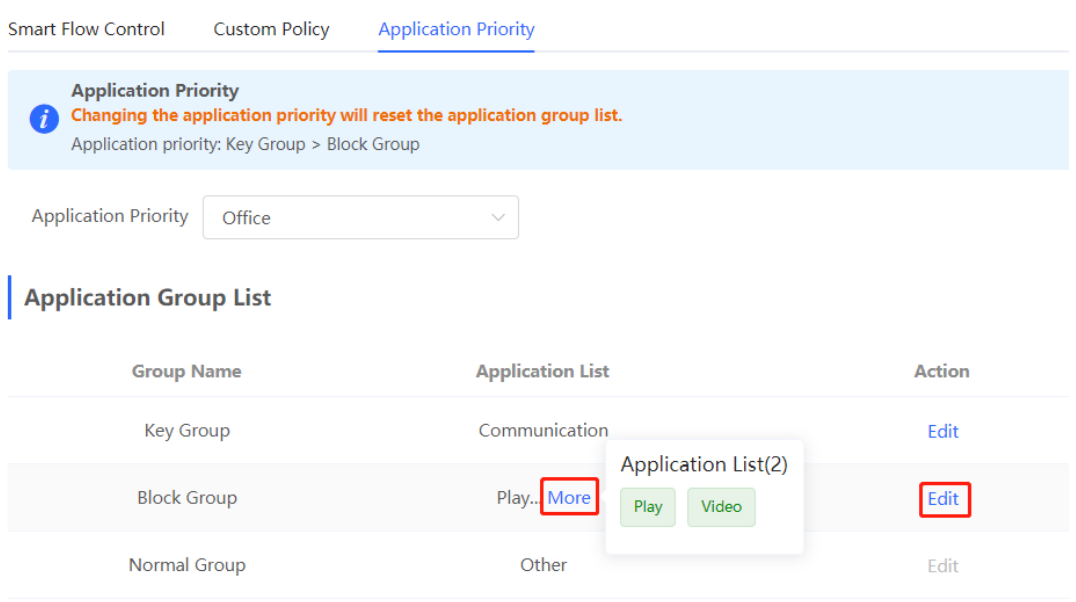
(2) Create an application group list.

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 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.



Application Priority

Changing the application priority will reset the application group list.

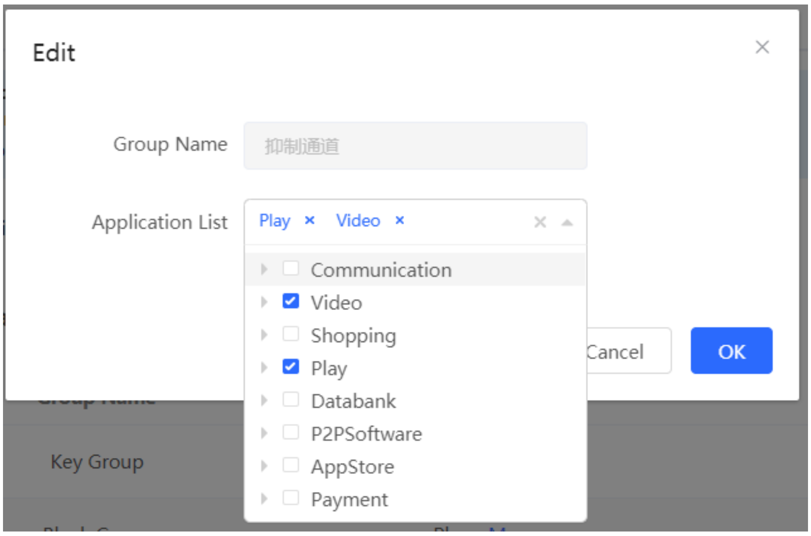
Application priority: Key Group > Block Group

Application Priority: Office

Application Group List

Group Name	Application List	Action
Key Group	Communication	Edit
Block Group	Play... More	Edit
Normal Group	Other	Edit

Application List(2)



Edit

Group Name: 抑制通道

Application List: Play × Video ×

- □ Communication
- ☑ Video
- □ Shopping
- ☑ Play
- □ Databank
- □ P2PSoftware
- □ AppStore
- □ Payment

Caution

The application list will be reset after you switch the application priority template.

6.8 Access Control

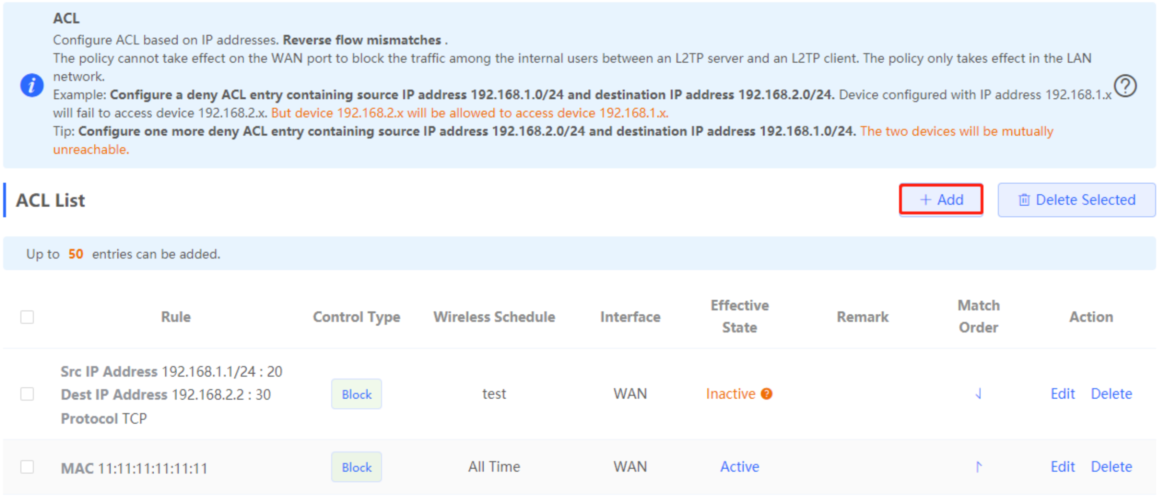
6.8.1 Overview

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.

6.8.2 Configuration Steps

Choose **Local Device** > **Behavior** > **Access Control**.

The access control rule list displays the created access control rules. Click **Add** to add an access control rule.



ACL

Configure ACL based on IP addresses. **Reverse flow mismatches** .

The policy cannot take effect on the WAN port to block the traffic among the internal users between an L2TP server and an L2TP client. The policy only takes effect in the LAN network.

Example: **Configure a deny ACL entry containing source IP address 192.168.1.0/24 and destination IP address 192.168.2.0/24.** Device configured with IP address 192.168.1.x will fail to access device 192.168.2.x. But device 192.168.2.x will be allowed to access device 192.168.1.x.

Tip: **Configure one more deny ACL entry containing source IP address 192.168.2.0/24 and destination IP address 192.168.1.0/24.** The two devices will be mutually unreachable.

ACL List

Up to 50 entries can be added.

□	Rule	Control Type	Wireless Schedule	Interface	Effective State	Remark	Match Order	Action
□	**Src IP Address** 192.168.1.1/24 : 20 **Dest IP Address** 192.168.2.2 : 30 **Protocol** TCP	Block	test	WAN	Inactive ?		↓	Edit Delete
□	**MAC** 11:11:11:11:11:11	Block	All Time	WAN	Active		↑	Edit Delete

Table 6-8 Access control rule information

Parameter	Description
Effective State	Indicate whether the rule takes effect. If **Inactive** is displayed, the current system time may not in the effective time range. Move the cursor to ? to view the detailed cause.
Match Order	All the created ACL 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 and delete a rule.

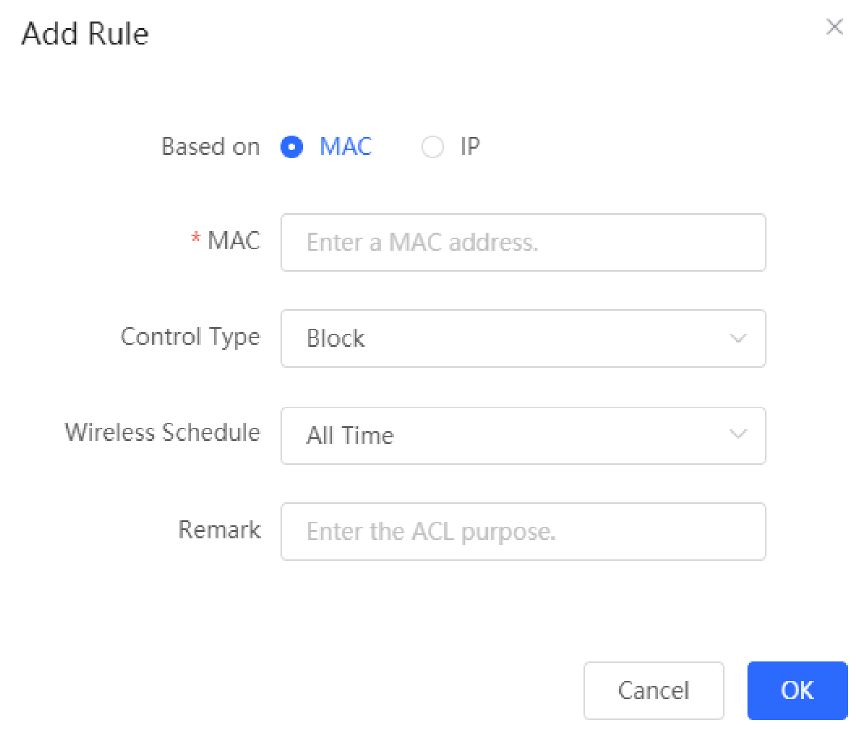
1. Configuring a MAC Address-based ACL Rule

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** to **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 ports by default.



Add Rule

Based on ● MAC ○ IP

* MAC: Enter a MAC address.

Control Type: Block

Wireless Schedule: All Time

Remark: Enter the ACL purpose.

Table 6-9 MAC address-based ACL configuration

Parameter	Description
MAC	Enter the client MAC address to be controlled by the ACL rule. After you click the input field, the current client information is displayed. You can click to automatically enter the corresponding MAC address.
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.
Wireless Schedule	You can select a time range defined in 6.3 Time Management from the drop-down list box, or select **Custom** and manually enter the specific time range.
Remark	Enter the rule description, which is used to uniquely identify a rule.

2. Configuring an IP Address-based ACL Rule

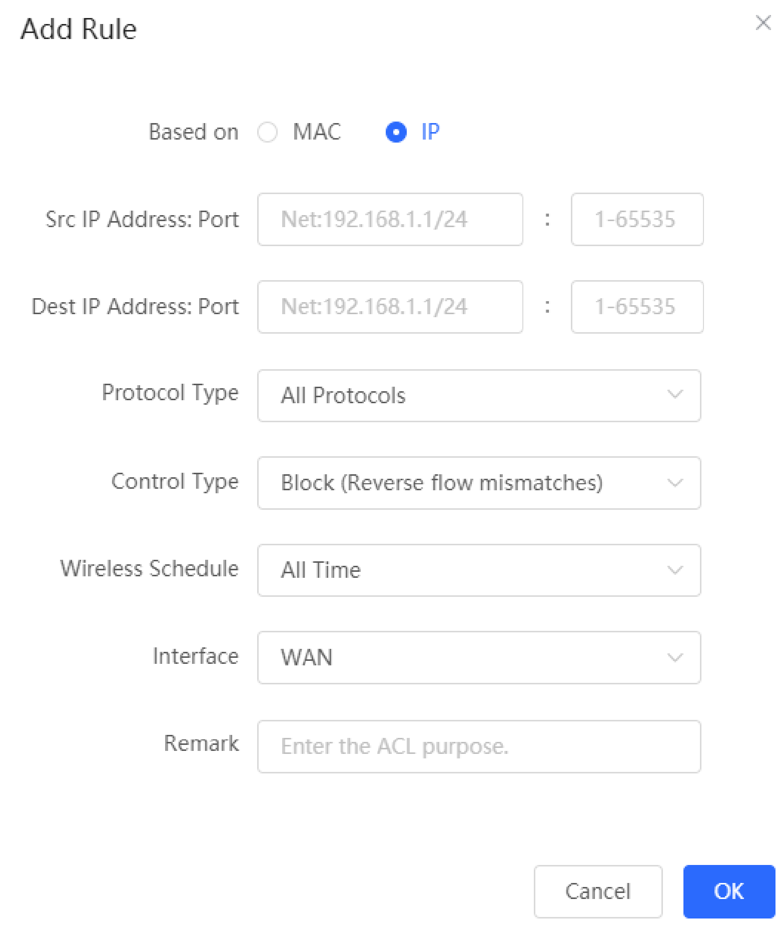
IP address-based ACL rules enable the device to match data flows according to the source IP address, destination IP address, and protocol number.

Set **Based on** to **IP**, 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.



Add Rule

Based on ○ MAC ● IP

Src IP Address: Port Net:192.168.1.1/24 : 1-65535

Dest IP Address: Port Net:192.168.1.1/24 : 1-65535

Protocol Type All Protocols

Control Type Block (Reverse flow mismatches)

Wireless Schedule All Time

Interface WAN

Remark Enter the ACL purpose.

Table 6-10 IP address-based ACL configuration

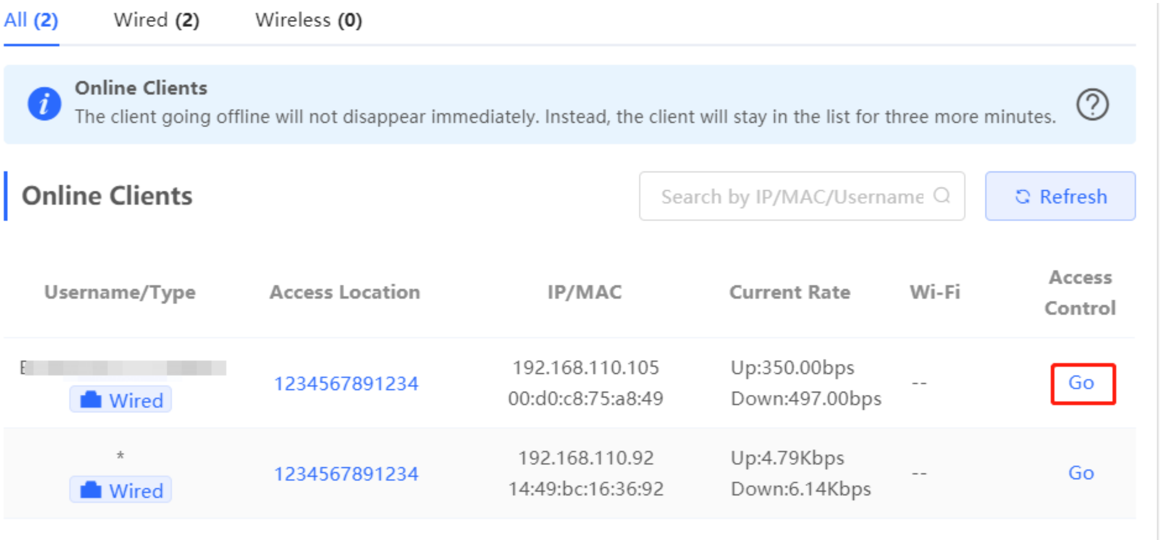
Parameter	**Description**
Src IP Address: Port	Enter the source IP address and port number for data packet matching. If this parameter is not specified, the device matches all the IP addresses and port numbers. The source IP address can be a single IP address (such as 192.168.1.1) or an IP address range (such as 192.168.1.1/24).

Parameter	Description
Dest IP Address: Port	Enter the destination IP address and port number for data packet matching. If this parameter is not specified, the device matches all the IP addresses and port numbers. The destination IP address can be a single IP address (such as 192.168.1.1) or an IP address range (such as 192.168.1.1/24).
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.
Wireless Schedule	You can select a time range defined in Section 6.3 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 port to control data packets received from or sent to the Internet.
Remark	Enter the rule description, which is used to uniquely identify a rule.

6.9 Online User Management

Choose **Clients** > **Online Clients**.

You can view the wired users and wireless users in the current network. Find the target online user and click **Go** in the **Access Control** column to create an ACL rule for the user, to control the online behavior and networking time range of the user client. For details on how to configure an ACL rule, see Section 6.8 .



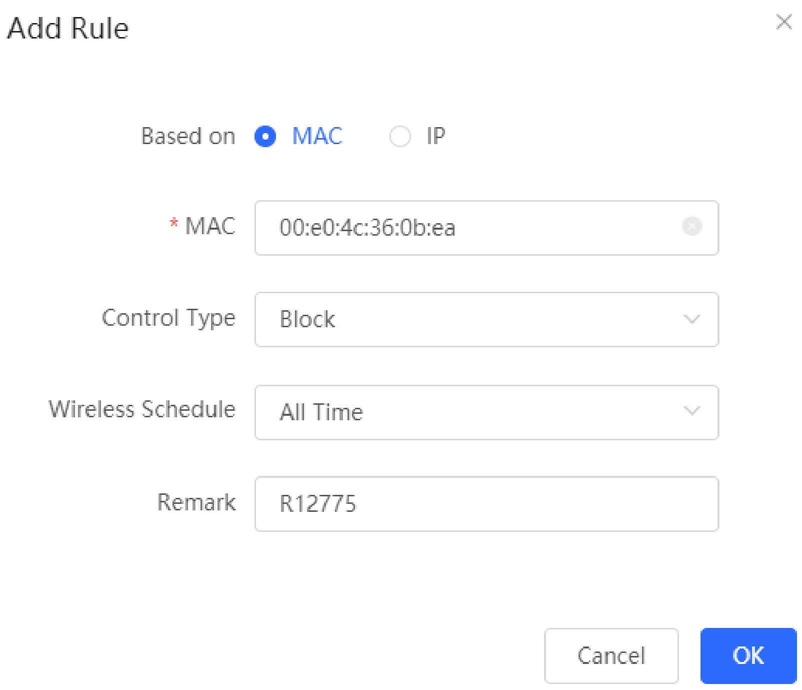
Online Clients
The client going offline will not disappear immediately. Instead, the client will stay in the list for three more minutes.

Online Clients

Username/Type	Access Location	IP/MAC	Current Rate	Wi-Fi	Access Control
E[redacted] Wired	1234567891234	192.168.110.105 00:d0:c8:75:a8:49	Up:350.00bps Down:497.00bps	--	Go
* Wired	1234567891234	192.168.110.92 14:49:bc:16:36:92	Up:4.79Kbps Down:6.14Kbps	--	Go

Table 6-11 Online user information

Parameter	Description
Username/Type	Indicate the name and access type of the client. The access type can be **Wireless** or **Wired**.
Access Location	Indicate the SN of the device to which the client connects in wired or wireless mode.
IP/MAC	Indicate the IP address and MAC address of the client.
Current Rate	Indicate the current uplink and downlink data transmission rates.
Wi-Fi	Indicate the wireless signal information displayed when **Username/Type** is set to **Wireless**. The information includes the channel, signal strength, online duration, and negotiated rate.


Add Rule

Based on ● MAC ○ IP

* MAC: 00:e0:4c:36:0b:ea

Control Type: Block

Wireless Schedule: All Time

Remark: R12775

7 VPN

7.1 Configuring IPsec VPN

7.1.1 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

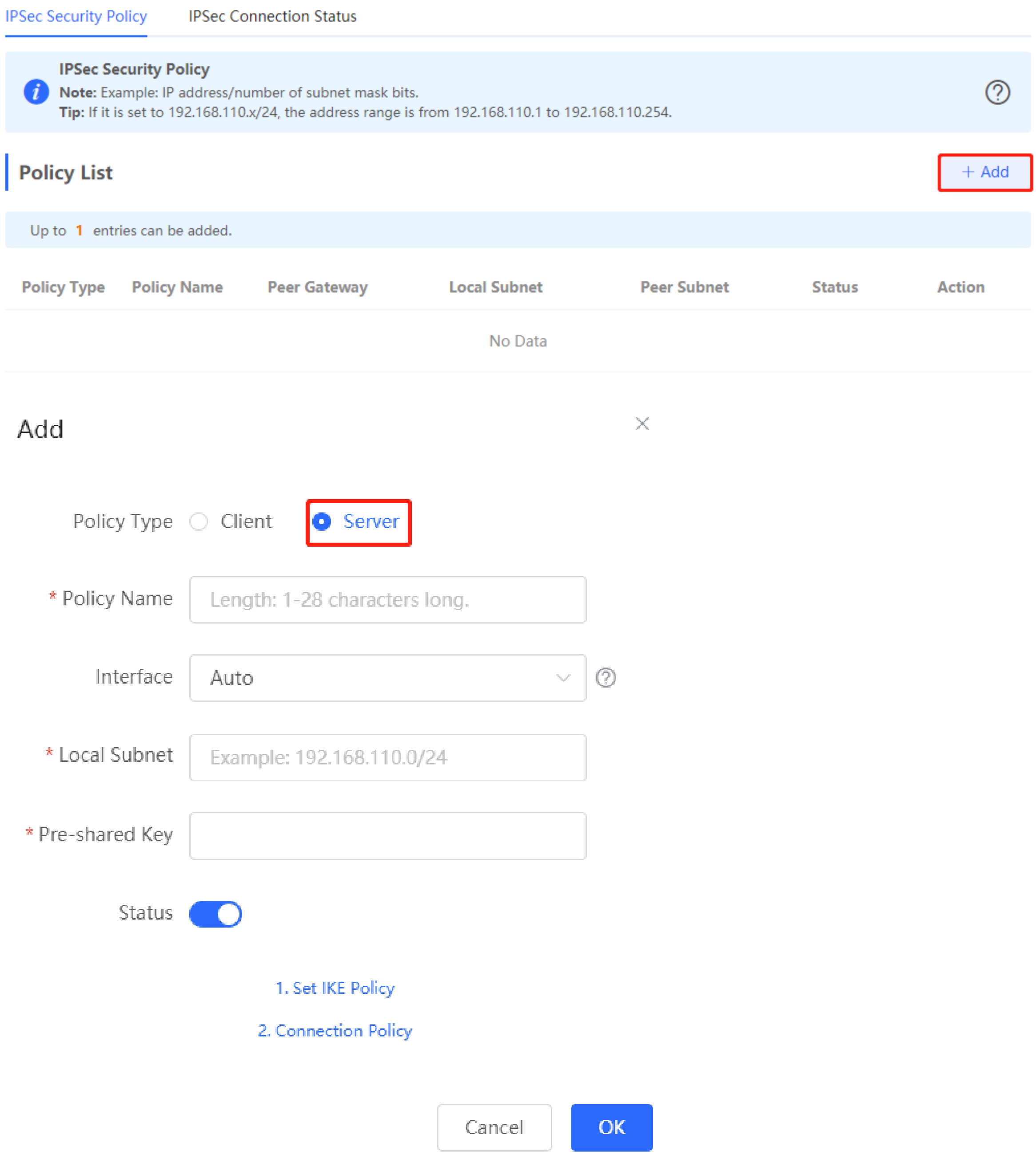
IPsec security policies define security proposals (equivalent to SA) for data flows. You can configure matching security policies on both parties engaged in the communication to establish IPsec tunnels between the IPsec client and the IPsec server, protecting the communication data. An IPsec security 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.

7.1.2 Configuring the IPsec Server

Choose **Local Device** > **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**.



IPSec Security Policy IPSec Connection Status

IPSec Security Policy

Note: Example: IP address/number of subnet mask bits.

Tip: If it is set to 192.168.110.x/24, the address range is from 192.168.110.1 to 192.168.110.254.

Policy List + Add

Up to 1 entries can be added.

Policy Type	Policy Name	Peer Gateway	Local Subnet	Peer Subnet	Status	Action
			No Data			

Add ×

Policy Type ○ Client ● Server

* Policy Name: Length: 1-28 characters long.

Interface: Auto

* Local Subnet: Example: 192.168.110.0/24

* Pre-shared Key:

Status: On

1. Set IKE Policy

2. Connection Policy

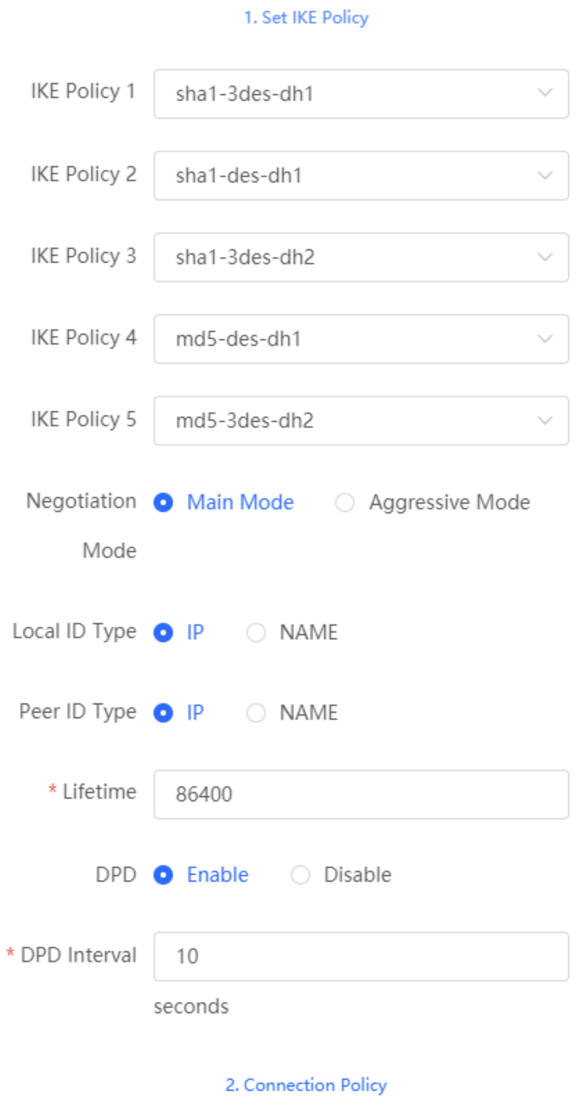
Cancel OK

Table 7-1 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.
Interface	Select a local WAN port 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 port specified here. In the multi-line scenario, you are advised to set this parameter to **Auto**.
Local Subnet	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.
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)

Click **1. Set IKE Policy** to expand the configuration items. Keep the default settings unless otherwise specified.



1. Set IKE Policy

IKE Policy 1: sha1-3des-dh1

IKE Policy 2: sha1-des-dh1

IKE Policy 3: sha1-3des-dh2

IKE Policy 4: md5-des-dh1

IKE Policy 5: md5-3des-dh2

Negotiation Mode: ● Main Mode ○ Aggressive Mode

Local ID Type: ● IP ○ NAME

Peer ID Type: ● IP ○ NAME

* Lifetime: 86400

DPD: ● Enable ○ Disable

* DPD Interval: 10 seconds

2. Connection Policy

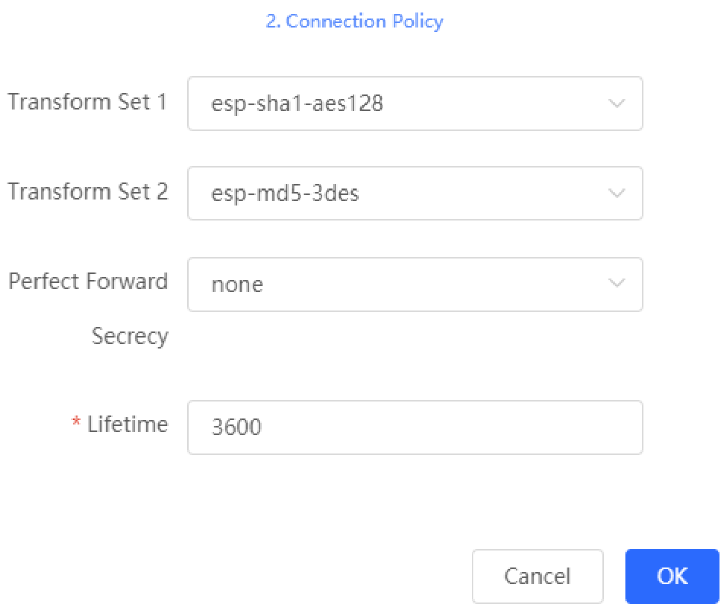
Table 7-2 IPsec server IKE policy configuration

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.
Lifetime	Specify the lifetime of the IKE SA. (The negotiated IKE SA lifetime prevails.) You are advised to use the default value.

Parameter	Description
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 **2. Connection Policy** to expand the configuration items. Keep the default settings unless otherwise specified.



2. Connection Policy

Transform Set 1: esp-sha1-aes128

Transform Set 2: esp-md5-3des

Perfect Forward Secrecy: none

* Lifetime: 3600

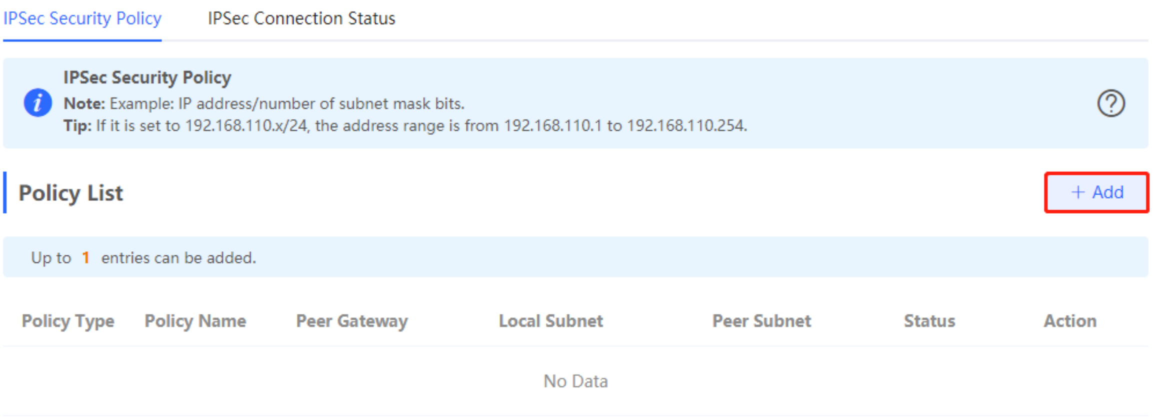
Table 7-3 IPsec server connection policy configuration

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: 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
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.

7.1.3 Configuring the IPsec Client

Choose **Local Device** > **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**.



