



**Ruijie Reyee Series Products**  
**Web-Based Configuration Guide**

## **Copyright Statement**

Ruijie Networks©2020

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</b> font	Commands, command options, and keywords are in <b>boldface</b> .
<i>italic</i> font	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**).

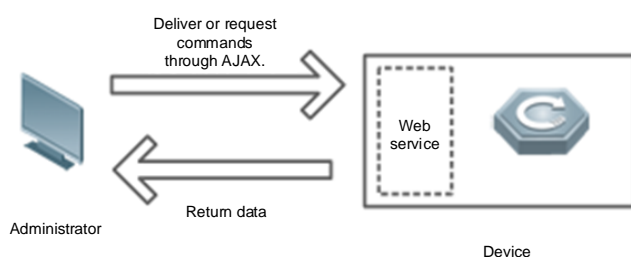
## 2 Configuration Guide

### 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 2-1-1 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 of an EG device is 192.168.110.1. Alternatively, you can set the IP assignment mode to **Obtain an IP address automatically**.

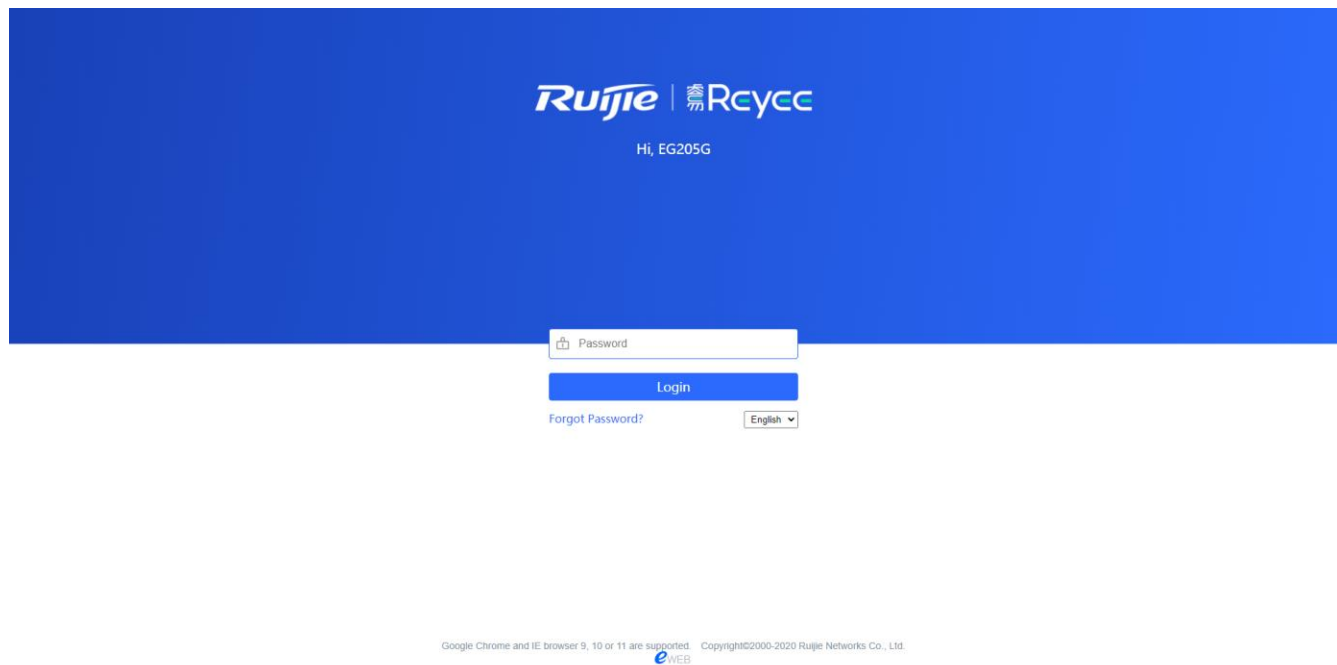
Server requirements:

- 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 2-1-2 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 2-2-1 Discover Device

**Total Devices: 4.**  
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

**My Network**

eg205g (4 devices)

	Model	SN	IP Address	MAC	Software Ver
Local Router	EG205G	H1LA0U100362A	192.168.110.1	00:74:9C:87:6D:85	EG_3.0(1)B11P30,Release(07210123)
Switch	NBS2100-16GT2SFP	MACC992570066	192.168.110.120	00:D0:F8:22:16:86	SWITCH_3.0(1)B11P20,Release(07171423)
A P	EAP602	MACC522376524	192.168.110.200	00:10:F8:75:33:72	AP_3.0(1)B2P32,Release(07210117)
Switch	RG-ES226GC-P	MACCCTCFVHUG1	192.168.110.16	00:D0:F8:48:45:88	ESW_1.0(1)B1P3,Release(07190916)

