



**Ruijie Reyee RG-EG Series Routers  
Web-Based Configuration Guide**

## **Copyright Statement**

Ruijie Networks©2021

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

## **Exemption Statement**

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. 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

---

Thank you for using our products.

## Audience

---

This manual is intended for:

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

## Obtaining Technical Assistance

---

- Ruijie Networks Website: <https://www.ruijienetworks.com/>
- 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](mailto:service_rj@ruijienetworks.com)
- Skype: [service\\_rj@ruijienetworks.com](https://www.ruijienetworks.com)

## Related Documents

---

Documents	Description
Command Reference	Describes the related configuration commands, including command modes, parameter descriptions, usage guides, and related examples.
Hardware Installation and Reference Guide	Describes the functional and physical features and provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors.

## Conventions

---

This manual uses the following conventions:

Convention	Description
<b>boldface font</b>	Commands, command options, and keywords are in <b>boldface</b> .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[ ]	Elements in square brackets are optional.
{ x   y   z }	Alternative keywords are grouped in braces and separated by vertical bars.
[ x   y   z ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

# 1 Overview

eWeb is a Web-based network management system that manages or configures devices. You can access eWeb via browsers such as Google Chrome.

Web-based management involves a Web server and a Web client. The Web server is integrated in a device, and is used to receive and process requests from the client, and return processing results to the client. The Web client usually refers to a browser, such as Google Chrome IE, or Firefox.

## 1.1 Conventions

In this document, texts in bold are names of buttons (for example, **OK**) or other graphical user interface (GUI) elements (for example, **DHCP Security**).

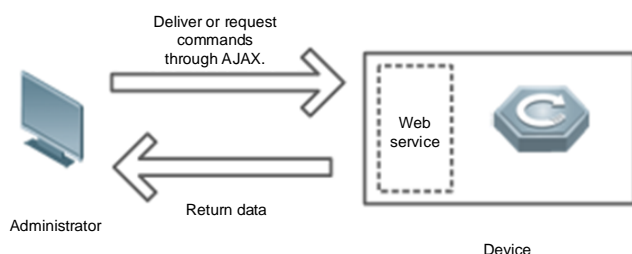
## 2 Configuration Guide

### 2.1 Preparation

#### Scenario

As shown in the figure below, an administrator can access the device from a browser and configure the device through the eWeb management system.

Figure 2-1 Data Exchange Principle



<b>Remarks</b>	The eWeb management system combines various device commands and then delivers them to the device through AJAX requests. The device then returns data based on the commands. A Web service is available on the device to process basic HTTP protocol requests.
----------------	---

#### Deployment

##### Configuration Environment Requirements

Client requirements:

- An administrator can log into the eWeb management system from a Web browser to manage devices. The client refers to a PC or some other mobile endpoints such as laptops or tablets.
- Google Chrome, Firefox, IE10.0 and later versions, and some Chromium-based browsers (such as 360 Extreme Explorer) are supported. Exceptions such as garble or format error may occur if an unsupported browser is used.
- 1024 x 768 or a higher resolution is recommended. If other resolutions are used, the page fonts and formats may not be aligned and the GUI is less artistic, or other exceptions may occur.
- The client IP address is set in the same LAN network as the device IP address, such as 192.168.110.X. The subnet mask is 255.255.255.0. The default management address is 192.168.110.1. Alternatively, you can set the IP assignment mode to **Obtain an IP address automatically**.

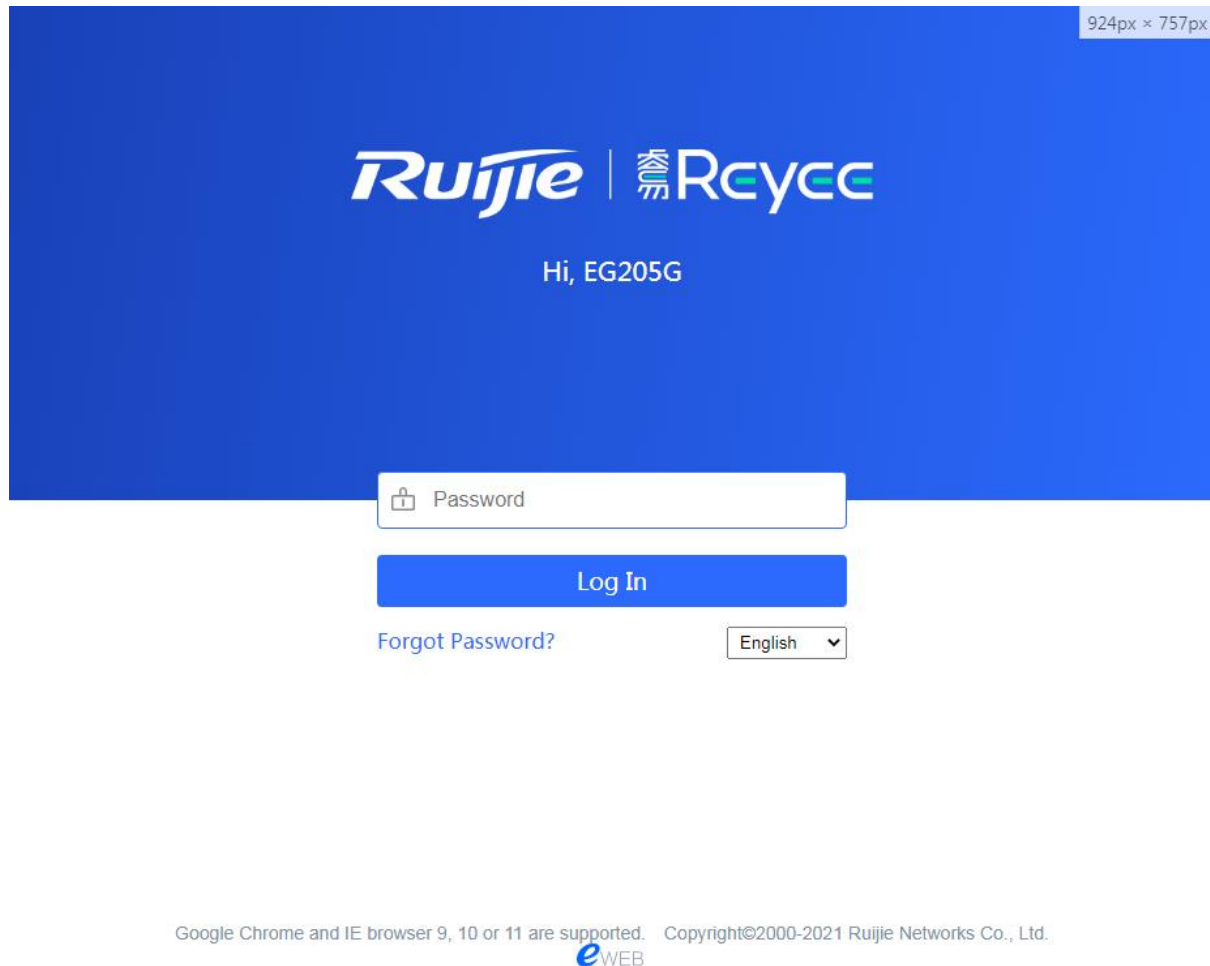
Server requirements:

- You can log into the eWeb management system through a LAN port or from Ruijie Cloud on an external network.
- The device is enabled with Web service (enabled by default).

- The device is enabled with login authentication (enabled by default).
- The default IP address of an EG device is 192.168.110.1. The default IP address of an AP is 10.44.77.254.

To log into the eWeb management system of an EG device, open the Google Chrome browser, and enter 192.168.110.1 into the address bar, and press **Enter**.

Figure 2-2 Login Page



Enter the password and click **Login**.

## 2.2 Network Setup

You will enter the **Network Setup** page without login at initial setup.

### 2.2.1 Discover Device

The page displays online device count and network status.

You can add the device to **My Network** before configuring the network. If the device works in the standalone mode, this feature is not supported.

Figure 2-3 Discover Device

Total Devices: 4. Other Devices (to be added manually): 1.

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

Net Status ( **Online Devices** / Total ) Refresh ↻

Internet — Router 1 — Switch 0 / 0 — APs 2 / 3 — Other Devices 1

---

**My Network**

eg205g (3 devices) ▼

	Model	SN	IP Address	MAC	Software Ver
<span>Local</span> Router	EG205G [Master]	H1LA0U100362A	192.168.110.1	00:74:9C:87:6D:85	[blurred]
AP	EAP101	CAL91GE01601C	192.168.110.249	00:74:9C:63:81:1A	[blurred]
AP	EAP602	MACC522376524	192.168.110.200	00:10:F8:75:33:72	[blurred]

## 2.2.2 Add to My Network

Select the target device and click **Add to My Network**. If the target device is not configured yet, you can add the device directly without a password.

Figure 2-4 Add Device to My Network

Total Devices: 3. Other Devices (to be added manually): 1.

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

Net Status ( **Online Devices** / Total ) Refresh ↻

Internet — Router 1 — Switch 0 / 0 — APs 1 / 4 — Other Devices 1

---

**My Network**

eg205g (2 devices) ▼

	Model	SN	IP Address	MAC	Software Ver
<span>Local</span> Router	EG205G [Master]	H1LA0U100362A	192.168.110.1	00:74:9C:87:6D:85	[blurred]
AP	EAP101	CAL91GE01601C	192.168.110.249	00:74:9C:63:81:1A	[blurred]

**Other Devices** ⓘ

Unnamed Network (1 devices) Add to My Network

## 2.2.3 Create Network & Connect

If the device is configured for the first time, the network name, management password and SSID are required. If the device is already configured, the management password will not be displayed here. You can navigate to **Network > Password** to change the management password.



If the device is detected disconnected to Ruijie Cloud, the Ruijie Cloud page will be embedded for you to bind your account after the device accesses the Internet successfully. If the device is already connected to Ruijie Cloud, the eWeb homepage will be displayed after this step.

Figure 2-5 Create Network

\* Network Name

IP Assignment  PPPoE  DHCP  Static IP  
Current Settings: DHCP

\* SSID

Security  Open

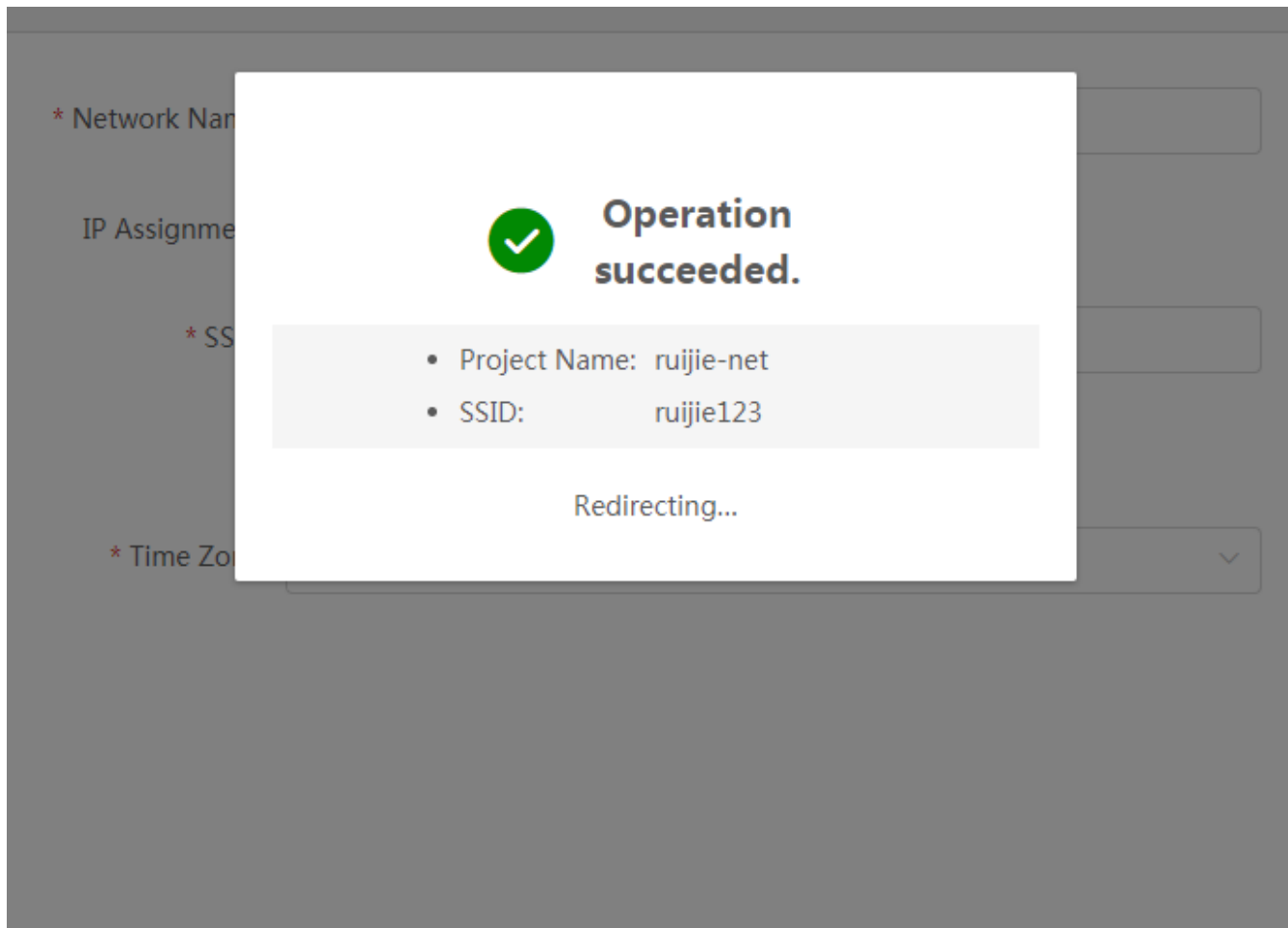
\* WiFi Password

\* Country/Region

\* Time Zone

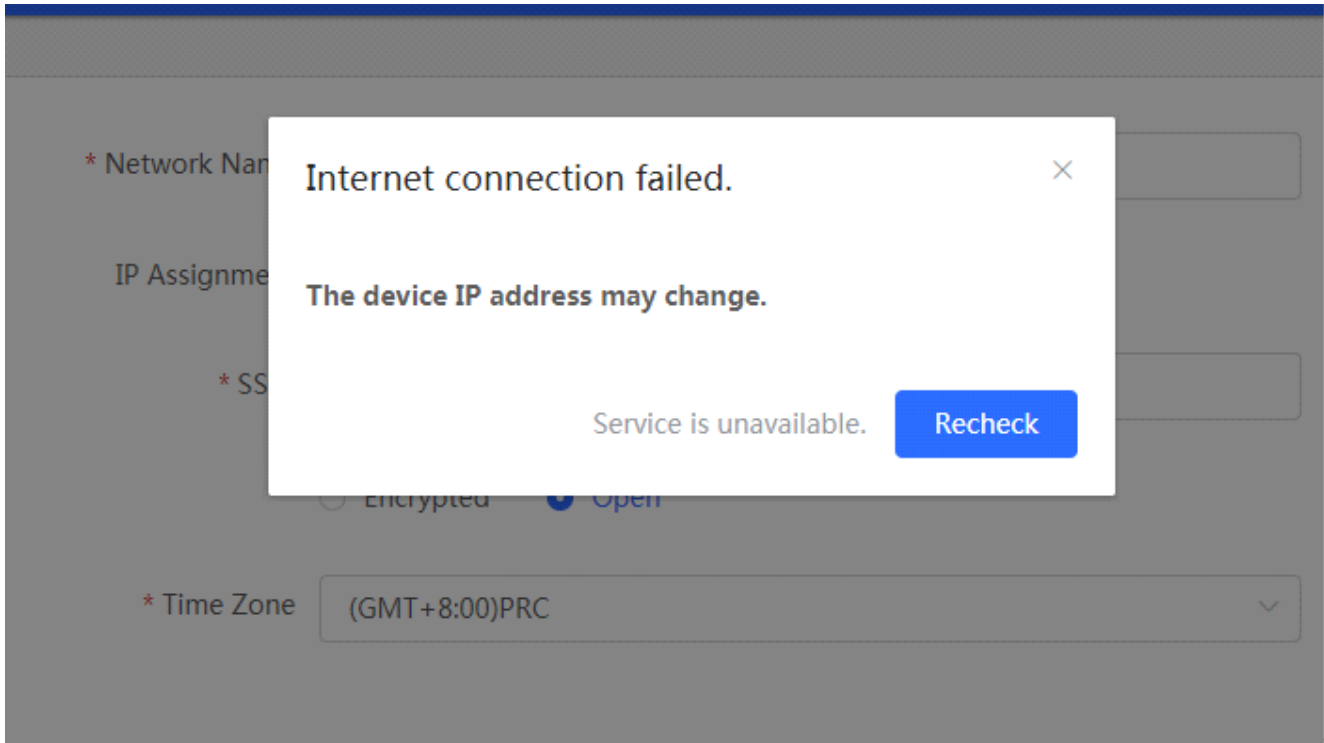
Click **Create Network & Connect**, and it takes about 60 seconds to deliver and activate settings. The following message will appear after Internet connection is set up.

Figure 2-6 Connect to Internet



If the Internet connection failed, please follow the instruction in the prompt message.

Figure 2-7 Failed Connection



## 2.2.4 Cloud Service

The **Network Setup** module requires a Ruijie Cloud account. If you are a new user, please register an account first at the [Ruijie Cloud](#) website.

Figure 2-8 Log In with Ruijie Cloud Account

Please enter your account to log in.

Please enter the username.

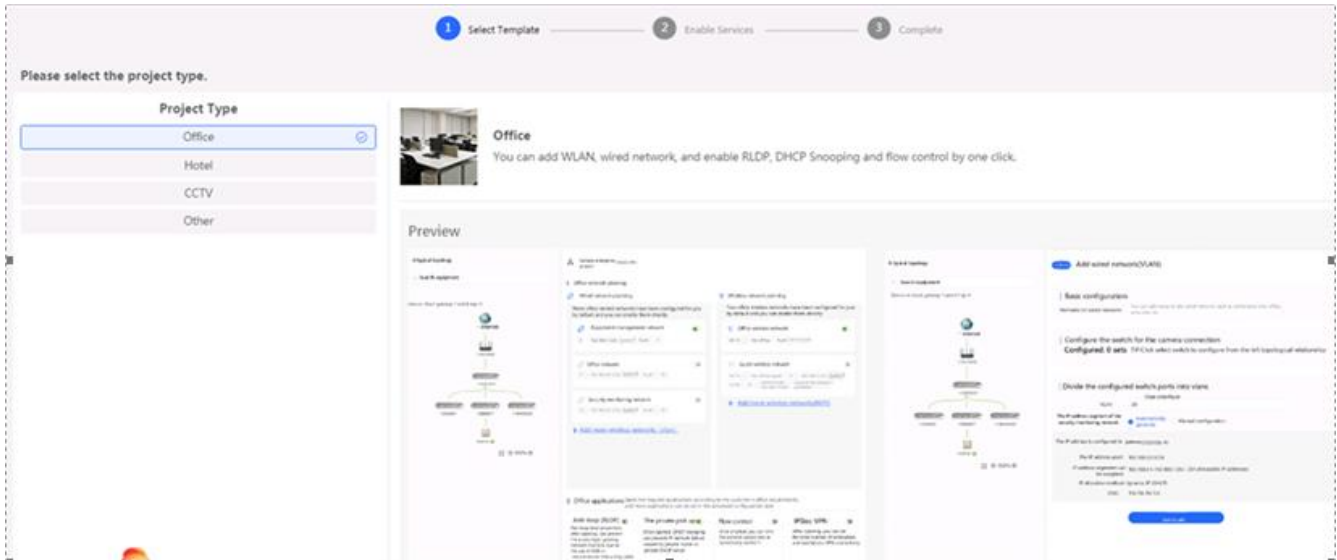
Please enter the password.

Login

I have read and agreed to [the Privacy Policy](#).

If the device works in the standalone mode, log in and the account will be binded with Ruijie Cloud automatically. If the device works in the self-organizing network mode, the following page will appear.

Figure 2-9 Select Template



It takes about 3 minutes to discover devices and generate a topology. The following confirmation box will appear:

Figure 2-10 Confirm Device Status

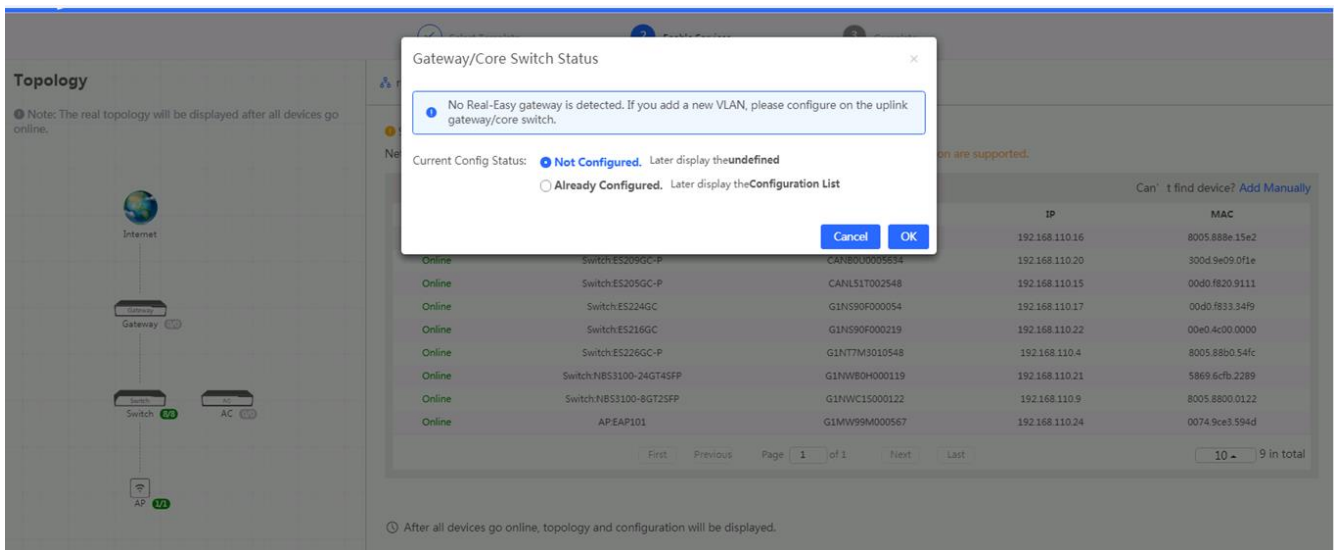
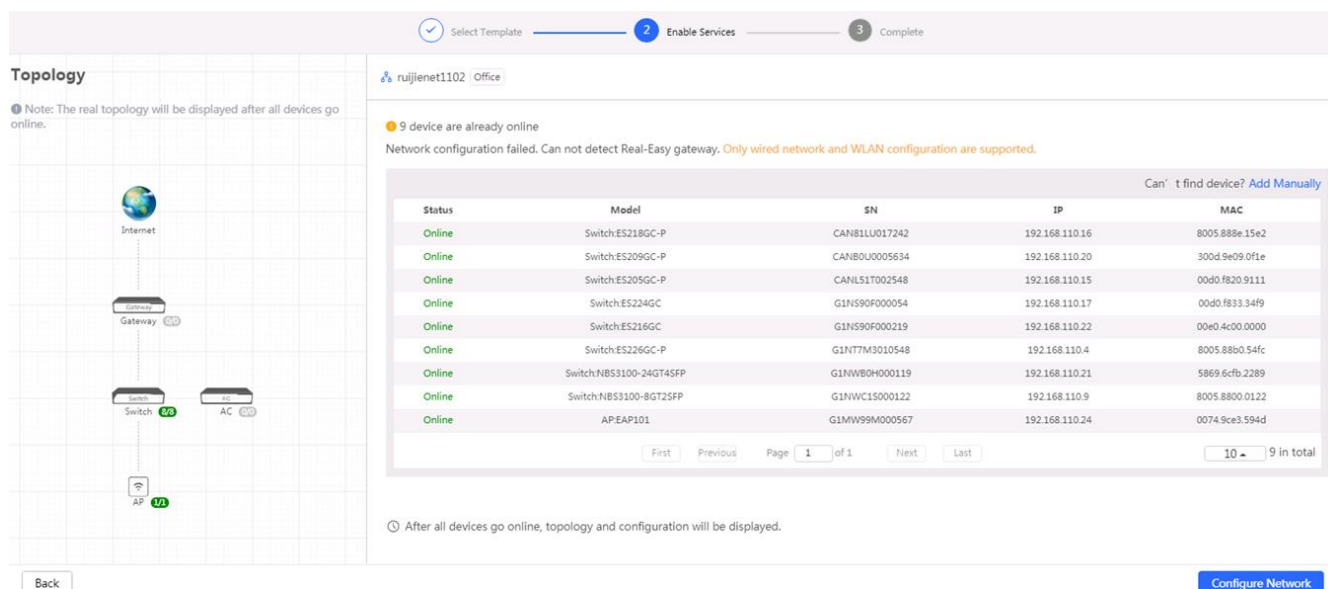


Figure 2-11 Enable Services



Click **Apply Config**. The following page will appear after configuration is delivered successfully.

Figure 2-12 Complete



## 2.3 Work Mode

The eWeb menu varies with different work modes. The EG device works in the **Router** mode and the EAP device works in the **AP** mode by default. The work mode is displayed on the **Route > Overview** page.