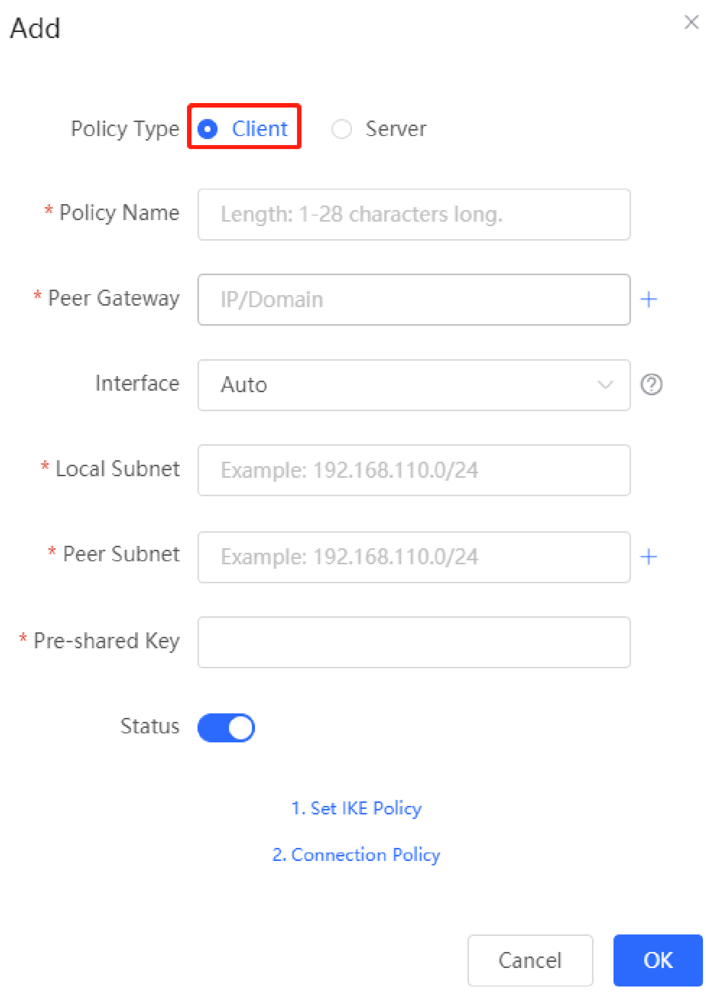
IPSec Security Policy   IPSec Connection Status

IPSec Security Policy
Note: Example: IP address/number of subnet mask bits.
Tip: If it is set to 192.168.110.x/24, the address range is from 192.168.110.1 to 192.168.110.254.

Policy List   + Add

Up to 1 entries can be added.

Policy Type	Policy Name	Peer Gateway	Local Subnet	Peer Subnet	Status	Action
No Data						



Add

Policy Type ● Client ○ Server

* Policy Name: Length: 1-28 characters long.

* Peer Gateway: IP/Domain +

Interface: Auto

* Local Subnet: Example: 192.168.110.0/24

* Peer Subnet: Example: 192.168.110.0/24 +

* Pre-shared Key:

Status: On

1. Set IKE Policy

2. Connection Policy

Cancel   OK

Table 7-4 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.
Peer Gateway	Enter the IP address or domain name of the peer device.

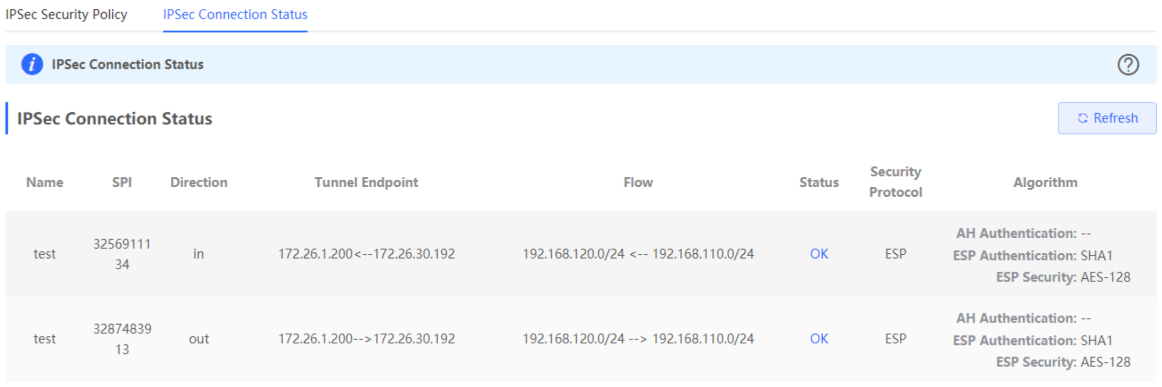
Parameter	Description
Interface	Select a WAN port used locally from the drop-down list box. In the multi-line scenario, you are advised to set this parameter to **Auto**.
Local Subnet	Specify the local subnet address range for the data flows to be protected, that is, the LAN port network segment of the server. The value is the combination of IP address and subnet mask.
Peer Subnet	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.
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).

7.1.4 Viewing the IPsec Connection Status

Choose **Local Device** > **VPN** > **IPSec** > **IPSec Connection Status**.

You can view the IPsec tunnel connection status on the current page.



IPSec Connection Status

Name	SPI	Direction	Tunnel Endpoint	Flow	Status	Security Protocol	Algorithm
test	3256911134	in	172.26.1.200<--172.26.30.192	192.168.120.0/24 <-- 192.168.110.0/24	OK	ESP	AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128
test	3287483913	out	172.26.1.200-->172.26.30.192	192.168.120.0/24 --> 192.168.110.0/24	OK	ESP	AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128

Table 7-5 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.

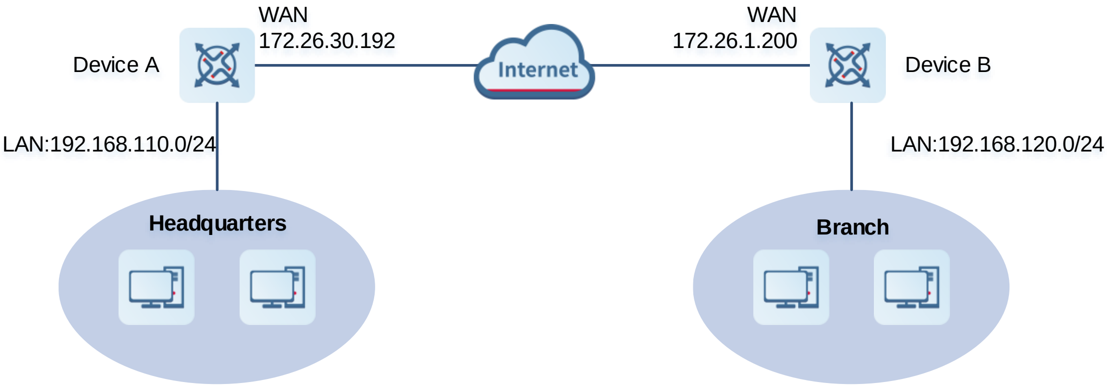
Parameter	Description
Direction	Indicate the direction of the IPsec connection. The value **in** indicates inbound, and the value **out** indicates outbound.
Tunnel Client	Indicate the gateway addresses on two ends of the IPsec connection. The arrow indicates the direction of data flows to be protected 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.
Security Protocol	Indicate the security protocol used by the IPsec connection.
Algorithm	Indicate the encryption algorithm and authentication algorithm used by the IPsec connection.

7.1.5 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



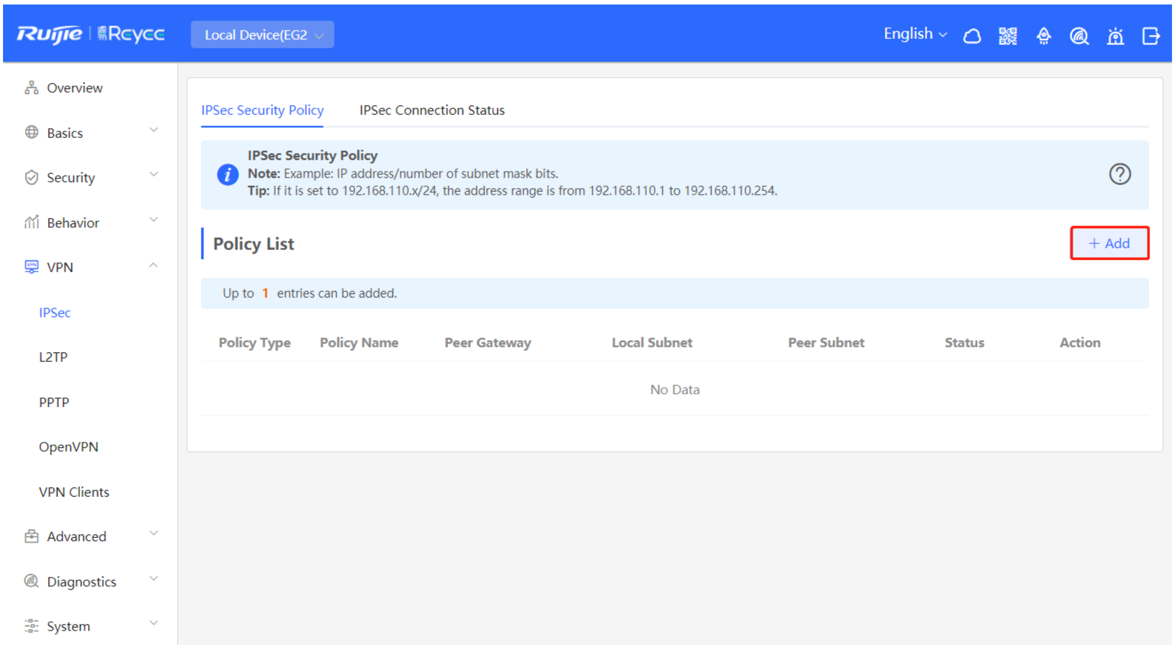
3. Configuration Roadmap

- Configure the HQ gateway Device A as the IPsec server.
- Configure the branch gateway Device B as the IPsec client.

4. Configuration Steps

(1) Configure the HQ gateway.

a Log in to the web management system and choose VPN > IPSec > IPSec Security Policy to access the IPSec Security Policy page.



IPSec Security Policy
Note: Example: IP address/number of subnet mask bits.
Tip: If it is set to 192.168.110.x/24, the address range is from 192.168.110.1 to 192.168.110.254.

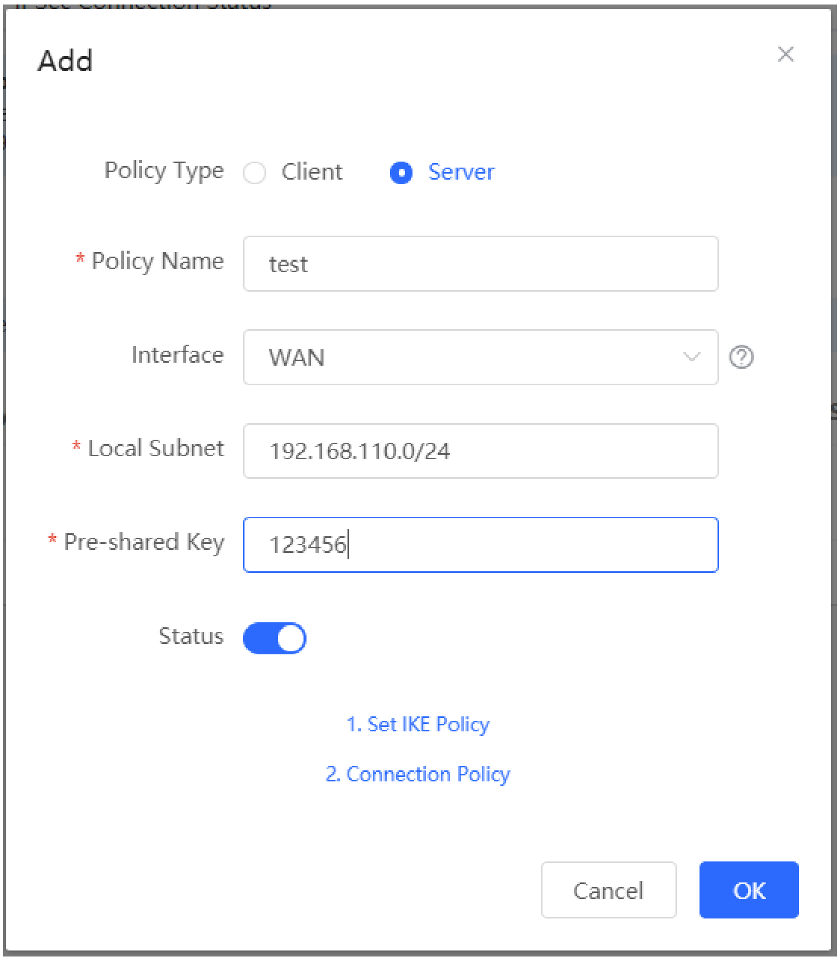
Policy List

Up to 1 entries can be added.

Policy Type	Policy Name	Peer Gateway	Local Subnet	Peer Subnet	Status	Action
No Data						

b 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.



Add

Policy Type ○ Client ● Server

* Policy Name: test

Interface: WAN

* Local Subnet: 192.168.110.0/24

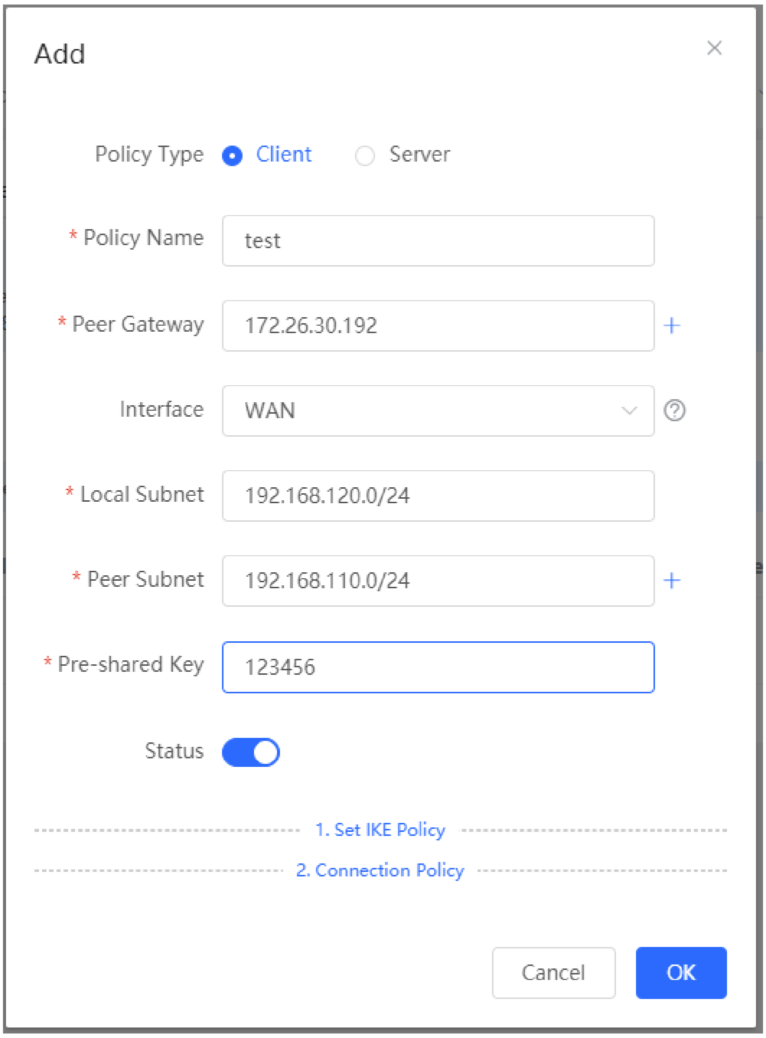
* Pre-shared Key: 123456

Status: on

(2) Configure the branch gateway.

a Log in to the web management system and access the IPSec Security Policy page.

b Click Add. In the dialog box that appears, set Policy Type to Client, enter the policy name, select the peer gateway (WAN port 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.



Add

Policy Type ● Client ○ Server

* Policy Name: test

* Peer Gateway: 172.26.30.192

Interface: WAN

* Local Subnet: 192.168.120.0/24

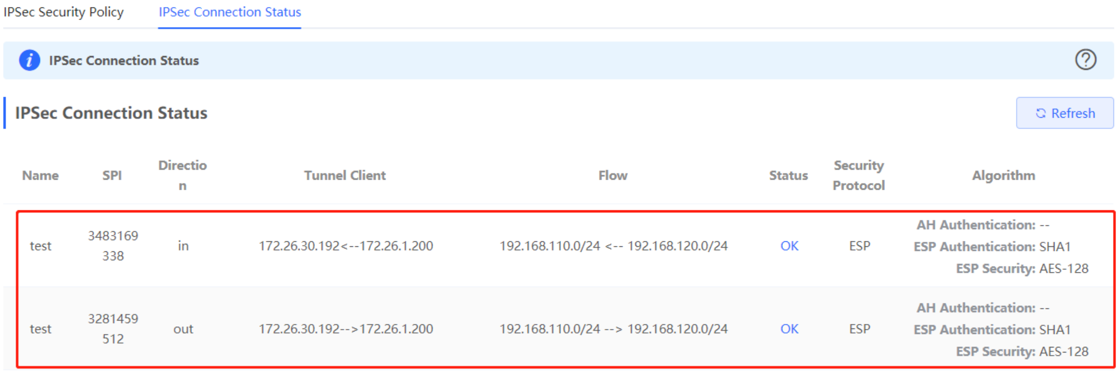
* Peer Subnet: 192.168.110.0/24

* Pre-shared Key: 123456

Status: On

5. Verifying Configuration

(1) Log in to the web management system of the HQ or branch gateway and choose **VPN** > **IPSec** > **IPSec Connection Status**. You can view the IPsec connection status between the HQ and branch.



IPSec Connection Status

Name	SPI	Direction	Tunnel Client	Flow	Status	Security Protocol	Algorithm
test	3483169338	in	172.26.30.192<--172.26.1.200	192.168.110.0/24 <-- 192.168.120.0/24	OK	ESP	AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128
test	3281459512	out	172.26.30.192-->172.26.1.200	192.168.110.0/24 --> 192.168.120.0/24	OK	ESP	AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128

(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.

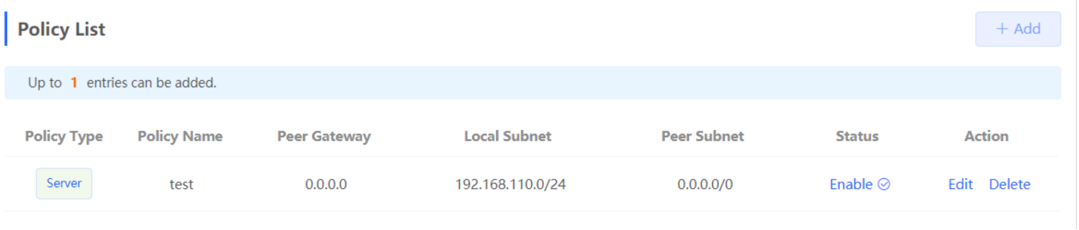
7.1.6 Solution to IPsec VPN Connection Failure

(1) Run the ping command to test the connectivity between the client and server. For details, see Section **错误!未找到引用源。**. 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.

Click **Diagnostics** > **Network Tools**. Then, you can start the ping operation. For details, see Section **错误!未找到引用源。**.

(2) Confirm that the configurations on the IPsec server and IPsec client are correct.

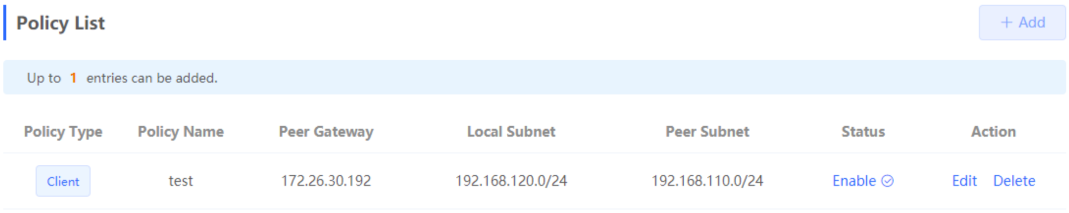
Choose **VPN** > **IPSec** > **IPSec Security Policy** and confirm that the security policies configured on the two ends are matching.



Policy List

Up to 1 entries can be added.

Policy Type	Policy Name	Peer Gateway	Local Subnet	Peer Subnet	Status	Action
Server	test	0.0.0.0	192.168.110.0/24	0.0.0.0/0	Enable ✓	Edit Delete

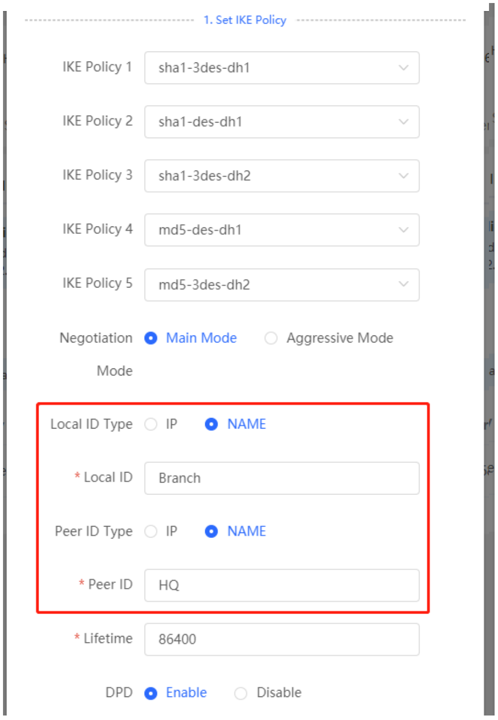


Policy List

Up to 1 entries can be added.

Policy Type	Policy Name	Peer Gateway	Local Subnet	Peer Subnet	Status	Action
Client	test	172.26.30.192	192.168.120.0/24	192.168.110.0/24	Enable ✓	Edit Delete

(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.



1. Set IKE Policy

IKE Policy 1: sha1-3des-dh1

IKE Policy 2: sha1-des-dh1

IKE Policy 3: sha1-3des-dh2

IKE Policy 4: md5-des-dh1

IKE Policy 5: md5-3des-dh2

Negotiation Mode: ● Main Mode ○ Aggressive Mode

Local ID Type: ○ IP ● NAME

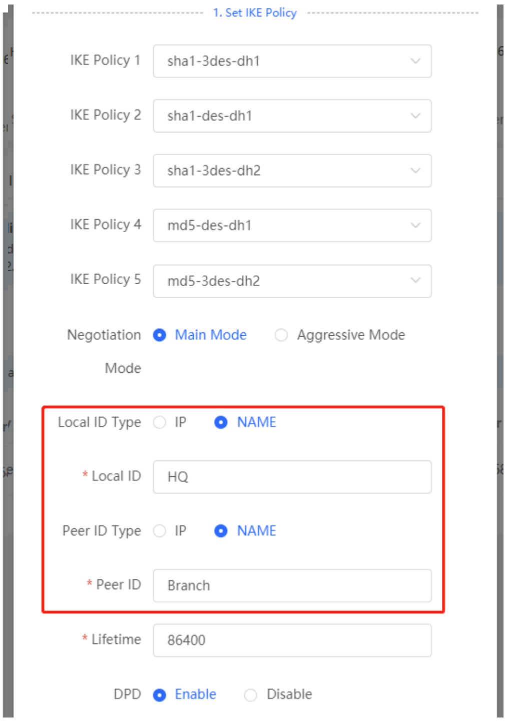
* Local ID: Branch

Peer ID Type: ○ IP ● NAME

* Peer ID: HQ

* Lifetime: 86400

DPD: ● Enable ○ Disable



1. Set IKE Policy

IKE Policy 1: sha1-3des-dh1

IKE Policy 2: sha1-des-dh1

IKE Policy 3: sha1-3des-dh2

IKE Policy 4: md5-des-dh1

IKE Policy 5: md5-3des-dh2

Negotiation Mode: ● Main Mode ○ Aggressive Mode

Local ID Type: ○ IP ● NAME

* Local ID: HQ

Peer ID Type: ○ IP ● NAME

* Peer ID: Branch

* Lifetime: 86400

DPD: ● Enable ○ Disable

7.2 Configuring L2TP VPN

7.2.1 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.

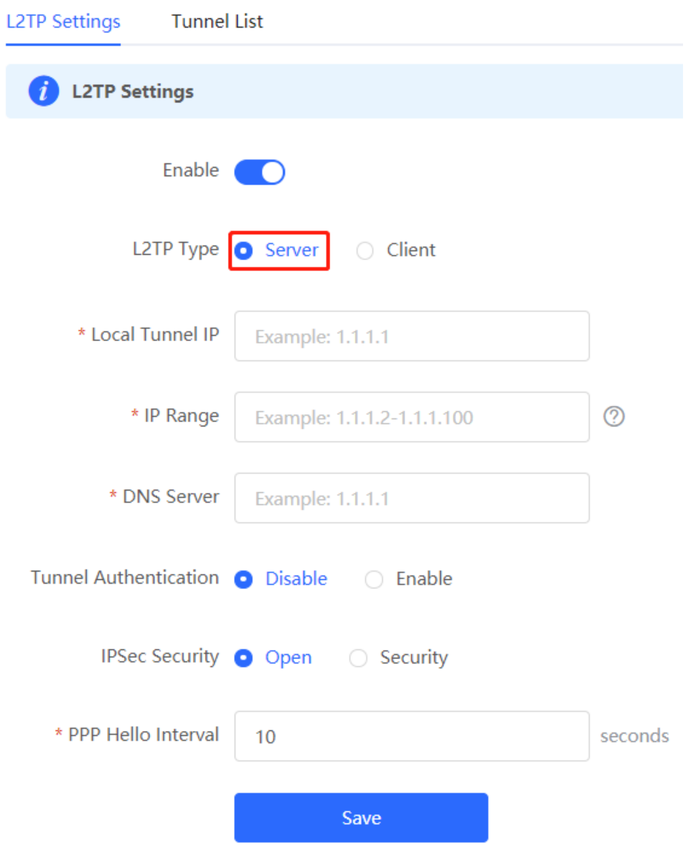
L2TP VPN can be used to establish secure tunnels between the enterprise HQ and branches and allow traveling employees to access the HQ. Currently, the device can be deployed as the L2TP server or client.

7.2.2 Configuring the L2TP Server

1. Basic Settings of L2TP Server

Choose **Local Device** > **VPN** > **L2TP** > **L2TP Settings**.

Turn on the L2TP function, set **L2TP Type** to **Server**, set L2TP server parameters, and click **Save**.



L2TP Settings | Tunnel List

L2TP Settings

Enable: on

L2TP Type: ● Server ○ Client

* Local Tunnel IP: Example: 1.1.1.1

* IP Range: Example: 1.1.1.2-1.1.1.100

* DNS Server: Example: 1.1.1.1

Tunnel Authentication: ● Disable ○ Enable

IPSec Security: ● Open ○ Security

* PPP Hello Interval: 10 seconds

Save

Table 7-6 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.
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.

Parameter	Description
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.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after L2TP VPN is deployed. You are advised to retain the default configuration.

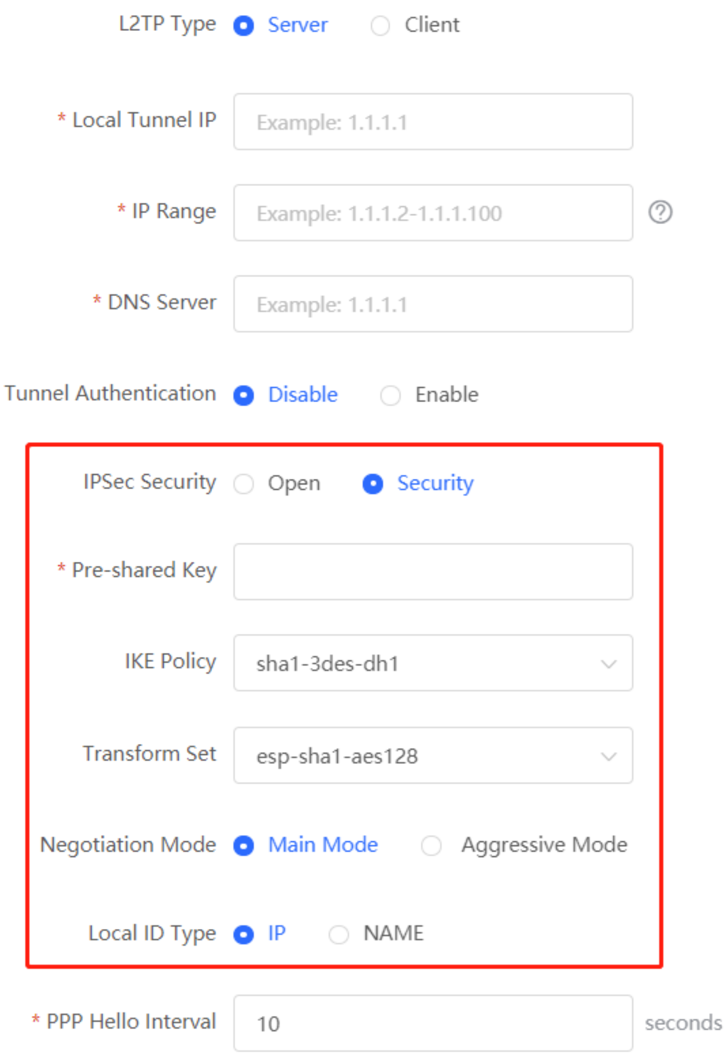
⚠ **Caution**

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 **Local Device** > **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 7.1 Configuring IPsec VPN.



L2TP Type ● Server ○ Client

* Local Tunnel IP: Example: 1.1.1.1

* IP Range: Example: 1.1.1.2-1.1.1.100

* DNS Server: Example: 1.1.1.1

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

Local ID Type ● IP ○ NAME

* PPP Hello Interval: 10 seconds

Table 7-7 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.
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

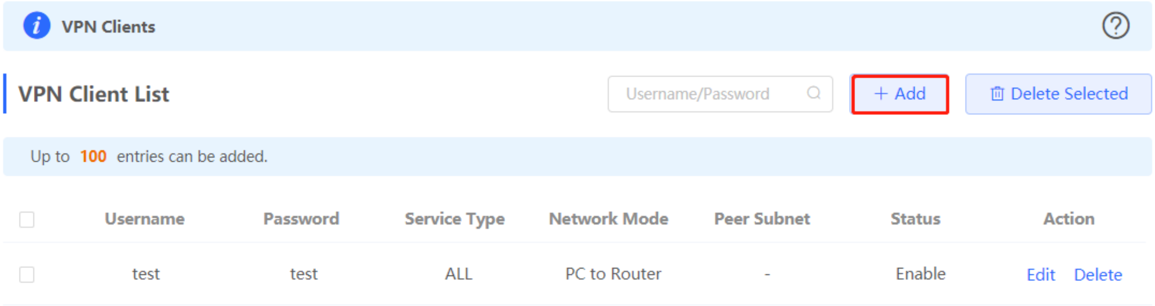
Parameter	Description
Negotiation Mode	Select **Main Mode** or **Aggressive Mode**. The negotiation mode on the server and client must be the same. Main Mode: This mode is applicable to communication between fixed public network IP addresses and point-to-point communication between devices. In this mode, 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 port 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 **Local Device** > **VPN** > **VPN Clients**.