Figure 2-13 Device Overview

The screenshot displays the configuration page for a Ruijie EG205G router. At the top, the device is identified as a Router (EG205G) with Hostname: Ruijie.abc, SN: H1LA0U100362A, and IP Address: 172.30.111.17. A Reboot button is visible in the top right corner. Below the header is a navigation menu with tabs for Overview, Basics, Security, Behavior, VPN, Advanced, Diagnostics, and System. The Overview section shows Memory Usage at 26%, 4 Online Clients, and a Status of Online with a duration of 7 days 23 hours 28 minutes 56 seconds. The Device Details section lists Model: EG205G, SN: H1LA0U100362A, Work Mode: Router, Hardware Ver: 1.00, Hostname: Ruijie.abc, MAC: 00:74:9C:87:6D:85, Role: Master AC, and Software Ver. The Interface Details section shows a legend for Connected (blue) and Disconnected (grey) states, with LAN0 and WAN interfaces connected and showing IP addresses 192.168.110.1 and 172.30.111.17 respectively.

Click the current work mode, and the following page will appear. You can switch over the work mode here.

Figure 2-14 Work Mode

**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.
5. The device will be restored and rebooted upon mode change.

Work Mode  ?

Self-Organizing  ? **Tip**

Network

AC  ?

### 2.3.1 Router Mode

The **Router** mode indicates NAT forwarding.

The EG device in the **Router** mode contains networking, network setup and gateway features including VPN and behavior management.

The AP in the **Router** mode contains networking, network setup and some radio features.

### 2.3.2 AC/AP Mode

The device in the **AC** mode supports router-on-a-stick.

The **AP** mode refers to fit AP mode. All WAN ports are enabled with DHCP by default. You can configure a WAN port with a static IP address or enable PPPoE manually.

## 2.4 Self-Organizing Network

Click the current work mode, and the following page will appear. You can enable or disable self-organizing network here.

Figure 2-15 Self-Organizing Network

### 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.
5. The device will be restored and rebooted upon mode change.

Work Mode

Self-Organizing    **Tip**

Network

AC

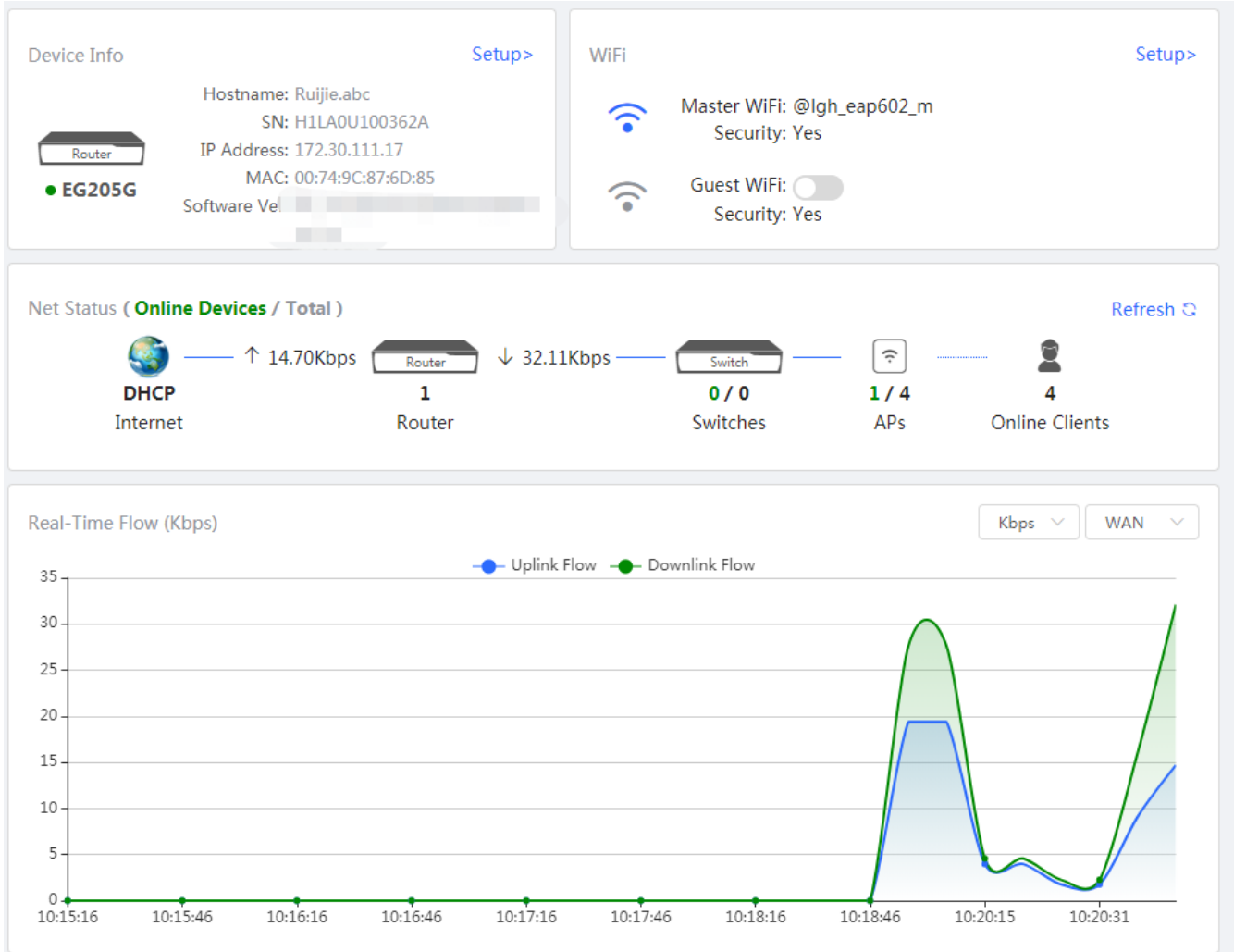
### 2.4.1 Enable

If self-organizing network is enabled, the device in the network will be discovered and discover other devices. These devices will form a network and be synchronized with network settings.

The menu on the left contains all network settings, including wireless management, switch management and system management.

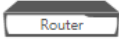
Figure 2-16 Enable Self-Organizing Network





If there is a wireless router enabled with self-organizing network in the network, the **Router** module will appear in the menu on the left. Click **Router** [Gateway](#), and a horizontal menu will be displayed.

Figure 2-17 Router Menu



Router

● **EG205G**

Hostname: Ruijie.abc      SN: H1LA0U100362A      IP Address: 172.30.111.17  
MAC: 00:74:9C:87:6D:85

[Reboot](#)

[Overview](#) [Basics](#) [Security](#) [Behavior](#) [VPN](#) [Advanced](#) [Diagnostics](#) [System](#)

### Overview






Memory Usage <b>26%</b>	Online Clients <b>4</b>	Status: <b>Online</b> Duration: 7 days 23 hours 30 minutes 23 seconds System: 2021-03-02 10:22:09
----------------------------	----------------------------	---

### Device Details

Model: EG205G	Hostname: <a href="#">Ruijie.abc</a>
SN: H1LA0U100362A	MAC: 00:74:9C:87:6D:85
Work Mode: <a href="#">Router</a>	Role: Master AC
Hardware Ver: 1.00	Software Ver: [blurred]

### Interface Details

Connected     Disconnected

 LAN0	 LAN1/WAN3	 LAN2/WAN2	 LAN3/WAN1	 WAN
	192.168.110.1			172.30.111.17

## 2.4.2 Disable

If self-organizing network is disabled, the device will work in the standalone mode.

After self-organizing network is disabled, a horizontal menu will be displayed vertically on the left.

Figure 2-18 Disable Self-Organizing Network

The screenshot displays a web interface for a network device configuration. On the left is a vertical navigation menu with the following items: Overview (selected), Online Clients, Basics, Security, Behavior, VPN, Advanced, Diagnostics, and System. The main content area is divided into three sections:

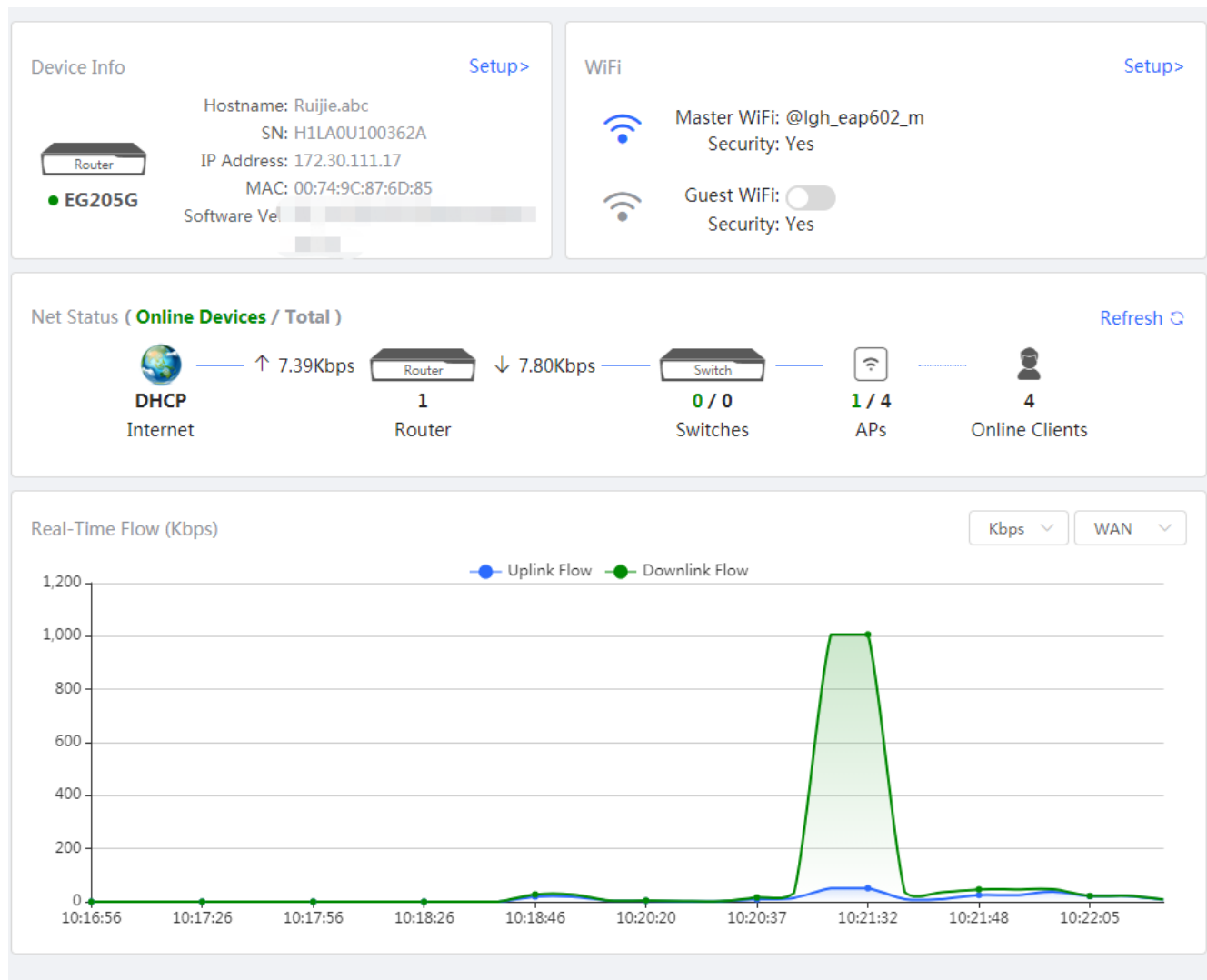
- Overview:** Contains three summary cards: Memory Usage at 30%, Online Clients at 6, and Status: Online with a duration of 44Min16Sec and system time of 2020-12-17 14:55:25.
- Device Details:** Lists hardware and software information: Model: EG205G, Hostname: Ruijie, SN: H1LA0U100362A, MAC: 00:74:9C:87:6D:85, Work Mode: Router, Hardware Ver: 1.00, and Software Ver: [redacted].
- Interface Details:** Shows a status bar for Connected and Disconnected interfaces. Below are five interface icons: LAN0 (connected), LAN1/WAN3 (connected, IP 192.168.110.1), LAN2/WAN2 (disconnected), LAN3/WAN1 (disconnected), and WAN (connected, IP 172.30.111.17).

### 3 eWeb Configuration

#### 3.1 Overview

The **Overview** page displays login device, wireless information, network status and real-time flow.

Figure 3-1 Overview



#### 3.2 Online Clients

The **Online Clients** module is supported by the **Router** mode of the EG device.

Figure 3-2 Online Clients

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

**Online Clients** Search by IP/MAC/Username  Refresh

Username/Type	IP Address/MAC	Current Rate	Wireless Info	Access Control
RAP2200E-150848 <span>Wired</span>	192.168.110.152 00:d0:f8:15:08:48	Up:0.00bps Down:0.00bps	--	<a href="#">Go</a>
EW1800GX-PRO-8C5826 <span>Wired</span>	192.168.110.14 30:0d:9e:8c:58:26	Up:2.96Kbps Down:5.87Kbps	--	<a href="#">Go</a>
R03605 <span>Wired</span>	192.168.110.136 c8:5b:76:94:00:3c	Up:211.00bps Down:0.00bps	--	<a href="#">Go</a>
-- <span>Wired</span>	192.168.110.13 90:e7:10:db:20:ae	Up:853.00bps Down:628.00bps	--	<a href="#">Go</a>

< 1 > 10/page Total 4

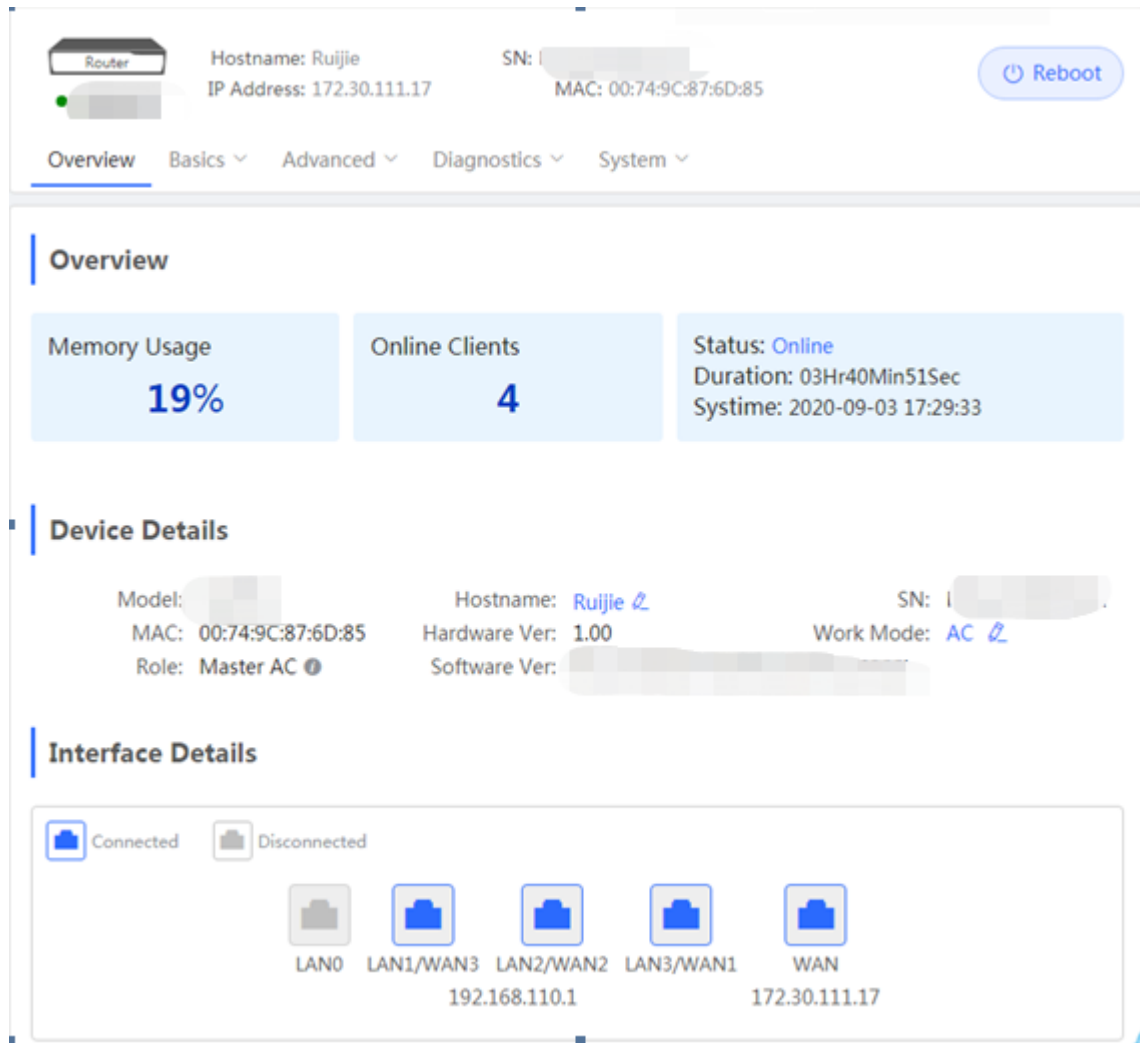
### 3.3 Router

If there is a wireless router enabled with self-organizing network in the network, the **Gateway** module will appear in the menu on the left. Click **Router**, and a horizontal menu will be displayed.

#### 3.3.1 Overview

If the EG device works in the **AC** mode, the **Router** module does not contain **Security**, **Behavior** and **VPN**.

Figure 3-3 Overview



This chapter describes the Web configuration process of an EG device in the **Router** mode.

Figure 3-4 Router Mode

The screenshot displays the Ruijie eWeb configuration interface for a Router (EG205G). At the top, it shows the Hostname (Ruijie.abc), SN (H1LA0U100362A), IP Address (172.30.111.17), and MAC (00:74:9C:87:6D:85). A Reboot button is visible in the top right. Below this is a navigation menu with tabs for Overview, Basics, Security, Behavior, VPN, Advanced, Diagnostics, and System. The Overview section shows Memory Usage at 24%, 4 Online Clients, and a Status of Online with a duration of 7 days 23 hours 34 minutes 30 seconds and a system time of 2021-03-02 10:26:16. The Device Details section lists Model (EG205G), SN (H1LA0U100362A), Work Mode (Router), Hardware Ver (1.00), Hostname (Ruijie.abc), MAC (00:74:9C:87:6D:85), Role (Master AC), and Software Ver. The Interface Details section shows a legend for Connected (blue) and Disconnected (grey) states, with LAN0, LAN1/WAN3, LAN2/WAN2, LAN3/WAN1, and WAN interfaces. LAN0 and WAN are connected, while the others are disconnected. The IP address 192.168.110.1 is associated with LAN1/WAN3 and LAN2/WAN2, and 172.30.111.17 is associated with LAN3/WAN1 and WAN.

### 3.3.2 Basics

#### 3.3.2.1 WAN

The **WAN** module allows you to configure WAN settings. There are three Internet types available: **Static IP Address**, **DHCP** and **PPPoE**. WAN settings support multiple lines (some models support only dual-line). If you select more than one line, you can configure each specific line, e.g., WAN and WAN1, and ISP/load settings.

Figure 3-5 WAN Settings

**WAN Settings**  
Configure WAN settings. ?

**Single Line** | Dual-Line | Three Lines | Four Lines

\* Internet

No username or password is required for DHCP clients.

IP Address 172.30.111.17

Subnet Mask 255.255.255.0

Gateway 172.30.111.1

DNS Server 172.30.44.20 192.168.5.28

---

[Advanced Settings](#)

\* MTU  Range: 576-1500.

\* MAC

802.1Q Tag

\* Default Preference  A smaller value indicates a higher preference.

Private Line  ?

**Save**

Figure 3-6 ISP/Load Settings



WAN Settings
?

Configure WAN settings.

Single Line
Dual-Line
Three Lines
Four Lines

WAN
WAN1
WAN2
ISP/Load Settings

### Load Balancing Settings

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

i 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

\* WAN2 Weight 1

Save

### 3.3.2.2 LAN

The LAN module contains LAN Settings, Port VLAN, DHCP Clients, Static IP Addresses, DHCP Option and DNS Proxy.

#### 3.3.2.2.1 LAN Settings

The LAN module allows you to set the IP address of the LAN port and DHCP status.

Figure 3-7 LAN Settings

**LAN Settings** ⓘ

**LAN Settings** + Add Delete Selected

Up to 8 entries can be added.

<input type="checkbox"/>	IP Address	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
<input type="checkbox"/>	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	254	30	<a href="#">Edit</a> <a href="#">Delete</a>

Click **Add** to add a VLAN. In the displayed dialog box, configure settings and click **OK**.

Figure 3-8 Add IP Address

**Add** ⓘ

\* IP Address

\* Subnet Mask

\* VLAN ID

Remark

\* MAC

DHCP Server

\* Start

\* IP Count

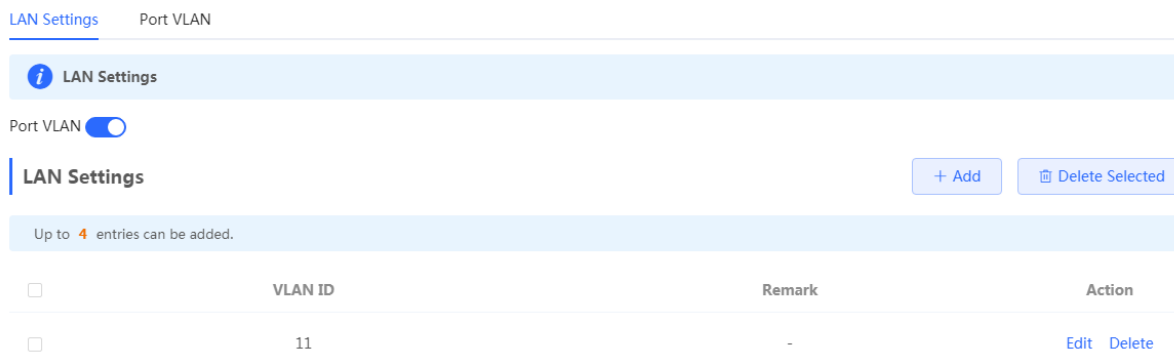
\* Lease Time(Min)

DNS Server - ⓘ

You can click ⓘ in the upper right corner to see description about each configuration item.

If an EAP device working in the AP mode supports port VLAN, there will be a port VLAN toggle displayed here.

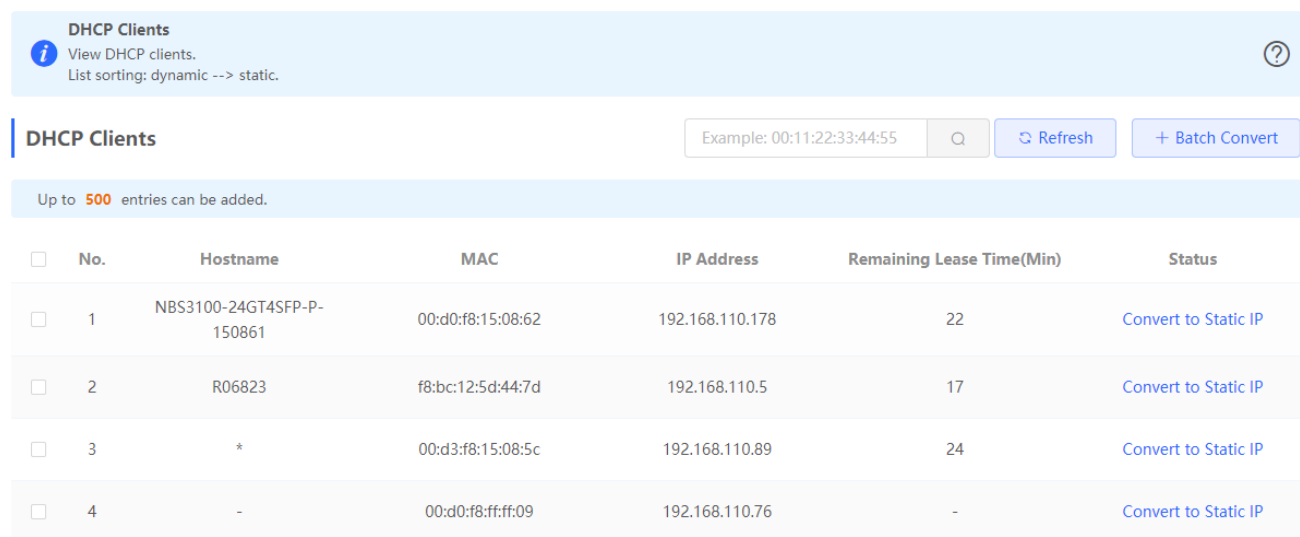
Figure 3-9 Port VLAN



### 3.3.2.2.2 DHCP Clients

The **DHCP Clients** page displays DHCP clients.

Figure 3-10 DHCP Clients

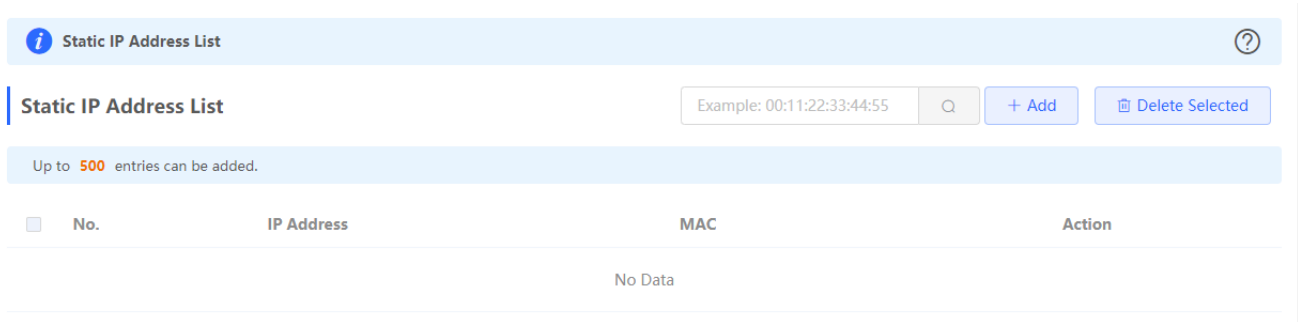


Click **Convert to Static IP** in the **Action** column to convert a DHCP-assigned IP address to a static IP address. Alternatively, select DHCP-assigned IP addresses and click **Batch Convert** to convert more than one IP address.

### 3.3.2.2.3 Static IP Addresses

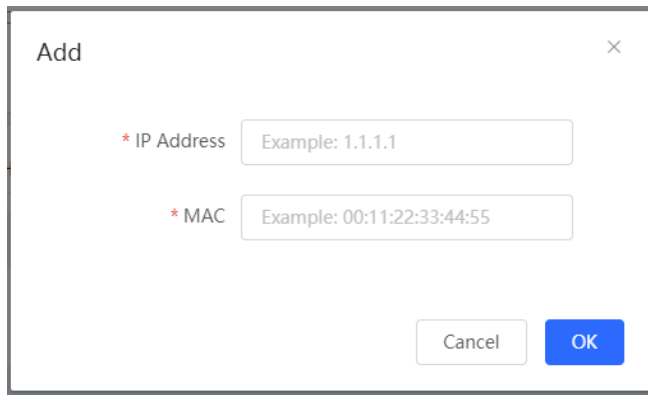
The **Static IP Addresses** module allows you to add, delete and edit static IP addresses.

Figure 3-11 Static IP Addresses



Click **Add** to add a static IP address manually. In the displayed dialog box, configure settings and click **OK**.

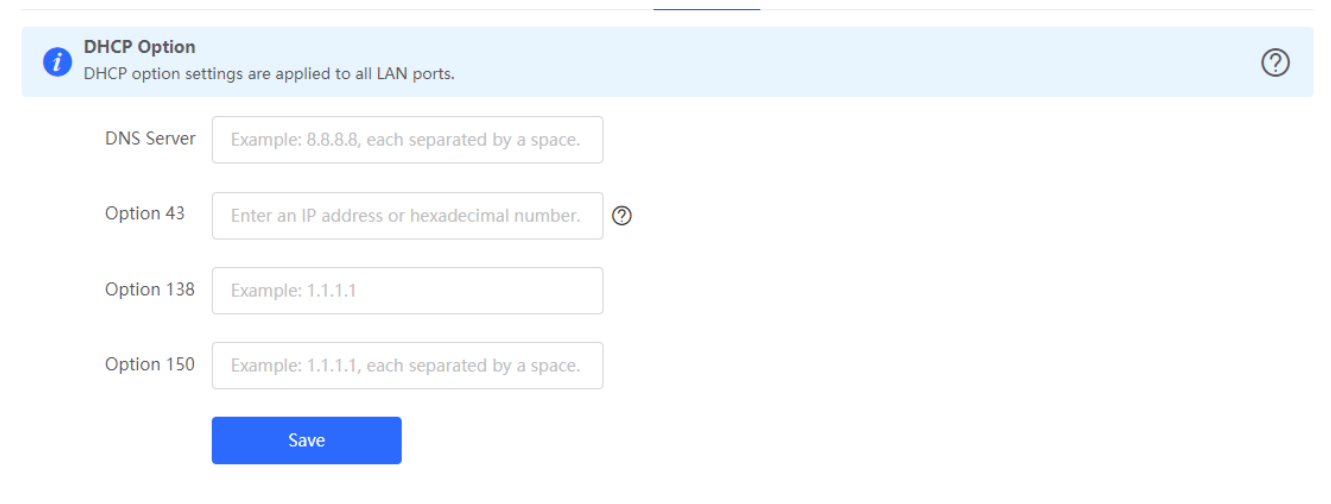
Figure 3-12 Add Static IP Address



### 3.3.2.2.4 DHCP Option

The **DHCP Option** module allows you to configure DHCP option settings.

Figure 3-13 DHCP Option



### 3.3.2.2.5 DNS Proxy

The **DNS Proxy** module allows you to configure DNS proxy settings.

Figure 3-14 DNS Proxy



### 3.3.2.3 IPv6 Address

After you enable **IPv6 Address**, the IPv6 tab pages of all WAN ports will be displayed in **WAN Settings**.

Figure 3-15 WAN Settings

### IPv6 Address

**i** 1. When IPv6 is enabled, the MTU of IPv4 WAN port must be greater 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.

IPv6 Address

[WAN Settings](#)   [LAN Settings](#)   [DHCPv6 Client](#)

**WAN\_V6**

\* Internet

No username or password is required for DHCP clients.

IPv6 Address 0:0::0

IPv6 Prefix

Gateway 0:0::0

DNS Server 0:0::0

NAT66

---

[Advanced Settings](#)

\* Default Preference  A smaller value indicates a higher preference.

Figure 3-16 LAN Settings

**IPv6 Address**

- 1. When IPv6 is enabled, the MTU of IPv4 WAN port must be greater 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.

IPv6 Address

WAN Settings   **LAN Settings**   DHCPv6 Client

**LAN Settings** + Add   Delete Selected

Up to 8 entries can be added.

<input type="checkbox"/>	VLAN ID	IPv6 Assignment	Subnet Prefix Name	Subnet ID	Subnet Prefix Length	IPv6 Address/Prefix Length	Action
<input type="checkbox"/>	Default	Auto		0	64		Edit Delete

Figure 3-17 Add LAN

Add ×

\* VLAN ID

IPv6 Assignment  ?

IPv6 Address/Prefix   ?  
Length

----- Advanced Settings -----

Subnet Prefix Name  ?

Subnet Prefix Length  ?

Subnet ID  ?

\* Lease Time(Min)  ?

DNS Server

Figure 3-18 DHCPv6 Client

**IPv6 Address**

- 1. When IPv6 is enabled, the MTU of IPv4 WAN port must be greater 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.

IPv6 Address

WAN Settings   LAN Settings   DHCPv6 Client

**DHCP Clients**

You can view the DHCP client information on this page.

**DHCP Clients**

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

< 1 > 10/page Total 0

### 3.3.2.4 PoE

The **PoE** page displays PoE status and power consumption. Only the models ending with -P, e.g., EG105G-P and EG210G-P, support this feature.

Figure 3-19 PoE

**PoE**

**PoE Consumption Details**

Max Consumption	Current Consumption	Remaining Consumption
30.0W	0.0W	30.0W

**PoE Device Panel**

Powered On    Powered Off

Current Consumption: 0.0W

Current Consumption: 0.0W

0

### 3.3.2.5 IPTV/VLAN

Figure 3-20 IPTV/VLAN



**i** IPTV/VLAN settings.

### IPTV/VLAN

\* Mode

\* LAN0

\* LAN1

\* LAN2

\* LAN3/WAN1

\* IPTV VLAN ID

\* IP-Phone VLAN ID

Internet VLAN  802.1Q Tag

#### 3.3.2.6 Port VLAN

The **Port VLAN** page displays VLAN information.

Figure 3-21 Port VLAN





**Port VLAN** ?

Please choose [LAN Settings](#) to create a VLAN first and configure port settings based on the VLAN.

---

**Port VLAN**

Connected  Disconnected

	 <b>Port 0</b>	 <b>Port 1</b>	 <b>Port 2</b>	 <b>Port 3</b>
Default VLAN	UNTAG ▾	UNTAG ▾	UNTAG ▾	UNTAG ▾

### 3.3.3 Security

#### 3.3.3.1 ARP List

The **ARP List** page displays ARP entries.

Figure 3-22 ARP List

### ARP List



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

ARP Guard

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

### ARP List

Example: 1.1.1.1



+ Add

Delete Selected

Up to 256 IP-MAC bindings can be added.

<input type="checkbox"/>	No.	MAC	IP Address	Type	Action
<input type="checkbox"/>	1	00:d3:f8:15:08:5c	192.168.110.89	Dynamic	Bind
<input type="checkbox"/>	2	00:d0:f8:15:10:68	192.168.110.212	Dynamic	Bind
<input type="checkbox"/>	3	00:d0:f8:15:08:62	192.168.110.178	Dynamic	Bind
<input type="checkbox"/>	4	f8:bc:12:5d:44:7d	192.168.110.5	Dynamic	Bind
<input type="checkbox"/>	5	00:d0:f8:15:01:a8	192.168.110.33	Dynamic	Bind
<input type="checkbox"/>	6	00:74:9c:71:00:b9	172.30.111.1	Dynamic	Bind

Total 6

10/page



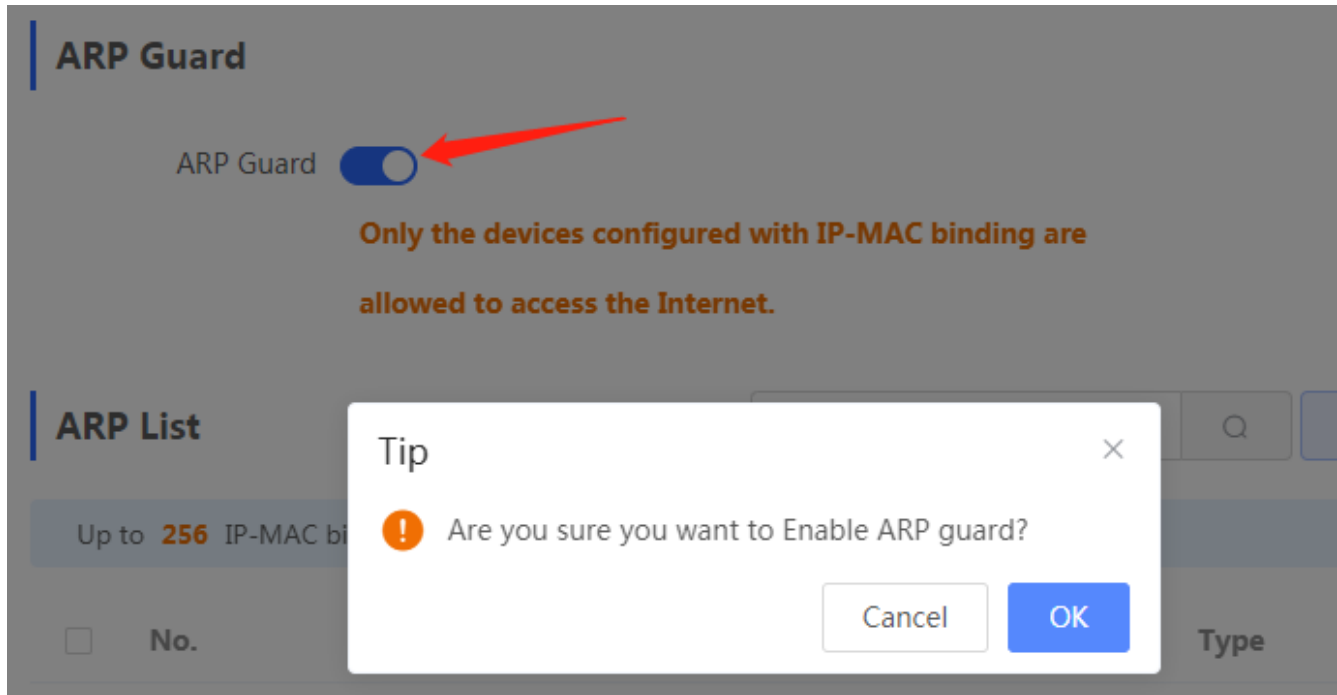
1



Go to page

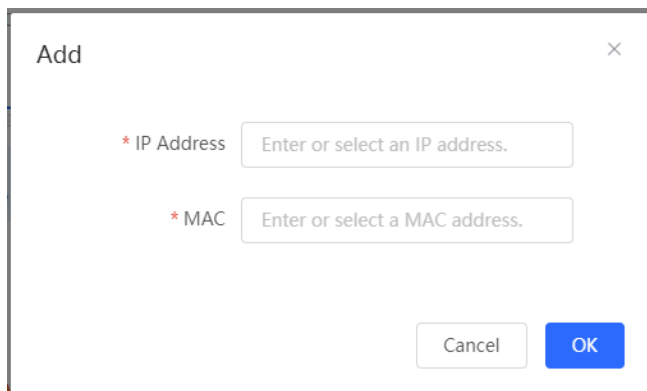
1

Figure 3-23 ARP Guard



Click **Add** to add an IP-MAC binding. In the displayed dialog box, enter or select an IP address and a MAC address and click **OK**.

Figure 3-24 Add IP-MAC Binding



Click **Delete** in the **Action** column. The message "Are you sure you want to delete the entry?" is displayed. In the displayed dialog box, click **OK**. The message "Delete operation succeeded." is displayed.

### 3.3.3.2 MAC Filtering

The **MAC Filtering** module allows you to add, delete and edit MAC filtering entries.

Figure 3-25 MAC Filtering

i **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

Save

### Filtering Rule List

+ Add
Delete Selected

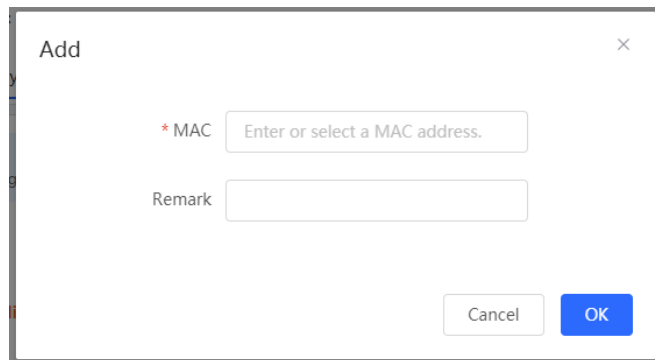
Up to 80 rules can be added.

	MAC	Remark	Action
☐			
No Data			

< 1 >
10/page
Total 0

Click **Add** to add a filtered MAC address. In the displayed dialog box, enter or select a MAC address and click **OK**.

Figure 3-26 Add Filtered MAC Address



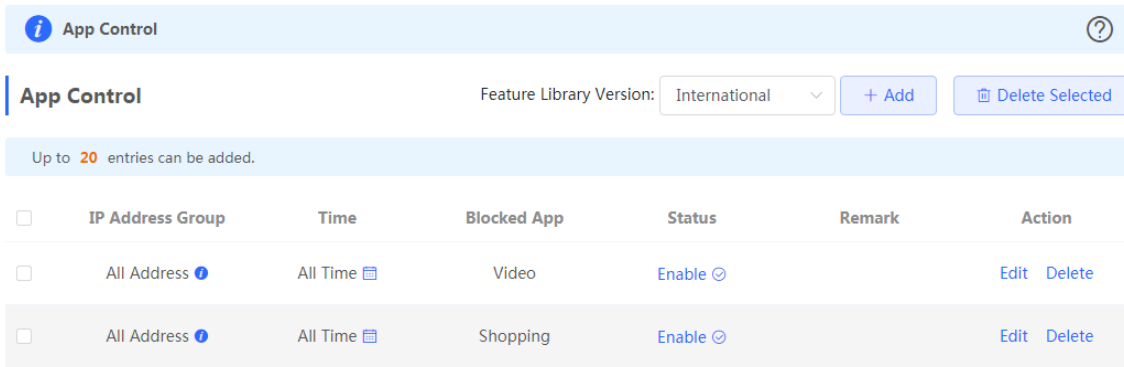
Click **Delete** in the **Action** column. The message "Are you sure you want to delete the entry?" is displayed. In the displayed dialog box, click **OK**. The message "Delete operation succeeded." is displayed.

### 3.3.4 Behavior

#### 3.3.4.1 App Control

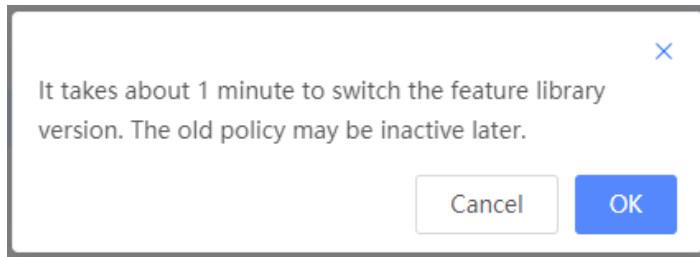
The **App Control** module allows you to add, delete and edit application control policies.

Figure 3-27 App Control



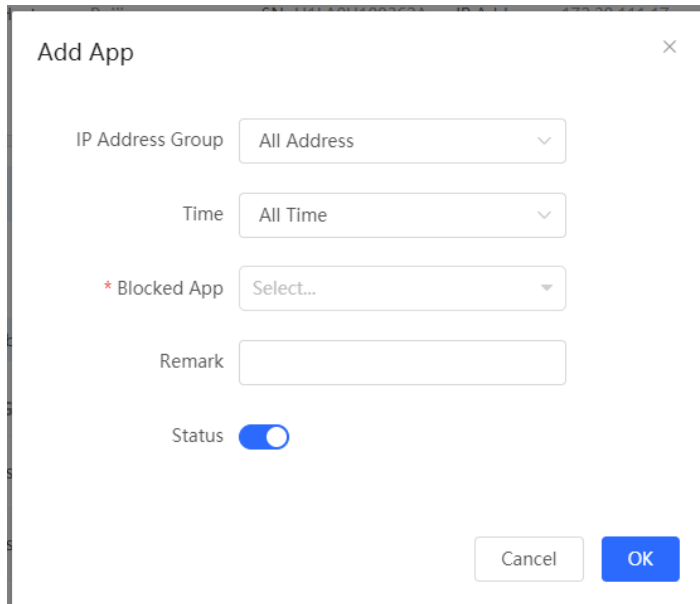
Select a feature library version from the dropdown list. In the displayed dialog box, click **OK** to confirm switchover.

Figure 3-28 Switch Feature Library Version



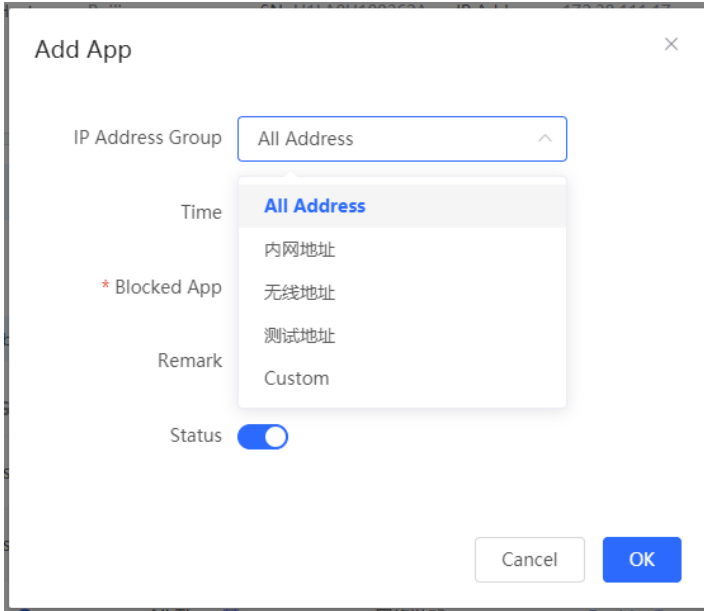
Click **Add** to add an application control policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-29 Add Application Control Policy



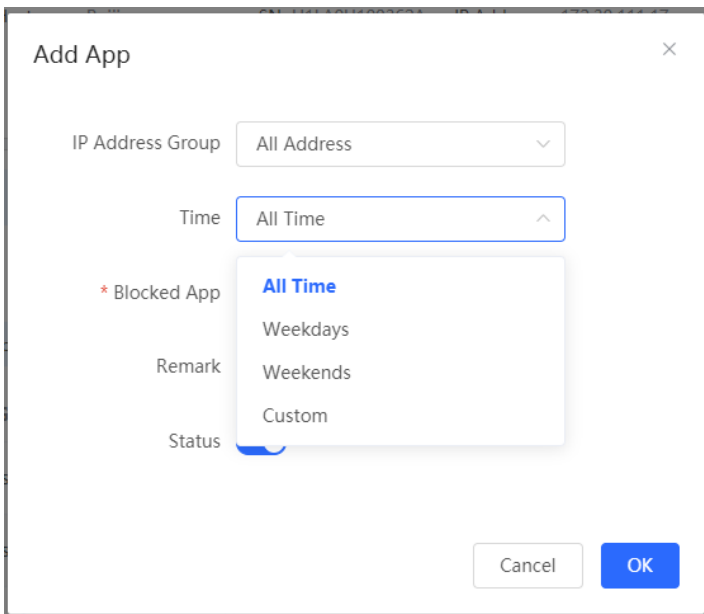
Define IP address groups on the **Address Management** page and you can select IP address groups here.

Figure 3-30 Select IP Address Group



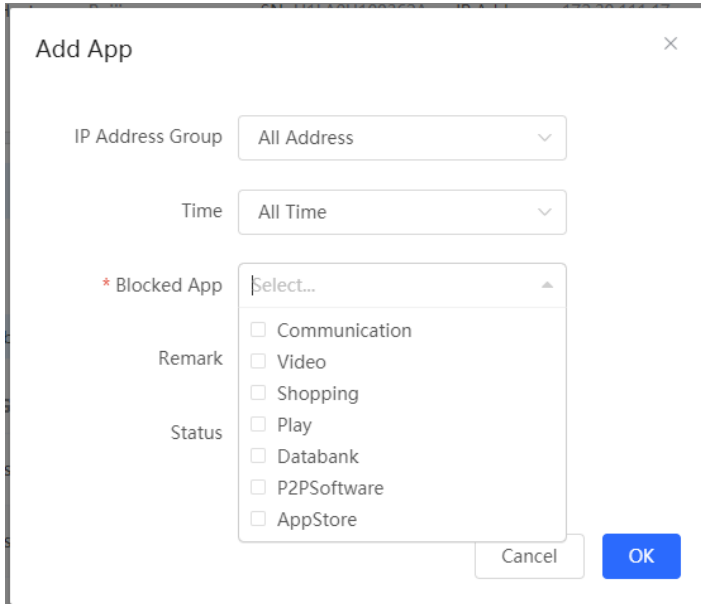
Define time objects on the **Time Management** page and you can select time objects here.

Figure 3-31 Select Time



Select the target application from the **Blocked App** dropdown list and click **OK**.

Figure 3-32 Select Blocked App

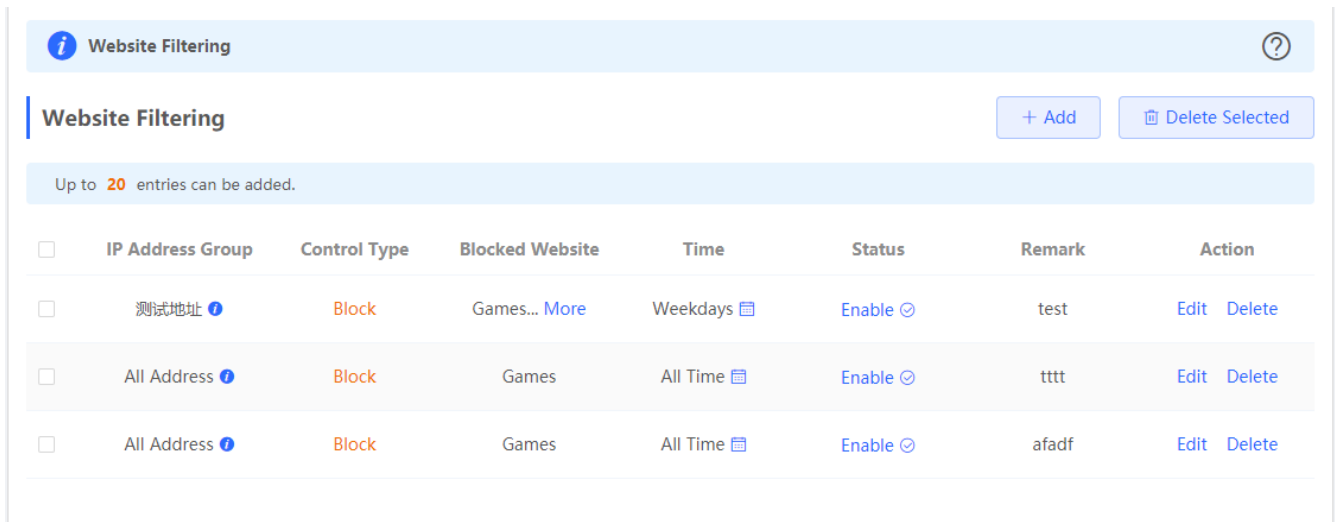


### 3.3.4.2 Website Management

#### 3.3.4.2.1 Website Filtering

The **Website Filtering** module allows you to add, delete and edit website filtering policies.

Figure 3-33 Website Filtering



Click **Add** to add a website filtering policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-34 Add Website Filtering Policy



Add Website Filtering
×

IP Address Group All Address ▾

Time All Time ▾

\* Blocked Website Select... ▾

Remark

Status

Cancel
OK

### 3.3.4.2.2 Website Group

The **Website Group** module allows you to add, delete and edit website grouping policies.

Figure 3-35 Website Group

Website Group
?