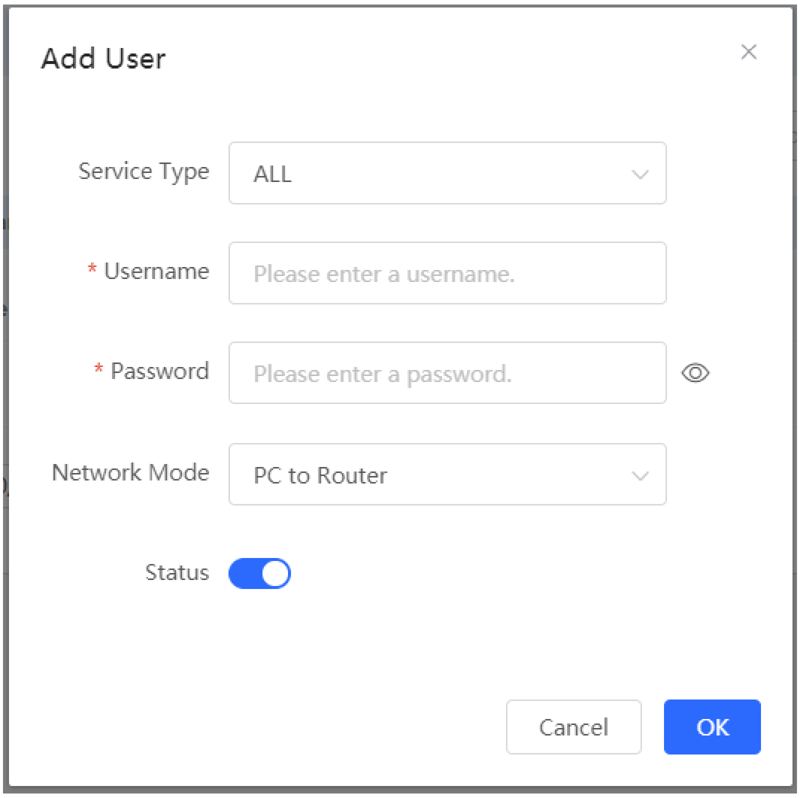
Only user accounts added to the VPN client list are allowed to dial up to connect to the L2TP server. Therefore, you need to manually configure user accounts for clients to access the L2TP server.

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**.



Up to 100 entries can be added.

□	Username	Password	Service Type	Network Mode	Peer Subnet	Status	Action
□	test	test	ALL	PC to Router	-	Enable	Edit Delete



Add User

Service Type ALL

* Username Please enter a username.

* Password Please enter a password.

Network Mode PC to Router

Status

Table 7-8 L2TP user configuration

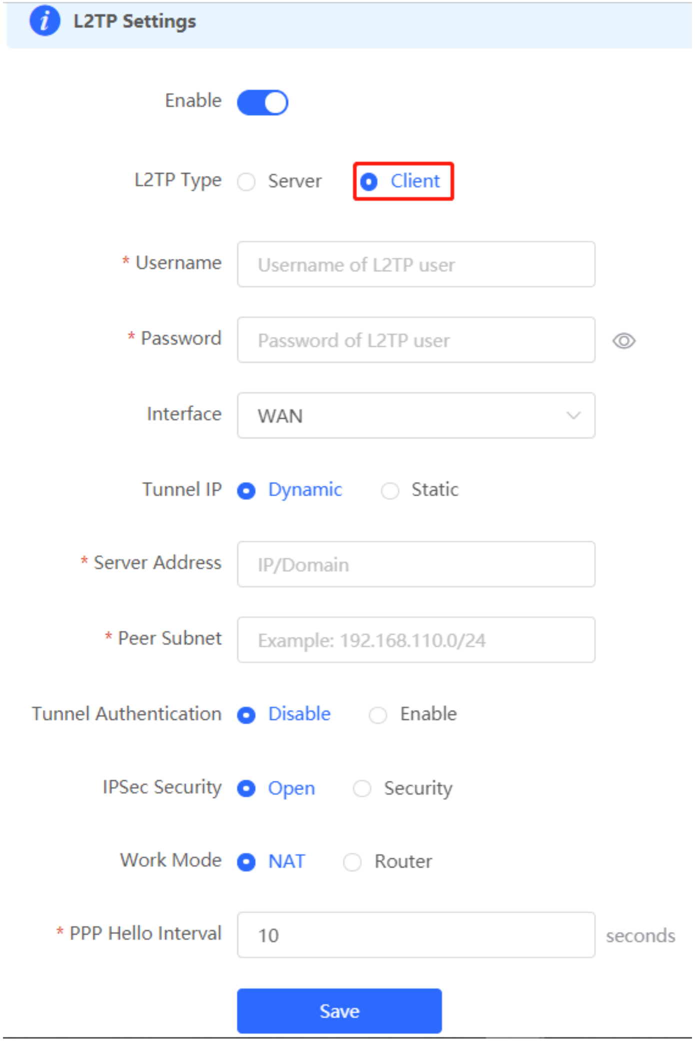
Parameter	Description
Username/Password	Specify the name and password of the L2TP user allowed to dial up to connect to the L2TP server. The username and password are used to establish a connection between the server and client.
Network Mode	PC to Router: The dial-up client is an individual. Select this 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.
Peer Subnet	Specify the IP address range used by the LAN on the peer end of the L2TP 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.
Status	Specify whether to enable the user account.

7.2.3 Configuring the L2TP Client

1. Basic Settings of L2TP Client

Choose **Local Device** > **VPN** > **L2TP** > **L2TP Settings**.

Turn on the L2TP function, set **L2TP Type** to **Client**, set L2TP client parameters, and click **Save**.



L2TP Settings

Enable ●

L2TP Type ○ Server ● Client

* Username: Username of L2TP user

* Password: Password of L2TP user

Interface: WAN

Tunnel IP ● Dynamic ○ Static

* Server Address: IP/Domain

* Peer Subnet: Example: 192.168.110.0/24

Tunnel Authentication ● Disable ○ Enable

IPSec Security ● Open ○ Security

Work Mode ● NAT ○ Router

* PPP Hello Interval: 10 seconds

Save

Table 7-9 L2TP client configuration

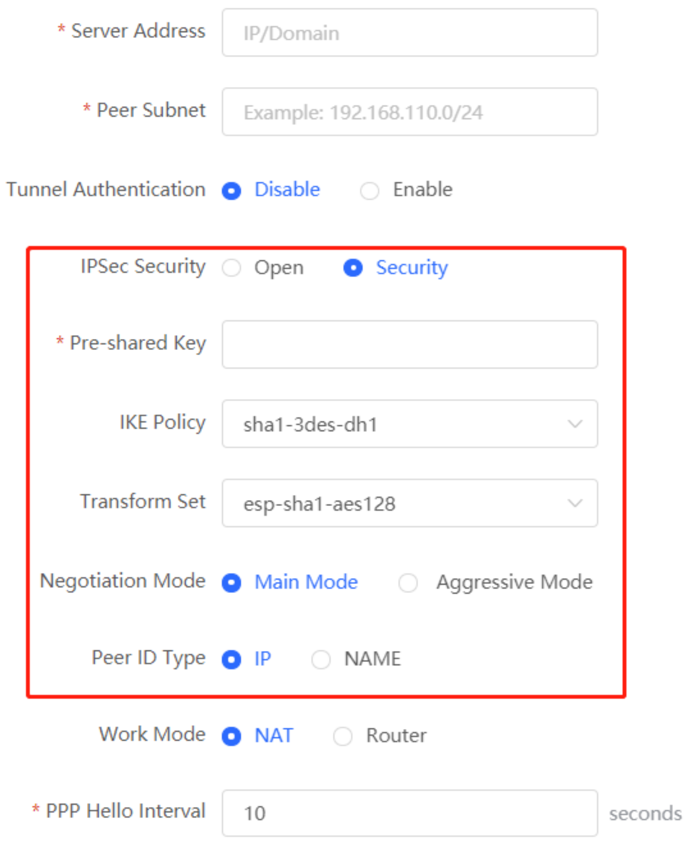
Parameter	Description
Username/Password	Specify the username and password for identity authentication for communication over the L2TP tunnel. The values must be the same as those configured on the L2TP server.
Interface	Specify the WAN port used by the client.
Tunnel IP	Specify the virtual IP address 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 port IP address or domain name of the server. This address must be a public network IP address.
Peer 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.

Parameter	Description
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.
Work 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 **Local Device** > **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.



* Server Address: IP/Domain

* Peer Subnet: Example: 192.168.110.0/24

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 ○ NAME

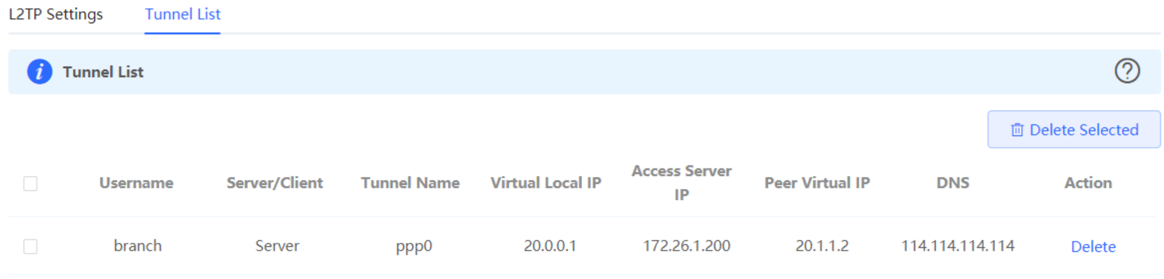
Work Mode: ● NAT ○ Router

* PPP Hello Interval: 10 seconds

7.2.4 Viewing the L2TP Tunnel Information

Choose **Local Device** > **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.



Tunnel List

□	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
□	branch	Server	ppp0	20.0.0.1	172.26.1.200	20.1.1.2	114.114.114.114	Delete

Table 7-10 L2TP 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 L2TP.

Parameter	Description
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.

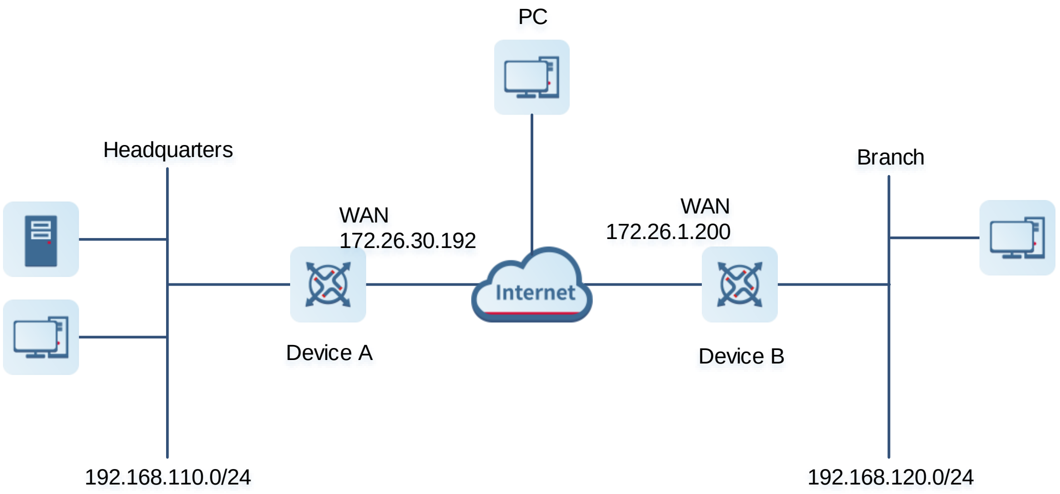
7.2.5 Typical Configuration Example

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.

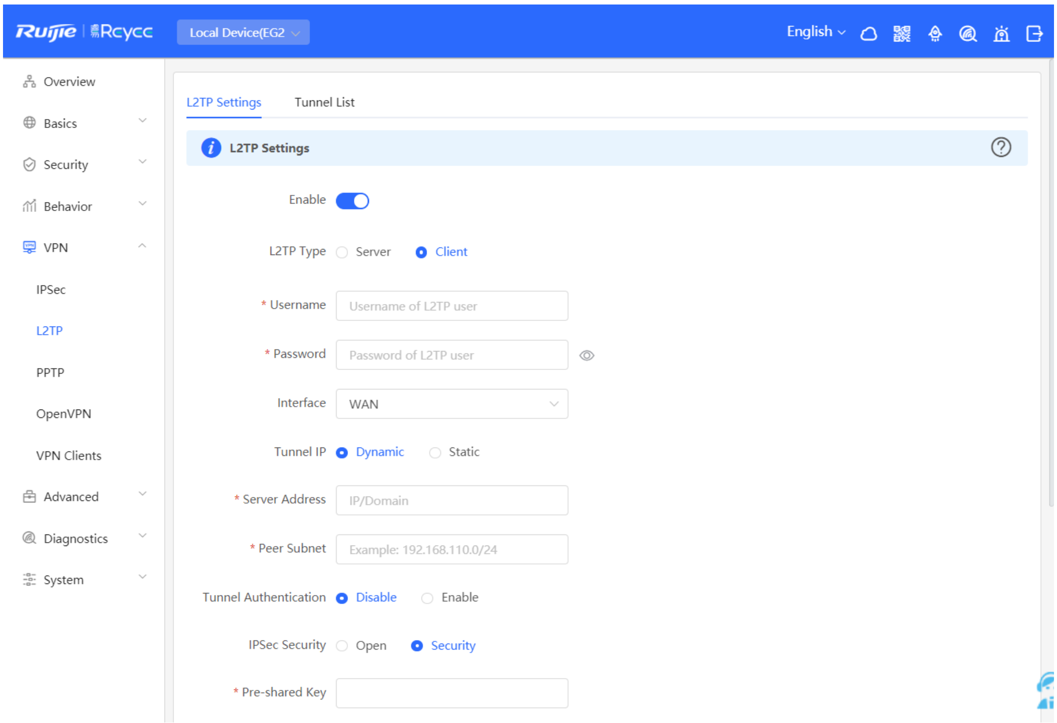
4. **Configuration Steps**

(1) Configure the HQ gateway.

Note

The LAN address of the HQ cannot conflict with that of the branch. Otherwise, resource access will fail.

a Log in to the web management system and choose **VPN** > **L2TP** > **L2TP Settings** to access the L2TP Settings page.



L2TP Settings

Enable ●

L2TP Type ○ Server ● Client

* Username Username of L2TP user

* Password Password of L2TP user

Interface WAN

Tunnel IP ● Dynamic ○ Static

* Server Address IP/Domain

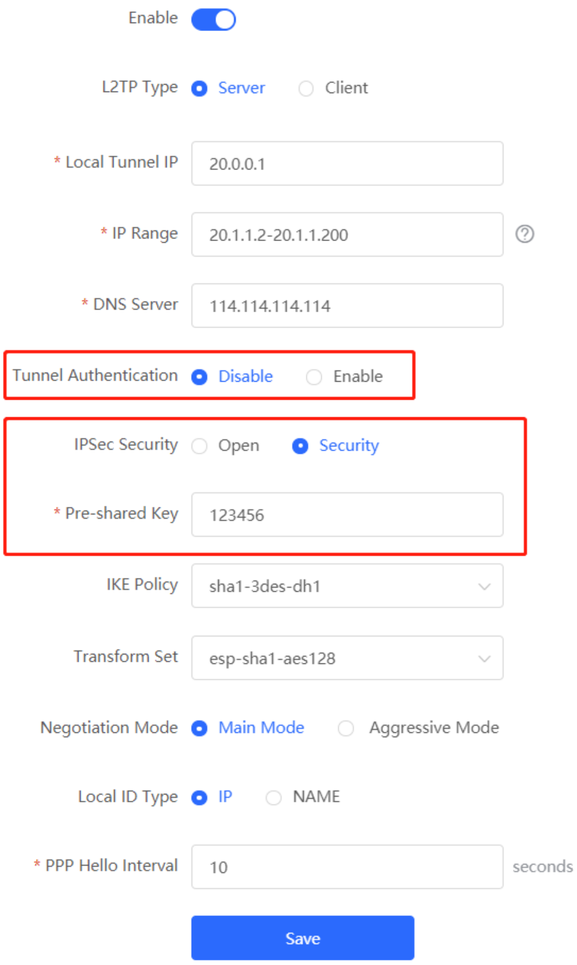
* Peer Subnet Example: 192.168.110.0/24

Tunnel Authentication ● Disable ○ Enable

IPSec Security ○ Open ● Security

* Pre-shared Key

b Turn on the L2TP function, set L2TP Type to Server, enter the local tunnel address, address pool IP address range, and DNS server address, specify whether to enable IPsec encryption and tunnel authentication, and click Save.



Enable

L2TP Type ● Server ○ Client

* Local Tunnel IP 20.0.0.1

* IP Range 20.1.1.2-20.1.1.200

* DNS Server 114.114.114.114

Tunnel Authentication ● Disable ○ Enable

IPSec Security ○ Open ● Security

* Pre-shared Key 123456

IKE Policy sha1-3des-dh1

Transform Set esp-sha1-aes128

Negotiation Mode ● Main Mode ○ Aggressive Mode

Local ID Type ● IP ○ NAME

* PPP Hello Interval 10 seconds

Table 7-11 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.
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.

Parameter	Description
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.
PPP Hello Interval	Keep the default settings unless otherwise specified.

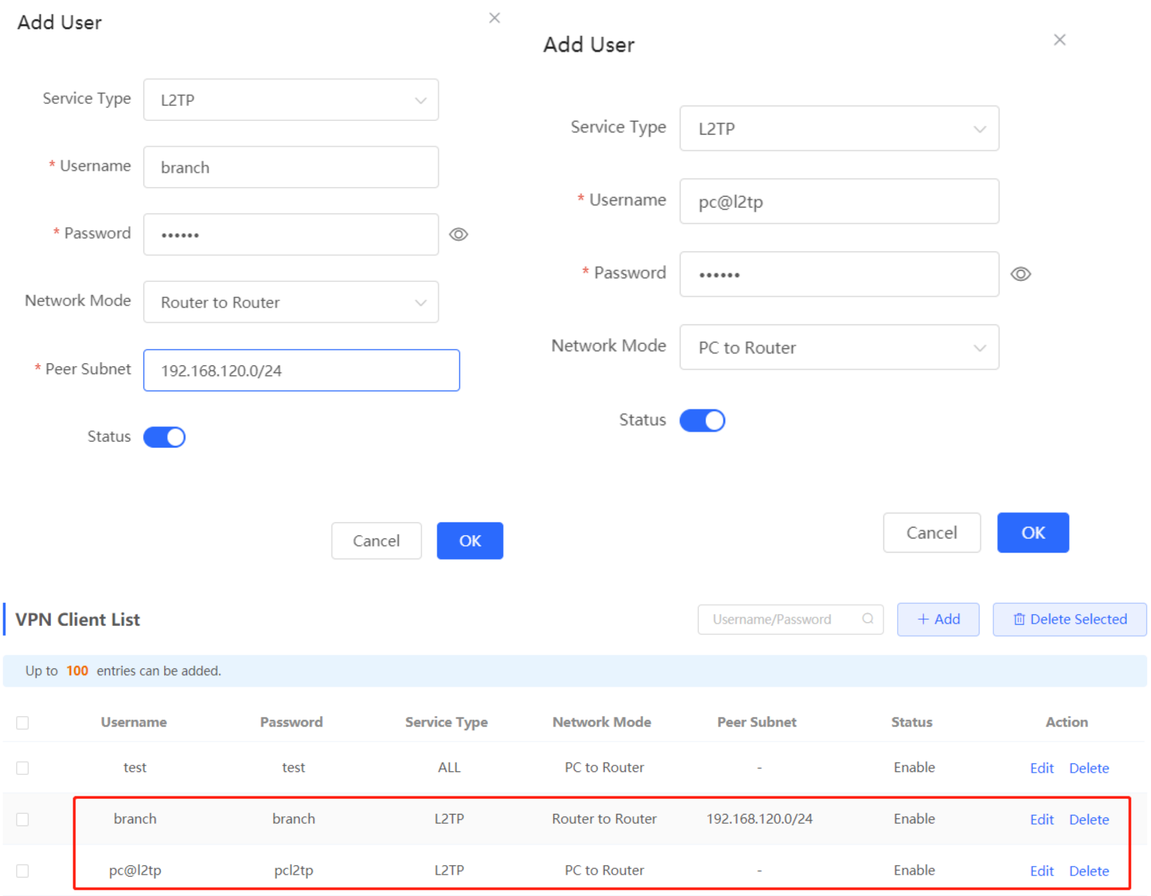
c Choose **VPN** > **VPN Clients** and add L2TP user accounts for the traveling employee and branch employee to access the HQ.

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, that is 192.168.120.0/24.

Caution

The LAN network segments of the server and client cannot overlap.



Add User

Service Type	L2TP
* Username	branch
* Password	••••••
Network Mode	Router to Router
* Peer Subnet	192.168.120.0/24
Status	●

Add User

Service Type	L2TP
* Username	pc@l2tp
* Password	••••••
Network Mode	PC to Router
Status	●

VPN Client List

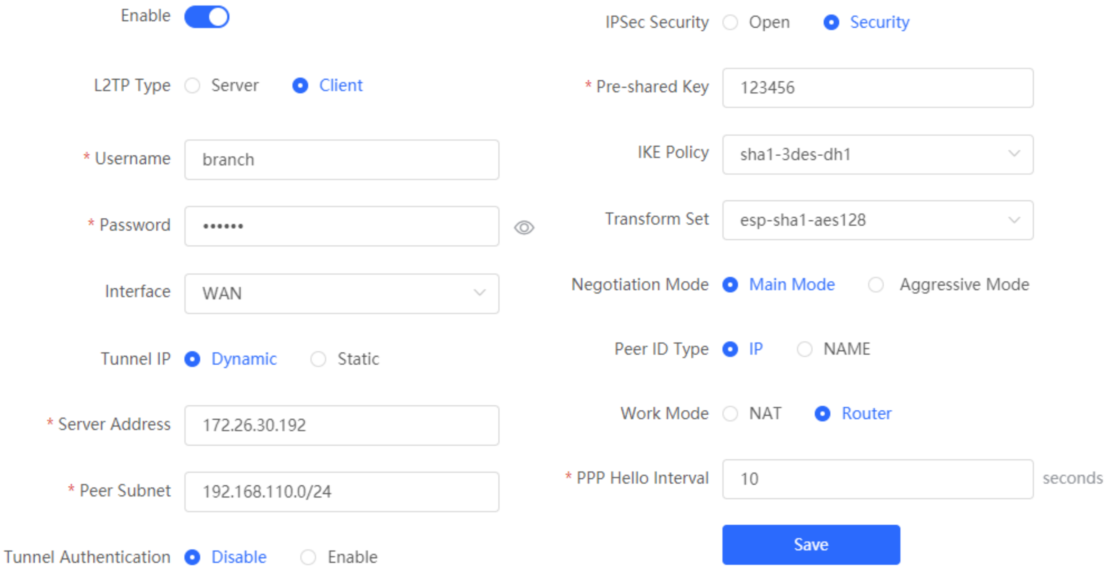
Up to 100 entries can be added.

□	Username	Password	Service Type	Network Mode	Peer Subnet	Status	Action
□	test	test	ALL	PC to Router	-	Enable	Edit Delete
□	branch	branch	L2TP	Router to Router	192.168.120.0/24	Enable	Edit Delete
□	pc@l2tp	pcl2tp	L2TP	PC to Router	-	Enable	Edit Delete

(2) Configure the branch gateway.

a Log in to the web management system and access the L2TP Settings page.

b 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 WAN

Tunnel IP ● Dynamic ○ Static

* Server Address 172.26.30.192

* Peer Subnet 192.168.110.0/24

Tunnel Authentication ● Disable ○ Enable

IPSec Security ○ Open ● Security

* Pre-shared Key 123456

IKE Policy sha1-3des-dh1

Transform Set esp-sha1-aes128

Negotiation Mode ● Main Mode ○ Aggressive Mode

Peer ID Type ● IP ○ NAME

Work Mode ○ NAT ● Router

* PPP Hello Interval 10 seconds

Table 7-12 L2TP client configuration

Parameter	Description
Username/Password	Enter the username and password configured on the server.
Interface	Select the WAN port 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 port address of the server, that is 172.26.30.192.
Peer Subnet	Enter the LAN network segment (LAN port IP address range) of the server, that is 192.168.110.0/24.
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.

Parameter	Description
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.
Work 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.

(3) Configure the PC of the traveling employee.

Note

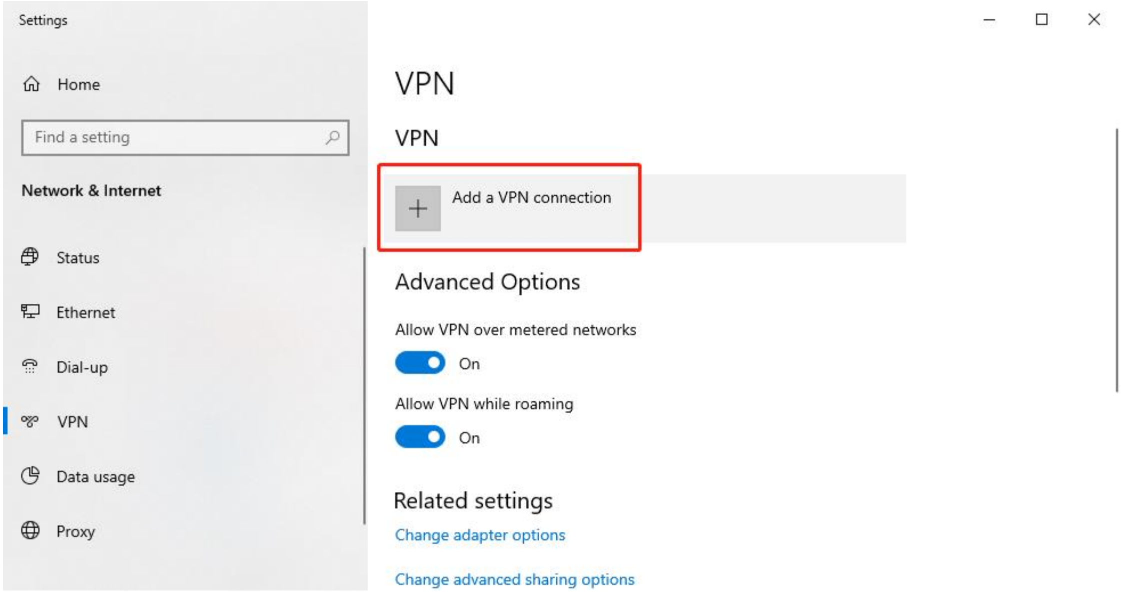
Configure the PC of a traveling employee as the L2TP client. The following uses the PC running Windows 10 operating system as an example.

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.

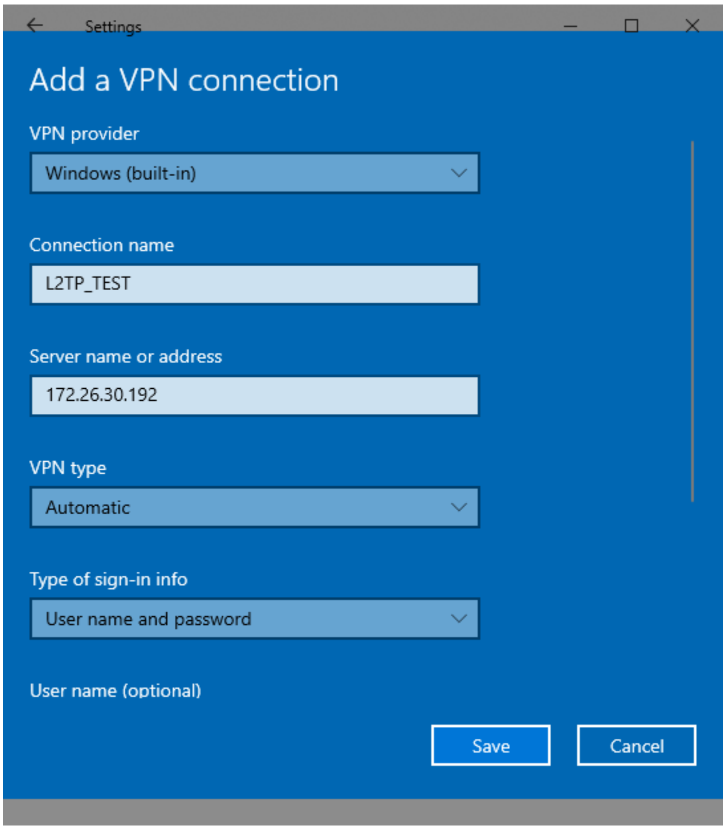
Neither the Win7/Win10 system nor the XP system supports L2TP tunnel authentication. Therefore, tunnel authentication must be disabled on the server.

Apple mobile phones support L2TP over IPsec but do not support IPsec encryption for L2TP dial-up.

a Choose **Settings** > **Network & Internet** > **VPN** to access the VPN page.



b 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**.



Add a VPN connection

VPN provider
Windows (built-in)

Connection name
L2TP_TEST

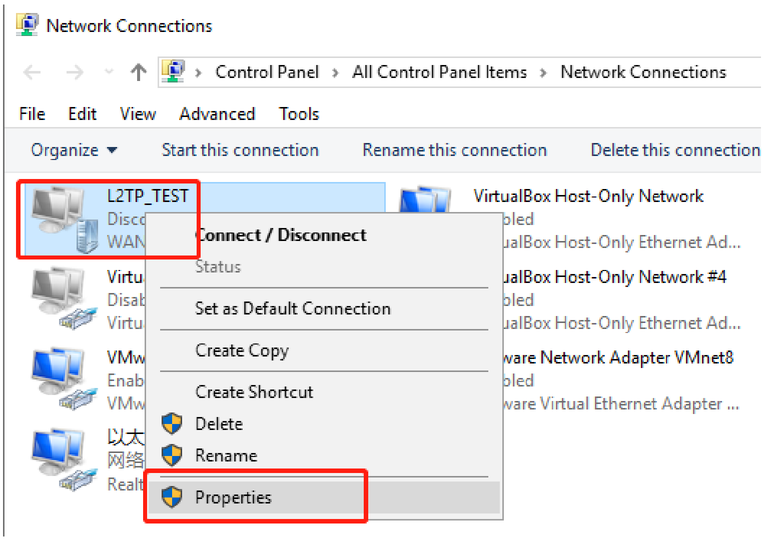
Server name or address
172.26.30.192

VPN type
Automatic

Type of sign-in info
User name and password

User name (optional)

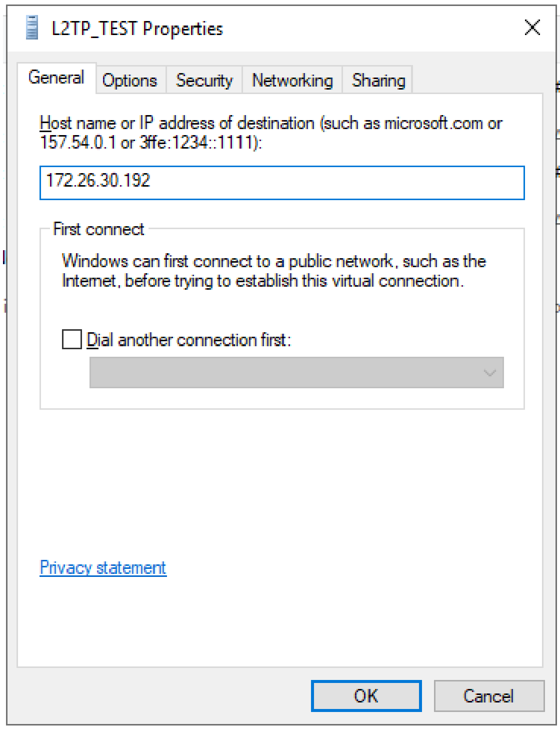
c Right-click the created VPN connection named **L2TP_TEST** and select Properties to view the properties of the network connection.