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

Website Group

+ Add
Delete Selected

Up to **20** entries can be added.

<input type="checkbox"/>	Group Name	Member	Action
<input type="checkbox"/>	Games	duowan.com... <a href="#">More</a>	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	Finance	*.10jqka.com.cn... <a href="#">More</a>	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	Communication	*.baihe.com... <a href="#">More</a>	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	Shopping	*.taobao.com... <a href="#">More</a>	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	Live	*.55bbs.com... <a href="#">More</a>	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	Lusic	*.1ting.com... <a href="#">More</a>	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	Entertainment	67.com... <a href="#">More</a>	<a href="#">Edit</a> <a href="#">Delete</a>

Click **Add** to add a website filtering policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-36 Add Website Grouping Policy

### 3.3.4.3 QQ Management

The **QQ Management** module allows you to add, delete and edit QQ management policies.

Figure 3-37 QQ Management

<input type="checkbox"/>	IP Address Group	Time	QQ	Status	Remark	Action
<input type="checkbox"/>	All Address <span style="color: blue;">i</span>	All Time <span style="color: blue;">📅</span>	1234567	Enable <span style="color: blue;">👁</span>	test	Edit Delete

Click **Add** to add a QQ management policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-38 Add QQ Management Policy

Add
×

IP Address Group All Address ▼

Time All Time ▼

\* QQ 

The QQ must be a string consisting of 5-11 digits, each separated by a newline character.

Remaining **199**

Remark

Status

Cancel
OK

### 3.3.4.4 Access Control

The **Access Control** module allows you to add, delete and edit access control policies.

Figure 3-39 Access Control

**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.

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

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

**ACL List** 
+ Add
Delete Selected

Up to **50** entries can be added.

	Rule	Control Type	Wireless Schedule	Interface	Effective State	Remark	Action
<input type="checkbox"/>	Src IP Address 1.1.1.1 : 1111 Dest IP Address 2.2.2.2 : 222 Protocol All Protocols	Allow	All Time	WAN	Active	test	<a href="#">Edit</a> <a href="#">Delete</a>

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

Click **Add** to add a MAC-based policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-40 Add MAC-Based ACL

The 'Add ACL' dialog box features a close button (X) in the top right corner. It contains the following fields and controls:

- Based on:** Radio buttons for 'MAC' (selected) and 'IP Address'.
- \* MAC:** A text input field with the placeholder text 'Enter a MAC address.'
- Control Type:** A dropdown menu currently set to 'Allow'.
- Wireless Schedule:** A dropdown menu currently set to 'All Time'.
- Remark:** A text input field with the placeholder text 'Enter the ACL purpose.'
- Buttons:** 'Cancel' and 'OK' buttons at the bottom right.

Click **Add** to add an IP address-based policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-41 Add IP Address-Based ACL

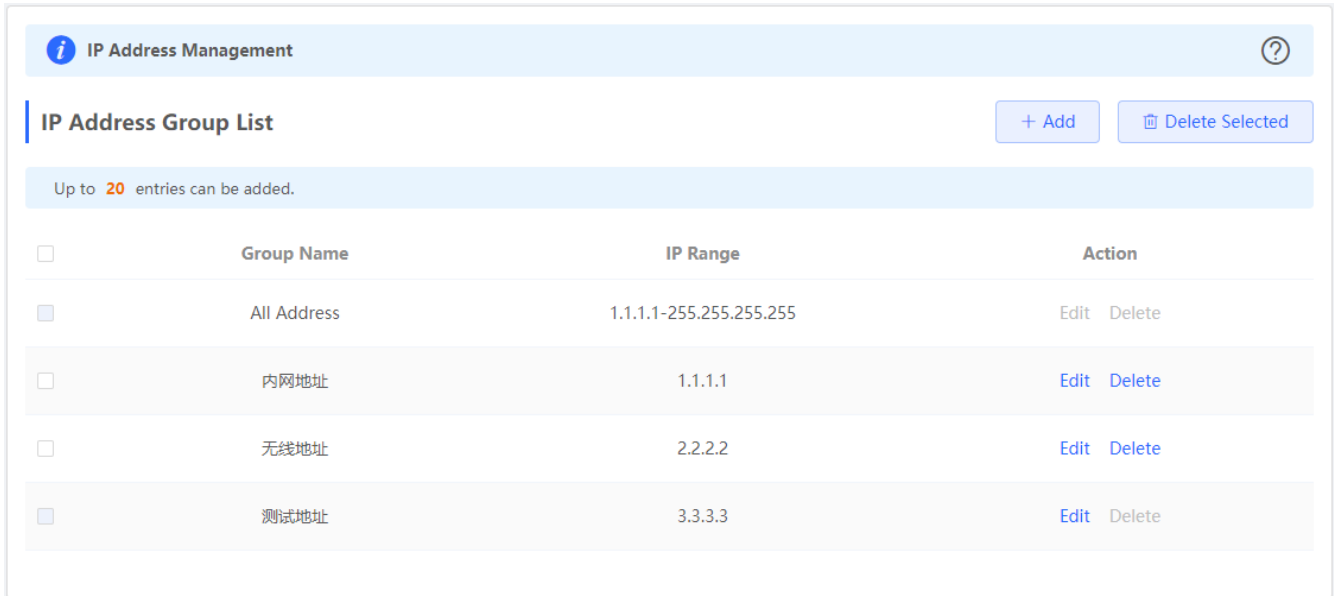
The 'Add ACL' dialog box features a close button (X) in the top right corner. It contains the following fields and controls:

- Based on:** Radio buttons for 'MAC' and 'IP Address' (selected).
- Src IP Address: Port:** Two input fields containing 'Net:192.168.1.1/24' and '1-65535' respectively, separated by a colon.
- Dest IP Address: Port:** Two input fields containing 'Net:192.168.1.1/24' and '1-65535' respectively, separated by a colon.
- Protocol Type:** A dropdown menu currently set to 'All Protocols'.
- Control Type:** A dropdown menu currently set to 'Allow'.
- Wireless Schedule:** A dropdown menu currently set to 'All Time'.
- Interface:** A dropdown menu currently set to 'WAN'.
- Remark:** A text input field with the placeholder text 'Enter the ACL purpose.'
- Buttons:** 'Cancel' and 'OK' buttons at the bottom right.

### 3.3.4.5 Address Management

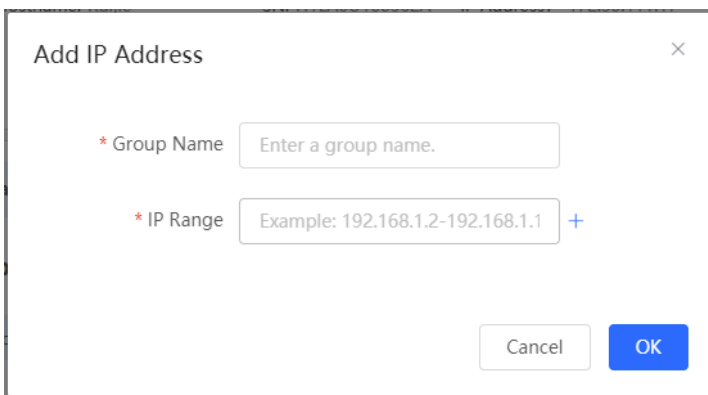
The **Address Management** module allows you to add, delete and edit IP address groups.

Figure 3-42 IP Address Management



Click **Add** to add an IP address group. In the displayed dialog box, configure settings and click **OK**.

Figure 3-43 Add IP Address Group



### 3.3.4.6 Time Management

The **Time Management** module allows you to add, delete and edit time objects.

Figure 3-3-41 Time List

**Time List** ?

**Time List** + Add Delete Selected

Up to 20 entries can be added.

<input type="checkbox"/>	Time Name	Time Span	Action
<input type="checkbox"/>	All Time		Edit Delete
<input type="checkbox"/>	Weekdays		Edit Delete
<input type="checkbox"/>	Weekends		Edit Delete

Click **Add** to add a time object. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-42 Add Time Object

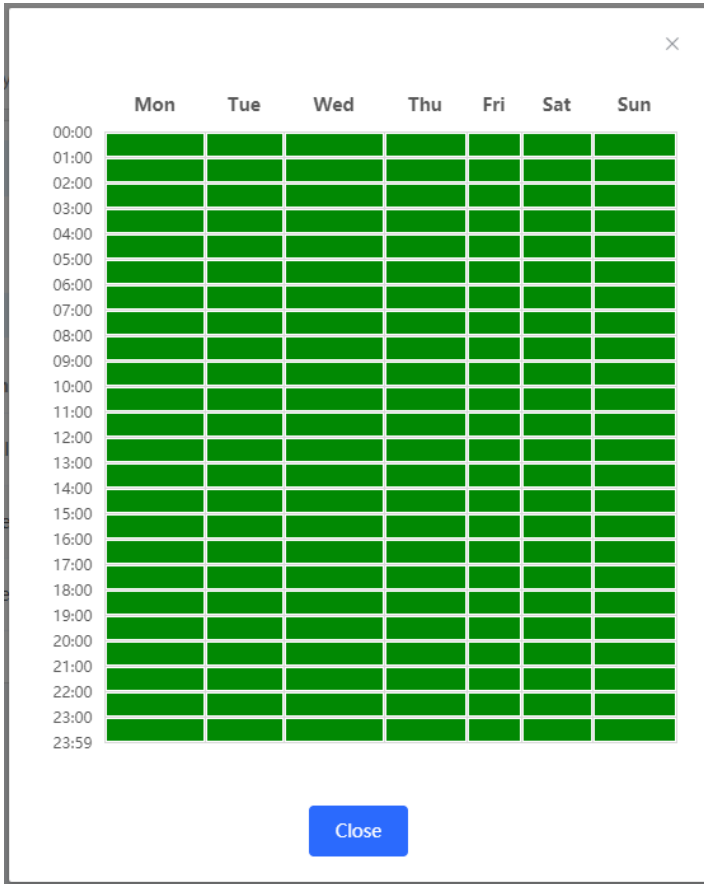
**Add Time** ×

\* Time Name

\* Time [Please Select Time](#)

Click in the time list or in the **Add Time** box, and a time management page will appear.

Figure 3-3-43 Select Time



Select the time and click **OK**.

### 3.3.5 VPN

#### 3.3.5.1 IPSec

The **IPSec** module contains **IPSec Security Policy** and **IPSec Connection Status**.

##### 3.3.5.1.1 IPSec Security Policy

The **IPSec Security Policy** module allows you to add, delete and edit IPSec security policies.

Figure 3-3-44 IPSec Security Policy

**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
Client	aaa	1.1.1.1	1.1.1.0/24	2.1.1.0/24	Enable ☺	<a href="#">Edit</a> <a href="#">Delete</a>

Click **Add** to add a client-based policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-45 Add Client-Based Policy

**Add**
×

Policy Type  Client  Server

\* Policy Name

\* Peer Gateway  +

Interface  ⌵ ?

\* Local Subnet

\* Peer Subnet  +

\* Pre-shared

Key

Status

---

1. Set IKE Policy

---

2. Connection Policy

Cancel
OK

Click **Add** to add a server-based policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-46 Add Server-Based Policy



Add ✕

Policy Type  Client  Server

\* Policy Name

Interface  ?

\* Local Subnet

\* Pre-shared

Key

Status

----- 1. Set IKE Policy -----

----- 2. Connection Policy -----

Only one policy can be added currently.

### 3.3.5.1.2 IPSec Connection Status

The **IPSec Connection Status** page displays IPSec connections.

Figure 3-3-47 IPSec Connection Status

**IPSec Connection Status** ?

**IPSec Connection Status** Refresh

Name	SPI	Direction	Tunnel Endpoint	Flow	Status	Security Protocol	Algorithm
No Data							

### 3.3.5.2 L2TP

#### 3.3.5.2.1 L2TP Settings

Layer 2 Tunneling Protocol (L2TP) is a computer networking protocol used by Internet service providers (ISPs) to enable virtual private network (VPN) operations. Because it does not provide any security for data such as encryption and confidentiality, an encryption protocol such as Internet Protocol security (IPsec) is often used with L2TP, namely, L2TP/IPsec.

Figure 3-3-48 L2TP Server Settings

**L2TP Settings** ?

Enable L2TP

L2TP Type  L2TP Server  L2TP Client

\* Local Address

\* IP Range  ?

\* DNS Server

IPSec Security  ▾

\* PPP Hello Interval  Sec

**Save**

Figure 3-3-49 L2TP Client Settings

**L2TP Settings** ?

Enable L2TP

L2TP Type  L2TP Server  L2TP Client

\* Username

\* Password  👁

Interface  ▼

Tunnel IP  Dynamic  Static

\* Server Address

\* Peer Subnet

IPSec Security  ▼

Work Mode  NAT  Router

\* PPP Hello Interval  Sec

### 3.3.5.2.2 Tunnel List

Figure 3-3-50 L2TP Tunnel List

**Tunnel List** ?

<input type="checkbox"/>	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
No Data								

### 3.3.5.3 PPTP

Figure 3-3-51 PPTP Server Settings

**PPTP Settings** ?

Enable PPTP

PPTP Type  PPTP Server  PPTP Client

\* Local Address

\* IP Range  ?

\* DNS Server

\* PPP Hello Interval  Sec

Figure 3-3-52 PPTP Client Settings

**PPTP Settings** ?

Enable PPTP

PPTP Type  PPTP Server  PPTP Client

\* Username

\* Password  👁

Interface  ▼

Tunnel IP  Dynamic  Static

\* Server Address

\* Peer Subnet

Work Mode  NAT  Router

\* PPP Hello Interval  Sec

Figure 3-3-53 PPTP Tunnel List

**Tunnel List** ?

<input type="checkbox"/>	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
No Data								

### 3.3.5.4 OpenVPN

#### 3.3.5.4.1 Overview

- Concepts

Virtual private tunnels are required between enterprises, individuals and companies due to security or cross-NAT concern. OpenVPN is an SSL/TLS based virtual private network solution. Compared with other VPNs, OpenVPN supports more flexible client authorization, including certificate and account authorization, and allows users to connect to the VPN's virtual interface through a firewall. OpenVPN runs on Linux, xBSD, Mac OS X and Windows2000/XP. The EG device supports VPN connection to PCs, Android/iOS-based mobile phones, routers and Linux-based devices, compatible with most OpenVPN devices on the market.

OpenVPN supports connections through most proxy servers and work well in NAT environments. The server can deliver certain configuration to the client, including IP address, routing and DNS configuration.

- Certificates

The advantage of OpenVPN lies in its own security, and OpenVPN security depends on certificate support.

The OpenVPN certificate system is as follows:



The client certificate includes ca.CRT, ca.key, client.CRT, client.key, and the server-side certificate includes ca.CRT, ca.key, server.CRT, server.key.

### 3.3.5.4.2 Configuration Tasks

The device supports OpenVPN server or client. The following describes the configuration parameters of the server and client.

1. Server Mode
2. Client Mode

### 3.3.5.4.3 Server Mode

#### ▾ Basic Settings

Choose **Router > VPN > OpenVPN**.

Figure 3-3-54 OpenVPN

i
OpenVPN

Enable

OpenVPN Type  Server  Client

Server Mode

Protocol

\* Server Address

\* Port ID  1-65535

\* IP Range  ?

Deliver Route   ? +

---

Expand

Client Config

Server Log

- Server Mode

The EG device supports three authentication modes: **Account**, **Certificate**, and **Account & Certificate**. In the **Account** mode, the client needs to enter the correct account, including the username and password, and import the CA certificate. In the **Certificate** mode, the client needs to use the CA certificate, client certificate, and private key to connect to the server. The **Account & Certificate** mode requires all configuration mentioned above, mainly applied in security-demanding scenarios.

- Protocol

All OpenVPN communication is based on a single IP port. The UDP protocol is used by default and TCP is also supported. When selecting a protocol, please pay attention to the network conditions about the encrypted tunnels. If there is a high delay or a lot of packet loss, please select the TCP protocol as the underlying protocol.

- Server Address

The server address can be either an IP address or a domain name.

- Port ID

The official IANA (Internet assigned numbers Authority) assigned port number is 1194. If the port is occupied or disabled on the local network, the server log will prompt that port binding fails and remind you to change the port ID.

- IP Range

The OpenVPN address pool, except for the first address reserved for the server, is assigned to the clients. For example, if you set 10.80.12.0/24, the virtual IP address of the OpenVPN server is 10.80.12.1.

- Deliver Route

The server informs clients to access the intranet by a VPN tunnel. This is the only way to inform clients of the access method.

- Client Config

Export a tar package containing client configuration.

1. If you select the **Account** mode, the package includes the configuration file (client.ovpn), CA certificate (ca.CRT), CA private key (ca.key).
2. If you select the **Certificate** mode, the package includes the configuration file (client.ovpn), CA certificate (ca.CRT), CA key (ca.key), client certificate (client.crt) and client key (client.key).
3. If TLS authentication is enabled, the package includes a TLS authentication key (tls.key) in addition to the files mentioned above.

- Server Log

Export the service log, including the server startup time and client dial-up logs.

- Save

When the basic settings are complete, you can view the server tunnel information in **Tunnel List**.

### ▾ Advanced Settings

Click **Expand**.

Figure 3-3-55 Expand

..... Expand .....

The following advanced settings are available, and can be left as default if there are no special needs.

Figure 3-3-56 Advanced Settings



[Collapse](#)

---

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

- TLS Authentication

The TLS key is used to enhance OpenVPN security by requiring both parties to have a shared key before the TLS handshake. After TLS authentication is enabled, the client must import a TLS key (The OpenVPN client version must be greater than 2.40).

- Allow Data Compression

This feature is used to compress the transmitted data by the LZO algorithm, which saves bandwidth, but consumes CPU resources. The configuration on the client side and on the server side must be consistent. Otherwise, the connection will not be set up.

- Route all Traffic over VPN

This feature is used to route all traffic over the VPN tunnel. The VPN tunnel will be used as the default route.

- Cipher

Encrypting the data before transmission will ensure that the information cannot be read even if the data packet is intercepted during transmission. If the server is set to the **Auto** mode, the client can configure any encryption algorithm and will use the default algorithm (AES-256-GCM) automatically. If the server is set to a specific encryption algorithm, the client must have the same configuration as the server. Otherwise, the connection will not be set up.

- Deliver DNS

The server pushes DNS information to the client, only the windows-based client.

- Auth

The server informs the client to use the default digest algorithm SHA1.

### 3.3.5.4.4 Client Mode

The EG device currently supports two client configuration modes: **Web Settings** and **Import Config**. **Web Settings** is typically used to connect to any server except the EG device. **Import Config** is mainly used to connect to an EG device because it working as a server supports exporting the client configuration file (client.ovpn).

Figure 3-3-57 Import Config

The screenshot shows the 'OpenVPN' configuration page. At the top, there are two tabs: 'OpenVPN' (active) and 'Tunnel List'. Below the tabs is a light blue header with an information icon and the text 'OpenVPN'. An 'Enable' toggle switch is turned on. Under 'OpenVPN Type', the 'Client' radio button is selected. A red box highlights the 'Client Config' section, where 'Import Config' is selected over 'Web Settings'. Below this, there are input fields for 'Username' (with placeholder 'Username of OpenVpn user') and 'Password' (with placeholder 'Password of OpenVpn user'), each with a help icon. The 'Client Config' field contains '.ovpn' and a 'Browse' button, with a message 'It already exists.' to the right. There is an 'Export' button for 'Client Log' and a 'Save' button at the bottom.

#### Basic Settings

Figure 3-3-58 Web Settings

OpenVPN
Tunnel List

---

i **OpenVPN**

Enable

OpenVPN Type  Server  Client

Device Mode

Client Config  Web Settings  Import Config

Server Mode

\* Username

\* Password

Protocol

\* Server Address

\* Server Port ID  1-65535

Expand

- Device Mode

The EG device working as a client supports both the TUN and TAP modes. The configuration must be consistent with the server. The EG device working as a server supports the TUN mode only.

- Server Mode

The server supports three authentication modes: **Account**, **Certificate**, and **Account & Certificate**.

- Protocol

Both UDP and TCP are supported. The configuration must be consistent with the server side.

- Server Address

Enter the server IP address or domain name.

- Server Port ID

Enter the server port ID.

➤ **Advanced Settings**

Click **Expand**.

Figure 3-3-59 Expand



The following advanced settings are available, and can be left as default if there are no special needs.

Figure 3-3-60 Advanced Settings



Use Explicit Signature for  ?  
Server Certificate

TLS Authentication  ?

Cipher  ?

Auth  ?

Allow Data Compression  ?

Use Route Pushed by  ?  
Server

- Use Explicit Signature for Server Certificate

This feature is enabled by default. If you want to connect to a Mikrotik router, please disable this feature.

- TLS Authentication

Please upload a TLS certificate for TLS authentication.

- Cipher

The configuration must be consistent with the server side.

- Auth

The following digest algorithms are available: SHA1, MD5, SHA256 and NULL. The configuration must be consistent with the server side.

- Allow Data Compression

Data compression is allowed, and the configuration must be consistent with the server side.

- Use Route pushed by Server

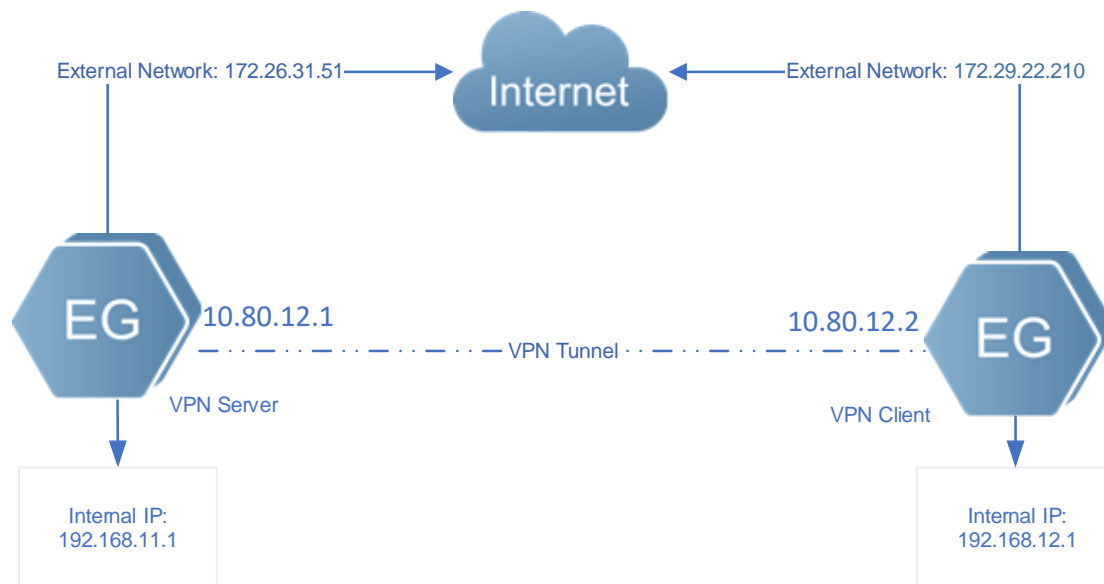
If this feature is disabled, the client will not receive the route delivered by the server. If you want to access the internal network of the server, please enable this feature.

### 3.3.5.4.5 Typical Applications

#### 3.3.5.4.5.1 Networking Topology

##### Scenario 1. An EG device connects to another EG device.

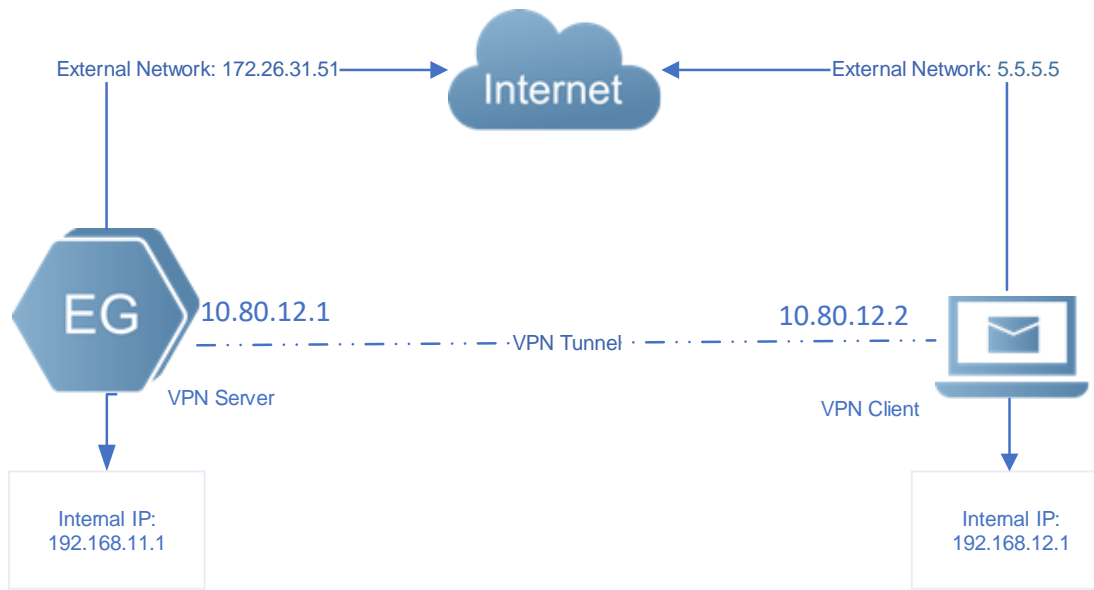
Figure 3-3-61 Scenario 1



The client (192.168.11.1) wants to connect to the server (192.168.12.1) by OpenVPN and achieve mutual access between the client network and the server network.

##### Scenario 2. An EG device connects to a PC.

Figure 3-3-62 Scenario 2



### 3.3.5.4.5.2 Notes

1. OpenVPN allows a PC to dial in to the VPN as a client, and supports connection between a router and another router.

**⚠** The client address pool cannot overlap with the internal network of the EG device.

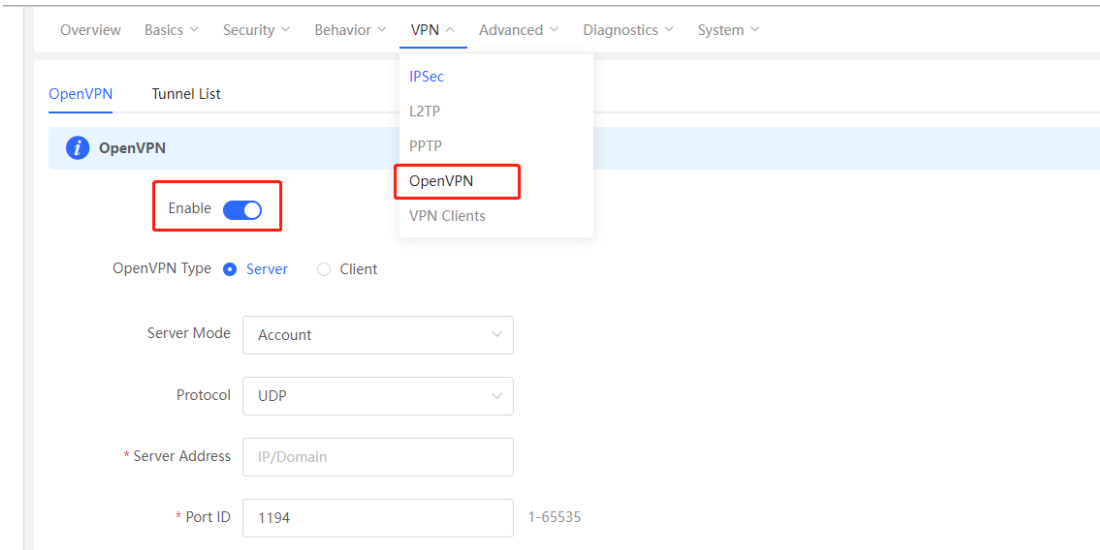
2. Enable **Deliver Router** on the server side and **Use Route Pushed by Server** on the client side. The client will be able to access the internal network of the server.
3. The external IP address of the EG device must be reachable from the client.
4. The configuration on the client side and the server side must be consistent.

### 3.3.5.4.5.3 Configuration Steps

#### 📌 Server

1. Log in to the web management system. Choose **Router > VPN > OpenVPN**.

Figure 3-3-63 OpenVPN



2. Set **OpenVPN Type** to **Server**. Select a server mode and a protocol, enter a port ID (default: 1194), a server address (local address, reachable from the client) and an IP address range. For example:

Figure 3-3-64 Server Settings

### *i* OpenVPN

Enable

OpenVPN Type  Server  Client

Server Mode

Protocol

\* Server Address

\* Port ID  1-65535




\* IP Range  ?

---

Expand

Client Config

Server Log

-  The local address and IP address range cannot overlap with the internal network.
-  The OpenVPN server assigns the IP address pool to the PC, and the server reserves the first address xx.xx.xx1 to itself. In the figure above, the virtual IP address of the OpenVPN server is 10.80.12.1.
-  The port ID ranges from 1 to 65536 (Default: 1194). If the port is occupied, the connection will not be set up.

3. If the EG device connects to another EG device, it is recommended to use default configuration. If the EG device connects to a device from other vendors, please make sure that the configuration on the client side and the server side are consistent. If the client wants to access the internal network 192.168.110.x, please add the route.

Figure 3-3-65 Deliver Route

Deliver Route   ? +



Enable **Deliver Router** on the server side and **Use Route Pushed by Server** on the client side. The client will be able to access the internal network of the server. Up to three routes can be added.

Figure 3-3-66 Deliver Route

Collapse

---

TLS Authentication  ?

Allow Data Compression Yes ?

Route All Traffic over VPN No ?

Cipher AES-128-CBC ?

Deliver Route 192.168.110.0 255.255.255.0 ? +

Deliver DNS Example: 1.1.1.1 ? +

Auth SHA1

### Remarks

- **Route all Traffic over VPN:** After this feature is enabled, all traffic will be routed over VPN.
  - **Cipher:** If the server is set to the **Auto** mode, the client can configure any encryption algorithm and will use the default algorithm (AES-256-GCM) automatically. If the server is set to a specific encryption algorithm, the client must have the same configuration as the server. Otherwise, the connection will not be set up.
  - **Allow Data Compression, Cipher and Auth** configuration must be consistent on the server side and the client side.
4. After the server is created successfully, you can view the server information in **Tunnel List**.

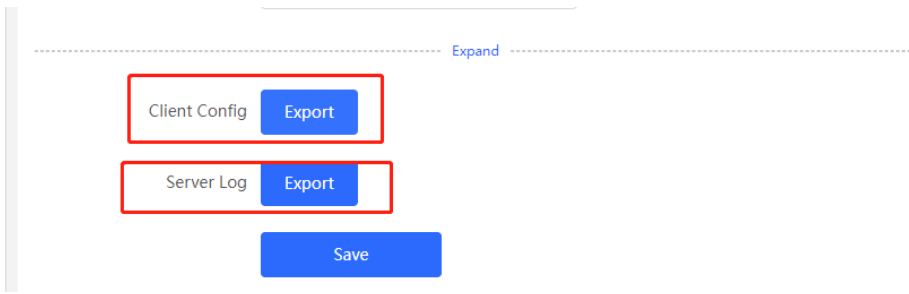
Figure 3-3-67 Tunnel List

OpenVPN Tunnel List

Tunnel List					
	Username	Server/Client	Status	Real IP Address	Virtual IP Address
<input type="checkbox"/>	openvpn	Server	OK	110.20.20.20	10.80.12.1

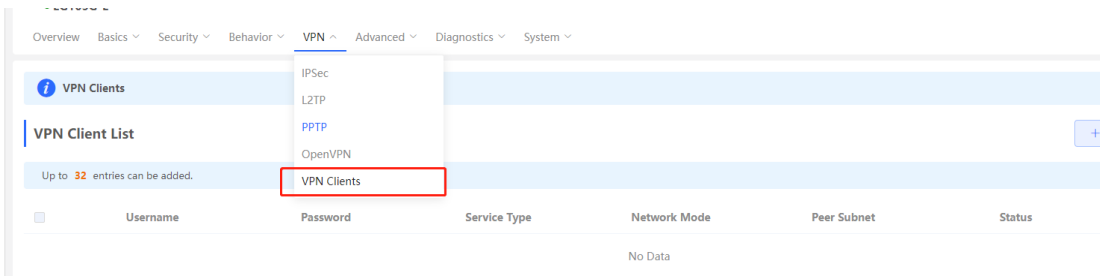
After the server is created successfully, you can export the configuration file of the client connected to the server. If you fail to create the server, please check log for failure prompt.

Figure 3-3-68 Export Config



5. Choose **VPN > VPN Clients** to create an account for OpenVPN.

Figure 3-3-69 OpenVPN Account



### Add User



Service Type

\* Username

\* Password

Status

 Select **OpenVPN** from the **Service Type** dropdown list.

### Client

1. Set **OpenVPN Type** to **Client**. Select **Import Config**. If the server is configured with the **Account** mode, please enter the correct account, including the username and password.

Figure 3-3-70 Client Settings

**OpenVPN**

Enable

OpenVPN Type  Server  Client

Client Config  Web Settings  Import Config

Username  ?

Password  ?

Client Config  Browse It already exists.

Client Log

2. View the tunnel information. If the client is created successfully, you can view the client information in **Tunnel List** on both the client side and the server side.

Figure 3-3-71 Tunnel List on Client Side

	Username	Server/Client	Status	Real IP Address	Virtual IP Address
<input type="checkbox"/>	456	Client	OK	172.26.31.53	10.80.12.3

Figure 3-3-72 Tunnel List on Server Side

	Username	Server/Client	Status	Real IP Address	Virtual IP Address
<input type="checkbox"/>	openvpn	Server	OK	172.26.31.51	10.80.12.1
<input type="checkbox"/>	456	Client	OK	172.26.31.53	10.80.12.3

3. You can also set **Client Config** to **Web Settings**. Select a device mode, server mode and protocol. If the server mode is set to **Account**, please enter the correct account, including username and password. The server address and server port ID are also required.

Figure 3-3-73 Client Settings

**i** OpenVPN

Enable

OpenVPN Type  Server  Client

Device Mode

Client Config  Web Settings  Import Config

Server Mode

\* Username

\* Password

Protocol

\* Server Address

\* Server Port ID  1-65535

**!** The **Device Mode**, **Protocol** and **Server Mode** must be consistent on the server and the client. The server address must be reachable from the client.

Figure 3-3-74 Client Settings

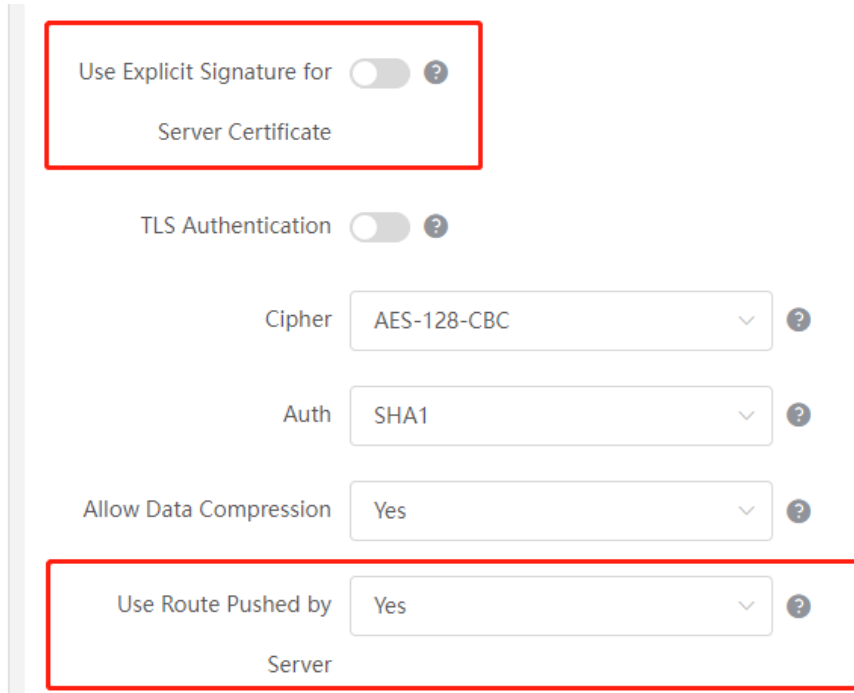
The screenshot shows a configuration interface for client settings. It includes the following elements:

- CA Certificate:** A text input field containing ".cert" and a "Browse" button.
- Client Key:** A text input field containing ".key" and a "Browse" button.
- Client Certificate:** A text input field containing ".cert" and a "Browse" button.
- Client Certificate Key:** An empty text input field with a question mark icon to its right.
- Client Log:** A blue button labeled "Export".
- Save:** A large blue button labeled "Save" at the bottom of the form.

If you select the **Certificate** mode, please import the CA certificate, client certificate and private key. If you select the **Account** mode, please import the CA certificate.

4. If an EG device working as a client connects to another EG device as a server, please use the default configuration. If an EG device connects to any server except the EG device, e.g., Mikrotik device, please disable **Use Explicit Signature for Server Certificate** on the client.

Figure 3-3-75 Client Settings



Use Explicit Signature for  Server Certificate

TLS Authentication

Cipher AES-128-CBC

Auth SHA1

Allow Data Compression Yes

Use Route Pushed by Yes Server

If the client wants to access the internal network of the server, please enable **Deliver Route** on the server and keep the other configuration consistent on the client and the server. Click **Save**, and you can view the created server and client in **Tunnel List**.

### 3.3.5.4.5 Validation

1. The server and client information are available in **Tunnel List**.

Figure 3-3-76 Tunnel List

Tunnel List					
	Username	Server/Client	Status	Real IP Address	Virtual IP Address
<input type="checkbox"/>	openvpn	Server	OK	172.26.31.51	10.80.12.1
<input type="checkbox"/>	456	Client	OK	172.26.31.53	10.80.12.3

2. Virtual addresses can ping each other and the client can access the internal network of the server.

### 3.3.5.5 VPN Clients

Figure 3-3-77 VPN Clients

**VPN Clients** ?

---

**VPN Client List** + Add    Delete Selected

Up to **30** entries can be added.

<input type="checkbox"/>	Username	Service Type	Network Mode	Peer Subnet	Status	Action
No Data						

Click **Add** to add a vpn client. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-78 VPN Clients

### Add User ×

Service Type

\* Username

\* Password  👁

Network Mode

Status

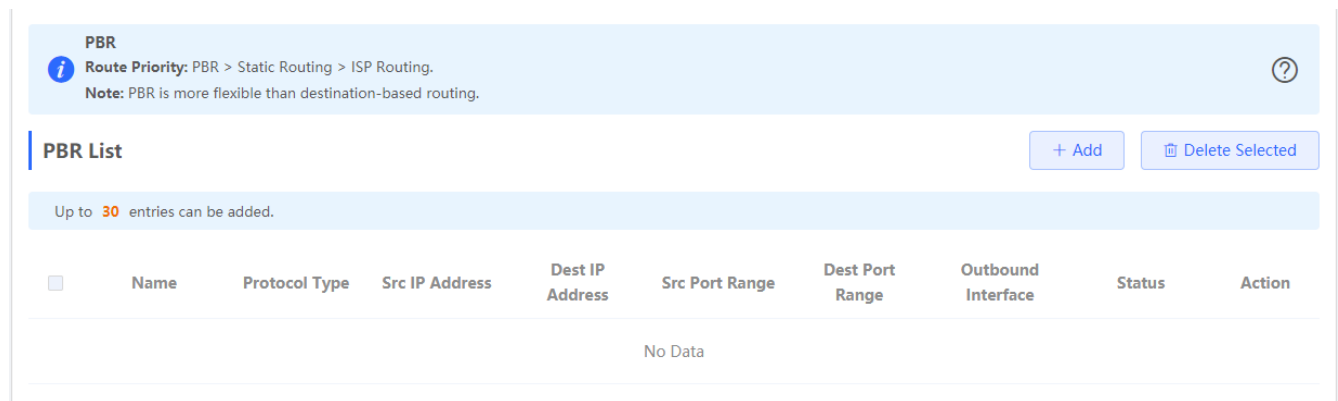
### 3.3.6 Advanced

#### 3.3.6.1 Routing

##### 3.3.6.1.1 PBR

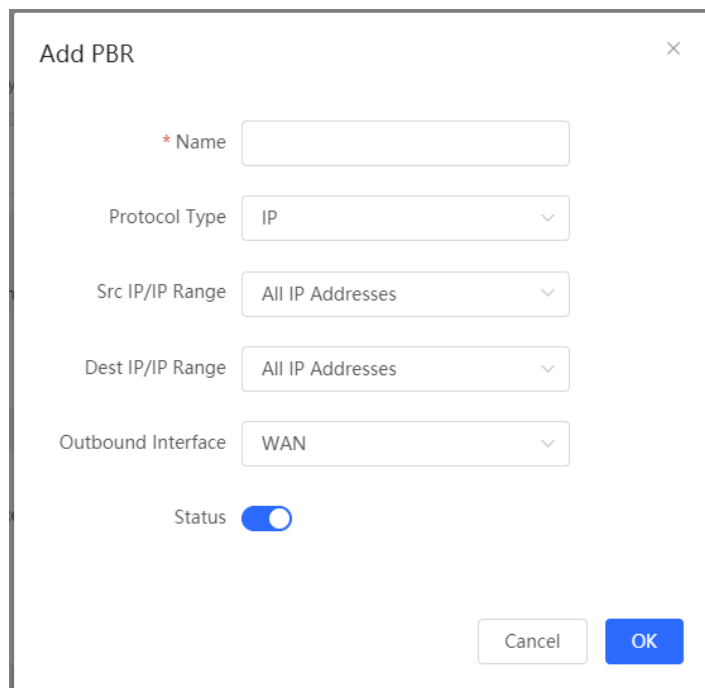
The **PBR** module allows you to add, delete and edit policy-based routes.

Figure 3-3-79 PBR List



Click **Add** to add a policy-based route. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-80 Add PBR

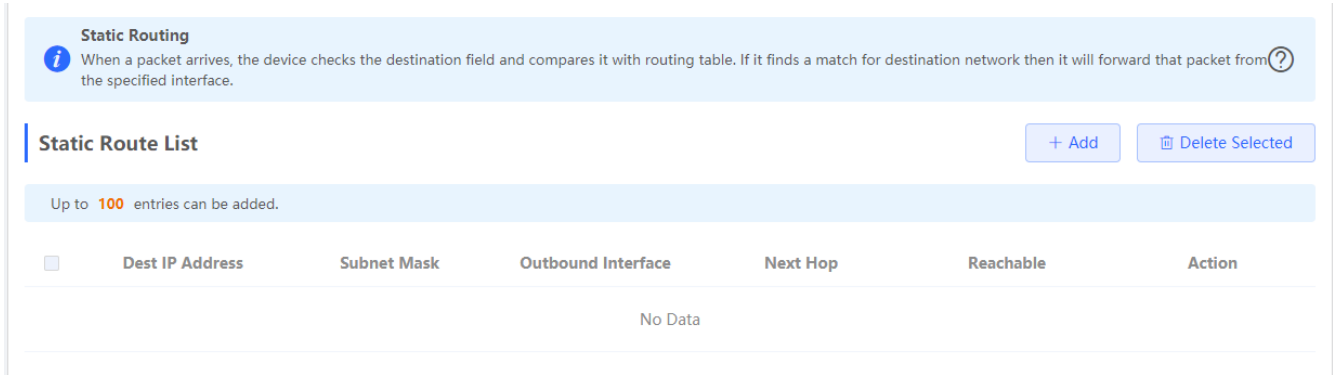




### 3.3.6.1.2 Static Routing

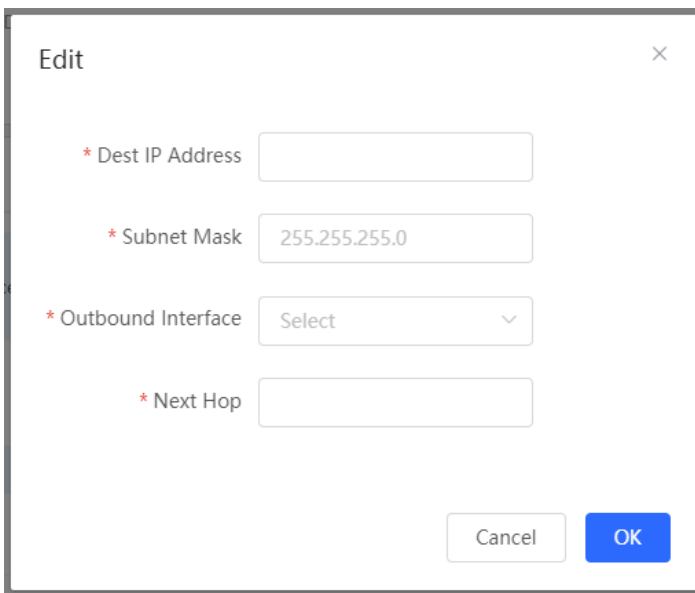
The **Static Routing** module allows you to add, delete and edit static routes.

Figure 3-3-81 Static Route List



Click **Add** to add a static route. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-82 Add Static Route



### 3.3.6.2 Flow Control

#### 3.3.6.2.1 Smart Flow Control

The **Smart Flow Control** module allows you to configure smart flow control.

Figure 3-3-83 Smart Flow Control

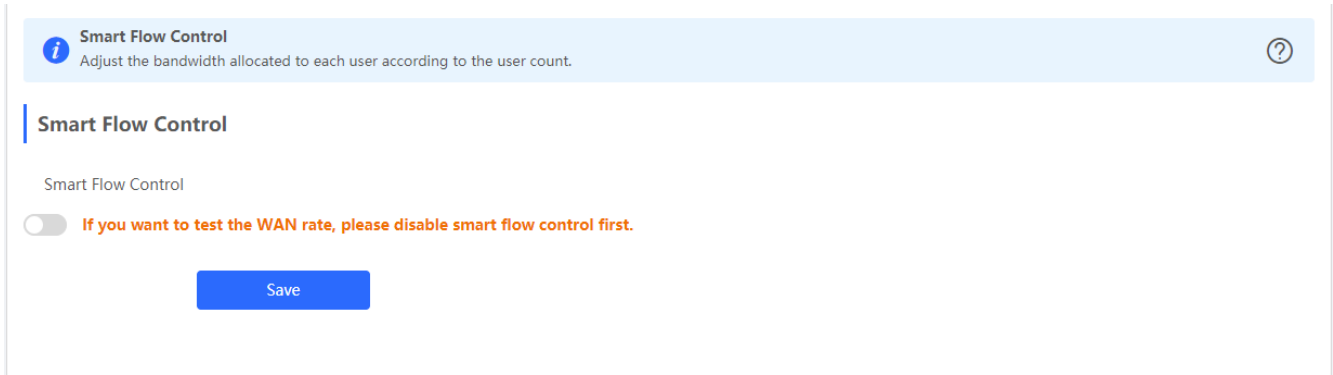
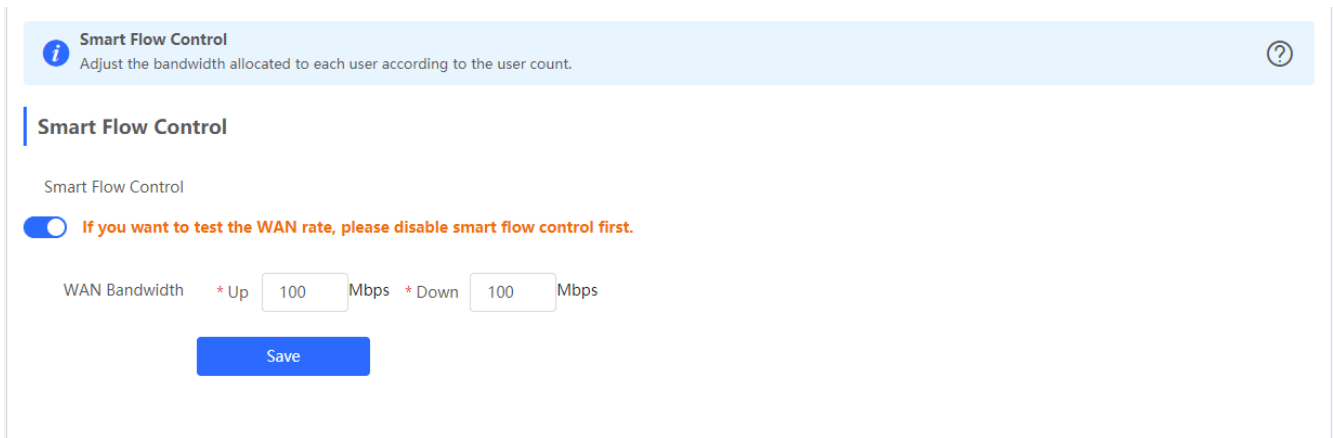


Figure 3-3-84 Enable Smart Flow Control

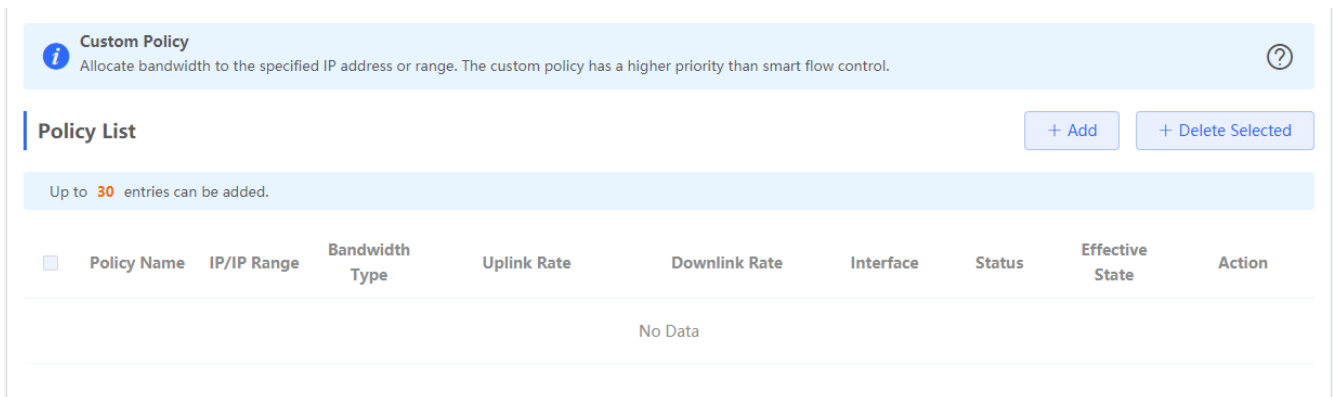


If there is more than one WAN port, **WAN Bandwidth** settings of each port will be displayed accordingly.

### 3.3.6.2.2 Custom Policy

The **Custom Policy** module allows you to add, delete and edit custom flow control policies.