Network Connections
Control Panel › All Control Panel Items › Network Connections
File Edit View Advanced Tools
Organize ▾
Start this connection
Rename this connection
Delete this connection
L2TP_TEST
Disco
WAN
VirtualBox Host-Only Network
bled
ualBox Host-Only Ethernet Ad...
Virtu
Disab
Virtu
ualBox Host-Only Network #4
bled
ualBox Host-Only Ethernet Ad...
VMw
Enab
VMw
ware Network Adapter VMnet8
bled
ware Virtual Ethernet Adapter ...
以太
网络
Realt
Connect / Disconnect
Status
Set as Default Connection
Create Copy
Create Shortcut
Delete
Rename
Properties

d 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 e .

If IPsec encryption is enabled on the L2TP server, perform Step e .



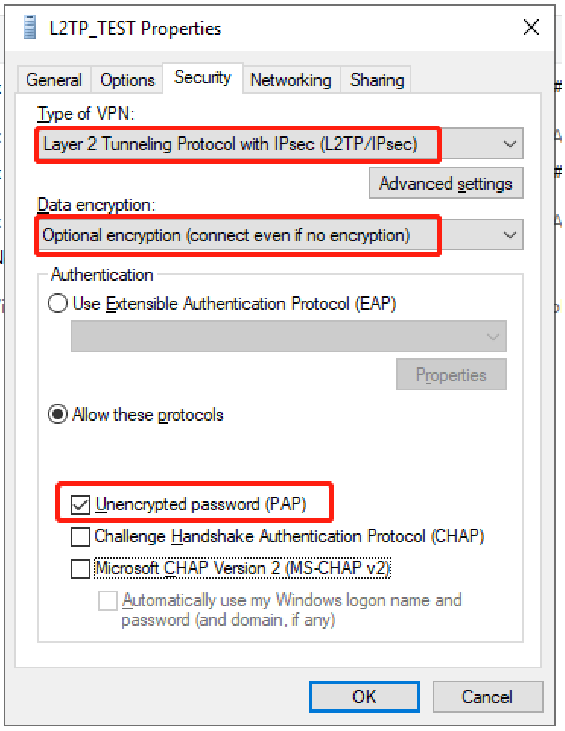
Host name or IP address of destination (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):

172.26.30.192

First connect

Windows can first connect to a public network, such as the Internet, before trying to establish this virtual connection.

□ Dial another connection first:



Type of VPN:

Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)

Data encryption:

Optional encryption (connect even if no encryption)

Authentication

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

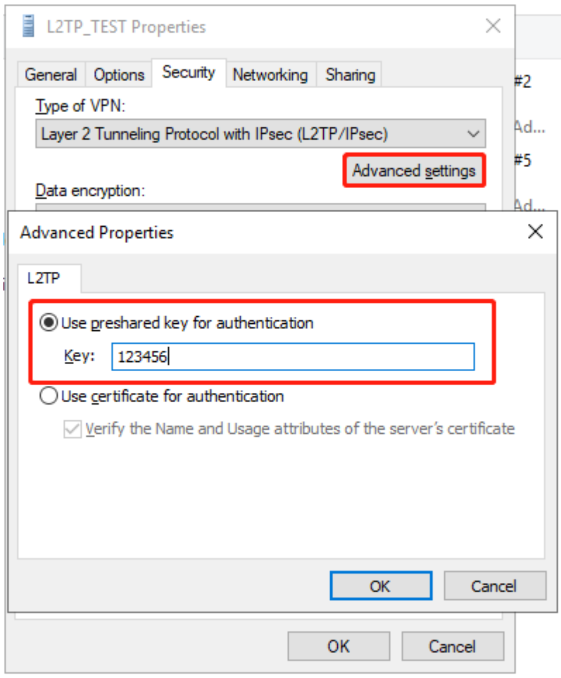
☑ Unencrypted password (PAP)

□ Challenge Handshake Authentication Protocol (CHAP)

□ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

e 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**.

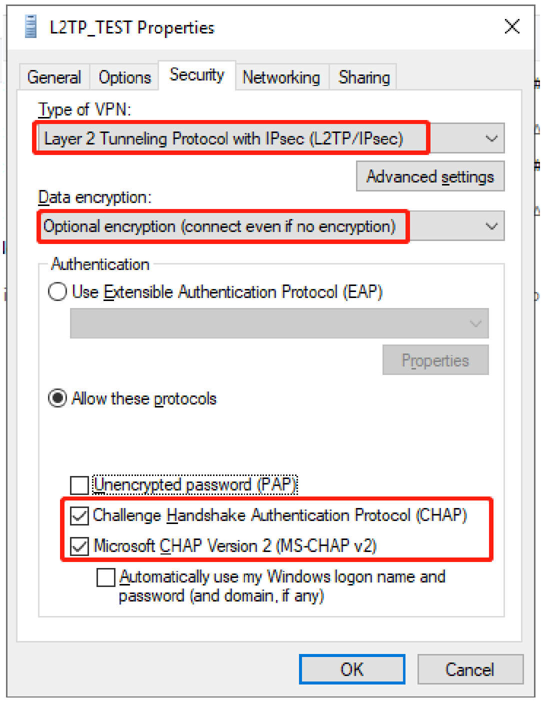


● Use preshared key for authentication

Key: 123456

○ Use certificate for authentication

☑ Verify the Name and Usage attributes of the server's certificate



Type of VPN:

Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)

Data encryption:

Optional encryption (connect even if no encryption)

Authentication

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

□ Unencrypted password (PAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

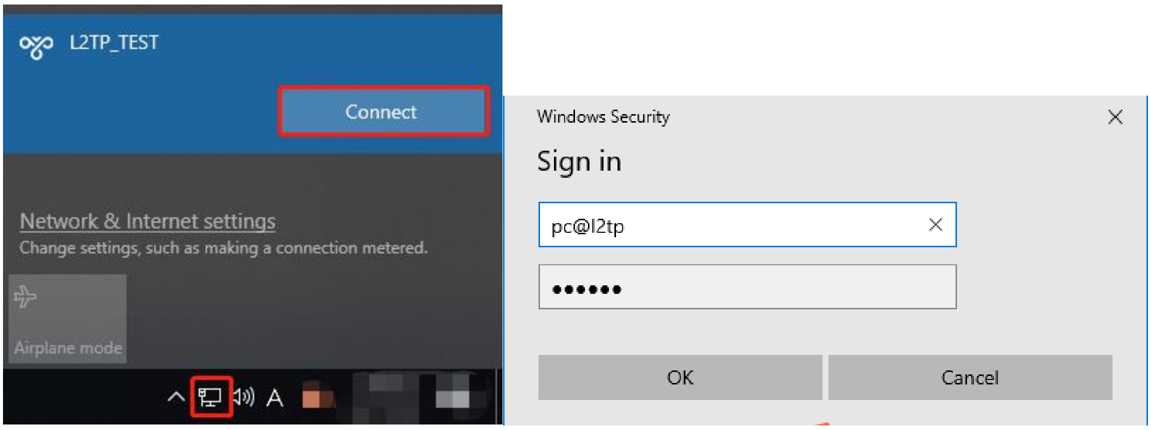
☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

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.

f 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.


L2TP_TEST
Connect
Network & Internet settings
Change settings, such as making a connection metered.
Airplane mode
Windows Security
Sign in
OK
Cancel

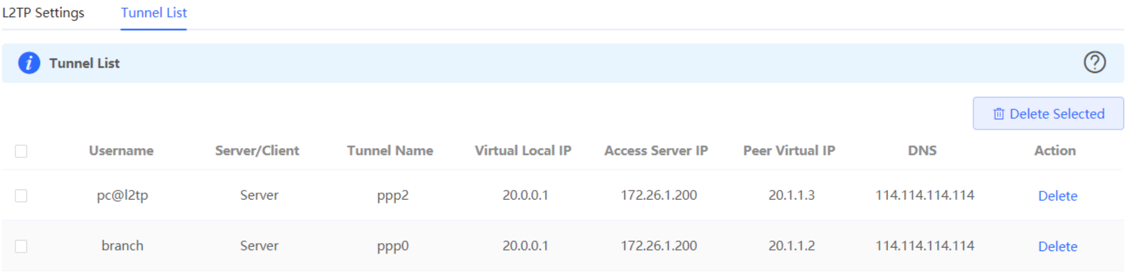
pc@l2tp

••••••

5. Verifying Configuration

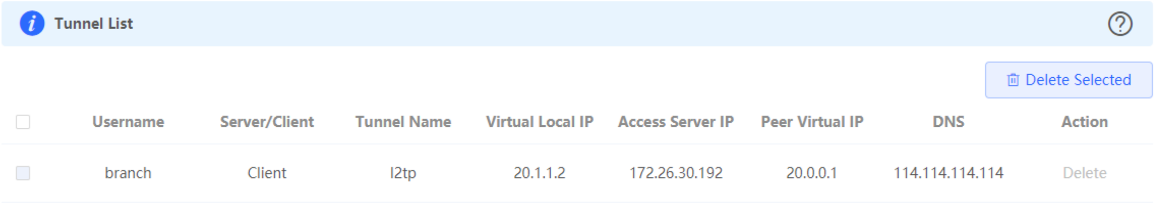
(1) After the server and client are configured, wait for about 1 minute. If you can view the L2TP tunnel connection information on the HQ server and branch client, the connection is successful.

HQ:



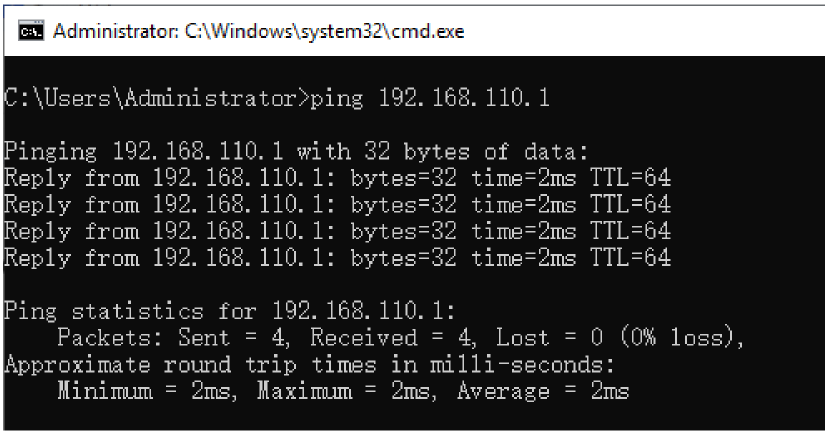
□	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
□	pc@l2tp	Server	ppp2	20.0.0.1	172.26.1.200	20.1.1.3	114.114.114.114	Delete
□	branch	Server	ppp0	20.0.0.1	172.26.1.200	20.1.1.2	114.114.114.114	Delete

Branch:



□	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
□	branch	Client	l2tp	20.1.1.2	172.26.30.192	20.0.0.1	114.114.114.114	Delete

(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.