Figure 3-3-85 Custom Flow Control Policy



Click **Add** to add a custom flow control policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-86 Add Flow Control Policy

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- \* Policy Name**: A text input field.
- \* IP/IP Range**: A text input field with the example text "Example: 192.168.1.2-192.168.1.100".
- Bandwidth Type**: A dropdown menu currently showing "Share".
- Uplink Rate**: Two input fields labeled "\* CIR" and "\* PIR" followed by "Kbps".
- Downlink Rate**: Two input fields labeled "\* CIR" and "\* PIR" followed by "Kbps".
- Interface**: A dropdown menu currently showing "WAN".
- Status**: A toggle switch that is currently turned on (blue).
- Buttons**: "Cancel" and "OK" buttons at the bottom right.

### 3.3.6.3 PPPoE Server

#### 3.3.6.3.1 Global Settings

Figure 3-3-87 Global Settings

**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  Disable

Mandatory PPPoE Dialup  Enable  Disable

\* Local Address

\* IP Range

VLAN

Primary DNS Server

Secondary DNS Server

\* Unanswered LCP  Range: 1-60  
Packet Limit

Auth Mode  PAP  CHAP  
 MSCHAP  MSCHAP2

**Save**

### 3.3.6.3.2 Account Settings

Figure 3-3-88 Account Settings

**Account Settings** ?  
The account management is not in effect. Enable smart flow control

---

**Account List** + Add    Delete Selected

Up to **65** entries can be added. Clients **0**

<input type="checkbox"/>	Username	Password	Expire Date	Status	Account Management	Remark	Action
No Data							

Click **Add** to add a account. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-89 Add Account Settings

### Add



\* Username

\* Password

Expire Date

Remark

Status

Flow Control

The account management is not in effect. Enable smart flow control

Cancel

OK

### 3.3.6.3.3 Account Management

Figure 3-3-90 Account Management

### Account Management List

Up to **10** entries can be added.  
The account management is not in effect. [Enable smart flow control](#)

<input type="checkbox"/>	Account Name	Uplink Rate	Downlink Rate	Interface	Action
No Data					

Click **Add** to add an IP address. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-91 Add Account

### Add



\* Account Name

Uplink Rate \* CIR  \* PIR  Kbps

Downlink Rate \* CIR  \* PIR  Kbps

Interface

### 3.3.6.3.4 Exceptional IP Address

Figure 3-3-92 Exceptional IP Address

**Exceptional IP Address** ?

---

**Exceptional IP Address List** + Add Delete Selected

Up to 5 entries can be added.

<input type="checkbox"/>	Start IP Address	End IP Address	Remark	Status	Action
No Data					

Click **Add** to add a IP In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-93 Add Exceptional IP Address

### Add ×

\* Start IP   
Address

\* End IP   
Address

Remark

Status



### 3.3.6.3.5 Online Clients

Figure 3-3-94 Online Clients

The screenshot shows a web interface for 'Online Clients'. At the top, there is a header bar with an information icon and the text 'Online Clients', and a help icon on the right. Below this is a section titled 'Account List' with two buttons: 'Disconnect' and 'Refresh'. A status bar below the title shows 'Online Clients 0'. The main content is a table with the following columns: a checkbox, 'Username', 'IP Address', 'MAC', 'Up on', and 'Action'. The table is currently empty, displaying 'No Data' in the center.

### 3.3.6.4 Authentication

#### 3.3.6.4.1 Cloud Auth

Figure 3-3-95 Cloud Auth

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

**If the IP address of the EAP device is in the authentication IP range, please choose Whitelist to add the EAP MAC address to the MAC address whitelist.**

Authentication

\* Server Type

\* Auth Server URL

Client Escape  Enable

\* IP/IP Range

### 3.3.6.4.2 Local Account Auth

Figure 3-3-96 Cloud Auth

### 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.**

**If the IP address of the EAP device is in the authentication IP range, please choose **Whitelist** to add the EAP MAC address to the MAC address whitelist.**

Local Account Auth

Accounts 0

\* Auth IP/IP Range

### Account Settings

Up to **200** accounts can be added.

<input type="checkbox"/>	Username	Password	MAC	Action
No Data				

Click **Add** to add an account. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-97 Add Account

### Add Account

×

\* Username

\* Password

### 3.3.6.4.3 Authorized Auth

Figure 3-3-98 Authorized Auth

**Authorized Auth**

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

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

If the IP address of the EAP device is in the authentication IP range, please choose **Whitelist** to add the EAP MAC address to the MAC address whitelist.

Authorized Auth

Popup Message

\* Auth IP/IP Range

Limit Online Duration

\* Authorization IP/IP   
Range

### 3.3.6.4.4 QR Code Auth

Figure 3-3-99 QR Code Auth

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

**i** **Make sure that the device can access the Internet. Otherwise, the Portal page may not pop up on the terminal.** **?**  
**If the IP address of the EAP device is in the authentication IP range, please choose Whitelist to add the EAP MAC address to the MAC address whitelist.**

QR Code Auth


\* Authorization IP/IP    
Range

Limit Online Duration

QR Code Generator

\* Dynamic QR   
Code

Popup   
Message



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

### 3.3.6.4.5 Whitelist

Figure 3-3-100 User Whitelist

**User Whitelist**

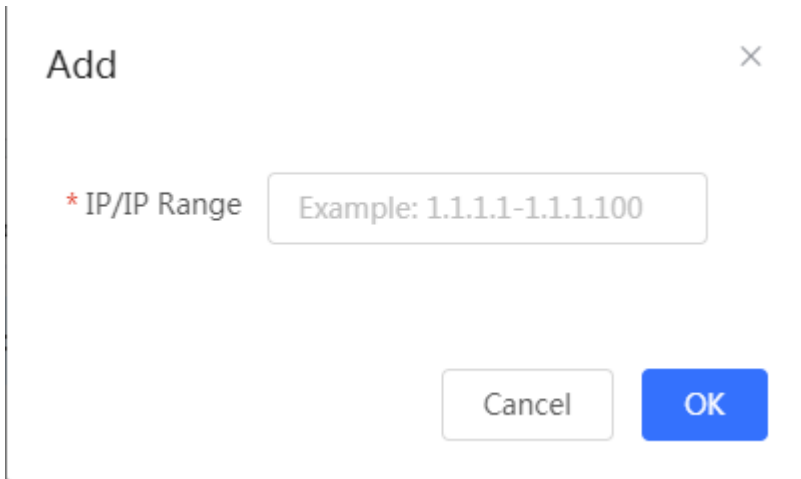
Up to **50** entries can be added.

<input type="checkbox"/>	IP/IP Range	Action
No Data		

< **1** >  Total 0

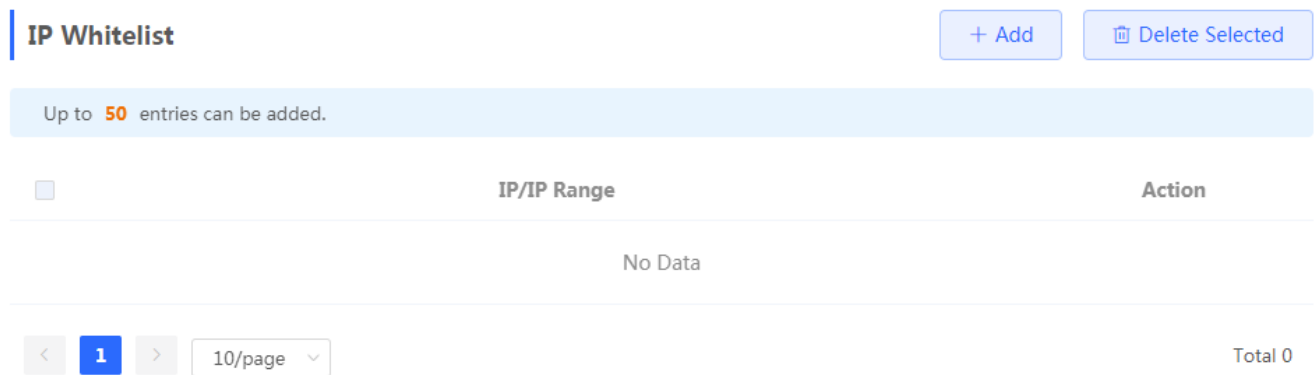
Click **Add** to add a User In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-101 Add User



The dialog box is titled "Add" and has a close button (X) in the top right corner. It contains a label "\* IP/IP Range" followed by a text input field with the placeholder text "Example: 1.1.1.1-1.1.1.100". At the bottom, there are two buttons: "Cancel" and "OK".

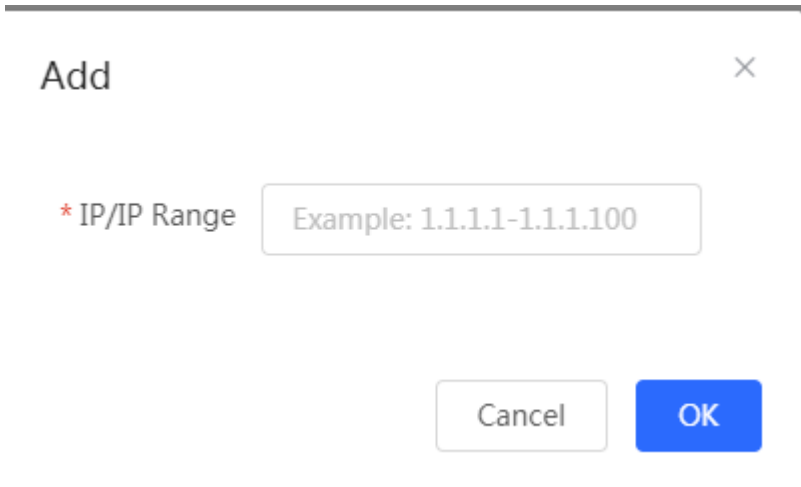
Figure 3-3-102 IP Whitelist



The interface shows the "IP Whitelist" section with a "+ Add" button and a "Delete Selected" button. A message states "Up to 50 entries can be added." Below is a table with columns for a checkbox, "IP/IP Range", and "Action". The table is currently empty, showing "No Data". At the bottom, there is a pagination control showing page 1 of 1, a "10/page" dropdown, and a "Total 0" label.

Click **Add** to add an IP address. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-103 Add IP



The dialog box is titled "Add" and has a close button (X) in the top right corner. It contains a label "\* IP/IP Range" followed by a text input field with the placeholder text "Example: 1.1.1.1-1.1.1.100". At the bottom, there are two buttons: "Cancel" and "OK".

Figure 3-3-104 URL Whitelist

**URL Whitelist** + Add Delete Selected

Up to **100** entries can be added.

<input type="checkbox"/>	URL	Action
<input type="checkbox"/>	ruijienetworks.com	<a href="#">Edit</a> <a href="#">Delete</a>

< **1** > 10/page Total 1

Click **Add** to add a URL. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-105 Add URL

**Add** ×

\* URL

Cancel OK

Figure 3-3-106 MAC Whitelist

**MAC Whitelist** + Add Delete Selected

Up to **250** entries can be added.

<input type="checkbox"/>	MAC	Action
No Data		

< **1** > 10/page Total 0

Click **Add** to add a MAC address. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-107 Add MAC

Add ×

\* MAC

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

Cancel OK

Figure 3-3-108 MAC Blacklist

**MAC Blacklist**

+ Add Delete Selected

Up to **250** entries can be added.

	MAC	Action
No Data		

< 1 > 10/page v

Total 0

Click **Add** to add a MAC address. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-109 Add MAC

Add ×

\* MAC

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

Cancel OK



### 3.3.6.4.6 Online Users

Figure 3-3-110 Online Users

i **Online Clients**

#### Auth Settings

Idle Client Timeout  Min (Range: 5-65535)

[Save](#)

#### Online Clients

Search by IP Address

Enter

Q

[Refresh](#)

[Delete Selected](#)

<input type="checkbox"/>	Username	IP	MAC	Up on	Duration(Sec)	Auth Type	Status	Action
No Data								

< 1 >

10/page

Total 0

### 3.3.6.5 Session Limit

The **Session Limit** module allows you to add, delete and edit session limit polices.

Figure 3-3-111 IP Session Limit

i **IP Session Limit** ?  
Configure the max number of IP sessions.

#### Rule List

[+ Add](#)
[Delete Selected](#)

Up to 20 entries can be added.

<input type="checkbox"/>	Name	IP Range	Session Count Limit	Status	Action
No Data					

Click **Add** to add a session limit policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-112 Add Session Limit Policy

Add
×

\* Name

\* Start IP Address

\* End IP Address

\* Session Count Limit

Status

### 3.3.6.6 Port Mapping

#### 3.3.6.6.1 Port Mapping

The **Port Mapping** module allows you to add, delete and edit port mapping policies.

Figure 3-3-113 Port Mapping List

**Port Mapping**
?

**Port Mapping List**

Up to **50** entries can be added.

	Name	Protocol	External IP Address	External Port	Internal IP Address	Internal Port	Action
<input type="checkbox"/>	est-ap	TCP	172.30.111.23	6677	192.168.110.73	80	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	est-cpe	TCP	172.30.111.23	6688	192.168.110.76	80	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	msw	TCP	172.30.111.23	3366	192.168.110.89	80	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	msw-ssh	TCP	172.30.111.23	6699	192.168.110.89	54133	<a href="#">Edit</a> <a href="#">Delete</a>

Click **Add** to add a port mapping policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-114 Add Port Mapping Policy

**Add** ×

\* Name

Protocol

External IP Address

\* External Port/Range

\* Internal IP Address

\* Internal Port/Range

### 3.3.6.6.2 NAT-DMZ

The **NAT-DMZ** module allows you to add, delete and edit NAT-DMZ rules.

Figure 3-3-115 NAT-DMZ Rule List

**NAT-DMZ** ?

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

**NAT-DMZ Rule List**

There are **1** outbound interfaces. Up to **1** rules can be added.

	Name	Outbound Interface	Dest IP Address	Status	Action
No Data					

Click **Add** to add a NAT-DMZ rule. In the displayed dialog box, configure settings and click **OK**.

Figure 3-3-116 Add NAT-DMZ Rule

Add Rule
×

\* Name

\* Dest IP Address

Outbound Interface

Status

### 3.3.6.7 Dynamic DNS

#### 3.3.6.7.1 Peanut Shell NAT

It is recommended to use WeChat or Peanut Shell to scan the QR code.

Figure 3-3-117 Peanut Shell NAT


i **Peanut Shell NAT**  
 It is recommended to use WeChat or Peanut Shell to scan the QR code.

**Peanut Shell NAT**

Enable  Click to switch the status.

Service Status Online

Scan to Login



#### 3.3.6.7.2 Dynamic DNS

It is recommended to use Peanut Shell for NAT, including TCP, UDP, HTTP and HTTPS mapping.

Figure 3-3-118 Dynamic DNS

**Dynamic DNS**  
It is recommended to use Peanut Shell for NAT, including TCP, UDP, HTTP and HTTPS mapping.

**Dynamic DNS**

\* Preferred Interface  ⓘ

\* Username

\* Password  ⓘ

Link Status [Connection success.](#)

Domain

### 3.3.6.7.3 No-IP DNS

Figure 3-3-119 No-IP DNS

**No-IP DNS**

\* Service Interface  ⓘ

\* Username  [Register](#)

\* Password

Domain  ⓘ

Link Status -

Domain -

### 3.3.6.7.4 DynDNS

Figure 3-3-120 Local DNS



### Peanut Shell NAT

It is recommended to use WeChat or Peanut Shell to scan the QR code.

Enable

Save

Service Status -

### 3.3.6.8 UPnP Settings

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

Figure 3-3-121 UPnP Settings



### UPnP Settings

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

Enable

Save

#### UPnP List

Protocol	App	Client IP Address	Internal Port	External Port
----------	-----	-------------------	---------------	---------------

UPnP Disabled

### 3.3.6.9 Local DNS

The **Local DNS** module allows you to configure a local DNS server.

Figure 3-3-122 Local DNS



### Local DNS server

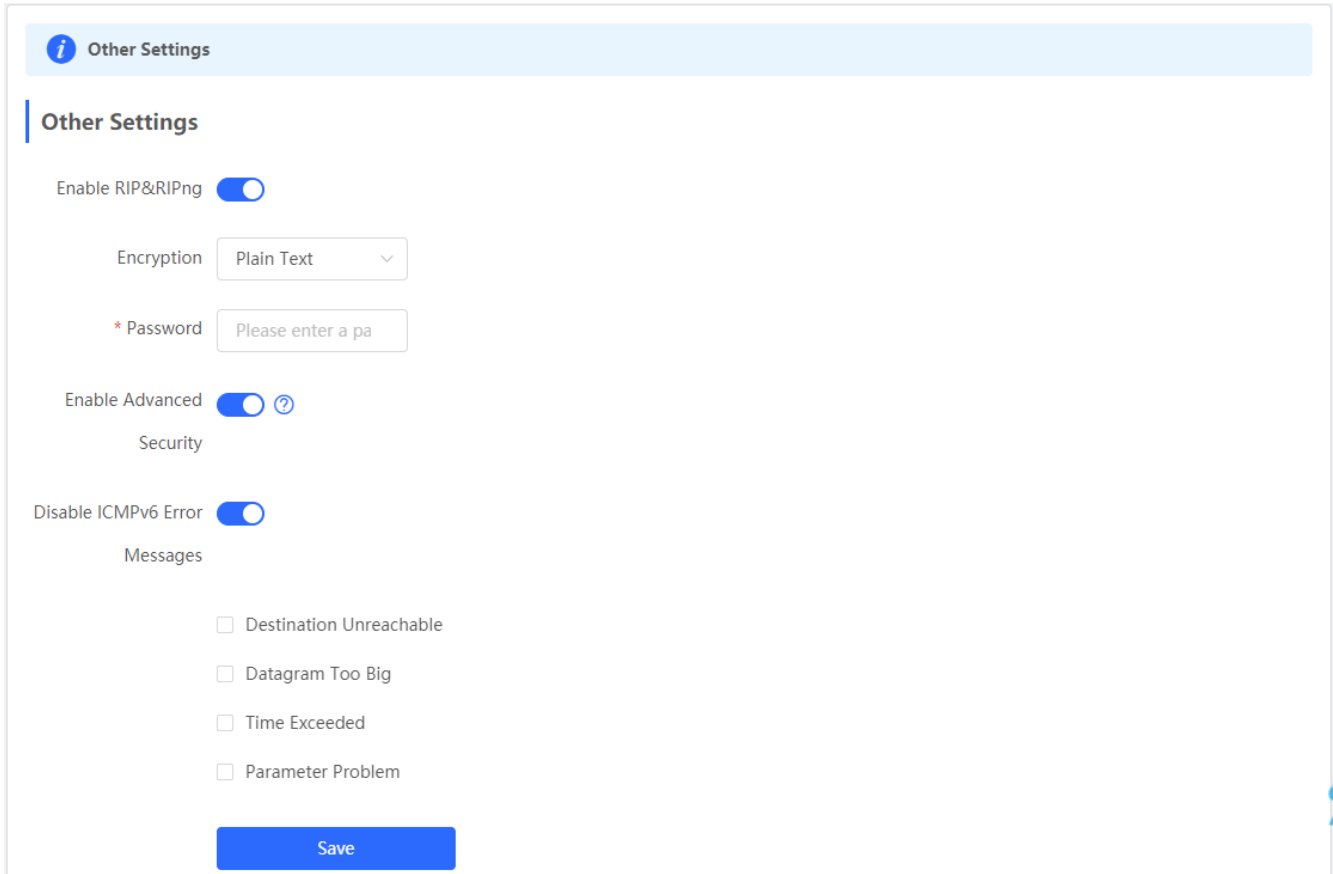
The local DNS server is not required to be configured. By default, the device will get the DNS server address from the uplink device.

Local DNS server

Save

### 3.3.6.10 Other Settings

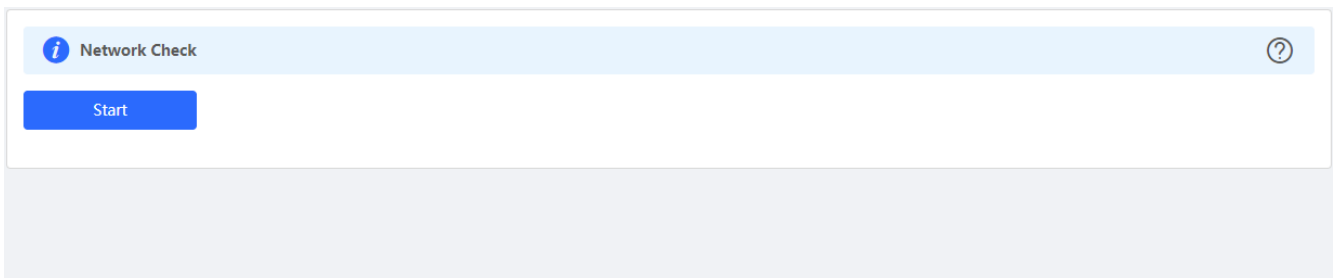
Figure 3-3-123 Other Settings



### 3.3.7 Diagnostics

#### 3.3.7.1 Network Check

Figure 3-3-124 Network Check



Click **Start**, and click **OK** in the confirmation box. After the test finishes, the result will be displayed.

Figure 3-3-125 Result

The screenshot shows the 'Network Check' interface. At the top, there is a blue header with an information icon and the text 'Network Check', and a question mark icon on the right. Below the header is a blue 'Recheck' button. A progress bar below the button is filled with blue and labeled '100%'. The main area contains a list of 14 items, each with a green checkmark on the right:

- WAN/LAN Cable
- Auto-Negotiated Speed
- WAN Port
- DHCP-Assigned IP Address
- LAN & WAN Address Conflict
- Loop
- DHCP Server Conflict
- IP Address Conflict
- Route
- Next Hop Connectivity
- DNS Server
- IP Session Count
- DHCP Capacity

If any problem occurs, the result will be displayed as follows:

Figure 3-3-126 Issue & Advice

The screenshot shows a section titled 'WAN/LAN Cable' with an orange background and an information icon on the right. It contains two sub-sections:

- Check WAN Cable**:
  - Result** : OK
- Check LAN Cable**:
  - Result** : The LAN cable is unplugged. Internet access may fail.
  - Advice** : Please verify that the device is plugged into the LAN port properly and check the cable and plug.

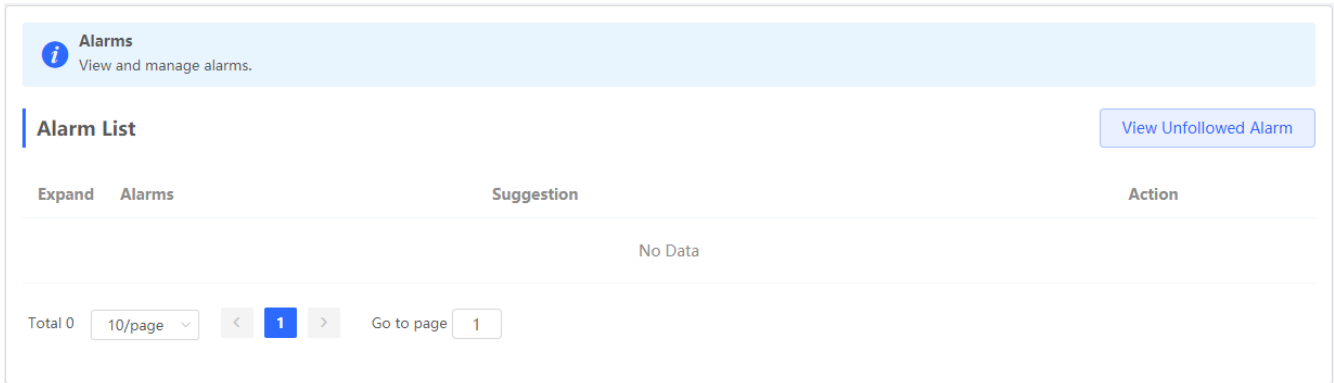
Please fix the problem by taking the suggested action.

### 3.3.7.2 Alarms

The **Alarms** module allows you to view and manage alarms in the network.