Administrator: C:\Windows\system32\cmd.exe

```
C:\Users\Administrator>ping 192.168.110.1

Pinging 192.168.110.1 with 32 bytes of data:
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.110.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

7.2.6 Solution to L2TP VPN Connection Failure

(1) Run the ping command to test the connectivity between the client and server. For details, see Section **错误!未找到引用源。**. 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 **Diagnostics** > **Network Tools**. Then, you can start the ping operation. For details, see Section **错误!未找到引用源。**.

(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 port IP address of your HQ EG is a public network IP address. If not, you need to configure DMZ on your egress gateway.

7.3 Configuring PPTP VPN

7.3.1 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.

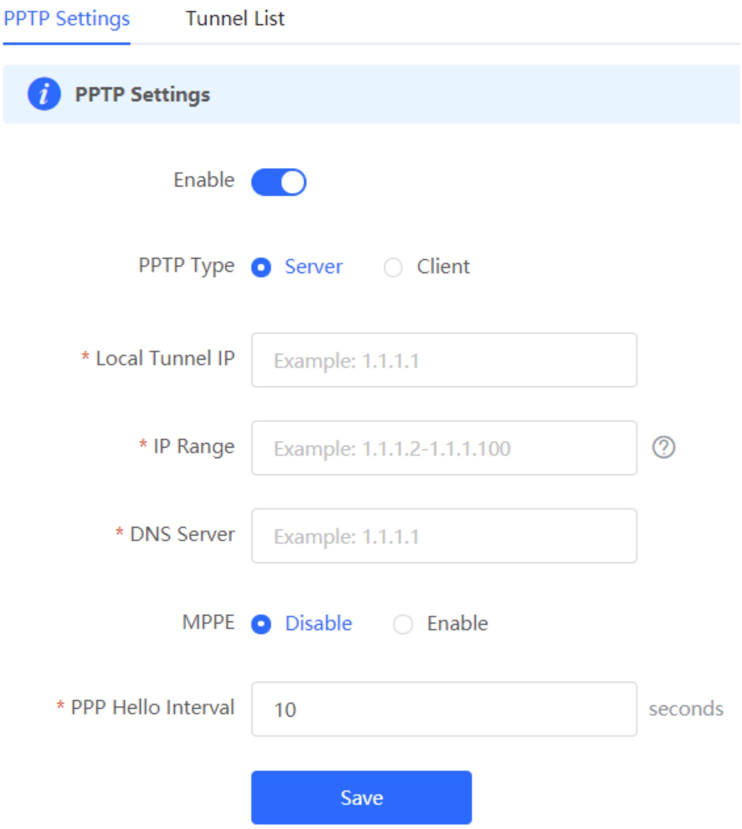
Currently, the device can be deployed as the PPTP server or client. It supports MPPE for encryption MSCHAP-v2 for identity authentication, and does not support EAP authentication.

7.3.2 Configuring the PPTP Service

1. Configuring the PPTP Server

Choose **Local Device** > **VPN** > **PPTP** > **PPTP Settings**.

Turn on the PPTP function, set **PPTP Type** to **Server**, configure PPTP server parameters, and click **Save**.



PPTP Settings

Enable ●

PPTP Type ● Server ○ Client

* Local Tunnel IP Example: 1.1.1.1

* IP Range Example: 1.1.1.2-1.1.1.100

* DNS Server Example: 1.1.1.1

MPPE ● Disable ○ Enable

* PPP Hello Interval 10 seconds

Table 7-13 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.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after PPTP VPN is deployed.

Caution

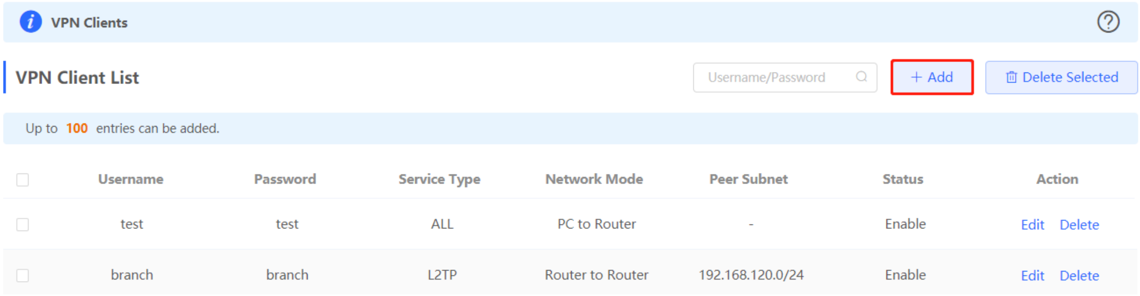
The local tunnel address and IP address range of the address pool cannot overlap the network segment of the LAN port on the device.

2. Configuring PPTP User

Choose **Local Device** > **VPN** > **VPN Clients**.

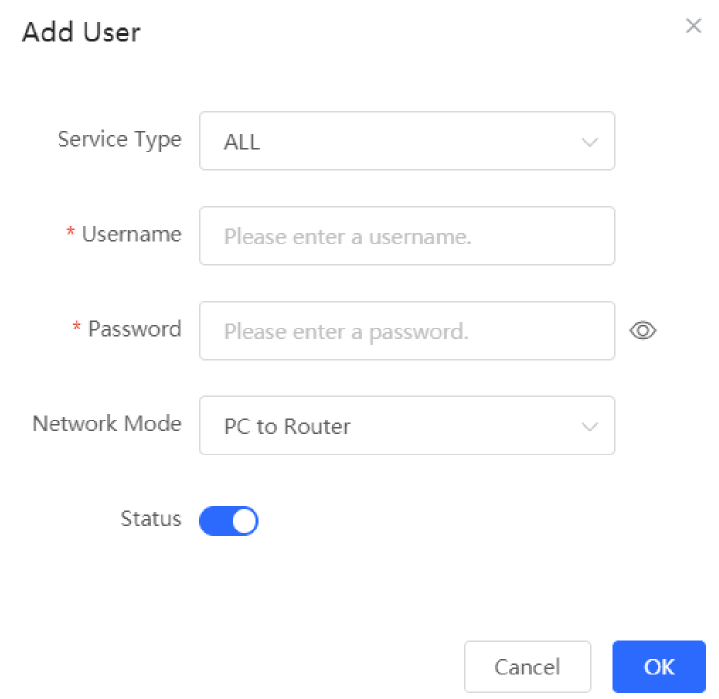
Only user accounts added to the VPN client list are allowed to dial up to connect to the PPTP server. Therefore, you need to manually configure user accounts for clients to access the PPTP server.

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**.



Up to 100 entries can be added.

□	Username	Password	Service Type	Network Mode	Peer Subnet	Status	Action
□	test	test	ALL	PC to Router	-	Enable	Edit Delete
□	branch	branch	L2TP	Router to Router	192.168.120.0/24	Enable	Edit Delete



Add User

Service Type: ALL

* Username: Please enter a username.

* Password: Please enter a password.

Network Mode: PC to Router

Status

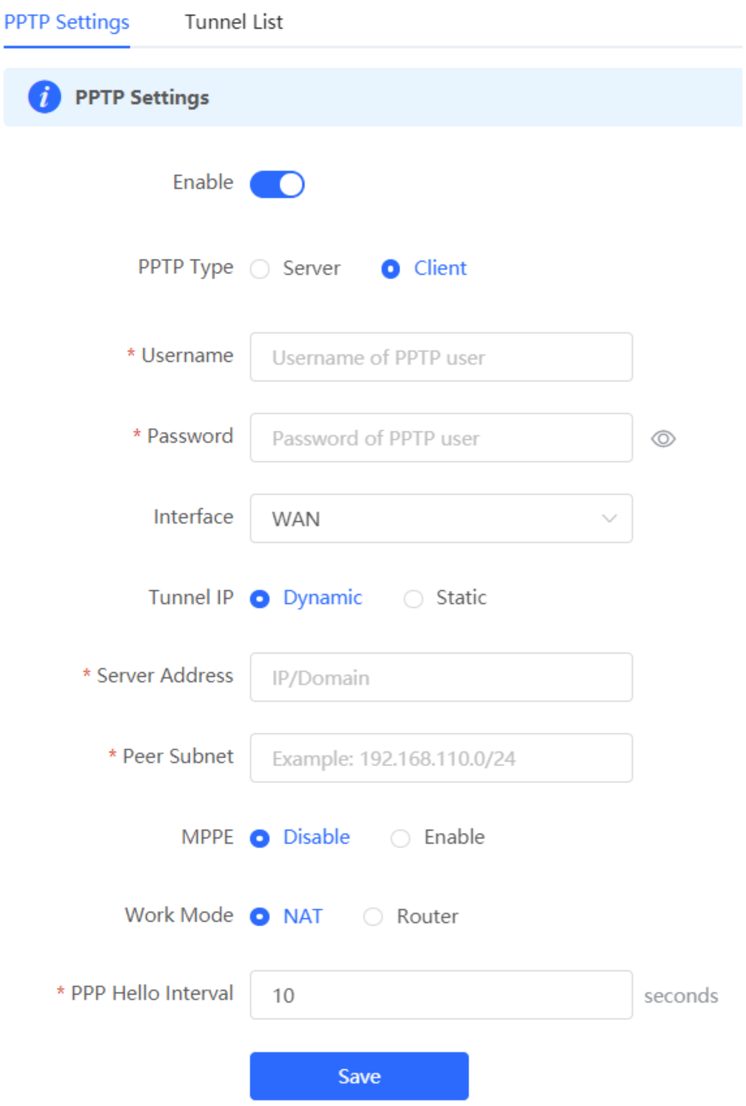
Table 7-14 PPTP user configuration

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.
Peer 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.
Status	Specify whether to enable the user account.

7.3.3 Configuring the PPTP Client

Choose **Local Device** > **VPN** > **PPTP** > **PPTP Settings**.

Turn on the PPTP function, set **PPTP Type** to **Client**, configure PPTP client parameters, and click **Save**.



PPTP Settings | Tunnel List

PPTP Settings

Enable: on

PPTP Type: ○ Server ● Client

* Username: Username of PPTP user

* Password: Password of PPTP user

Interface: WAN

Tunnel IP: ● Dynamic ○ Static

* Server Address: IP/Domain

* Peer Subnet: Example: 192.168.110.0/24

MPPE: ● Disable ○ Enable

Work Mode: ● NAT ○ Router

* PPP Hello Interval: 10 seconds

Save

Table 7-15 PPTP client configuration

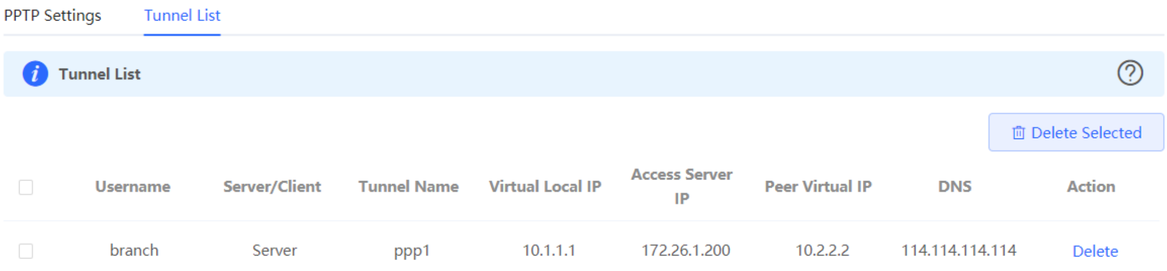
Parameter	Description
Username/Password	Specify the username and password for identity authentication for communication over the PPTP tunnel. The values must be the same as those configured on the PPTP server.
Interface	Specify the WAN port used by the client.
Tunnel IP	Specify the virtual IP address 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 port IP address or domain name of the server. This address must be a public network IP address.

Parameter	Description
Peer 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.
MPPE	Specify whether to use MPPE to encrypt the PPTP tunnel. The value must be the same as that on the server.
Work 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.

7.3.4 Viewing the PPTP Tunnel Information

Choose **Local Device** > **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.



□	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
□	branch	Server	ppp1	10.1.1.1	172.26.1.200	10.2.2.2	114.114.114.114	Delete

Table 7-16 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.

Parameter	Description
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.

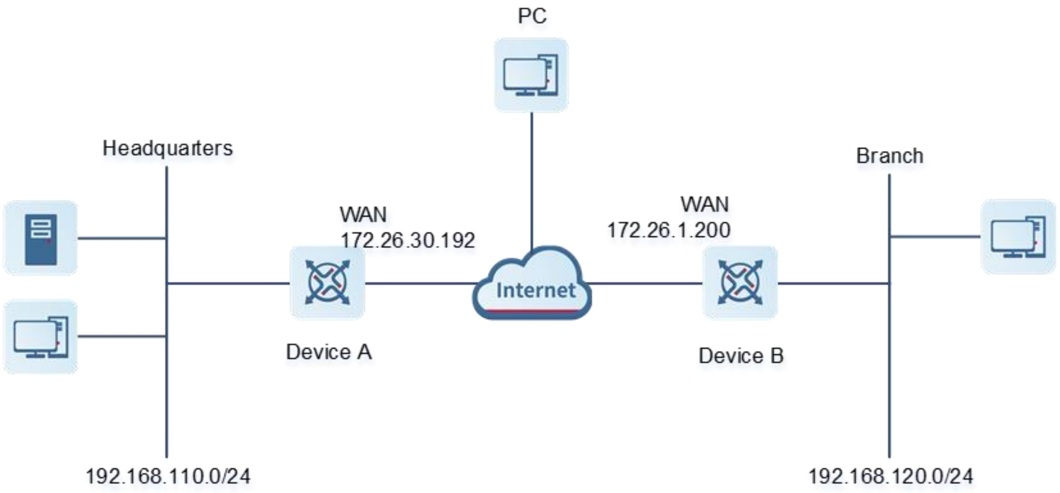
7.3.5 Typical Configuration Example

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.

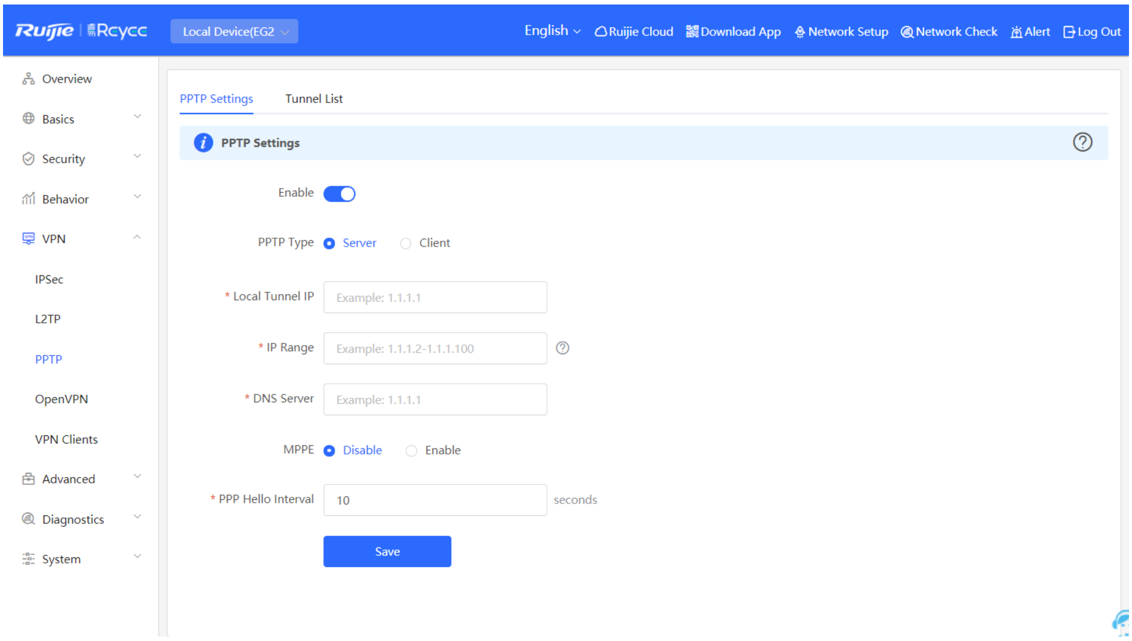
4. Configuration Steps

(1) Configure the HQ gateway.

Note

The LAN address of the HQ cannot conflict with that of the branch. Otherwise, resource access will fail.

a Log in to the web management system and choose VPN > PPTP > PPTP Settings to access the PPTP Settings page.



PPTP Settings

Enable

PPTP Type ● Server ○ Client

* Local Tunnel IP: Example: 1.1.1.1

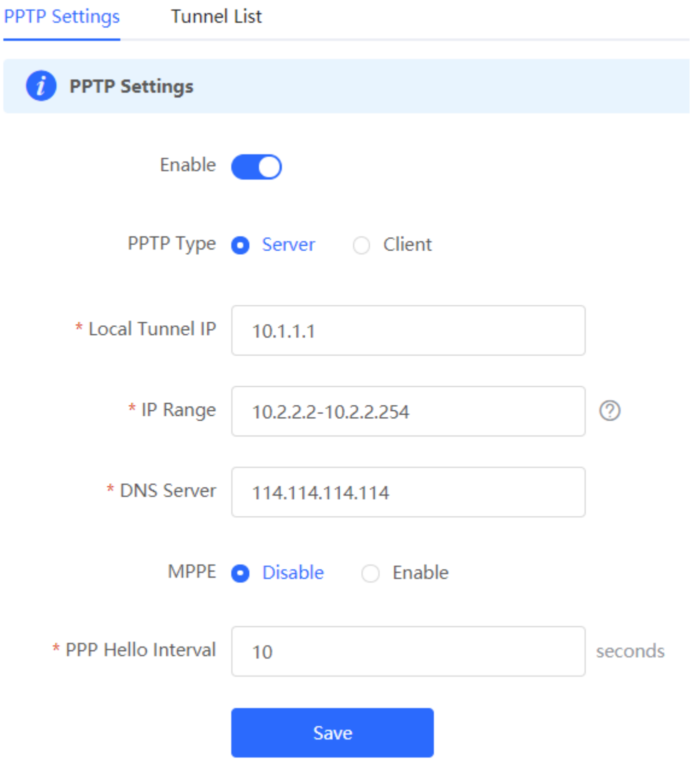
* IP Range: Example: 1.1.1.2-1.1.1.100

* DNS Server: Example: 1.1.1.1

MPPE ● Disable ○ Enable

* PPP Hello Interval: 10 seconds

b Turn on the PPTP function, set PPTP Type to Server, enter the local tunnel address, address pool IP address range, and DNS server address, specify whether to enable MPPE encryption, and click Save.



PPTP Settings

Enable

PPTP Type ● Server ○ Client

* Local Tunnel IP: 10.1.1.1

* IP Range: 10.2.2.2-10.2.2.254

* DNS Server: 114.114.114.114

MPPE ● Disable ○ Enable

* PPP Hello Interval: 10 seconds

Table 7-17 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.
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.
PPP Hello Interval	Keep the default settings unless otherwise specified.

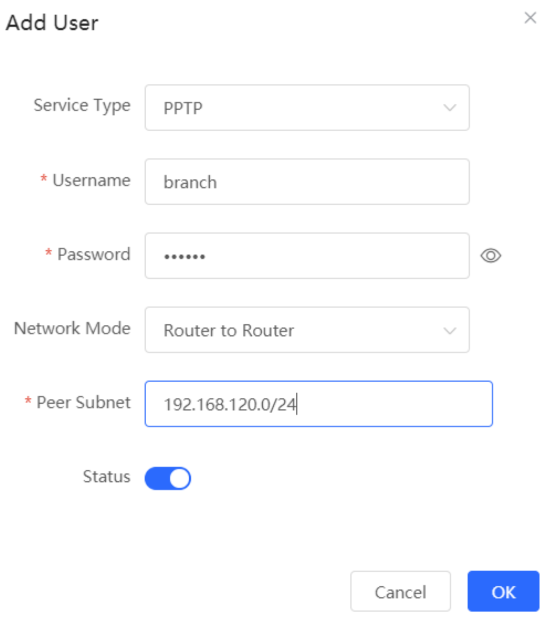
c Choose **VPN** > **VPN Clients** and add PPTP user accounts for the traveling employee and branch employee to access the HQ.

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 **Peer Subnet** to the LAN network segment of the branch gateway.

⚠ **Caution**

The LAN network segments of the server and client cannot overlap.



Add User

Service Type: PPTP

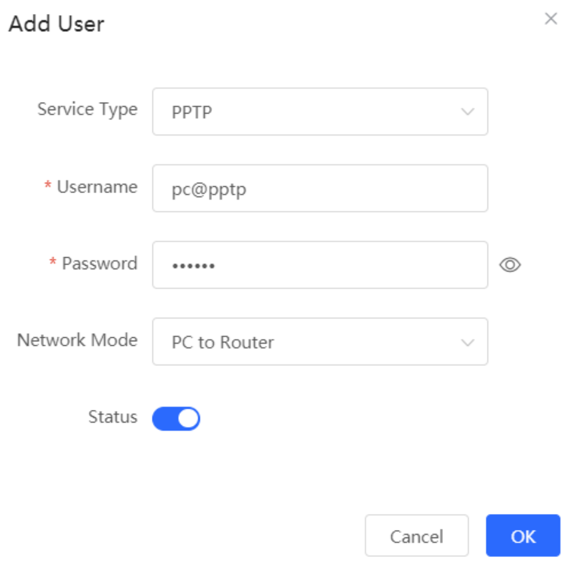
* Username: branch

* Password: ••••••

Network Mode: Router to Router

* Peer Subnet: 192.168.120.0/24

Status: ●



Add User

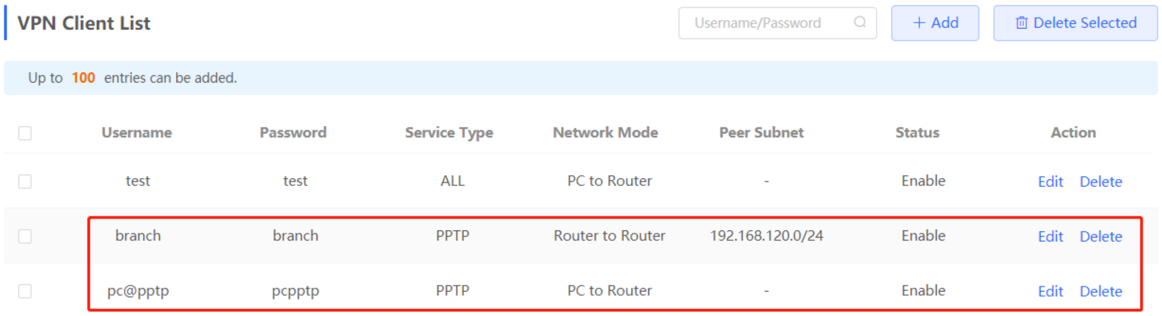
Service Type: PPTP

* Username: pc@pptp

* Password: ••••••

Network Mode: PC to Router

Status: ●



VPN Client List

Username/Password | + Add | Delete Selected

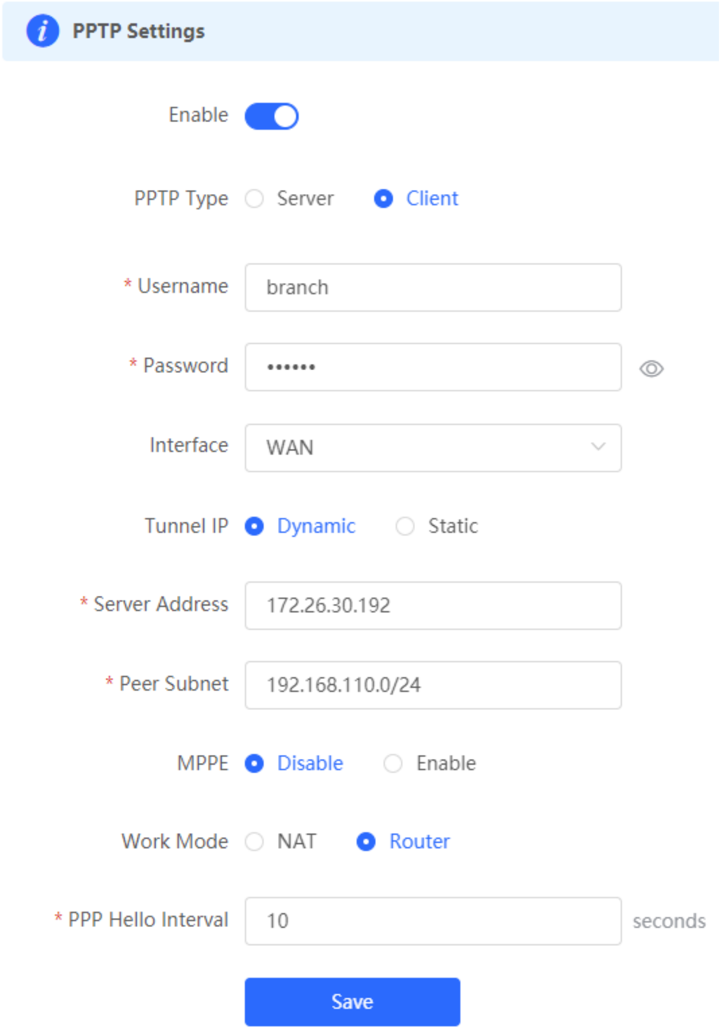
Up to 100 entries can be added.

	Username	Password	Service Type	Network Mode	Peer Subnet	Status	Action
□	test	test	ALL	PC to Router	-	Enable	Edit Delete
□	branch	branch	PPTP	Router to Router	192.168.120.0/24	Enable	Edit Delete
□	pc@pptp	pcpptp	PPTP	PC to Router	-	Enable	Edit Delete

(2) Configure the branch gateway.

a Log in to the web management system and access the PPTP Settings page.

b 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.



PPTP Settings

Enable: On

PPTP Type: ○ Server ● Client

* Username: branch

* Password: ••••••

Interface: WAN

Tunnel IP: ● Dynamic ○ Static

* Server Address: 172.26.30.192

* Peer Subnet: 192.168.110.0/24

MPPE: ● Disable ○ Enable

Work Mode: ○ NAT ● Router

* PPP Hello Interval: 10 seconds

Save

Table 7-18 PPTP client configuration

Parameter	Description
Username/Password	Enter the username and password configured on the server.

Parameter	Description
Interface	Select the WAN port 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 port address of the server.
Peer Subnet	Enter the LAN network segment (LAN port IP address range) of the server.
MPPE	The value must be the same as that on the server.
Work 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.

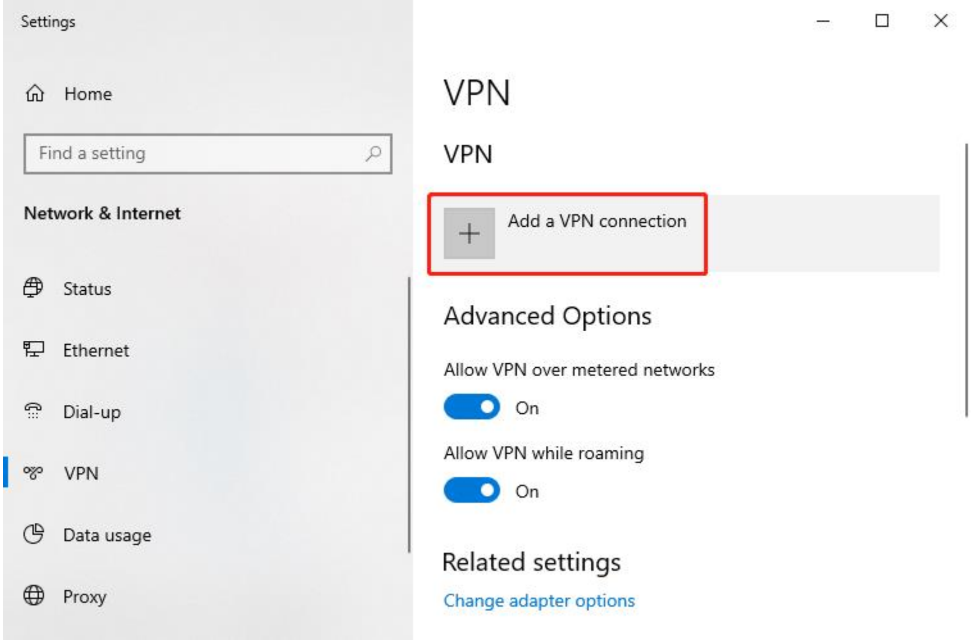
(3) Configure the PC of the traveling employee.

Note

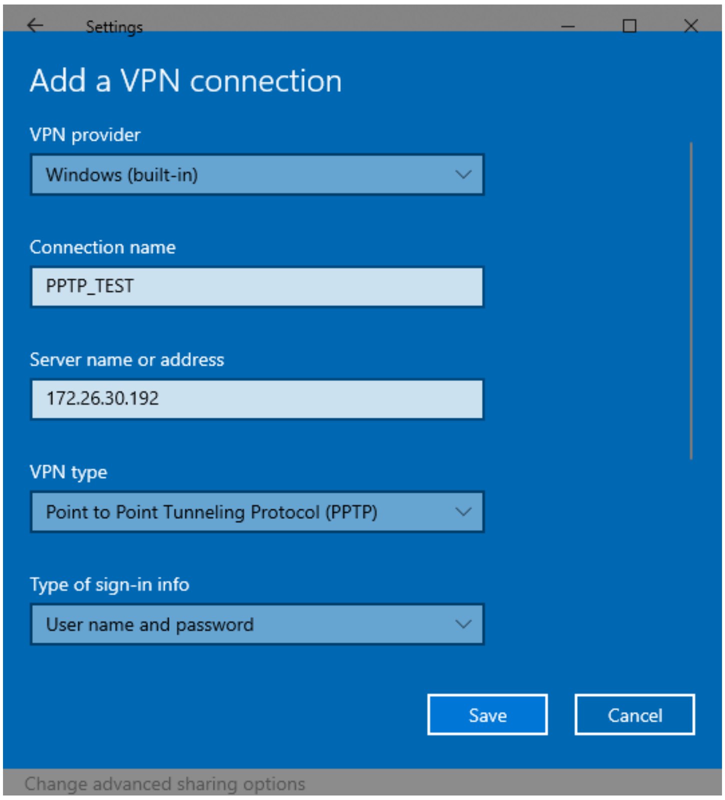
Configure the PC of a traveling employee as the PPTP client. The following uses the PC running Windows 10 operating system as an example.

Enable ports 1723 (PPTP) and 47 (GRE) on the PC firewall.

a Choose Settings > Network & Internet > VPN to access the VPN page.



b 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**.



Settings

Add a VPN connection

VPN provider: Windows (built-in)

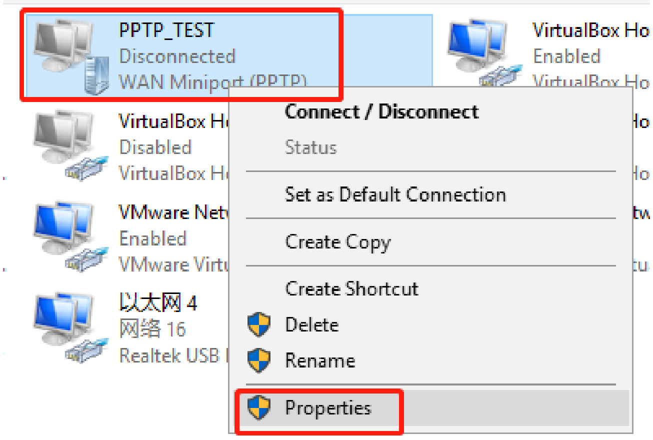
Connection name: PPTP_TEST

Server name or address: 172.26.30.192

VPN type: Point to Point Tunneling Protocol (PPTP)

Type of sign-in info: User name and password

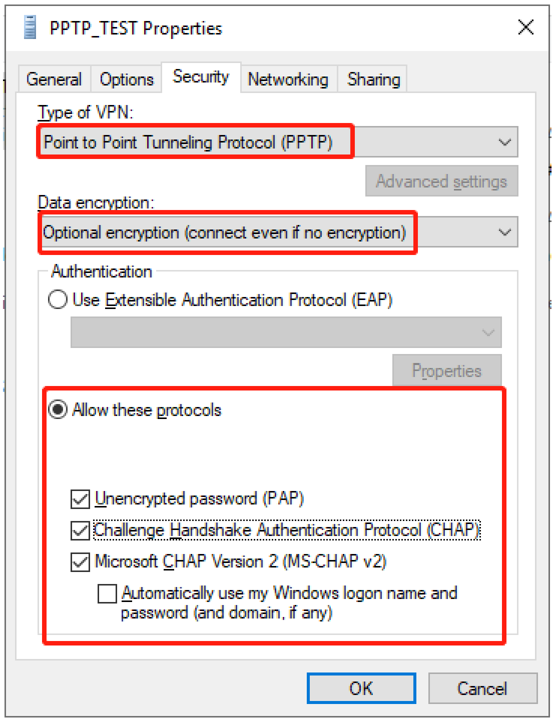
c Right-click the created VPN connection named **PPTP_TEST** and select Properties to view the properties of the network connection.



d 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.



Type of VPN: Point to Point Tunneling Protocol (PPTP)

Data encryption: Optional encryption (connect even if no encryption)

Authentication

○ Use Extensible Authentication Protocol (EAP)

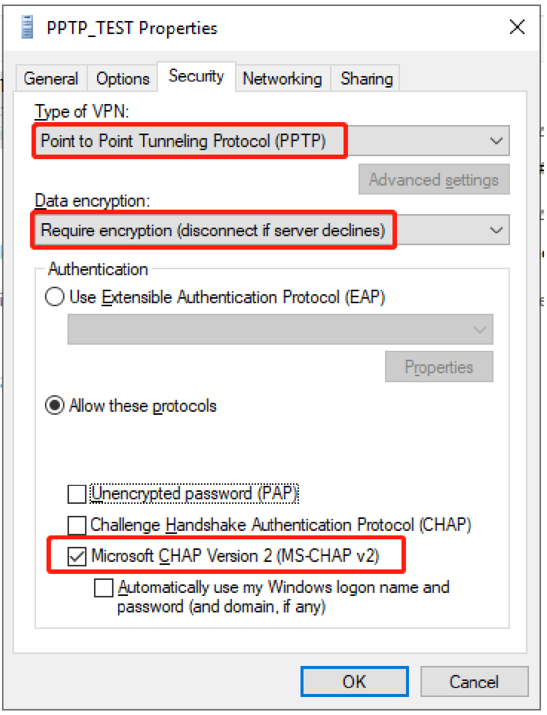
● Allow these protocols

☑ Unencrypted password (PAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)



Type of VPN: Point to Point Tunneling Protocol (PPTP)

Data encryption: Require encryption (disconnect if server declines)

Authentication

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

□ Unencrypted password (PAP)

□ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

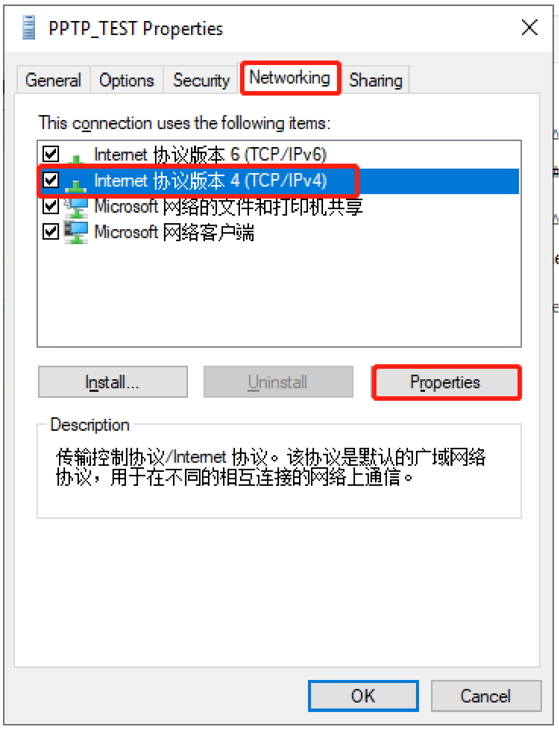
Note

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.

e When the PC functions as a dial-up client, configure the PC by using either of the following methods:

o Add a route to the VPN peer network segment on the PC as the administrator.

o 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.



PPTP_TEST Properties

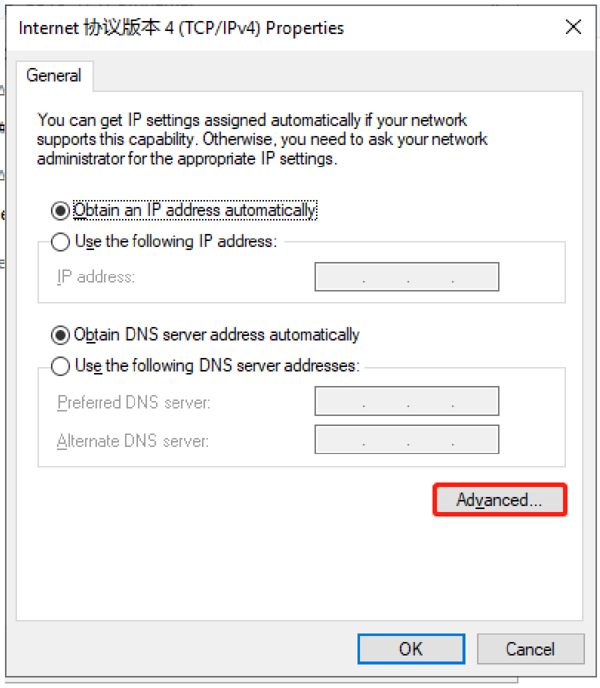
General | Options | Security | **Networking** | Sharing

This connection uses the following items:

- ☑ Internet 协议版本 6 (TCP/IPv6)
- ☑ Internet 协议版本 4 (TCP/IPv4)
- ☑ Microsoft 网络的文件和打印机共享
- ☑ Microsoft 网络客户端

Description

传输控制协议/Internet 协议。该协议是默认的广域网络协议，用于在不同的相互连接的网络上通信。

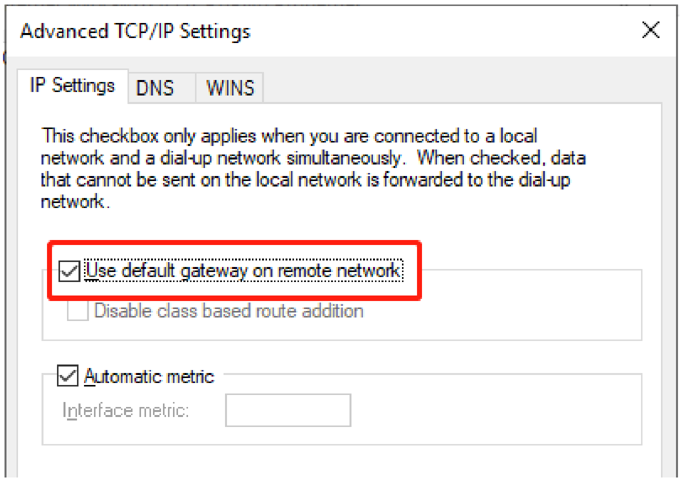


Internet 协议版本 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

- ● Obtain an IP address automatically
- ○ Use the following IP address:
  - IP address: . . .
- ● Obtain DNS server address automatically
- ○ Use the following DNS server addresses:
  - Preferred DNS server: . . .
  - Alternate DNS server: . . .



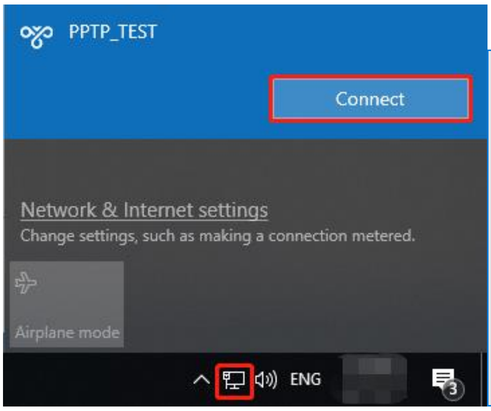
Advanced TCP/IP Settings

IP Settings | DNS | WINS

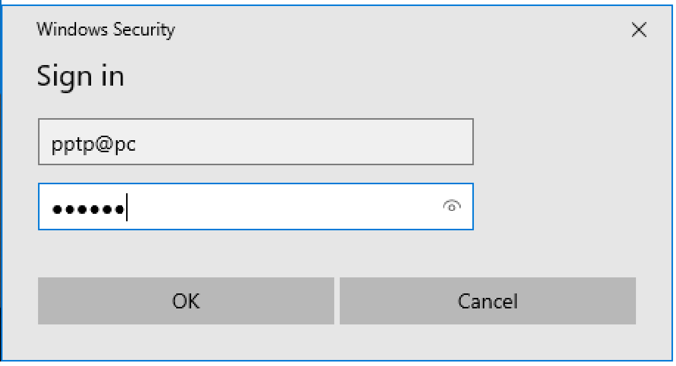
This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.

- ☑ Use default gateway on remote network
- □ Disable class based route addition
- ☑ Automatic metric
- Interface metric:

f 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.



PPTP_TEST
Connect
Network & Internet settings
Change settings, such as making a connection metered.
Airplane mode
ENG



Windows Security

Sign in

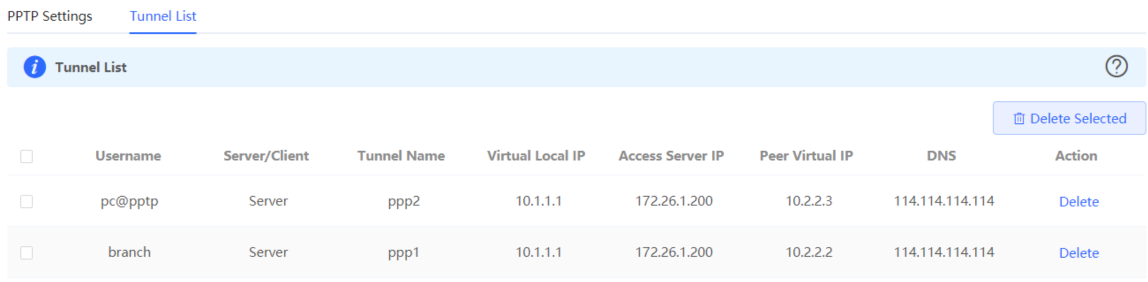
pptp@pc

••••••

5. Verifying Configuration

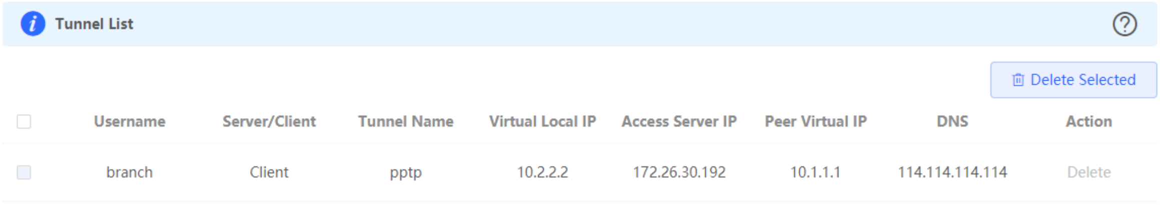
(1) After the server and client are configured, wait for about 1 minute. If you can view the PPTP tunnel connection information on the HQ server and branch client, the connection is successful.

HQ:



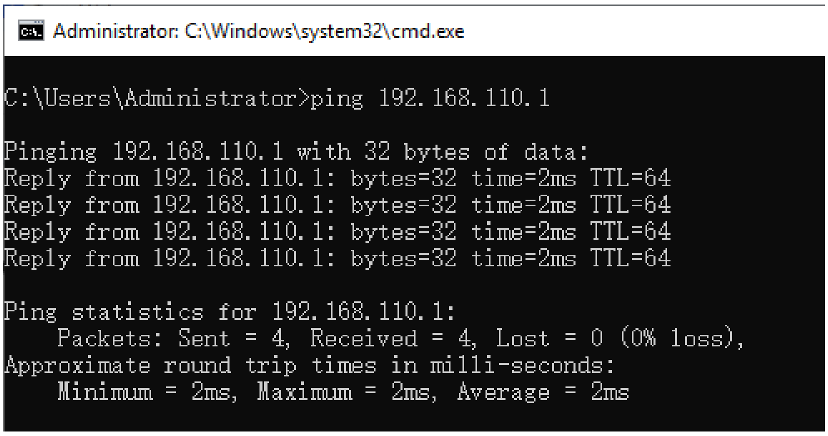
□	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
□	pc@pptp	Server	ppp2	10.1.1.1	172.26.1.200	10.2.2.3	114.114.114.114	Delete
□	branch	Server	ppp1	10.1.1.1	172.26.1.200	10.2.2.2	114.114.114.114	Delete

Branch:



□	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
□	branch	Client	pptp	10.2.2.2	172.26.30.192	10.1.1.1	114.114.114.114	Delete

(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.



```
C:\Users\Administrator>ping 192.168.110.1

Pinging 192.168.110.1 with 32 bytes of data:
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.110.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

7.4 OpenVPN

7.4.1 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.

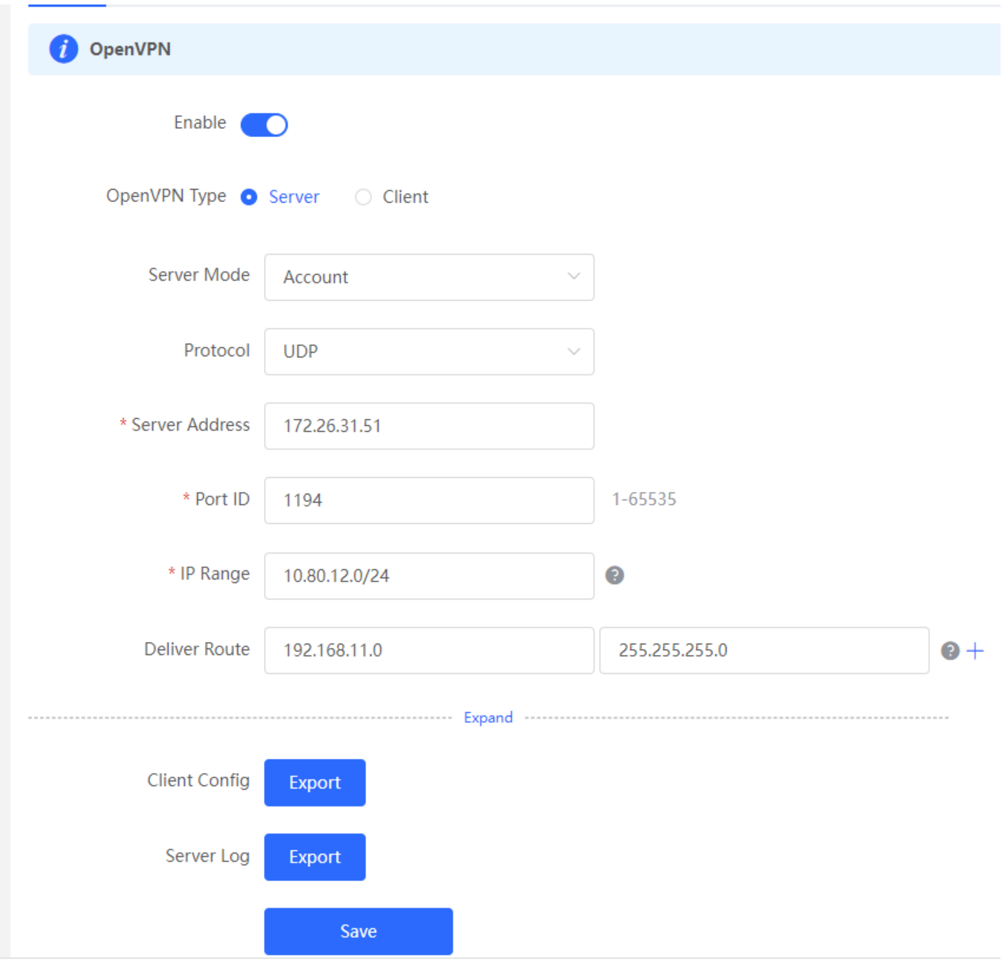
The OpenVPN client supports certificates **ca.crt**, **ca.key**, **client.crt**, and **client.key** and the OpenVPN server supports certificates **ca.crt**, **ca.key**, **server.crt**, and **server.key**.

7.4.2 Configuring the OpenVPN Server

Choose **Local Device** > **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.



OpenVPN

Enable: On

OpenVPN Type: ● Server ○ Client

Server Mode: Account

Protocol: UDP

* Server Address: 172.26.31.51

* Port ID: 1194 (1-65535)

* IP Range: 10.80.12.0/24

Deliver Route: 192.168.11.0 255.255.255.0

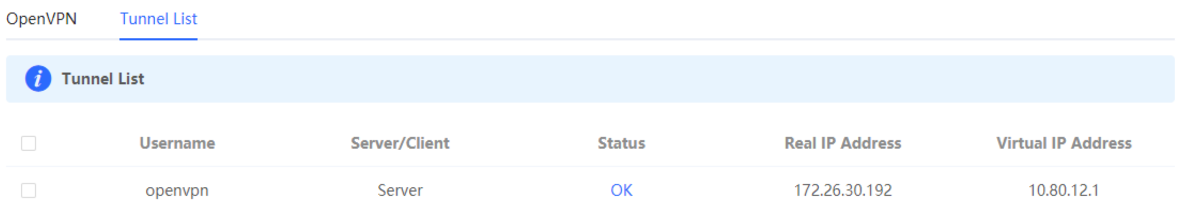
Table 7-19 OpenVPN server basic settings

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.
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.

Parameter	Description
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.

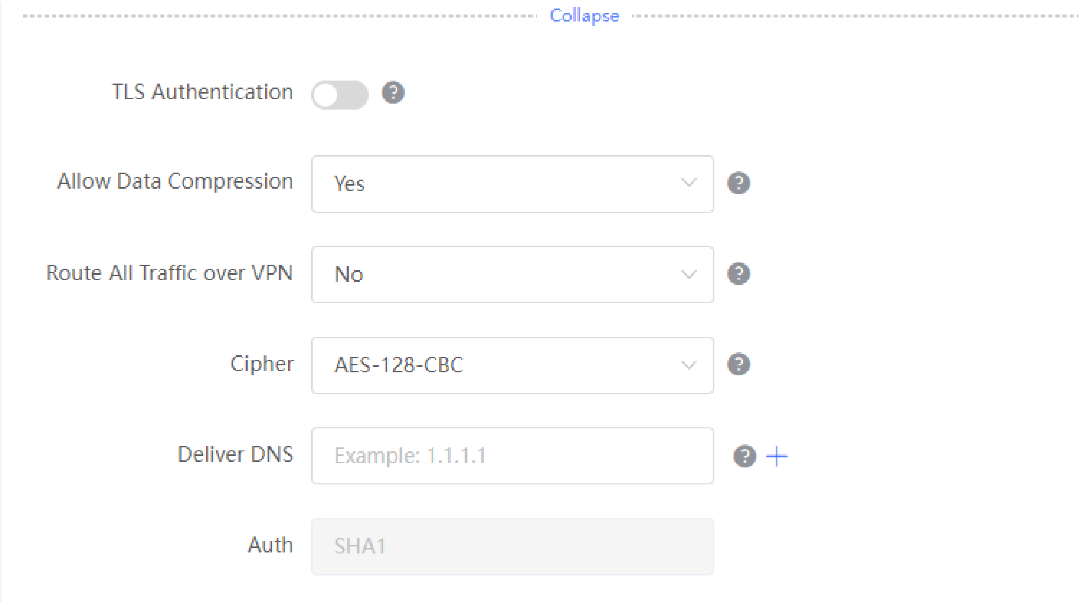


Tunnel List

□	Username	Server/Client	Status	Real IP Address	Virtual IP Address
□	openvpn	Server	OK	172.26.30.192	10.80.12.1

2. Advanced Settings

Click **Expand** to configure the advanced parameters. Keep the default settings unless otherwise specified.