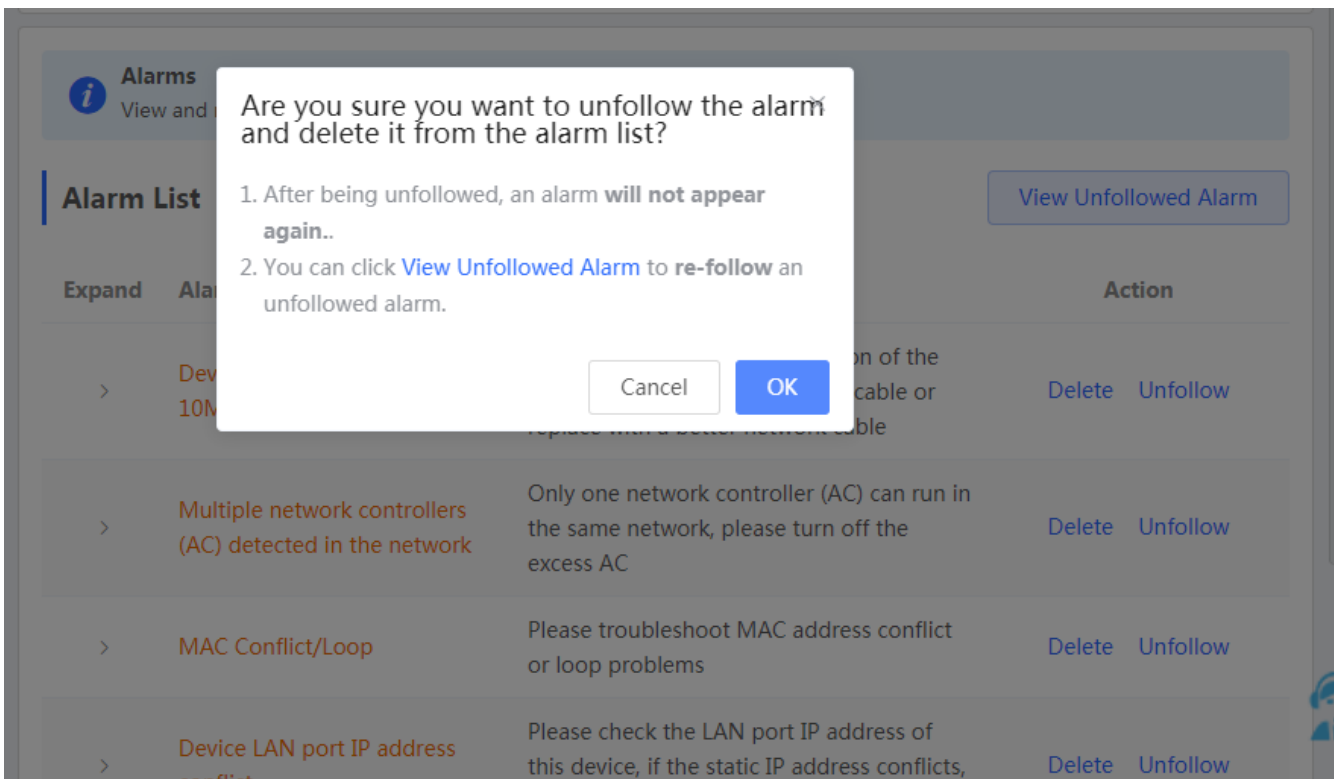
Figure 3-3-127 Alarms





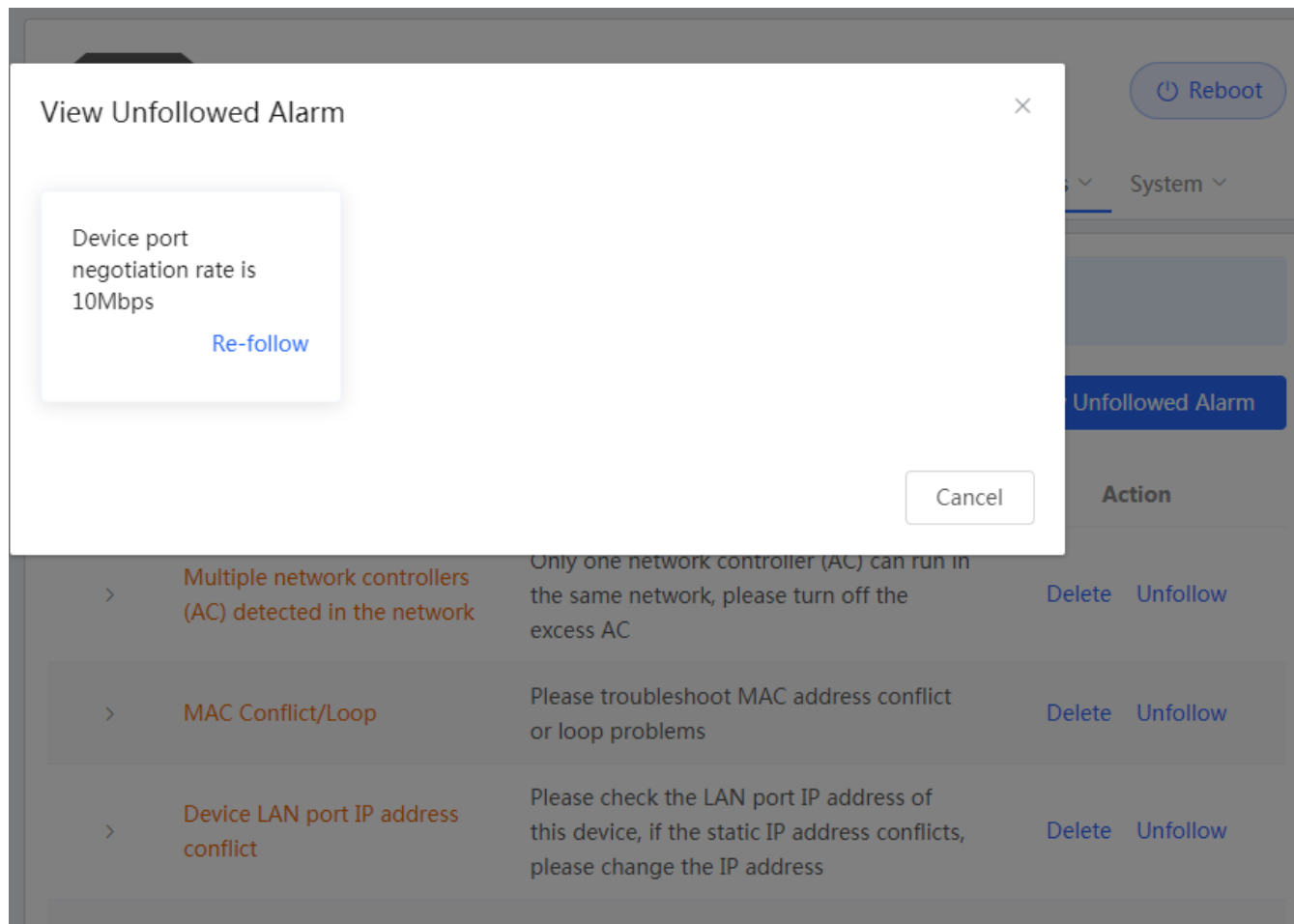
Click **Unfollow** in the **Action** column to unfollow an alarm. In the confirmation box, click **OK**.

Figure 3-3-128 Unfollow Alarm



Click **View Unfollowed Alarm**, and you can view and follow the alarm again.

Figure 3-3-129 Re-follow Alarm



### 3.3.7.3 Network Tools

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

Figure 3-3-130 Ping Test and Result

The screenshot shows the 'Network Tools' section with the 'Ping' tool selected. The configuration fields are: IP Address/Domain: www.google.com; Ping Count: 4; Packet Size: 64 Bytes. There are 'Start' and 'Stop' buttons and a 'Result' text area below.

Figure 3-3-131 Traceroute Test and Result

The screenshot shows the 'Network Tools' section with the 'Traceroute' tool selected. The configuration fields are: IP Address/Domain: www.google.com; Max TTL: 20. There are 'Start' and 'Stop' buttons and a 'Result' text area below.

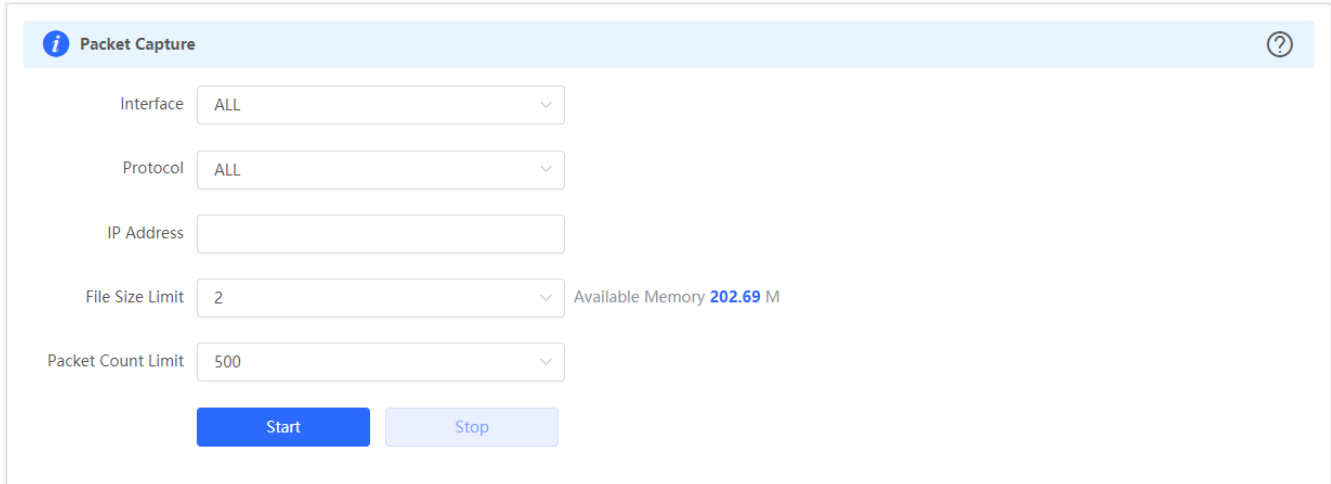
Figure 3-3-132 DNS Lookup Test and Result

The screenshot shows the 'Network Tools' section with the 'DNS Lookup' tool selected. The configuration field is: IP Address/Domain: www.google.com. There are 'Start' and 'Stop' buttons and a 'Result' text area below.

### 3.3.7.4 Packet Capture

The **Packet Capture** module allows you to perform packet capture and download the result for troubleshooting.

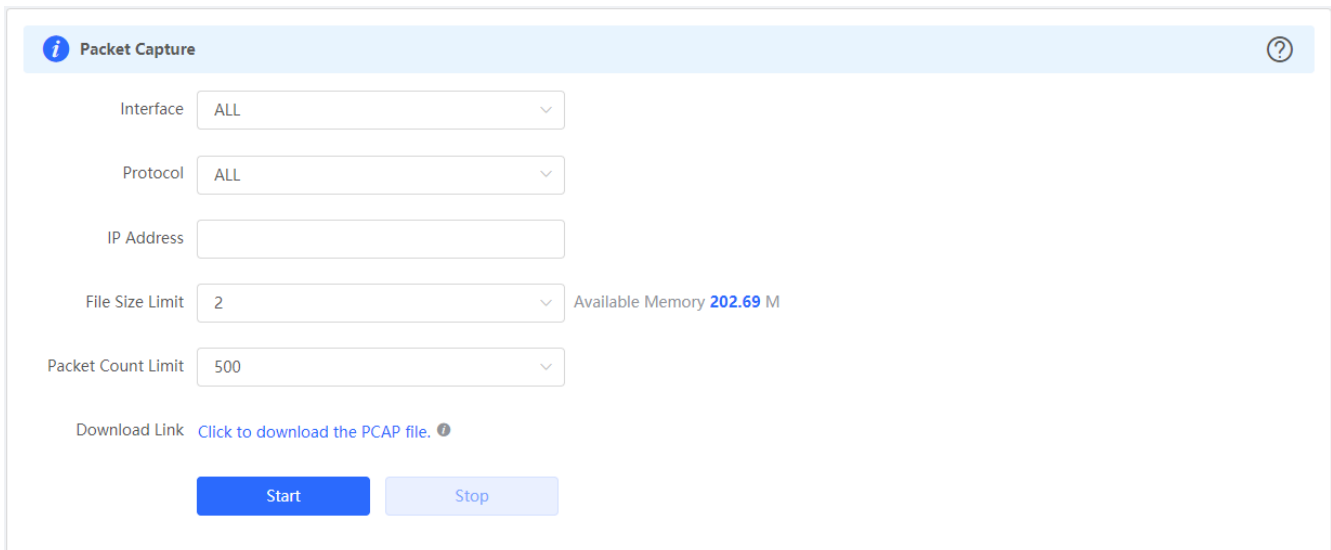
Figure 3-3-133 Packet Capture



The screenshot shows the 'Packet Capture' configuration interface. It features a light blue header with an information icon and a help icon. Below the header, there are several configuration fields: 'Interface' (dropdown menu set to 'ALL'), 'Protocol' (dropdown menu set to 'ALL'), 'IP Address' (text input field), 'File Size Limit' (dropdown menu set to '2'), and 'Packet Count Limit' (dropdown menu set to '500'). To the right of the 'File Size Limit' field, it displays 'Available Memory 202.69 M'. At the bottom, there are two buttons: a blue 'Start' button and a light blue 'Stop' button.

Specify an IP address and click **Start**. After a few seconds, click **Stop**.

Figure 3-3-134 Start Packet Capture



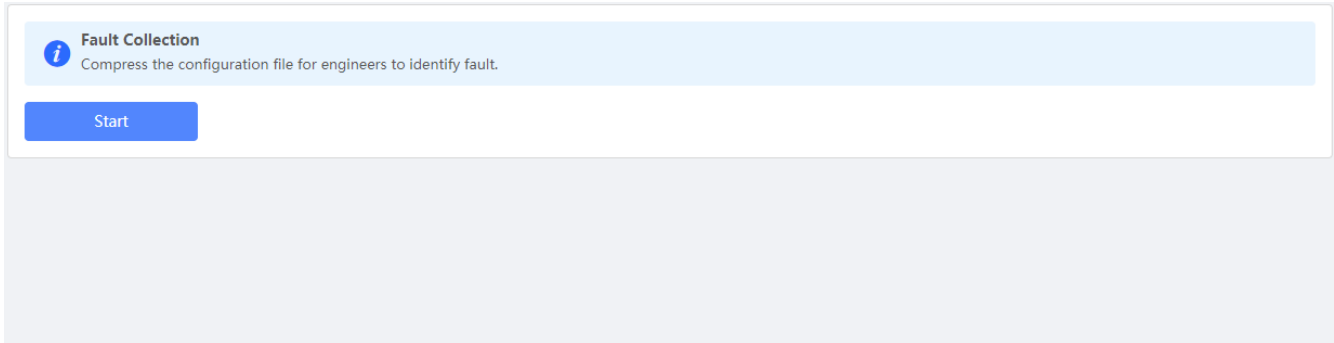
This screenshot is identical to the previous one, showing the 'Packet Capture' configuration page. However, a new 'Download Link' has appeared below the configuration fields, with the text 'Click to download the PCAP file.' and a small help icon. The 'Start' and 'Stop' buttons remain at the bottom.

Click to download the packet capture result in the PCAP format.

### 3.3.7.5 Fault Collection

The **Fault Collection** module allows you to collect faults by one click and download the fault information to the local device.

Figure 3-3-135 Fault Collection

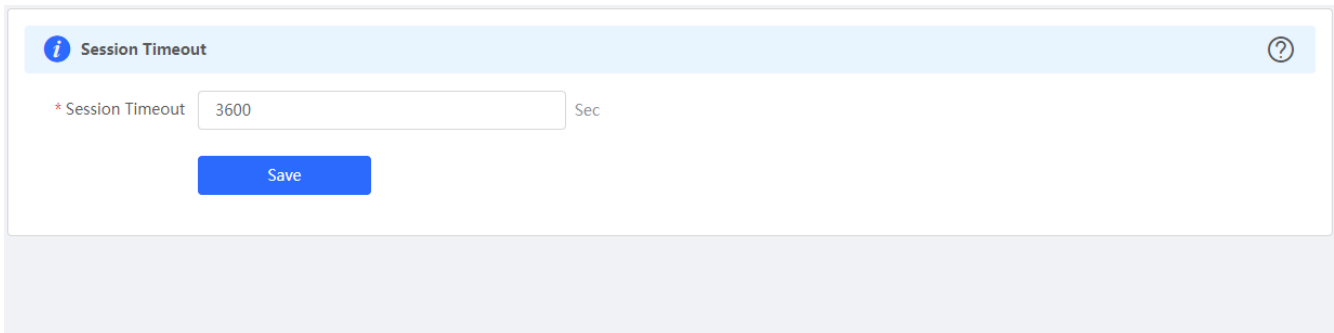


### 3.3.8 System

#### 3.3.8.1 Session Timeout

The **Session Timeout** module allows you to set the session timeout period for login to the eWeb management system.

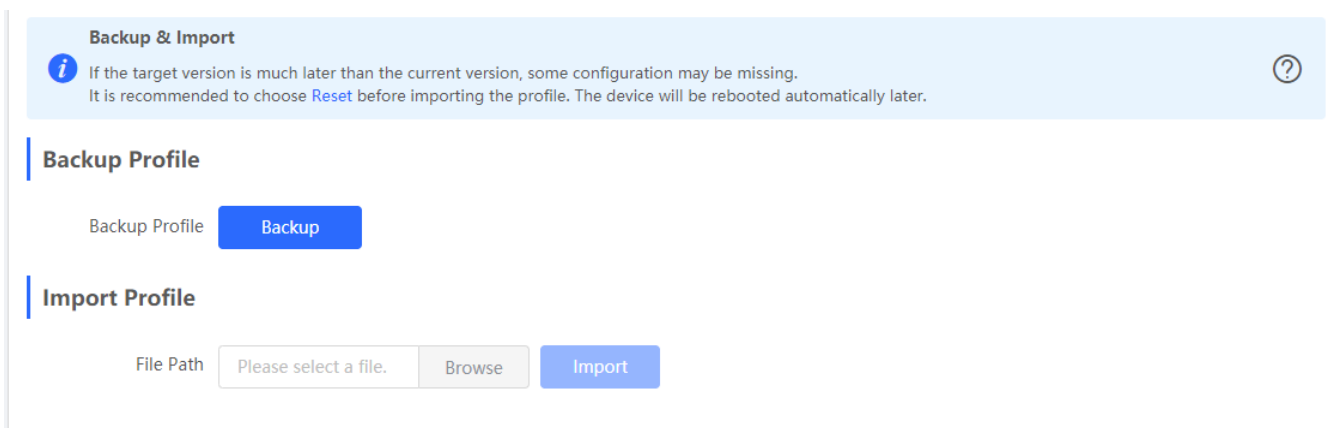
Figure 3-3-136 Session Timeout



#### 3.3.8.2 Backup & Import

The **Backup & Import** module allows you to import a configuration file and apply the imported settings. It also allows exporting the configuration file to generate a backup.

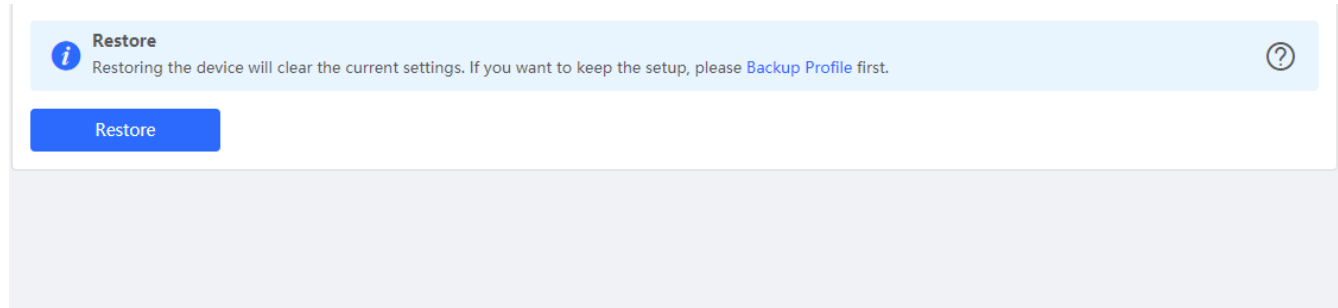
Figure 3-3-137 Backup & Import



### 3.3.8.3 Restore

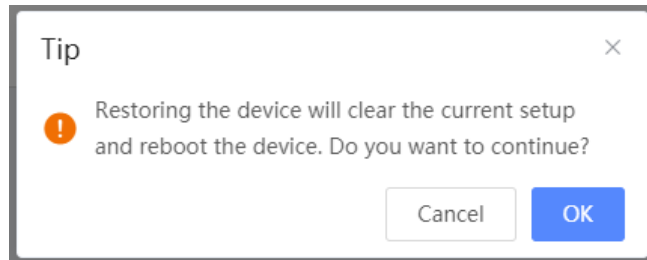
The **Restore** module allows you to restore the device to factory settings.

Figure 3-3-138 Restore



Please exercise caution if you want to restore the factory settings.

Figure 3-3-139 Confirm Restore



Click **OK** to restore all default values. This function is recommended when the network configuration is incorrect or the network environment is changed..

### 3.3.8.4 Online upgrade

Click **Upgrade Now**. The device downloads the upgrade package from the network, and upgrades the current version. The upgrade operation retains configuration of the current device. Alternatively, you can select **Download File** to the local device and import the upgrade package on the **Local Upgrade** page. If there is no available new version, the device displays a prompt indicating that the current version is the latest.

Figure 3-3-140 Online Upgrade

**Online Upgrade**  
Online upgrade will keep the current setup. Please do not refresh the page or close the browser. You will be redirected to the login page automatically after upgrade.

Current Version EG\_3.0(1)B11P35,Release(07241700) (It is the latest version.)

### 3.3.8.5 Local Upgrade

Click **Browse** to select an upgrade package, and click **Upload**. After uploading and checking the package, the device displays the upgrade package information and a prompt asking for upgrade confirmation. Click **OK** to start the upgrade.

Figure 3-3-141 Local Upgrade

**Local Upgrade**  
Please do not refresh the page or close the browser.

Model EG205G

Current Version EG\_3.0(1)B11P35,Release(07241700) 1.00

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

Mode

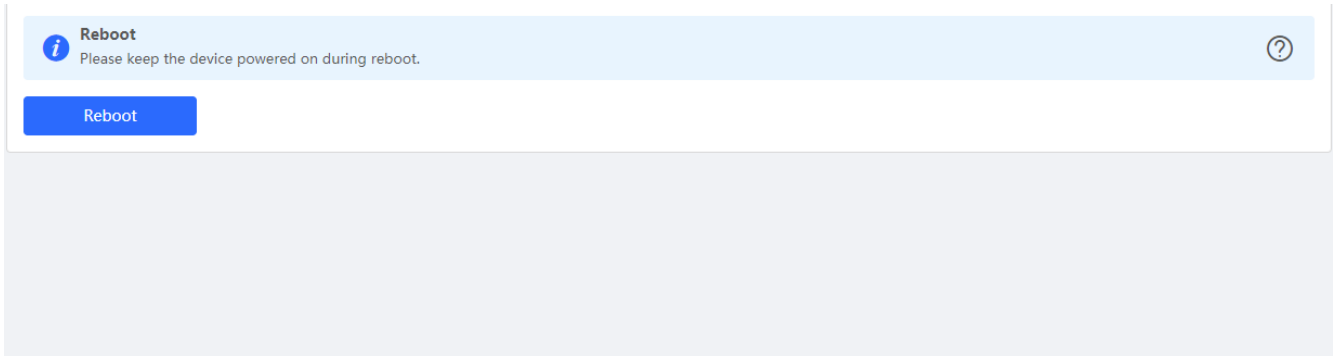
Keep Setup  (If the target version is much later than the current version, it is recommended not to keep the setup.)

File Path

### 3.3.8.6 Reboot

The **Reboot** module allows you to reboot the device immediately.

Figure 3-3-142 Reboot

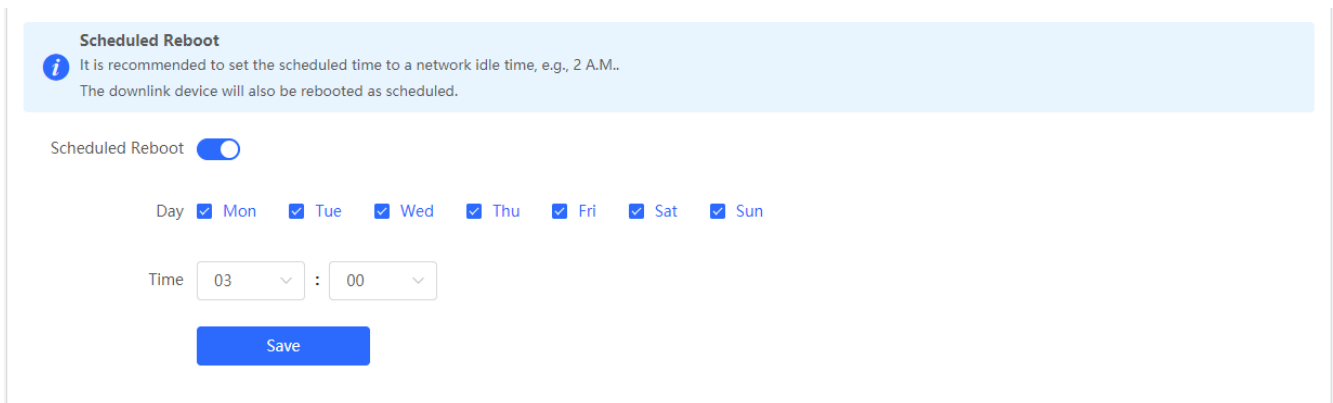


Click **Reboot**, and click **OK** in the confirmation box. The device is rebooted and you need to log into the eWeb management system again after the reboot. Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the eWeb service becomes available, you will be redirected to the login page of the eWeb management system.

### 3.3.8.7 Scheduled Reboot

The **Scheduled Reboot** module allows you to reboot the device at a scheduled time.

Figure 3-3-143 Scheduled Reboot



Enable scheduled reboot, select the time and click **Save**.

## 3.4 Wireless

### 3.4.1 APs

The **APs** module allows you to group, upgrade and delete APs.