TLS Authentication: ○

Allow Data Compression: Yes

Route All Traffic over VPN: No

Cipher: AES-128-CBC

Deliver DNS: Example: 1.1.1.1

Auth: SHA1

Table 7-20 OpenVPN server advanced settings

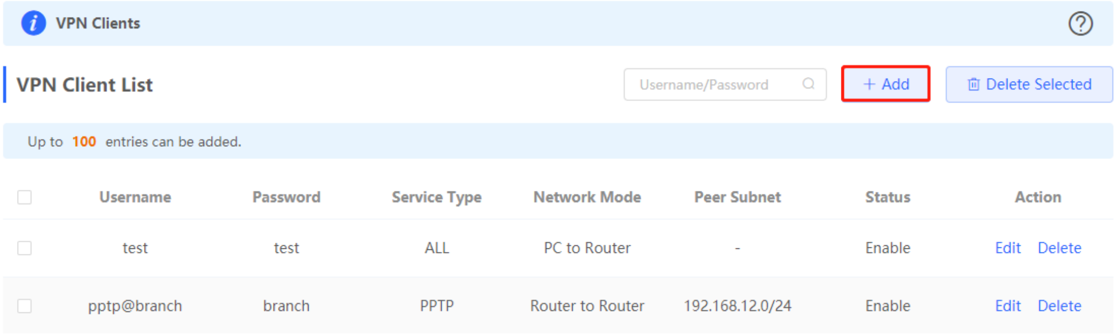
Parameter	Description
TLS Authentication	Specify the TLS key for enhanced OpenVPN security by allowing the communicating parties to possess the shared key before TLS handshake. After TLS authentication is enabled, you must import the TLS key on the client. (The version of the peer OpenVPN client must 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.
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 **Local Device** > **VPN** > **VPN Clients**.

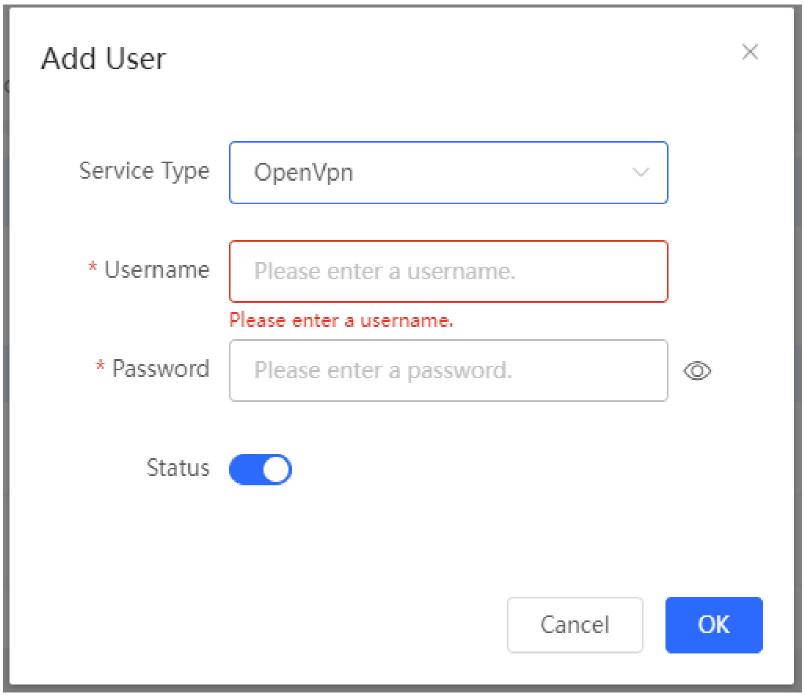
Only user accounts added to the VPN client list are allowed to dial up to connect to the OpenVPN server. Therefore, you need to manually configure user accounts for clients to access the OpenVPN server.

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.



Up to 100 entries can be added.

□	Username	Password	Service Type	Network Mode	Peer Subnet	Status	Action
□	test	test	ALL	PC to Router	-	Enable	Edit Delete
□	pptp@branch	branch	PPTP	Router to Router	192.168.12.0/24	Enable	Edit Delete



Service Type: OpenVpn

* Username: Please enter a username.

Please enter a username.

* Password: Please enter a password.

Status: ●

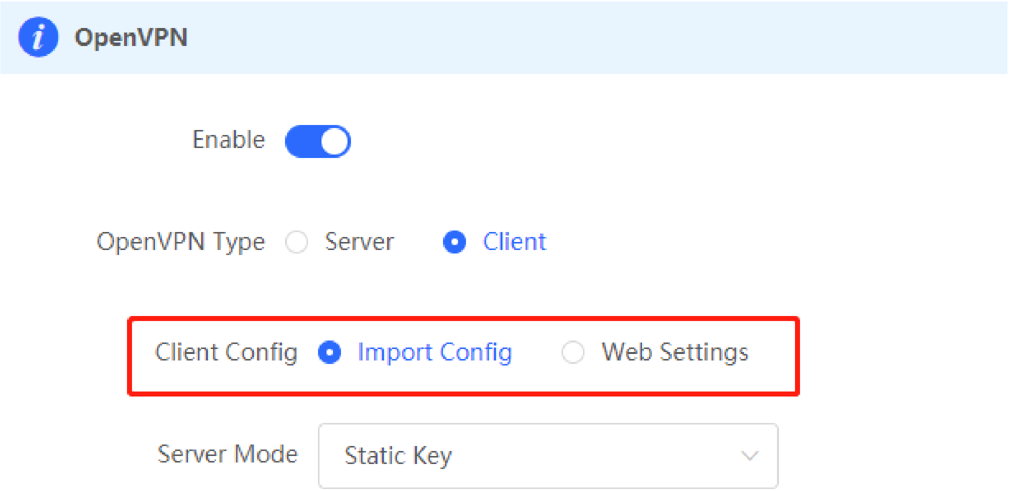
7.4.3 Configuring the OpenVPN Client

Choose **Local Device** > **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.



OpenVPN

Enable

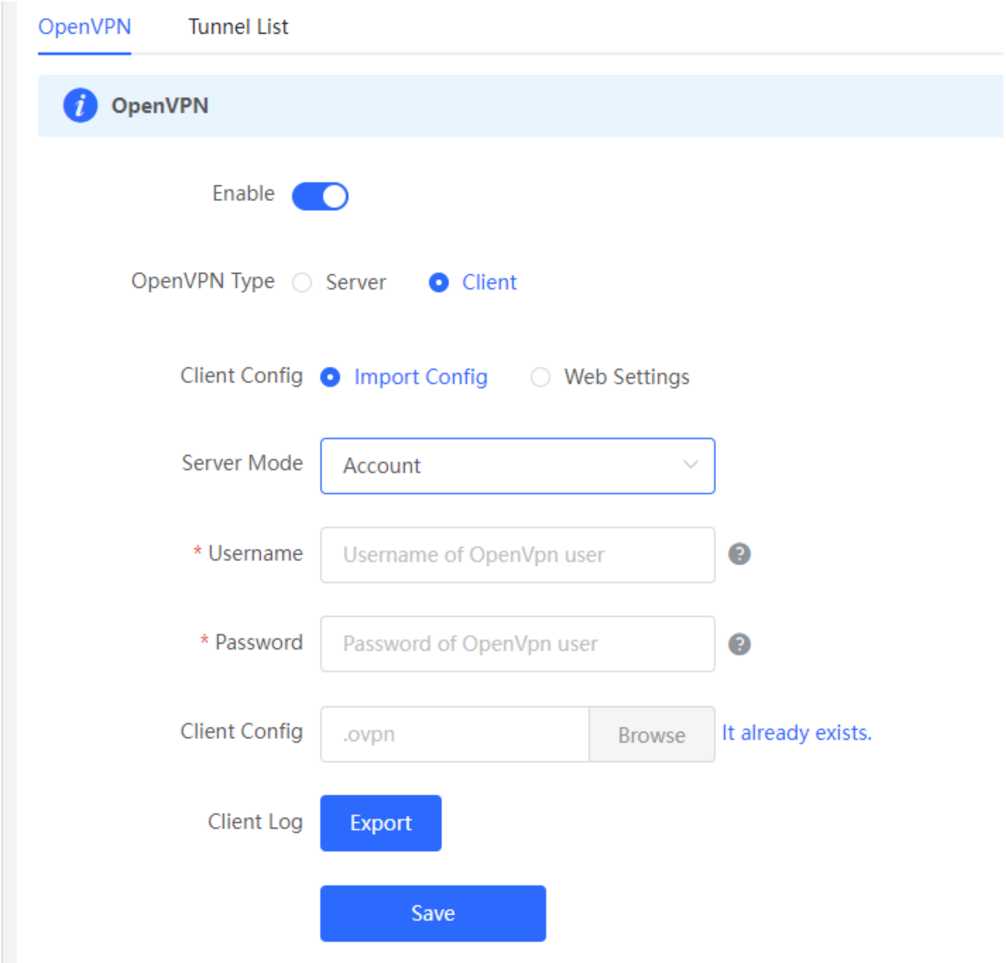
OpenVPN Type ○ Server ● Client

Client Config ● Import Config ○ Web Settings

Server Mode: Static Key

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.



OpenVPN

Enable

OpenVPN Type ○ Server ● Client

Client Config ● Import Config ○ Web Settings

Server Mode: Account

* Username: Username of OpenVpn user

* Password: Password of OpenVpn user

Client Config: .ovpn Browse It already exists.

Client Log: Export

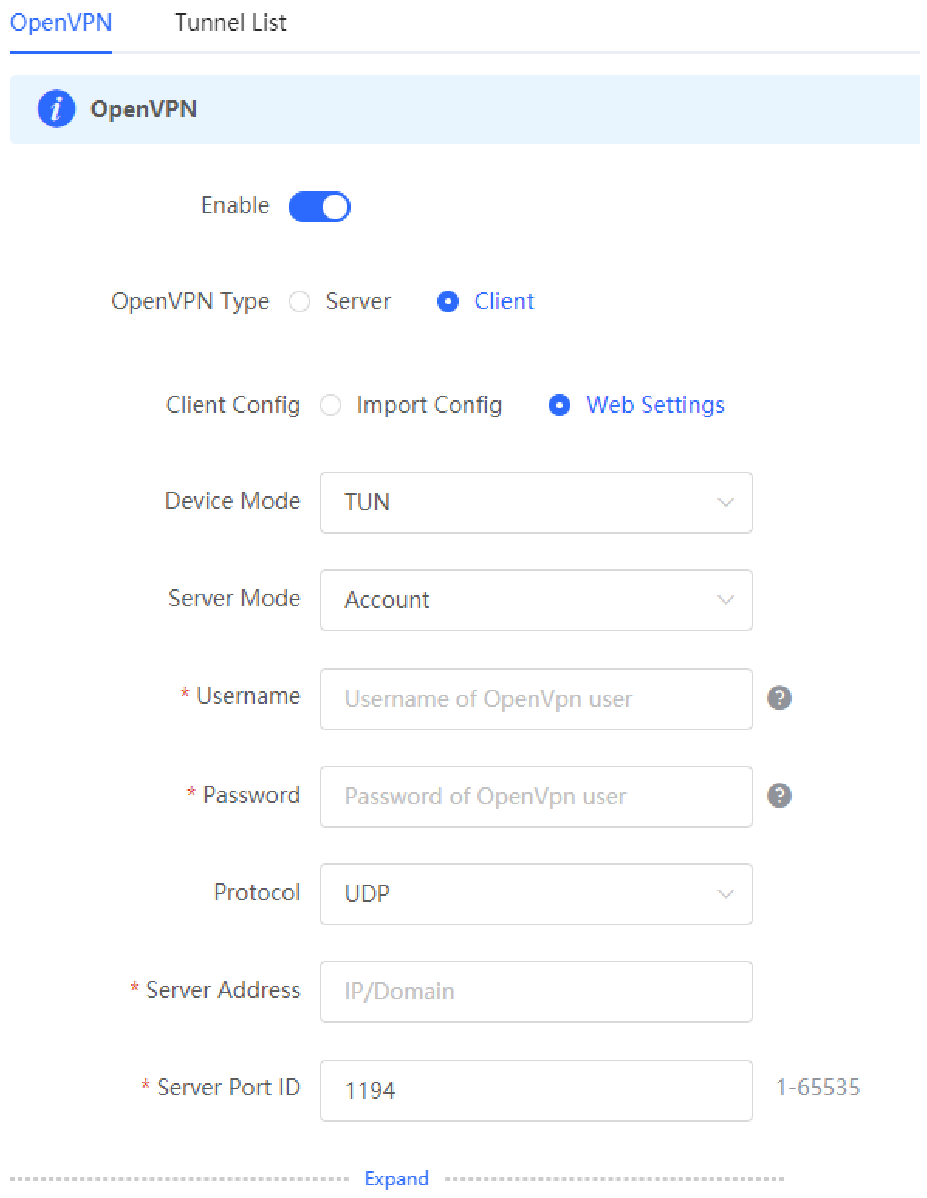
Table 7-21 OpenVPN client configuration in Import Config method

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. Pre-Shared 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	Click **Browse**, select the pre-shared key file, and upload the file.
Workmode	This parameter is available only when **Server Mode** is set to **Pre-Shared 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.
Client Log	Click **Export** to export the client log file.

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



Enable ●

OpenVPN Type ○ Server ● Client

Client Config ○ Import Config ● Web Settings

Device Mode: TUN

Server Mode: Account

* Username: Username of OpenVpn user

* Password: Password of OpenVpn user

Protocol: UDP

* Server Address: IP/Domain

* Server Port ID: 1194 1-65535

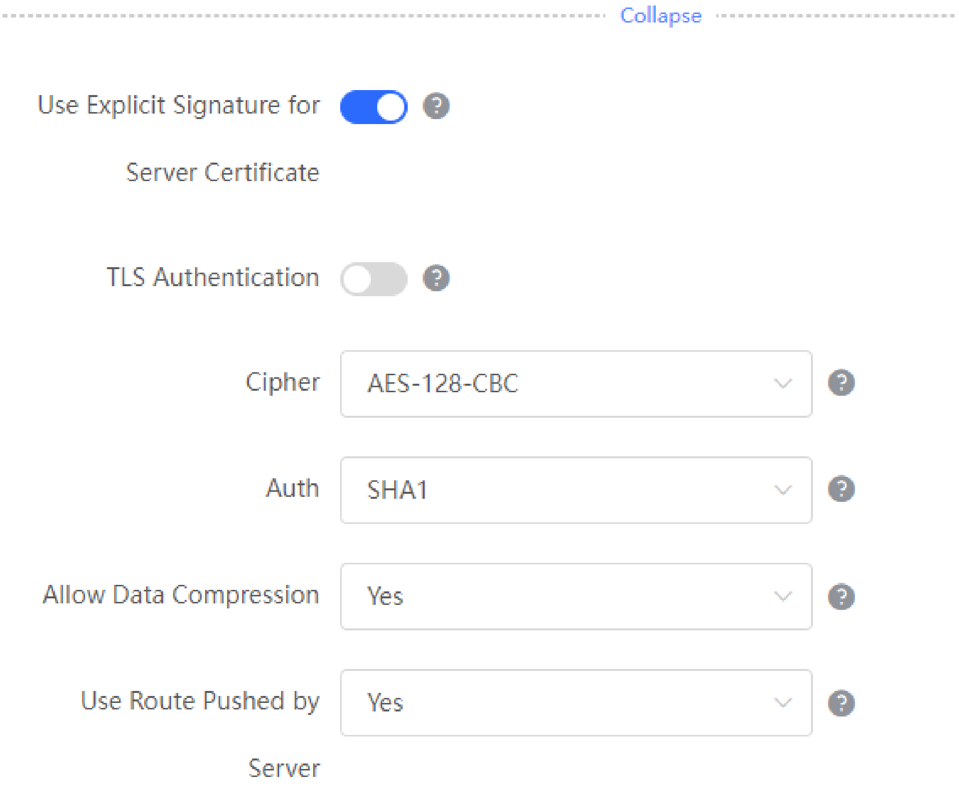
Table 7-22 OpenVPN client configuration in Web Settings method

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.

Parameter	Description
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.
Client Log	Click **Export** to export the client log file.

(2) Advanced Settings

Click **Expand** to configure the advanced parameters. Keep the default settings unless otherwise specified.



Use Explicit Signature for Server Certificate: ●

TLS Authentication: ○

Cipher: AES-128-CBC

Auth: SHA1

Allow Data Compression: Yes

Use Route Pushed by Server: Yes

Table 7-23 OpenVPN client configuration in Web Settings method

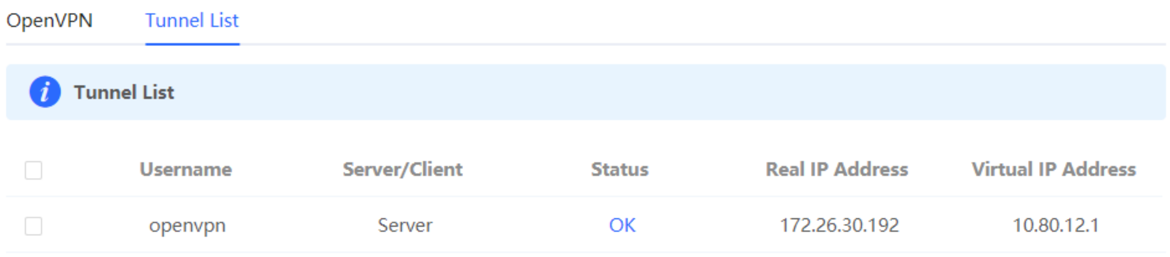
Parameter	Description
Use Explicit Signature for Server Certificate	Specify whether to verify the server certificate using explicit signature. By default, this function is enabled. If the server certificate does not use explicit signature, for example, the MikroTik server, you need to disable this function. 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**.

7.4.4 Viewing the OpenVPN Tunnel Information

Choose **Local Device** > **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.



□	Username	Server/Client	Status	Real IP Address	Virtual IP Address
□	openvpn	Server	OK	172.26.30.192	10.80.12.1

Table 7-24 OpenVPN tunnel information

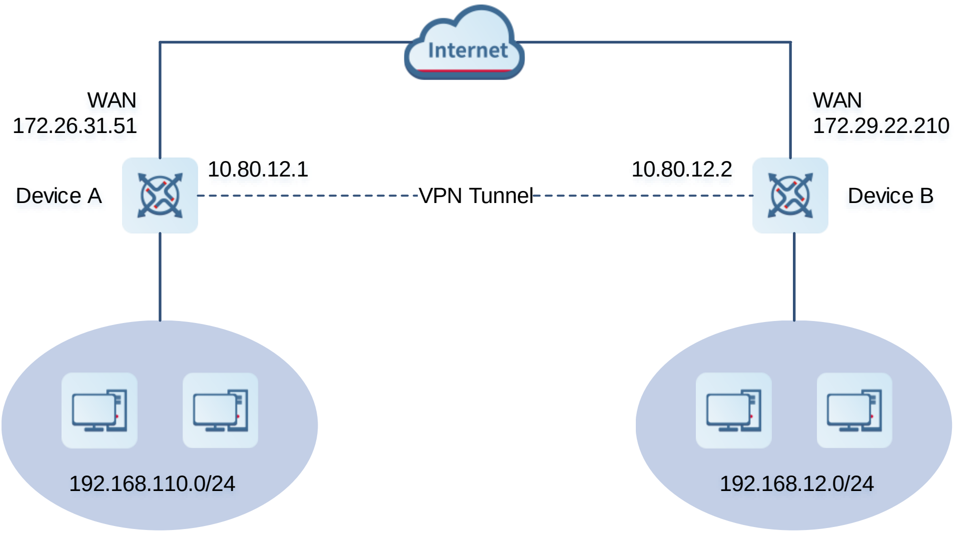
Parameter	Description
Username	Indicate the username used by the client for identity authentication. By default, the username displayed on the server is **openvpn**.
Server/Client	Indicate the role of the local end of the tunnel, which can be client or server.
Status	Indicate the tunnel establishment 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.

7.4.5 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



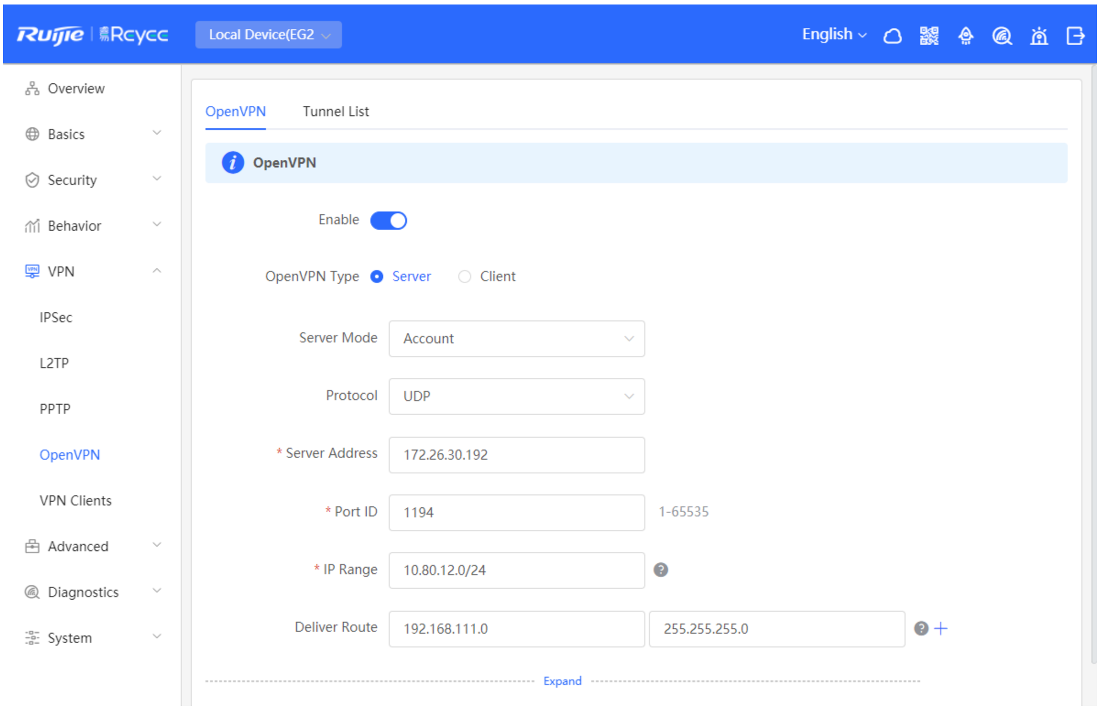
3. Configuration Roadmap

- 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

(1) Configure Device A.

a Log in to the web management system and choose VPN > OpenVPN > OpenVPN to access the OpenVPN page.



OpenVPN

Enable: ●

OpenVPN Type: ● Server ○ Client

Server Mode: Account

Protocol: UDP

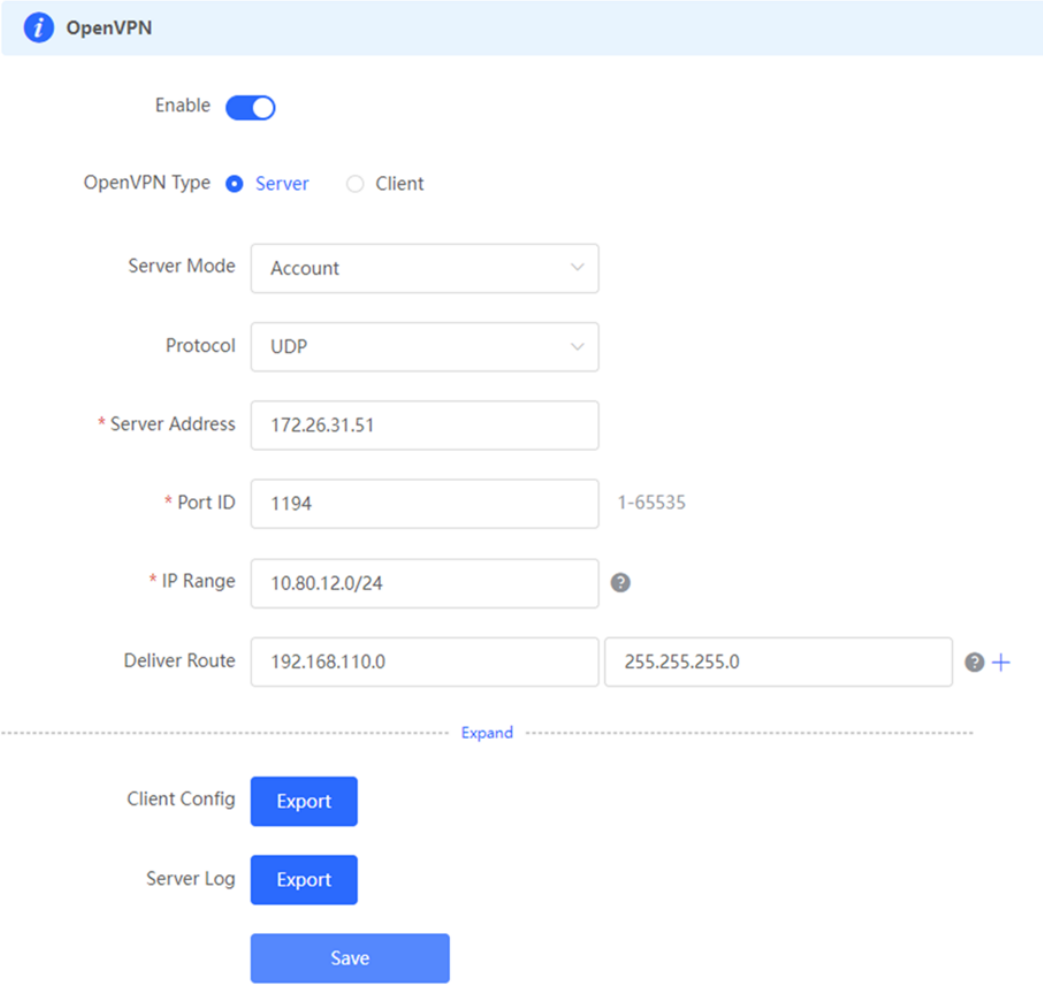
* Server Address: 172.26.30.192

* Port ID: 1194 1-65535

* IP Range: 10.80.12.0/24

Deliver Route: 192.168.111.0 255.255.255.0

b 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.



OpenVPN

Enable: on

OpenVPN Type: ● Server ○ Client

Server Mode: Account

Protocol: UDP

* Server Address: 172.26.31.51

* Port ID: 1194 1-65535

* IP Range: 10.80.12.0/24

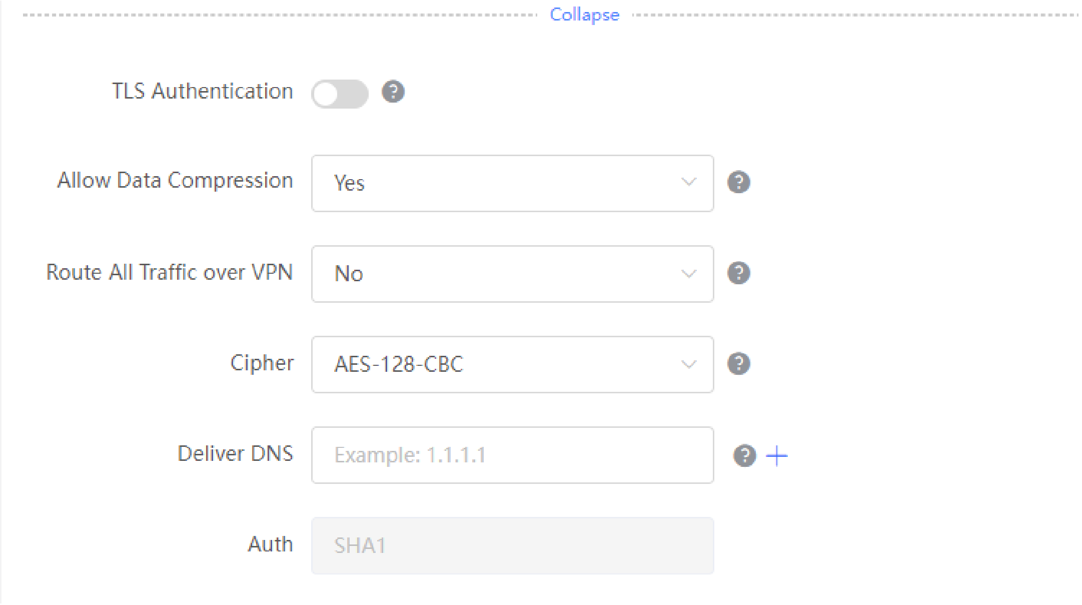
Deliver Route: 192.168.110.0 255.255.255.0

Table 7-25 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 port address of the server, that 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.

Parameter	Description
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	Add routes to the corresponding network segment if the client wants to the LAN network segment where the server resides.

c Click Expand 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.



TLS Authentication: off

Allow Data Compression: Yes

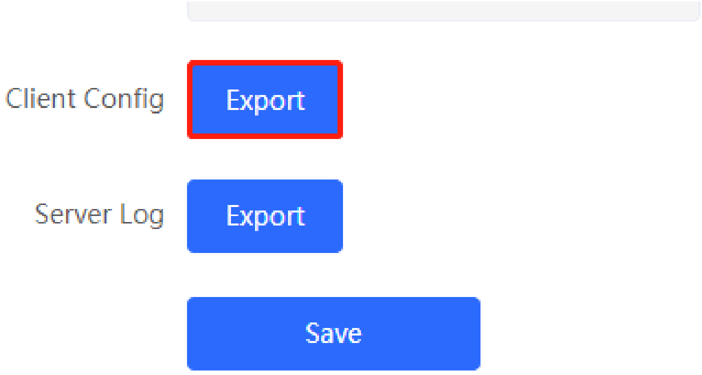
Route All Traffic over VPN: No

Cipher: AES-128-CBC

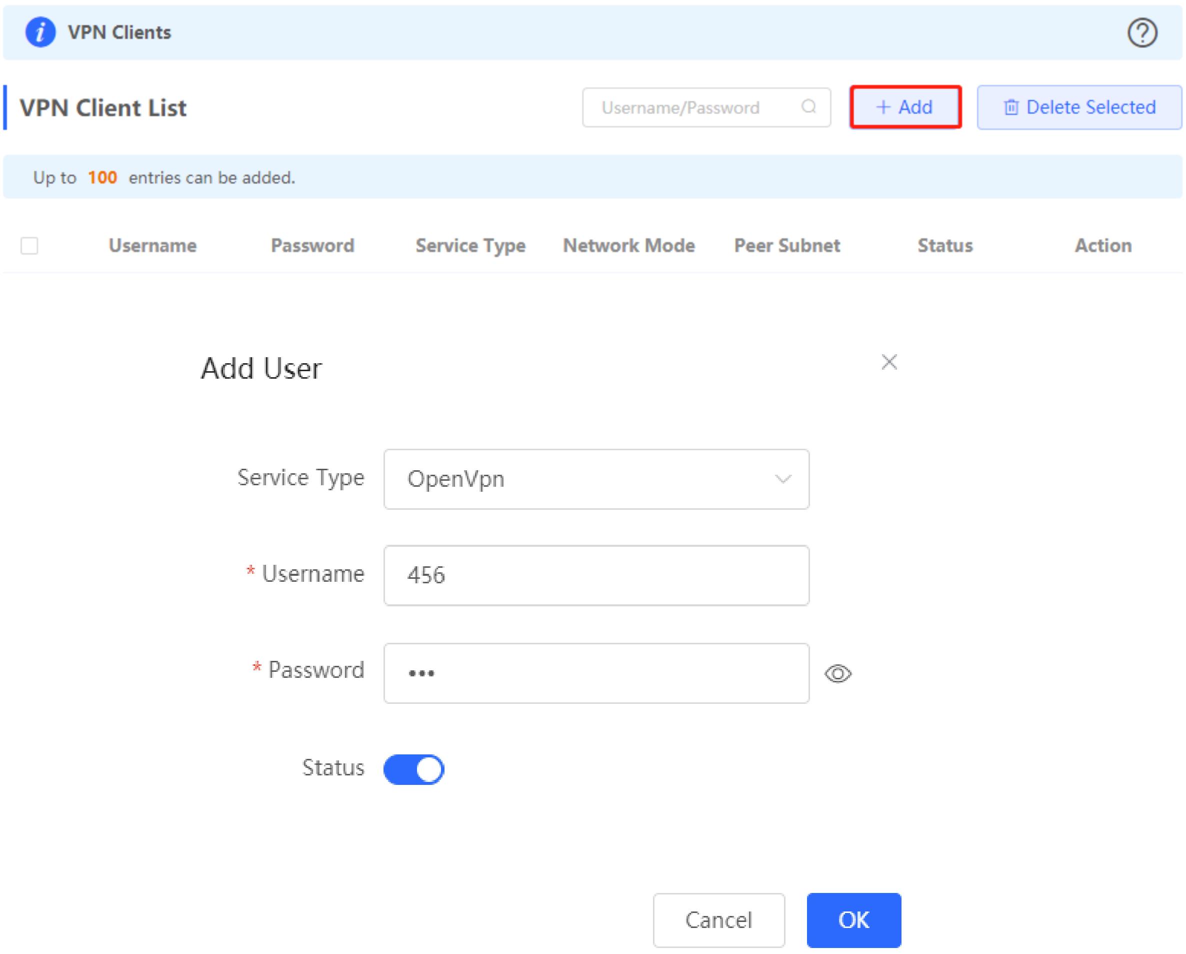
Deliver DNS: Example: 1.1.1.1

Auth: SHA1

d 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.



e Choose **VPN** > **VPN Clients** and add an OpenVPN user account.