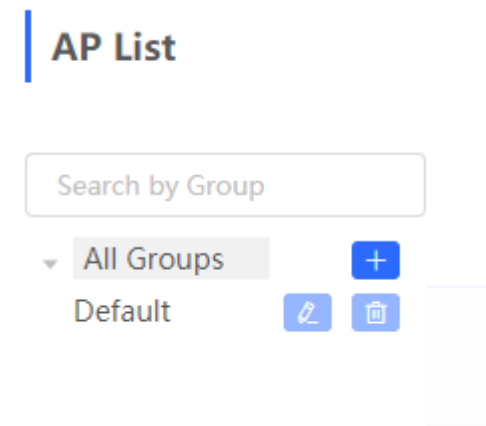
Figure 3-4-1 AP List



The screenshot shows the 'AP List' management interface. At the top, there is a header with an information icon and a help icon. Below the header, the title 'AP List' is followed by a 'Group: All Groups' dropdown and buttons for 'Expand', 'Advanced Search', 'List Filter', and 'Batch Action'. The main area contains a table with the following columns: Action, Hostname, IP Address, MAC, Status, Model, Clients, and Software Ver. A single row of data is displayed for an AP with Hostname 'Rujjie', IP Address '192.168.110.200', MAC '00:10:F8:75:33:72', Status 'Online', Model 'EAP602', Clients '0', and Software Ver 'AP\_3.0(1)B2P32,Release(07210117)'. Below the table, there is a pagination control showing 'Total 1', '10/page', and 'Go to page 1'.

Click **Expand**, and all groups will be displayed on the left column. You can add, delete, edit and search groups. Up to 8 groups can be added.

Figure 3-4-2 Group Management



Click **Advanced Search**, and you can search APs by SN, model, software version, MAC address and status.

Figure 3-4-3 Advanced Search

Group: **All Groups**

Advanced Search

SN

Model

Software

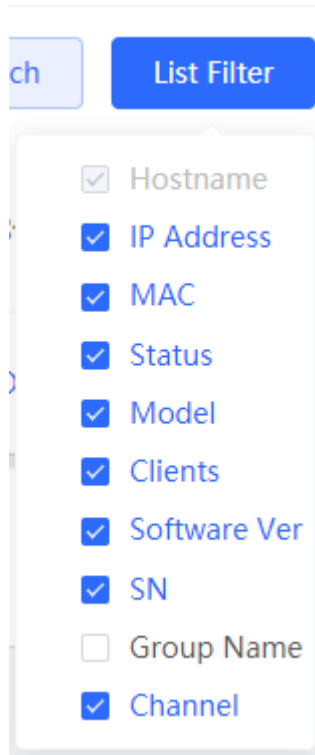
Ver

MAC

Status

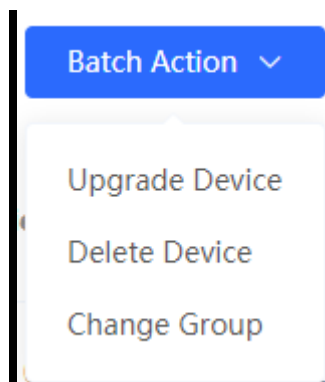
Click **List Filter**, and you can select columns to be displayed in the list.

Figure 3-4-4 List Filter



Select the target devices and click **Batch Action**. The following actions are available:

Figure 3-4-5 Batch Action



**Upgrade Device:** If there is a new version available, you can upgrade the devices in batches.

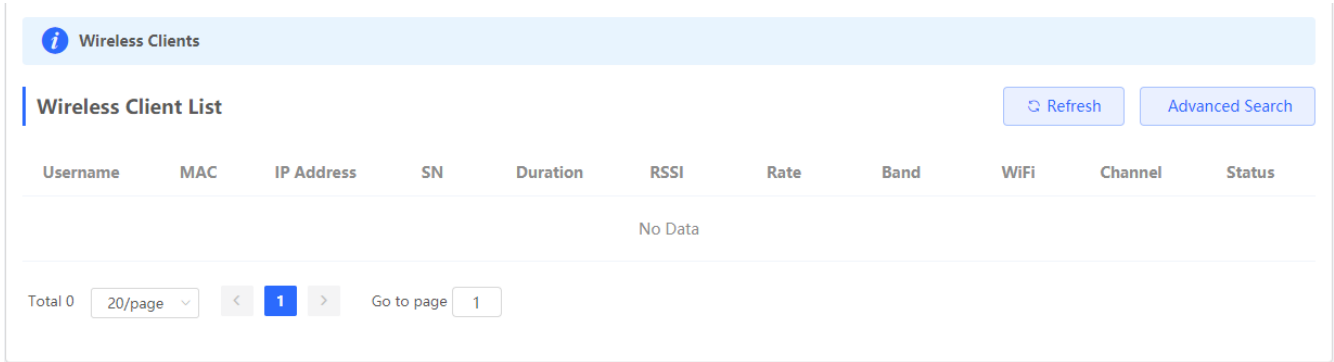
**Delete Device:** You can delete the devices in batches.

**Change Group:** You can move the devices from one group to another. The devices will be applied with the new group settings.

### 3.4.2 Clients

The **Clients** module displays the wireless clients.

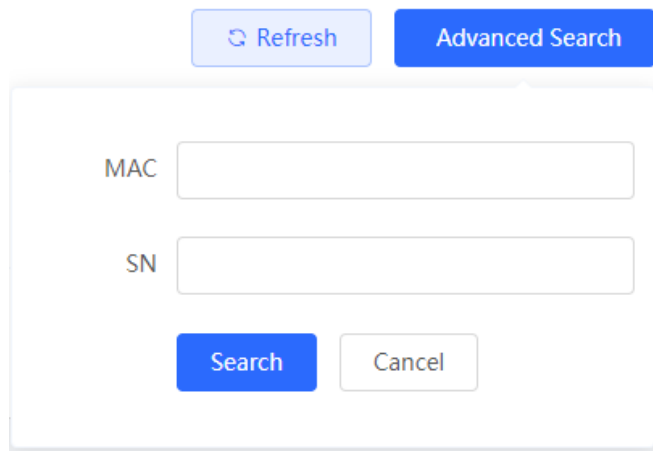
Figure 3-4-6 Wireless Client List



Click **Advanced Search**, and you can search clients by SN and MAC address.

This is a fuzzy search. You can enter an incomplete MAC address or part of an SN.

Figure 3-4-7 Advanced Search



### 3.4.3 Blacklist/Whitelist

The **Blacklist/Whitelist** module allows you to configure global blacklist/whitelist and SSID-based blacklist/whitelist.

#### 3.4.3.1 Global Blacklist/Whitelist

Figure 3-4-8 Global Blacklist/Whitelist

All STAs except blacklisted STAs are allowed to access WiFi.  Only the whitelisted STAs are allowed to access WiFi.

### Blocked WLAN Clients

[+ Add](#) [Delete Selected](#)

Up to **30** members can be added.

<input type="checkbox"/>	MAC	Remark	Action
<input type="checkbox"/>	00:74:9C:63:81:AA	test	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	22:16:87 <span style="border: 1px solid green; padding: 2px;">OUI</span>	test	<a href="#">Edit</a> <a href="#">Delete</a>

Click **Add** to add a blacklisted or whitelisted client. In the displayed dialog box, configure settings and click **OK**.

Figure 3-4-9 Add Client

**Add** ×

Match Type  Full  Prefix (OUI)

\* MAC

Remark

### 3.4.3.2 SSID-based Blacklist/Whitelist

Select an SSID from the left column and configure its blacklist or whitelist.

Figure 3-4-10 SSID-basd Blacklist/Whitelist

Blacklist/Whitelist is used to allow or reject a client's request to connect to the WiFi 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 WiFi network.
2. In the Whitelist mode, only the clients in the whitelist are allowed to connect to the WiFi network.

Device Group: Default

SSID-Based Blacklist/Whitelist

All STAs except blacklisted STAs are allowed to access WiFi.  Only the whitelisted STAs are allowed to access WiFi.

**Blocked WLAN Clients** + Add Delete Selected

Up to 30 members can be added.

<input type="checkbox"/>	MAC	Remark	Action
<input type="checkbox"/>	8C:AB:8E:A2:21:67	test	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	9C:AB:8E <span>OUI</span>	OUI	<a href="#">Edit</a> <a href="#">Delete</a>

### 3.4.4 Radio Frequency

The **Radio Frequency** module allows you to configure client count limit and channel width.

Figure 3-4-11 Radio Frequency (EG Device)

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

**Radio Frequency** Device Group: Default

Country/Region: China (CN)

**2.4G** Channel Width: Auto **5G** Channel Width: Auto

Client Count Limit: 32 Client Count Limit: 32

Save

Only the AP supports power and roaming sensitivity settings.

Figure 3-4-12 Radio Frequency (EAP)

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

### Radio Frequency

Country/Region

2.4G Channel Width

5G Channel Width

Client Count Limit

Client Count Limit

The settings are valid for only **current device**

2.4G Channel

5G Channel

Transmit Power

Transmit Power

Roaming Sensitivity

Roaming Sensitivity

**Save**

## 3.4.5 WiFi

The **WiFi** module allows you to configure WiFi settings for all devices.

### 3.4.5.1 WiFi Settings

The **WiFi Settings** module allows you to configure the primary WiFi.

Figure 3-4-13 WiFi Settings

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

**WiFi Settings** Device Group:

\* SSID

Band

Security

\* WiFi Password

[Expand](#)

**Save**

### 3.4.5.2 Guest WiFi

The guest WiFi is disabled by default. You can enable guest WiFi on this page or homepage.

AP isolation is enabled by default and cannot be edited.

Set a schedule, and the guest WiFi will be enabled only during this period time. When the time expires, the guest WiFi will be disabled.

Figure 3-4-14 Guest WiFi

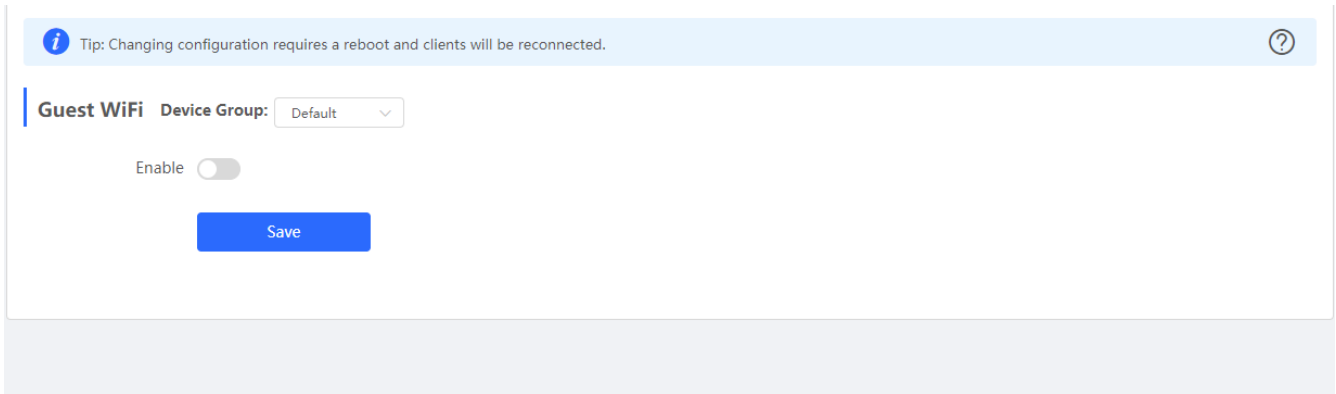
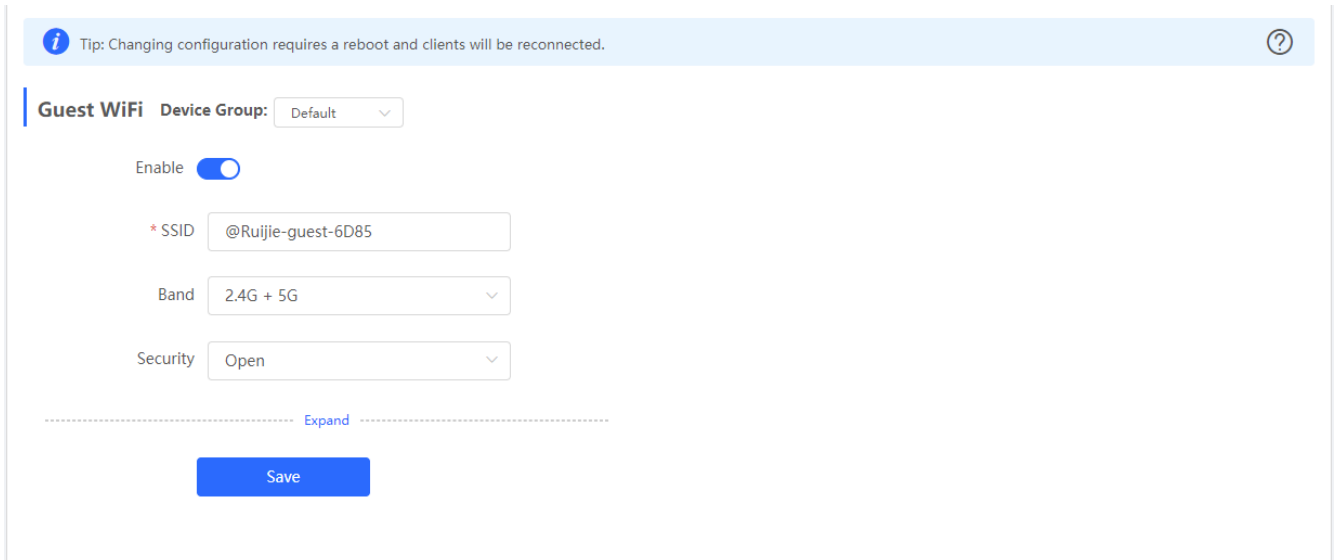


Figure 3-4-15 Enable Guest WiFi



### 3.4.5.3 WiFi List

The **WiFi List** displays all WiFi networks. The primary WiFi is also listed here and cannot be deleted.

Figure 3-4-16 WiFi List



**WiFi List** Device Group: Default + Add

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
lghtest	2.4G	WPA_WPA2-PSK	No	Default VLAN	<a href="#">Edit</a> <a href="#">Delete</a>
ttttt	2.4G + 5G	OPEN	No	Default VLAN	<a href="#">Edit</a> <a href="#">Delete</a>
333	2.4G + 5G	OPEN	No	Default VLAN	<a href="#">Edit</a> <a href="#">Delete</a>
lghtest_5g	5G	WPA_WPA2-PSK	No	Default VLAN	<a href="#">Edit</a> <a href="#">Delete</a>

Click **Add** to add a WiFi network. In the displayed dialog box, configure settings and click **OK**.

Figure 3-4-17 Add WiFi

**Add** ×

**i** The configuration will take effect after being delivered to EAP.

\* SSID

Band 2.4G + 5G ▼

Security Open ▼

----- [Expand](#) -----

Cancel OK

You can click ? in the upper right corner to see description about each configuration item.

### 3.4.5.4 Healthy Mode

The **Healthy Mode** module allows you to enable health mode and set a schedule.

Figure 3-4-18 Healthy Mode

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

**Healthy Mode** Device Group: Default

Healthy Mode

[Save](#)

### 3.4.5.5 Load Balancing

**Load Balancing** [+ Add](#) [Delete Selected](#)

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.

<input type="checkbox"/>	Group Name	Type	Rule	Members	Action
<input type="checkbox"/>	111111	Client Load Balancing	Threshold: 1 Client Count Difference: 1 Max Denial Count: 2	<a href="#">7Members Details</a>	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	testliu	Client Load Balancing	Threshold: 5 Client Count Difference: 5 Max Denial Count: 5	<a href="#">12Members Details</a>	<a href="#">Edit</a> <a href="#">Delete</a>

Click **Add** to add a Load Balancing. In the displayed dialog box, configure settings and click **OK**.

**Add**
✕

**\* Group Name**

**\* Type** Client Load Balancing ▼

**\* Rule** 3 i 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. ▼

Cancel
OK

### 3.4.6 LAN Ports

The **LAN Ports** module allows you to configure LAN ports.

Figure 3-4-19 LAN Ports

**LAN Port Settings**

i The configuration takes effect only for the AP with a LAN port, e.g., EAP101.  
Note: The configured LAN port settings prevail. The EAP 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 EAP device with no LAN port settings i

[Save](#)

**LAN Port Settings** [+ Add](#) [Delete Selected](#)

Up to 8 VLAN IDs or 32 APs can be added (0 APs have been added).

<input type="checkbox"/>	VLAN ID ⇅	Applied to	Action
No Data			

Click **Add** to add a LAN port. In the displayed dialog box, configure settings and click **OK**.

Figure 3-4-20 Add LAN Port

Add
×

VLAN ID

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

\* Applied to

Cancel
OK

### 3.4.7 LED

The **LED** module allows you to enable LED.

Figure 3-4-21 LED

**LED Status Control**  
Control the LED status of **the downlink AP**.

LED

**Save**

### 3.4.8 WIO

#### 3.4.8.1 Network Optimization



**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



### Scheduled Optimization

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

Enable

Day Sun

Time 03 : 00

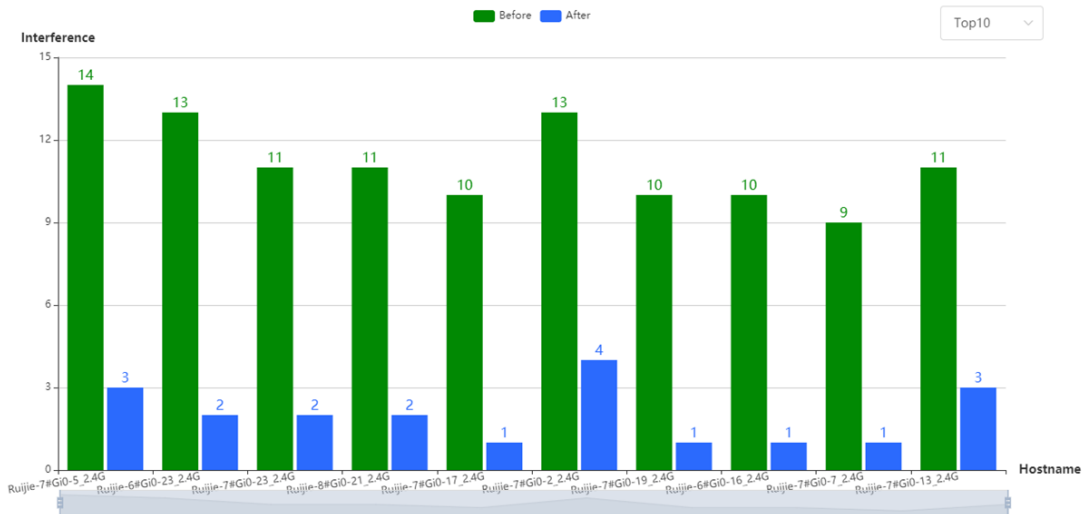
Save

### 3.4.8.2 Optimization Record

#### Overview

Last Optimized   
You have optimized 101 APs and improved the performance by 75.77%

Overview Details



#### Details

Last Optimized: [redacted]  
You have optimized 101 APs and improved the performance by 75.77%!

Overview Details

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-7#Gi0-5	2.4G	CAN [redacted]	0/6	20	auto/45	0/74	14/3	0	14/3
Ruijie-6#Gi0-23	2.4G	GI [redacted]	0/11	20	100/45	0/80	13/2	0	13/2
Ruijie-7#Gi0-23	2.4G	CA [redacted]	0/6	20	100/45	0/74	11/2	0	11/2
Ruijie-8#Gi0-21	2.4G	C [redacted]	0/6	20	auto/45	0/74	11/2	0	11/2
Ruijie-7#Gi0-17	2.4G	CA [redacted]	0/1	20	100/45	0/74	10/1	0	10/1
Ruijie-7#Gi0-2	2.4G	CAN [redacted]	0/11	20	auto/45	0/74	13/4	0	13/4
Ruijie-7#Gi0-19	2.4G	CA [redacted]	0/1	20	100/45	0/74	10/1	0	10/1
Ruijie-6#Gi0-16	2.4G	GI [redacted]	0/1	20	100/45	0/80	10/1	0	10/1
Ruijie-7#Gi0-7	2.4G	C [redacted]	0/1	20	100/45	0/74	9/1	0	9/1
Ruijie-7#Gi0-13	2.4G	CA [redacted]	0/1	20	auto/45	0/74	11/3	0	11/3

< 1 2 3 4 5 6 ... 20 > 10/page Total 200

### 3.5 Switches

The **Switches** page displays all switches in the current network.

Figure 3-5-1 Switch List

**Switch List**  
View switches in the current network.

Delete Offline Devices Batch Upgrade

<input type="checkbox"/>	Action	Hostname	IP Address	MAC	Status	Model	Software Ver	SN
<input type="checkbox"/>	Manage	Ruijie <a href="#">ℹ</a>	192.168.110.89	00:D3:F8:15:08:5B	Online	NBS5200-24SFP/8GT4XS	[redacted]	G1NW31N000:
<input type="checkbox"/>	Manage	Ruijie <a href="#">ℹ</a>	192.168.110.178	00:D0:F8:15:08:61	Online	NBS3100-24GT4SFP-P	[redacted]	12349425700

< 1 > 10/page Total 2

Click **Manage** in the **Action** column, and the switch management page will be displayed.

Figure 3-5-2 Switch Management

Switch

● **NBS5200-24SFP/8GT4XS**

Hostname: Ruijie      SN: G1NW31N000172      IP Address: 192.168.110.89

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

Reboot

[Home](#)   [VLAN](#)   [Monitor](#) ▾   [Ports](#) ▾   [L2 Multicast](#)   [L3 Interfaces](#)   [Security](#) ▾   [Advanced](#) ▾   [Diagnostics](#) ▾   [System](#) ▾

---

### Basic Info

Hostname: [Ruijie](#) ↗

Model: NBS5200-24SFP/8GT4XS

Status: ● Online

Master Device IP: [192.168.110.1](#)

Work Mode: [Self-Organizing Network](#) ↗

MGMT IP: [192.168.110.89](#) Ⓞ

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

SN: G1NW31N000172

Software Ver: ██████████

System: 2021-03-02 14:53:46

Duration: 03Hr03Min37Sec

---

### Port Info 🔍 [Panel View](#)

The flow data will be updated every 5 minutes. [🔄 Refresh](#)

Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
Gi1	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi2	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi3	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi4	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi5	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0

See *Ruijie RG-NBS Series Switches Web-Based Configuration Guide* for details.

## 3.6 System

### 3.6.1 Time

The **Time** module allows you to set the system time. The system time is synchronized with the NTP server by default.

Select a time zone and set at least one NTP server, and click **Save**.

Figure 3-6-1 System Time

116



System Time
?

Configure and view system time (The device has no RTC module. The time settings will not be saved upon reboot).

Current Time 2020-06-23 14:46:52 Edit

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

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

1.cn.pool.ntp.org Delete

cn.pool.ntp.org Delete

pool.ntp.org Delete

asia.pool.ntp.org Delete

europe.pool.ntp.org Delete

rdate.darkorb.net Delete

Save

You can also edit the tiime manually by clicking **Edit**.

Edit
×

\* Time ⌚ Select a time. Current Time

Cancel
OK

### 3.6.2 Password

The **Device Password** module allows you to set the device's login password. You need to log into the system again after changing the password.

Figure 3-6-2 Device Password

**Device Password** ?

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

\* Old Password

\* New Password

\* Confirm Password

**Save**

### 3.6.3 Scheduled Reboot

The **Scheduled Reboot** module allows you to reboot all devices at a scheduled time.

Figure 3-6-3 Scheduled 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.

Scheduled Reboot

**Save**

### 3.6.4 Reboot & Reset

The **Reboot & Reset** module allows you to reboot or reset all devices in the network.

Figure 3-6-4 Reboot

**Network Management** ?

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

**Network Management**

Action **Reboot** Reset

Select **All Devices** Specified Devices

**OK**

If you click **Reboot**, you will be allowed to select all devices or specified devices for the action.

If you click **Reset**, all devices in the network will be reset to the factory settings. You can select whether to unbind the account.

Figure 3-6-5 Reset

**Network Management** ?

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

**Network Management**

Action

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

## 4 FAQs

### Q1: I failed to log into the eWeb management system. What can I do?

Perform the following steps:

- (1) Check that the network cable is properly connected to the LAN port of the device and the corresponding LED indicator blinks or is steady on.
- (2) Before accessing the configuration GUI, set the IP assignment mode to **Obtain an IP address automatically** (recommended), so that the server with DHCP enabled can automatically assign an IP address to the PC. To designate a static IP address to the PC, set the IP address of the PC in the same network segment as the IP address of the management interface. For example, if the default IP address of the management interface is 192.168.110.1 and the subnet mask is 255.255.255.0, set the IP address of the PC to 192.168.110.X (X is any integer ranging from 2 to 254), and the subnet mask is 255.255.255.0.
- (3) Run the **ping** command to test the connectivity between the PC and the device.
- (4) If the login failure persists, restore the device to factory settings.

### Q2: What can I do if I forget my username and password? How to restore the factory settings?

To restore the factory settings, power on the device, and press and hold the **Reset** button for 5s or more, and release the **Reset** button after the system LED indicator blinks. The device automatically restores the factory settings and restarts. The original configuration will be lost after the factory settings are restored. After the restoration, the default management address is http://10.44.77.200. You can set the username and password upon first login.

### Q3: The subnet mask value needs to be specified to divide the address range for certain functions. What are the common subnet mask values?

A subnet mask is a 32-bit binary address that is used to differentiate between the network address and host address. The subnet and the quantity of hosts in the subnet vary with the subnet mask.

Common subnet mask values include 8 (default subnet mask 255.0.0.0 for class A networks), 16 (default subnet mask 255.255.0.0 for class B networks), 24 (default subnet mask 255.255.255.0 for class C networks), and 32 (default subnet mask 255.255.255.255 for a single IP address).