Up to 100 entries can be added.

☐	Username	Password	Service Type	Network Mode	Peer Subnet	Status	Action

Add User

Service Type: OpenVpn

* Username: 456

* Password: •••

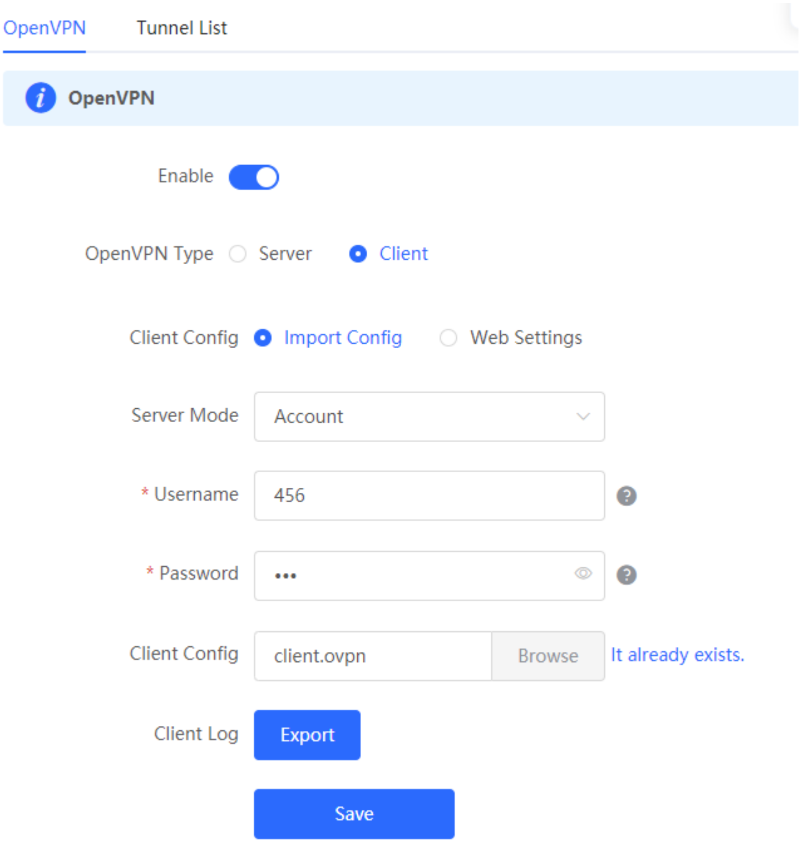
Status: ●

(2) Configure Device B.

a Log in to the web management system and access the OpenVPN page.

b 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:



Enable ●

OpenVPN Type ○ Server ● Client

Client Config ● Import Config ○ Web Settings

Server Mode Account

* Username 456

* Password •••

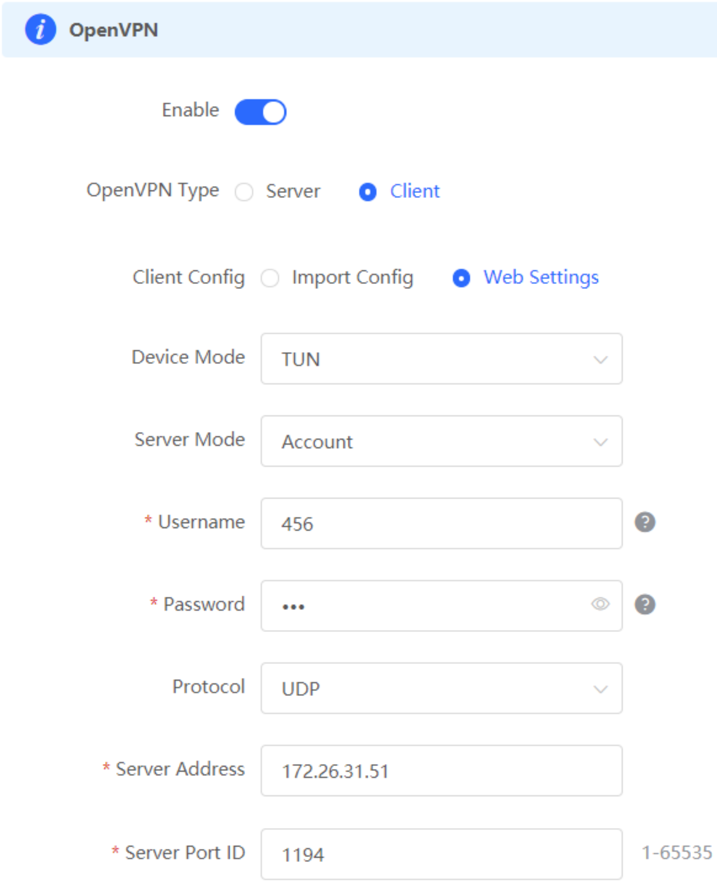
Client Config client.ovpn Browse It already exists.

Client Log Export

Table 7-26 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, 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

Enable: On

OpenVPN Type: ○ Server ● Client

Client Config: ○ Import Config ● Web Settings

Device Mode: TUN

Server Mode: Account

* Username: 456

* Password: •••

Protocol: UDP

* Server Address: 172.26.31.51

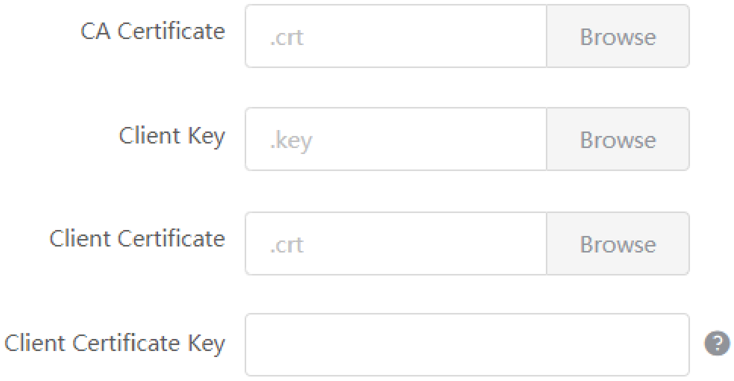
* Server Port ID: 1194 1-65535

Table 7-27 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**.
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, that 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**.



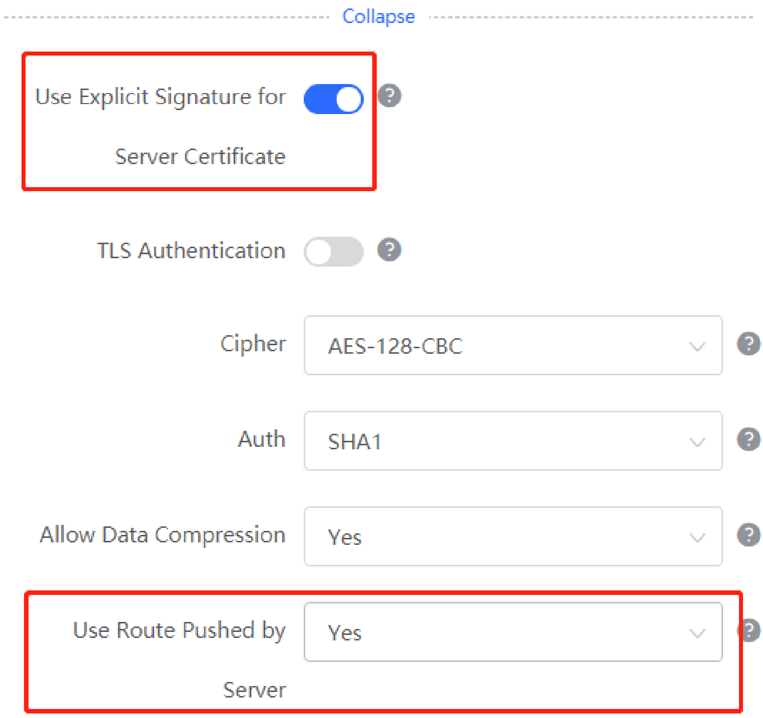
CA Certificate: .crt Browse

Client Key: .key Browse

Client Certificate: .crt Browse

Client Certificate Key:

Click **Expand** 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**.



Use Explicit Signature for Server Certificate: On

TLS Authentication: Off

Cipher: AES-128-CBC

Auth: SHA1

Allow Data Compression: Yes

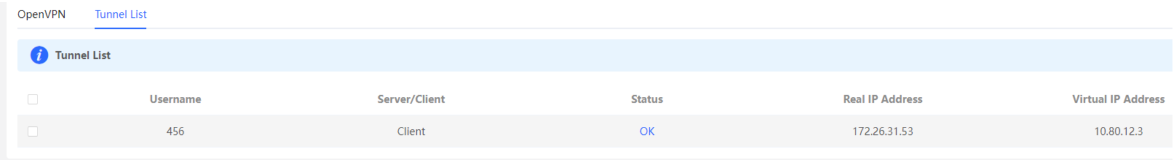
Use Route Pushed by Server: Yes

c 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.

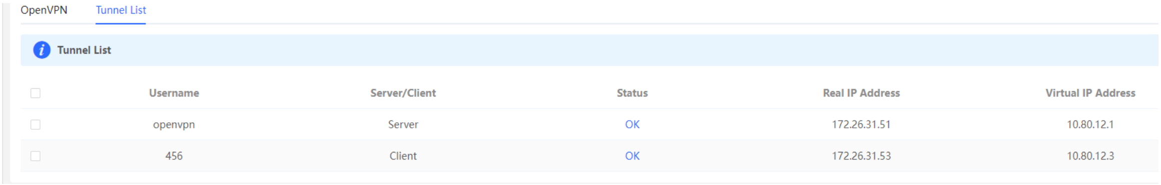
Client:



Tunnel List

□	Username	Server/Client	Status	Real IP Address	Virtual IP Address
□	456	Client	OK	172.26.31.53	10.80.12.3

Server:



Tunnel List

□	Username	Server/Client	Status	Real IP Address	Virtual IP Address
□	openvpn	Server	OK	172.26.31.51	10.80.12.1
□	456	Client	OK	172.26.31.53	10.80.12.3

8 System Management

8.1 Setting the Login Password

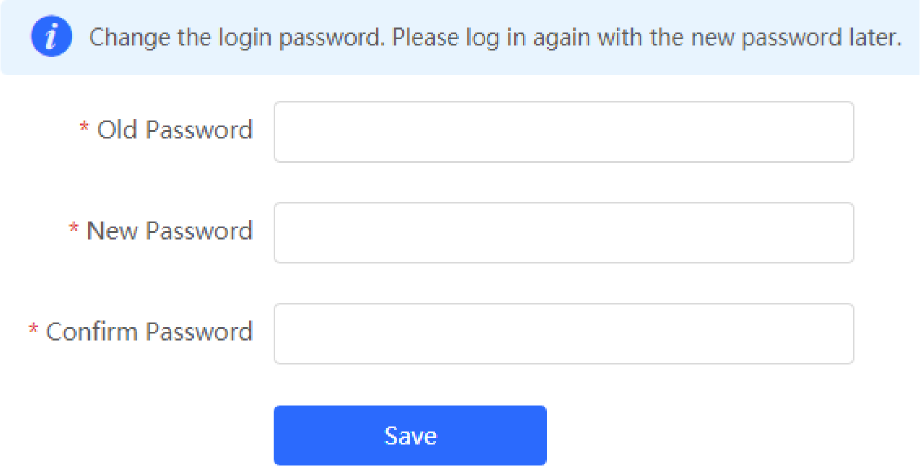
Turn off **Self-Organizing Network Discovery**. Choose **System** > **Login** > **Login Password**.

Turn on **Self-Organizing Network Discovery**. Choose **Network** > **System** > **Login 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.


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

* Old Password

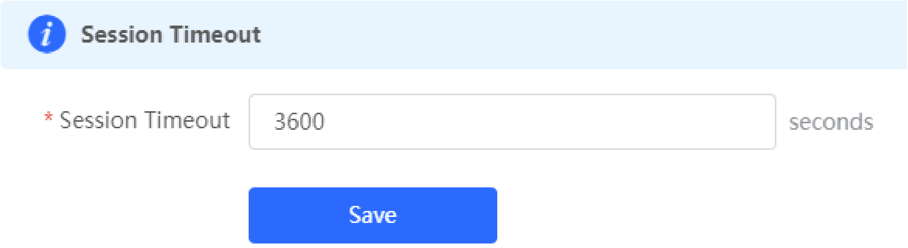
* New Password

* Confirm Password

8.2 Setting the Session Timeout Duration

Choose **Local Device** > **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.


Session Timeout

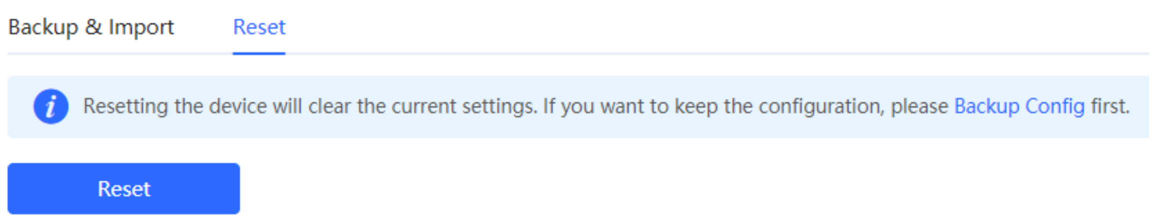
* Session Timeout 3600 seconds

8.3 Restoring Factory Settings

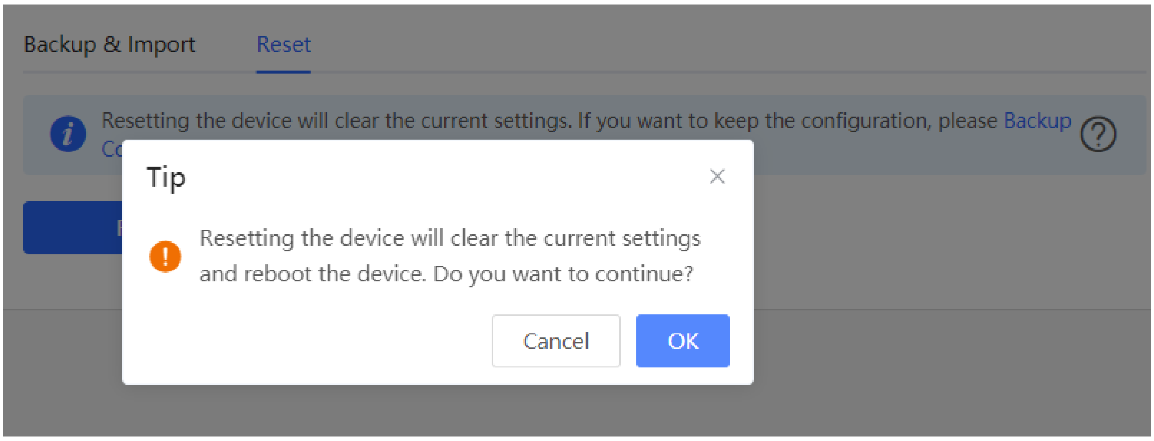
8.3.1 Restoring the Current Device to Factory Settings

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

Click **Reset** to restore the current device to the factory settings.



Resetting the device will clear the current settings. If you want to keep the configuration, please Backup Config first.



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

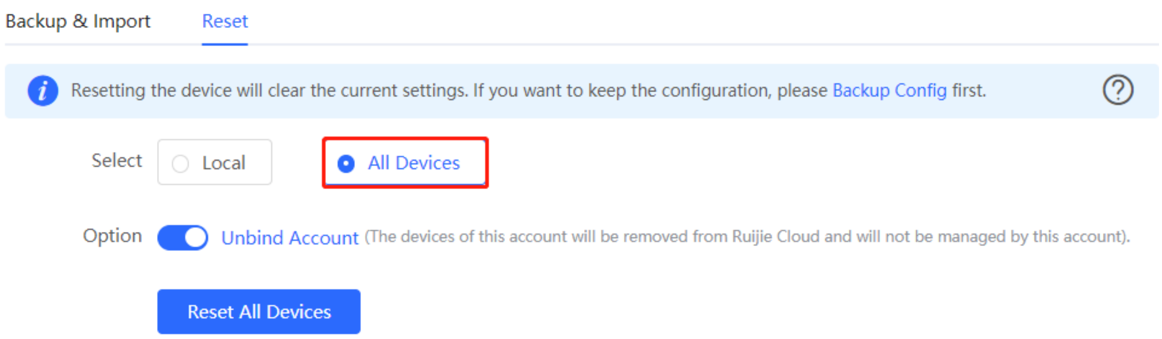
Caution

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 Configuring Backup and Import.) Therefore, exercise caution when performing this operation.

8.3.2 Restoring All Devices to Factory Settings

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

Click **All Devices**, select whether to enable **Unbind Account**, and click **Reset All Devices**. All devices in the network will be restored to factory settings.



Resetting the device will clear the current settings. If you want to keep the configuration, please Backup Config first.

Select ○ Local ● All Devices

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

Caution

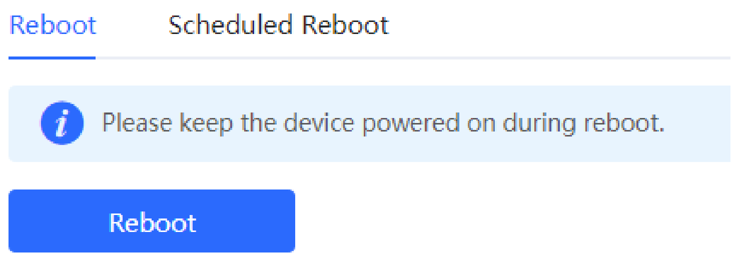
The operation will clear all configuration of all devices in the network. Therefore, exercise caution when performing this operation.

8.4 Configuring Reboot

8.4.1 Rebooting the Current Device

Choose **Local Device** > **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.

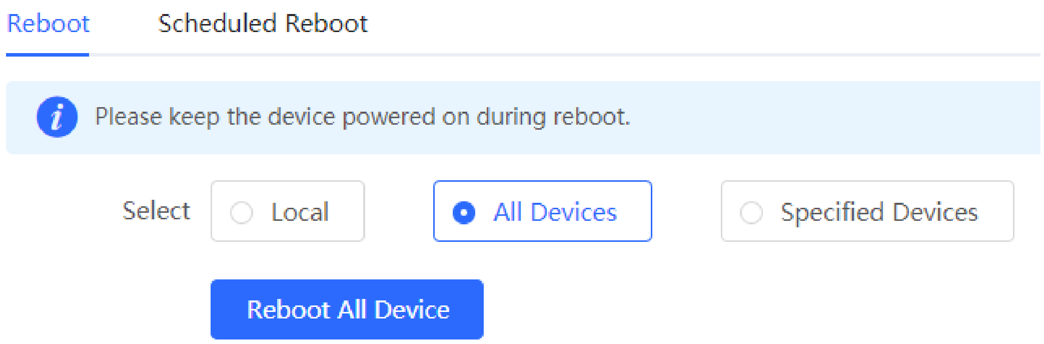


Please keep the device powered on during reboot.

8.4.2 Rebooting All Devices in the Network

Choose **Local Device** > **System** > **Reboot** > **Reboot**.

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



Please keep the device powered on during reboot.

Select ○ Local ● All Devices ○ Specified Devices

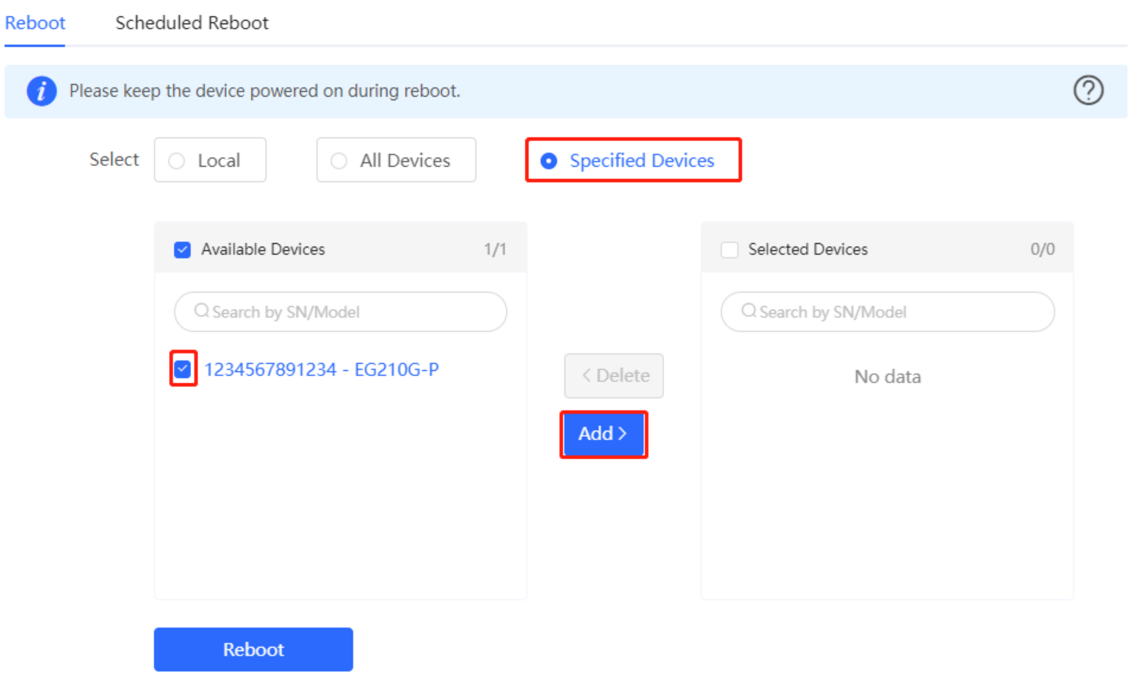
Caution

The operation takes some time and affects the whole network. Therefore, exercise caution when performing this operation.

8.4.3 Rebooting the Specified Device

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



Reboot Scheduled Reboot

Please keep the device powered on during reboot.

Select ○ Local ○ All Devices ● Specified Devices

☑ Available Devices 1/1

Search by SN/Model

☑ 1234567891234 - EG210G-P

< Delete

Add >

□ Selected Devices 0/0

Search by SN/Model

No data

Reboot

8.5 Configuring Scheduled Reboot

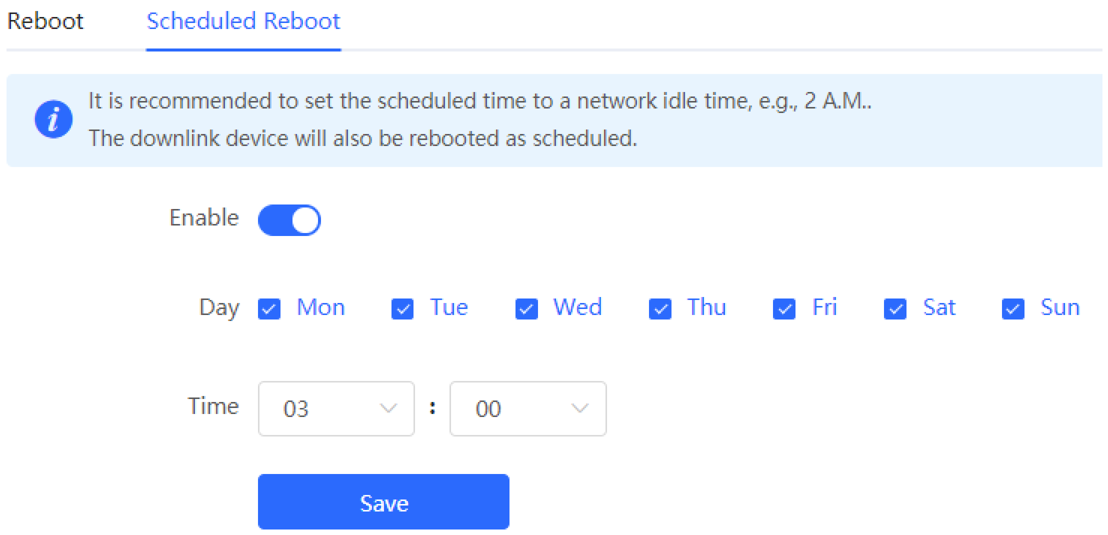
Confirm that the system time is accurate to avoid network interruption caused by device reboot at wrong time. For details about how to configure the system time, see Setting and Displaying System Time.

Choose **System** > **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.



Reboot Scheduled Reboot

It is recommended to set the scheduled time to a network idle time, e.g., 2 A.M..
The downlink device will also be rebooted as scheduled.

Enable

Day ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

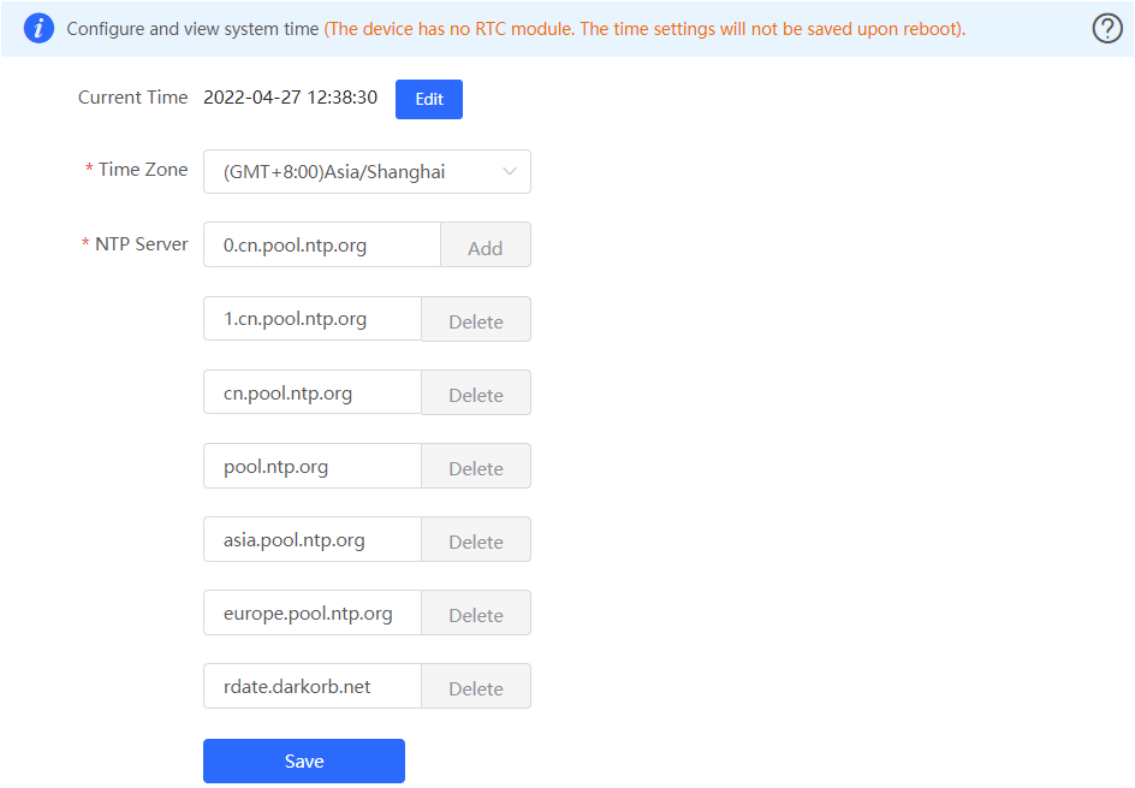
Time 03 : 00

Save

8.6 Setting and Displaying System Time

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

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



Configure and view system time (The device has no RTC module. The time settings will not be saved upon reboot).

Current Time 2022-04-27 12:38:30

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

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

1.cn.pool.ntp.org

cn.pool.ntp.org

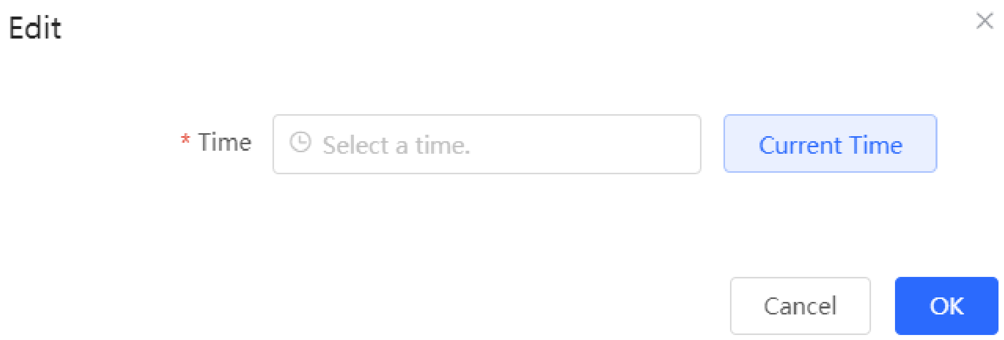
pool.ntp.org

asia.pool.ntp.org

europe.pool.ntp.org

rdate.darkorb.net

Click **Current Time**, and the current system time will be filled in automatically.



Edit

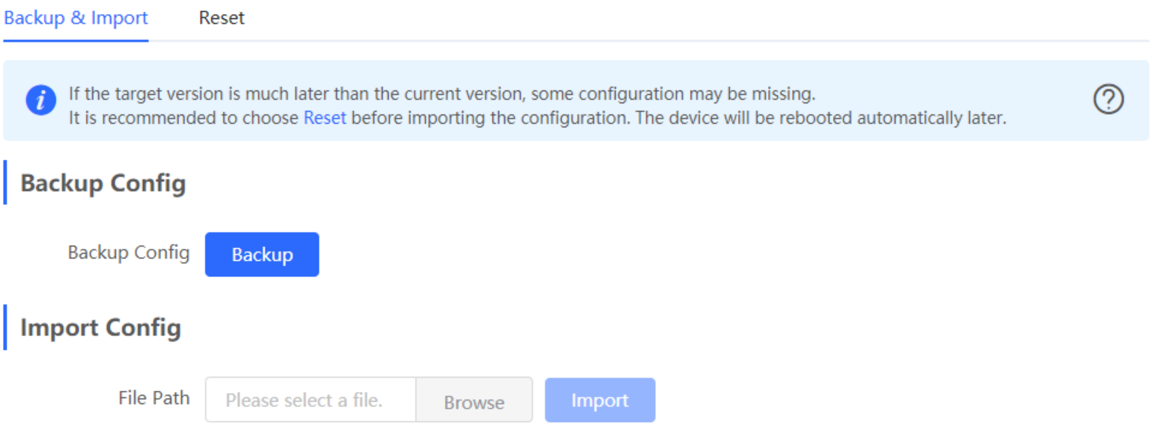
* Time Select a time.

8.7 Configuring Backup and Import

Choose **System** > **Management** > **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.



Backup & Import Reset

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

Backup Config

Backup Config: Backup

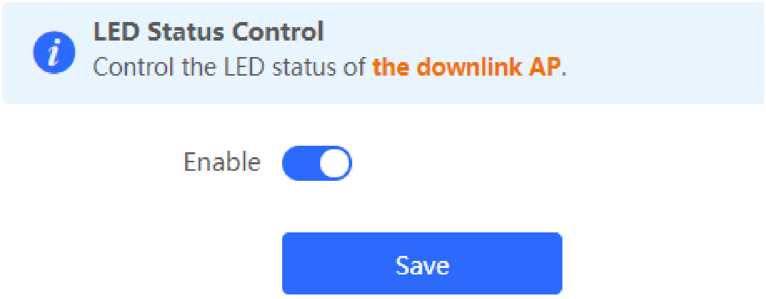
Import Config

File Path: Please select a file. Browse Import

8.8 Configuring LED Status Control

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

Turn on **Enable** and click **Save** to deliver the configuration.



LED Status Control
Control the LED status of the downlink AP.

Enable

Save

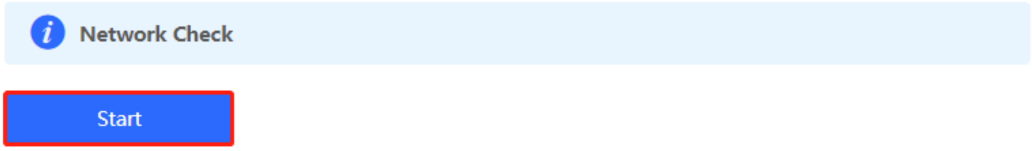
8.9 Configuring Diagnostics

8.9.1 Network Check

When a network error occurs, perform **Network Check** to identify the fault and take the suggested action.

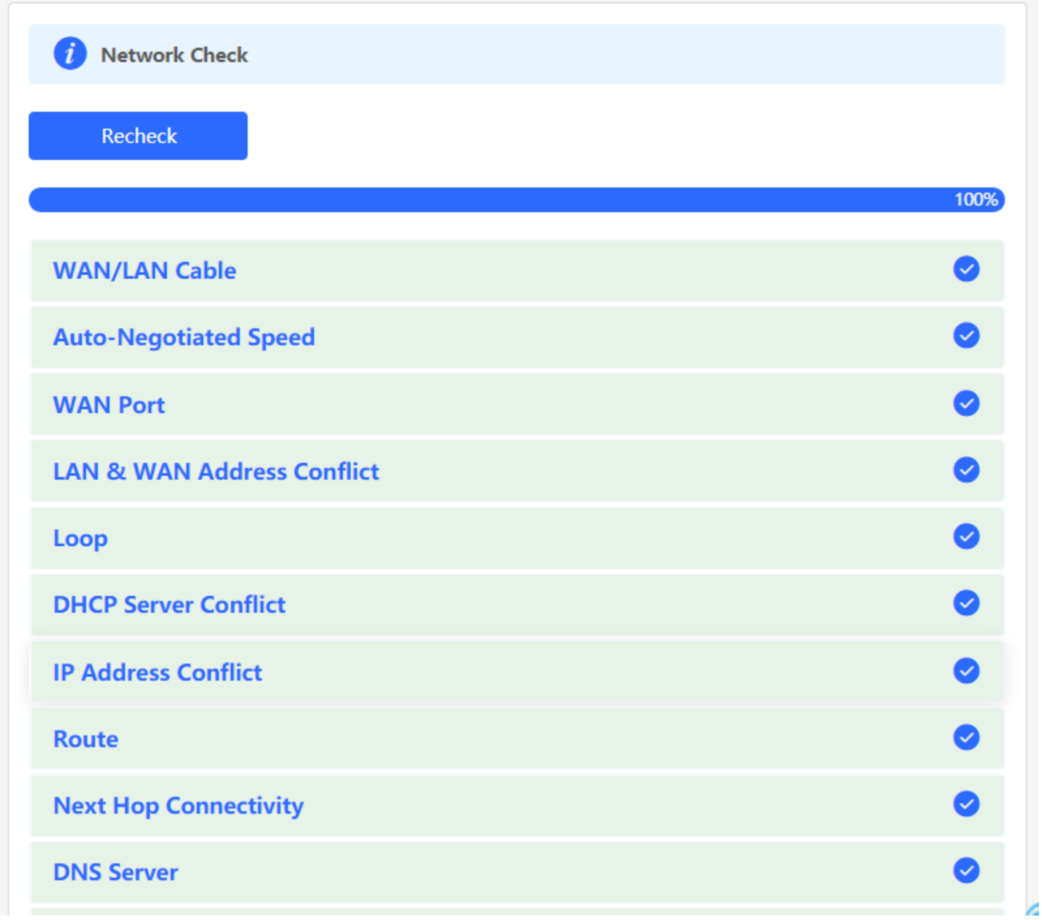
Choose **Local Device** > **Diagnostics** > **Network Check**.

Click **Start** to perform the network check and show the result.



Network Check

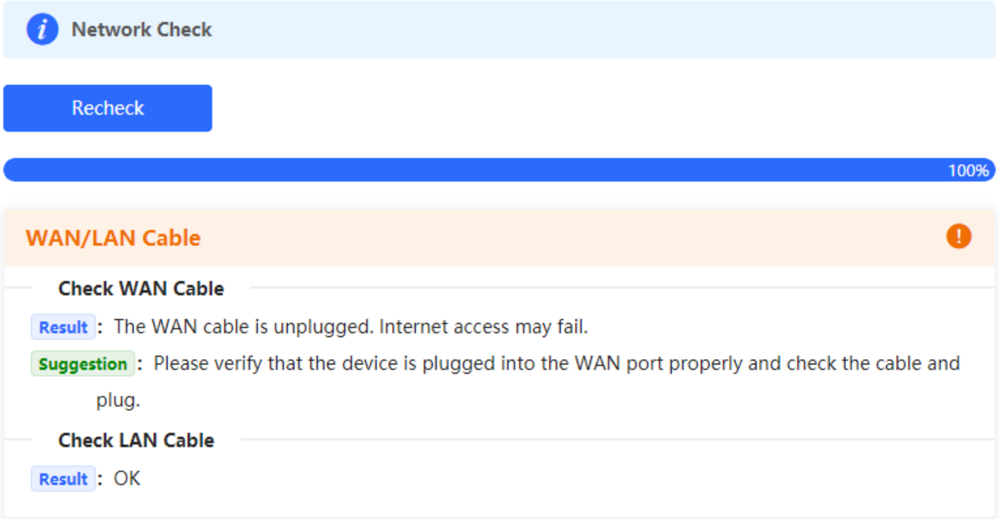
Start



Network Check

- WAN/LAN Cable ✓
- Auto-Negotiated Speed ✓
- WAN Port ✓
- LAN & WAN Address Conflict ✓
- Loop ✓
- DHCP Server Conflict ✓
- IP Address Conflict ✓
- Route ✓
- Next Hop Connectivity ✓
- DNS Server ✓

If a network error occurs, its symptom and suggested action will be displayed.



Network Check

WAN/LAN Cable !

Check WAN Cable

Result : The WAN cable is unplugged. Internet access may fail.

Suggestion : Please verify that the device is plugged into the WAN port properly and check the cable and plug.

Check LAN Cable

Result : OK

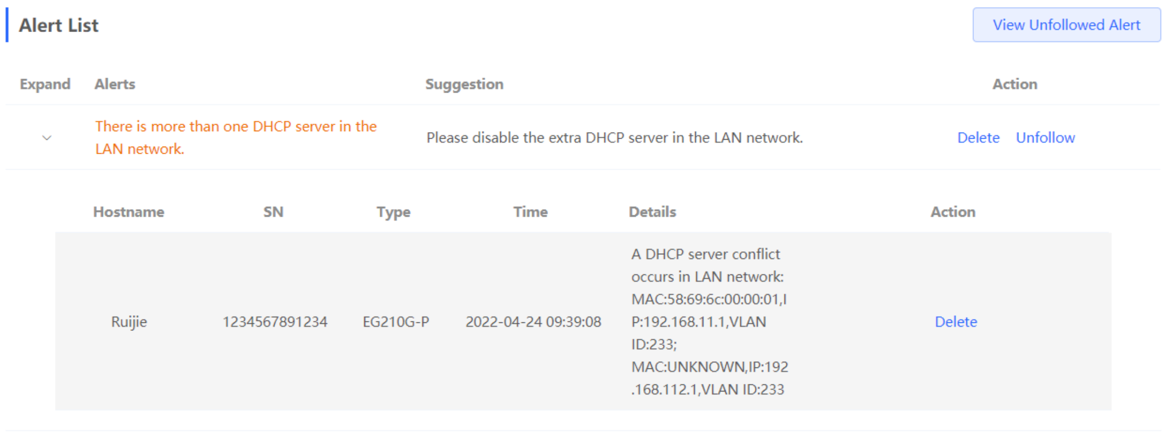
8.9.2 Alerts

Choose **Network** > **Alerts**.

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

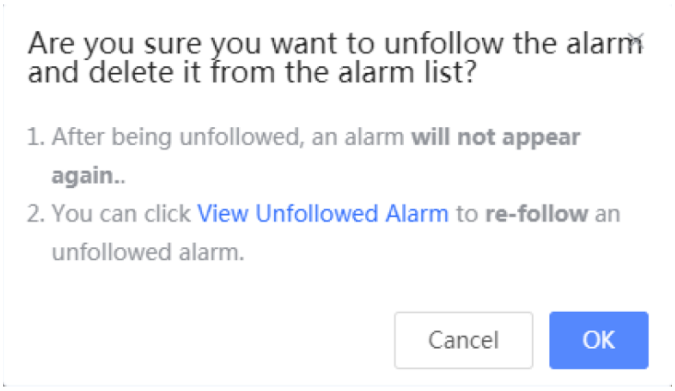
After unfollowing a specified alert type, you will not discover and process all alerts of this type promptly. Therefore, exercise caution when performing this operation.



Alert List

Expand	Alerts	Suggestion	Action
⌄	There is more than one DHCP server in the LAN network.	Please disable the extra DHCP server in the LAN network.	Delete Unfollow

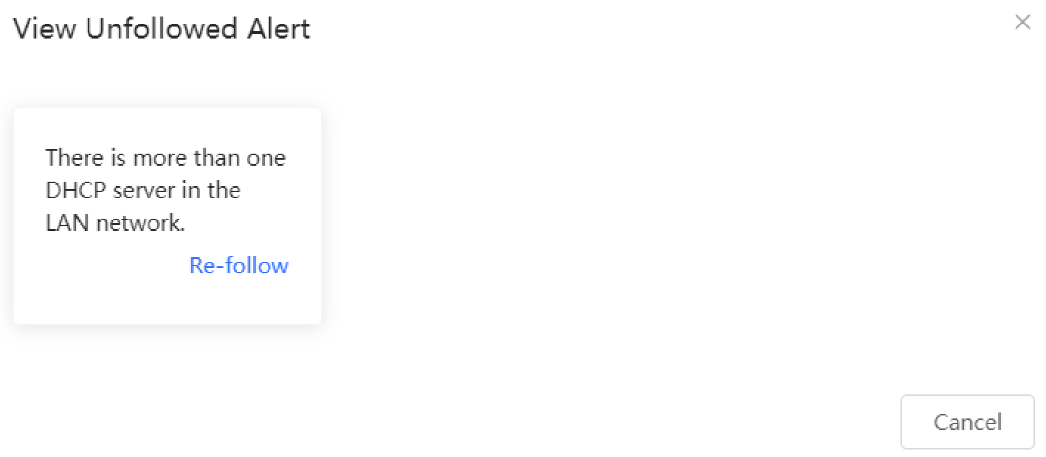
Hostname	SN	Type	Time	Details	Action
Ruijie	1234567891234	EG210G-P	2022-04-24 09:39:08	A DHCP server conflict occurs in LAN network: MAC:58:69:6c:00:00:01,IP:192.168.11.1,VLAN ID:233; MAC:UNKNOWN,IP:192.168.112.1,VLAN ID:233	Delete



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

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

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



View Unfollowed Alert

There is more than one DHCP server in the LAN network.

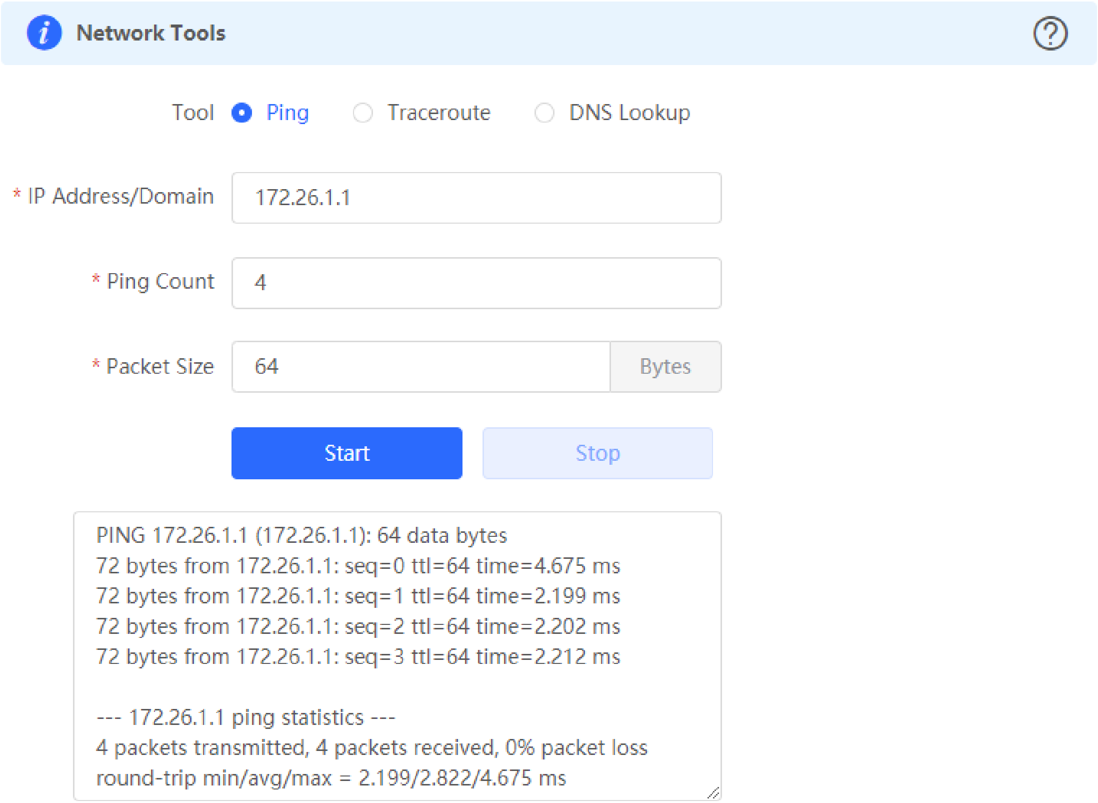
8.9.3 Network Tools

Choose **Local Device** > **Diagnostics** > **Network Tools**.

Select a diagnostic method, enter an IP address or URL, and click **Start**.

The ping method is used to test the connectivity between the tested device and the specified IP address or URL. If ping fails, the device is not connected to the IP address or URL.

The traceroute method is used to trace network paths to the specified IP address or URL. The DNS lookup method is used to check the DNS server address for URL parsing.



Network Tools

Tool ● Ping ○ Traceroute ○ DNS Lookup

* IP Address/Domain: 172.26.1.1

* Ping Count: 4

* Packet Size: 64 Bytes

```
PING 172.26.1.1 (172.26.1.1): 64 data bytes
72 bytes from 172.26.1.1: seq=0 ttl=64 time=4.675 ms
72 bytes from 172.26.1.1: seq=1 ttl=64 time=2.199 ms
72 bytes from 172.26.1.1: seq=2 ttl=64 time=2.202 ms
72 bytes from 172.26.1.1: seq=3 ttl=64 time=2.212 ms

--- 172.26.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.199/2.822/4.675 ms
```

8.9.4 Packet Capture

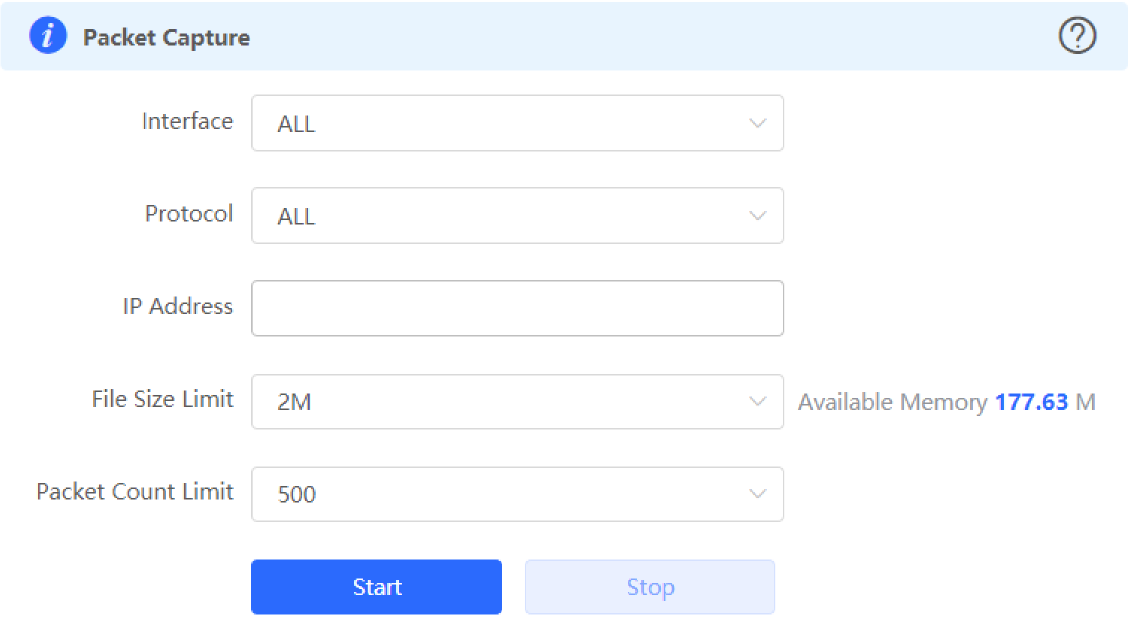
Choose **Local Device** > **Diagnostics** > **Packet Capture**.

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

Interface: ALL

Protocol: ALL

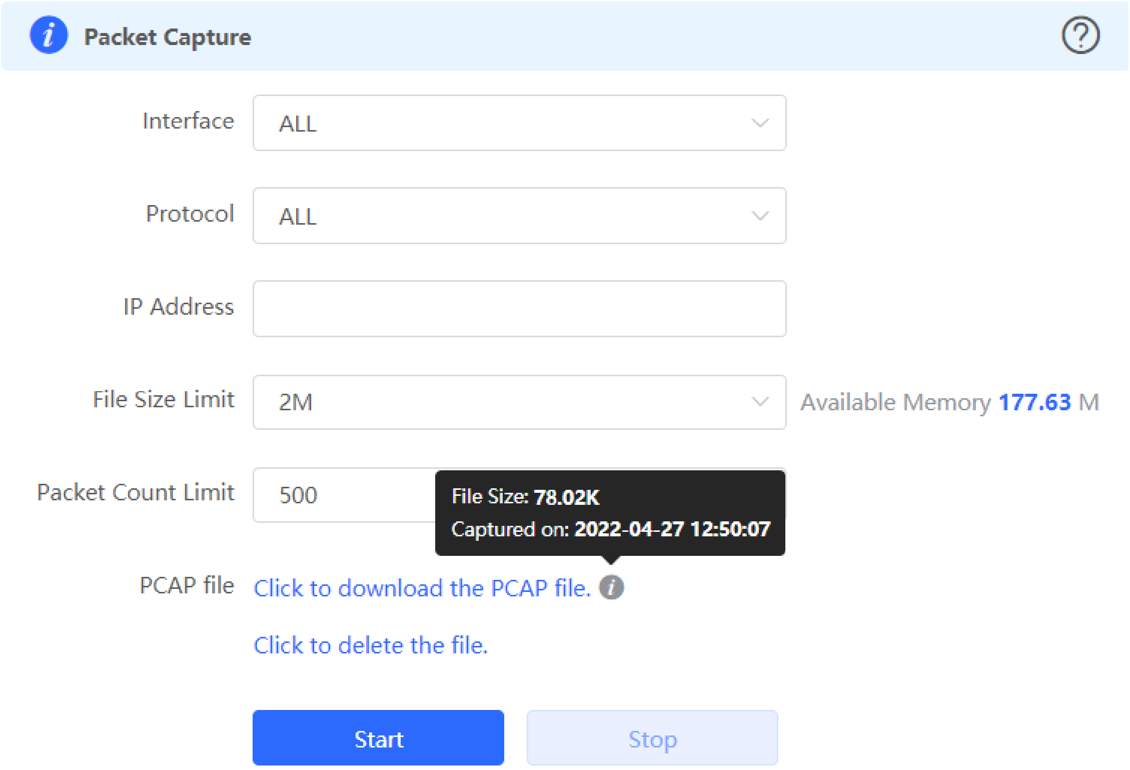
IP Address:

File Size Limit: 2M

Available Memory 177.63 M

Packet Count Limit: 500

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.



Packet Capture

Interface: ALL

Protocol: ALL

IP Address:

File Size Limit: 2M

Available Memory 177.63 M

Packet Count Limit: 500

File Size: 78.02K
Captured on: 2022-04-27 12:50:07

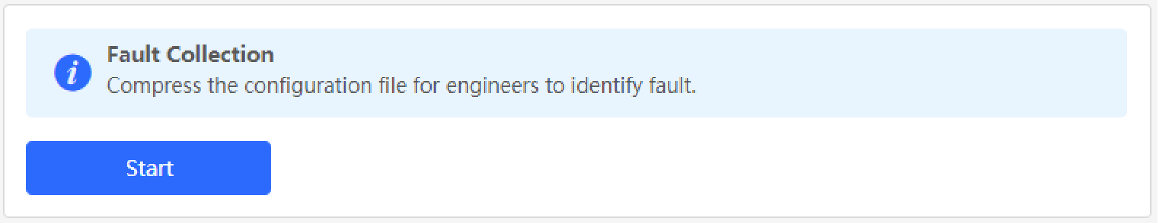
PCAP file: Click to download the PCAP file.

Click to delete the file.

8.9.5 Fault Collection

Choose **Local Device** > **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.



Fault Collection

Compress the configuration file for engineers to identify fault.

8.10 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.

8.10.1 Online Upgrade

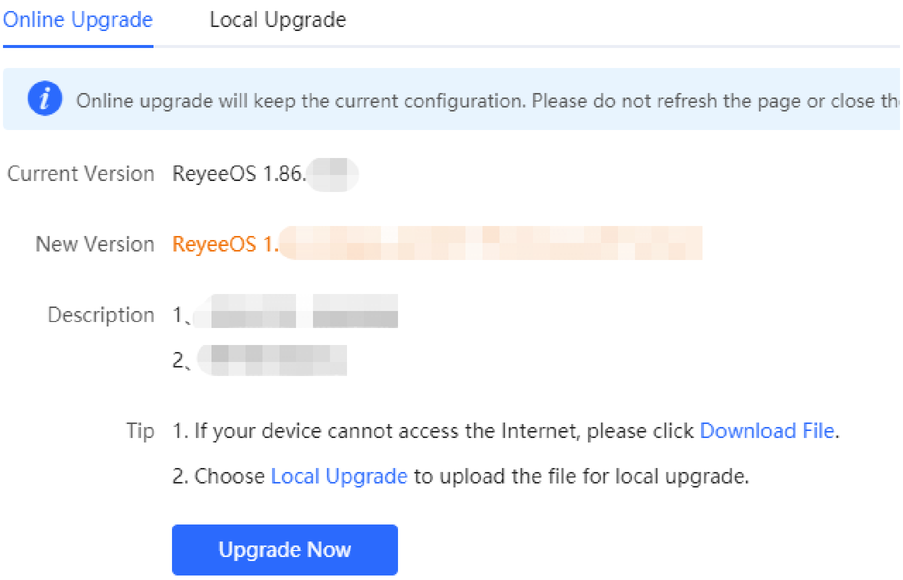
Choose **Local Device** > **System** > **Upgrade** > **Online Upgrade**.

The current page displays the current system version and allows you to detect whether a later version is available. If a new version is available, click **Upgrade Now** to perform online upgrade. If the network environment does not support online upgrade, click **Download File** to download the upgrade installation package locally and then perform local upgrade.

Note

Online upgrade will retain the current configuration.

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



Online upgrade will keep the current configuration. Please do not refresh the page or close th

Current Version ReyeeOS 1.86.[redacted]

New Version ReyeeOS 1.[redacted]

Description 1、[redacted]

2、[redacted]

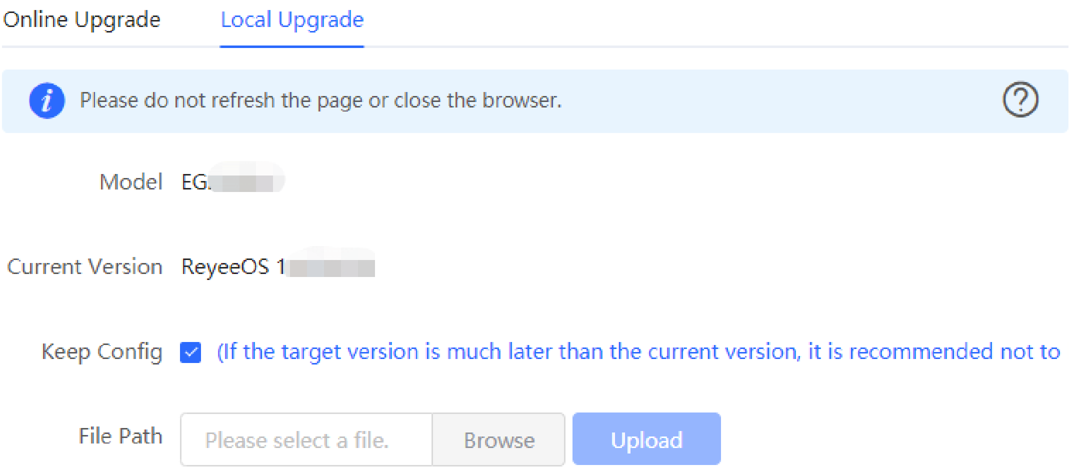
Tip 1. If your device cannot access the Internet, please click Download File.

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

8.10.2 Local Upgrade

Choose **Local Device** > **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.



Please do not refresh the page or close the browser.

Model EG[redacted]

Current Version ReyeeOS 1[redacted]

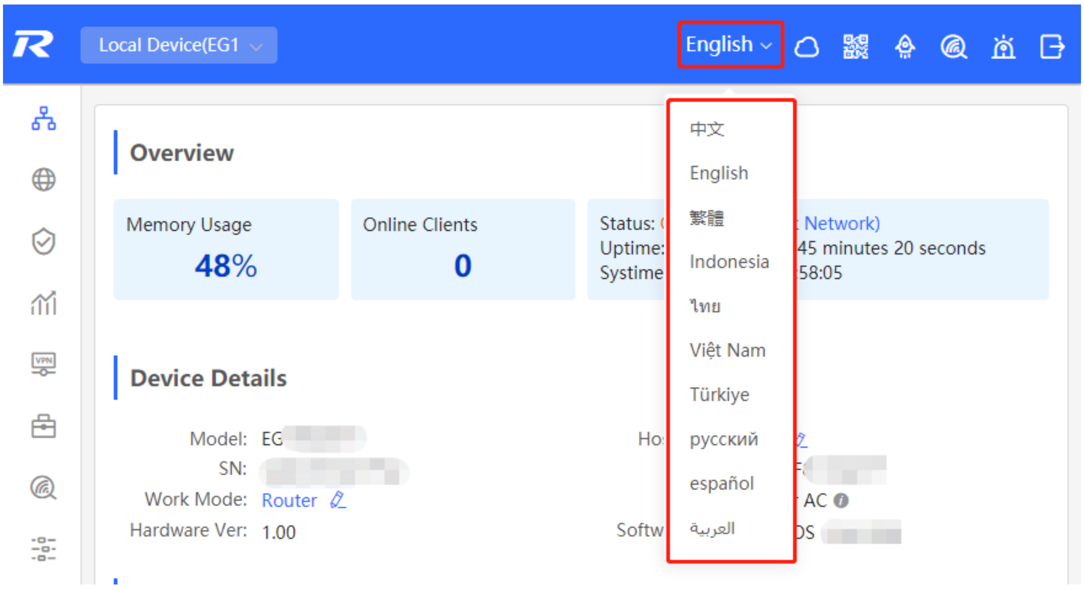
Keep Config ☑ (If the target version is much later than the current version, it is recommended not to

File Path Please select a file. Browse Upload

8.11 Switching System Language

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

Click a required language to switch the system language.



Status: (
Uptime:
Systime
Network)
45 minutes 20 seconds
58:05

Model: EG[redacted]
SN: [redacted]
Work Mode: Router
Hardware Ver: 1.00

9 FAQ

9.1 What Can I Do If I Fail to Log In to the Web Page?

(1) Confirm that the network cable is correctly connected to the LAN port of the device, and the corresponding indicator is flashing or steady On.

(2) Before you access the Settings 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.

9.2 How Do I Restore 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.

9.3 What Can I Do If I Forget the Device Login Password?

Try to log in using the Wi-Fi password. If the fault persists, restore the factory settings.

9.4 What Can I Do If Internet Access Through PPPoE Dial-Up Fails?

(1) Check whether the PPPoE account is correct. Please see **错误!未找到引用源。**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 **错误!未找到引用源。**for details.

(4) Check whether VLAN tagging should be configured for PPPoE. VLAN tagging is disabled by default. Please see 3.2.5 for details.