Rediscover Start Setup

## 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 2-2-2 Add Device to My Network

**Total Devices: 5. Other Devices (to be added manually): 3.**  
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

**My Network**

ruijie-net (2 devices)

	Model	SN	IP Address	MAC	Software Ver
Local Router	EG205G [Master]	MACC123201234	192.168.110.1	00:D0:F8:15:6D:8F	EG_3.0(1)B11P32,Release(07203101)
Switch	NBS5200-24SFP/8GT4XS	G1NW50E000024	172.30.111.35	00:E0:4C:00:00:2C	SWITCH_3.0(1)B11P31,Release(07203100)

**Other Devices** ⓘ

Rediscover Start Setup



## 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 2-2-3 Create Network

\* Network Name

IP Assignment  PPPoE  DHCP  Static IP  
Current Settings: DHCP

\* SSID

Security  Open

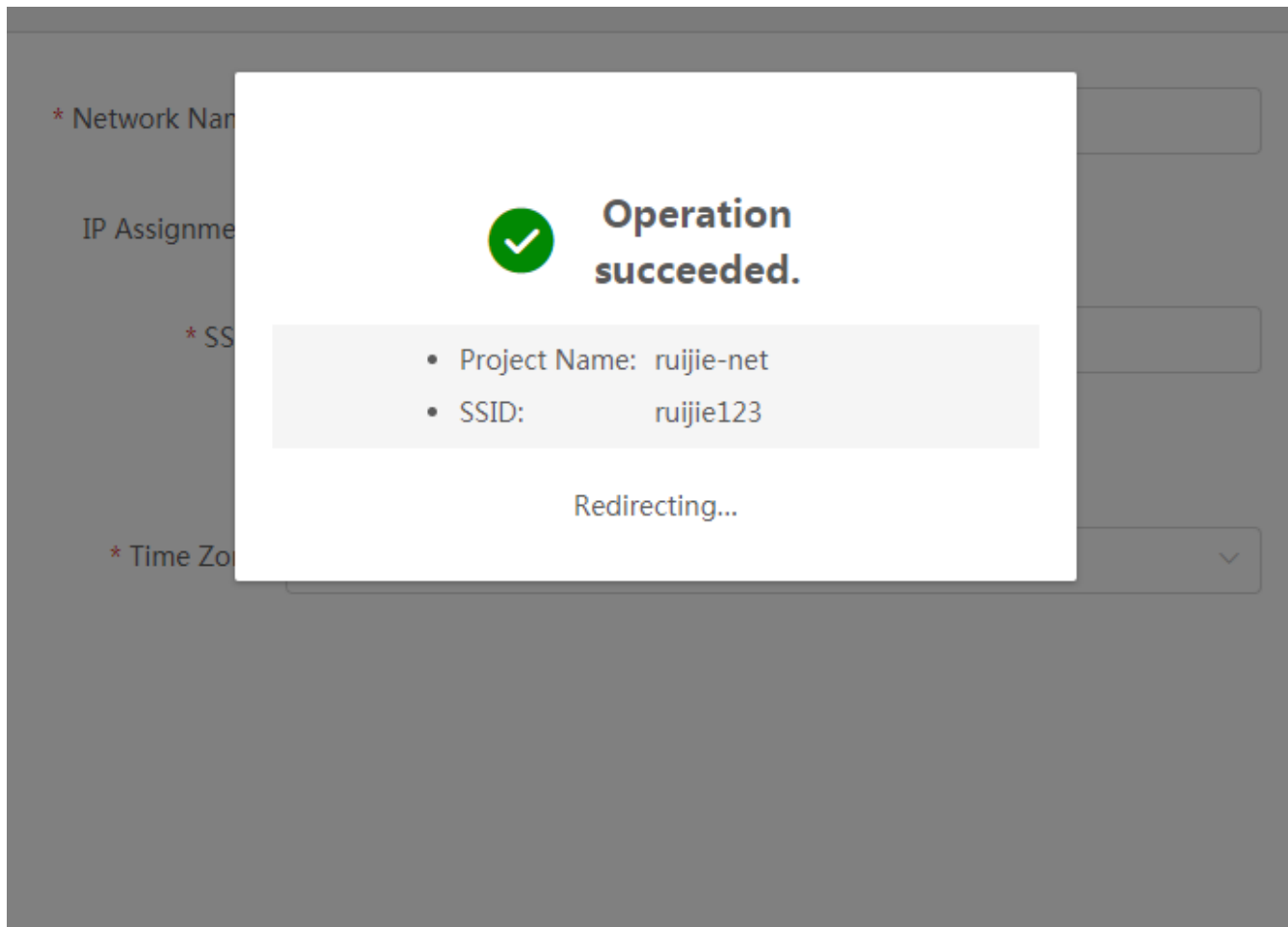
\* WiFi Password

\* Country/Region

\* Time Zone

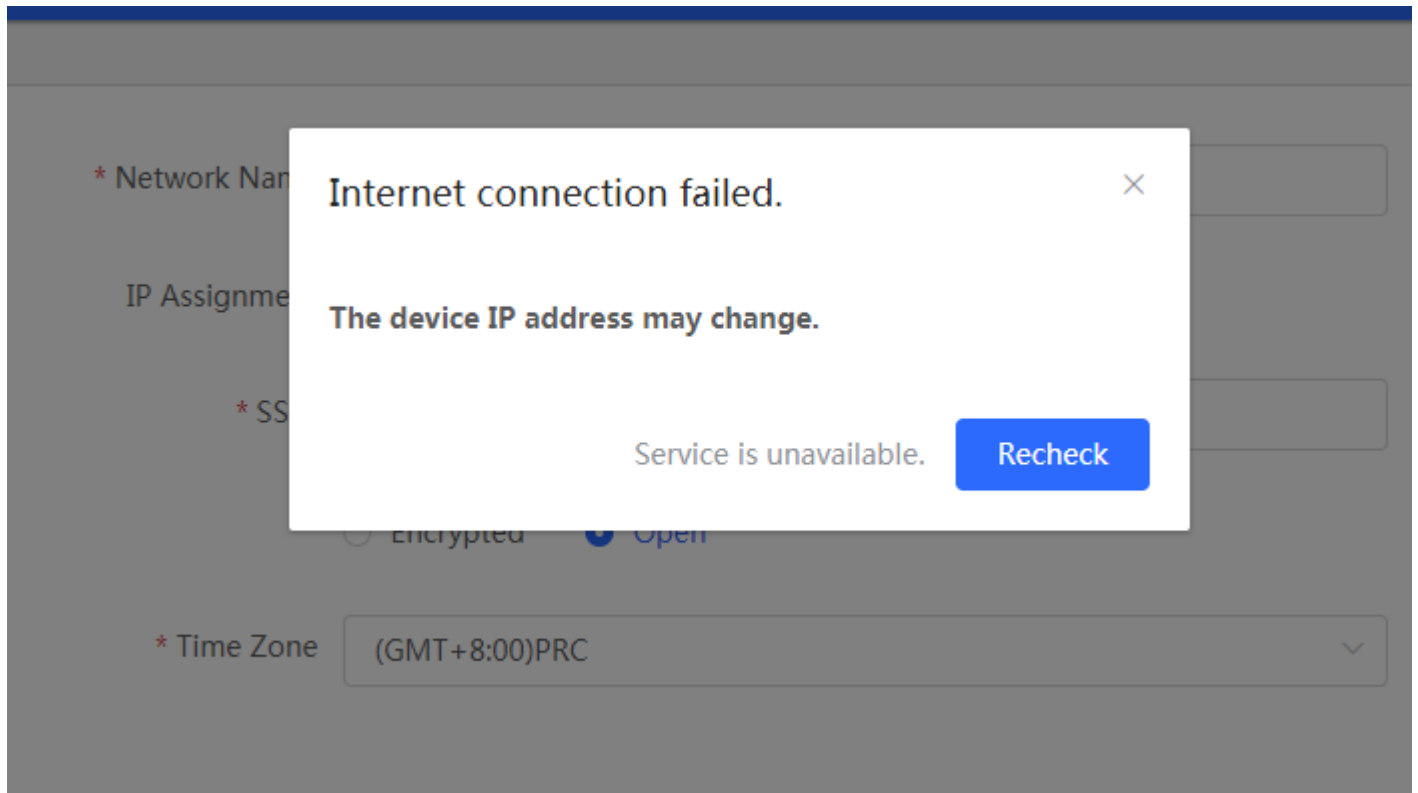
Click **Create Network & Connect**, and it takes about 60 seconds to deliver and activate settings. The following message will appear after Internet connection is set up.

Figure 2-2-4 Connect to Internet



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

Figure 2-2-5 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 2-2-6 Log In with Ruijie Cloud Account

Please enter your account to log in.

Please enter the username.

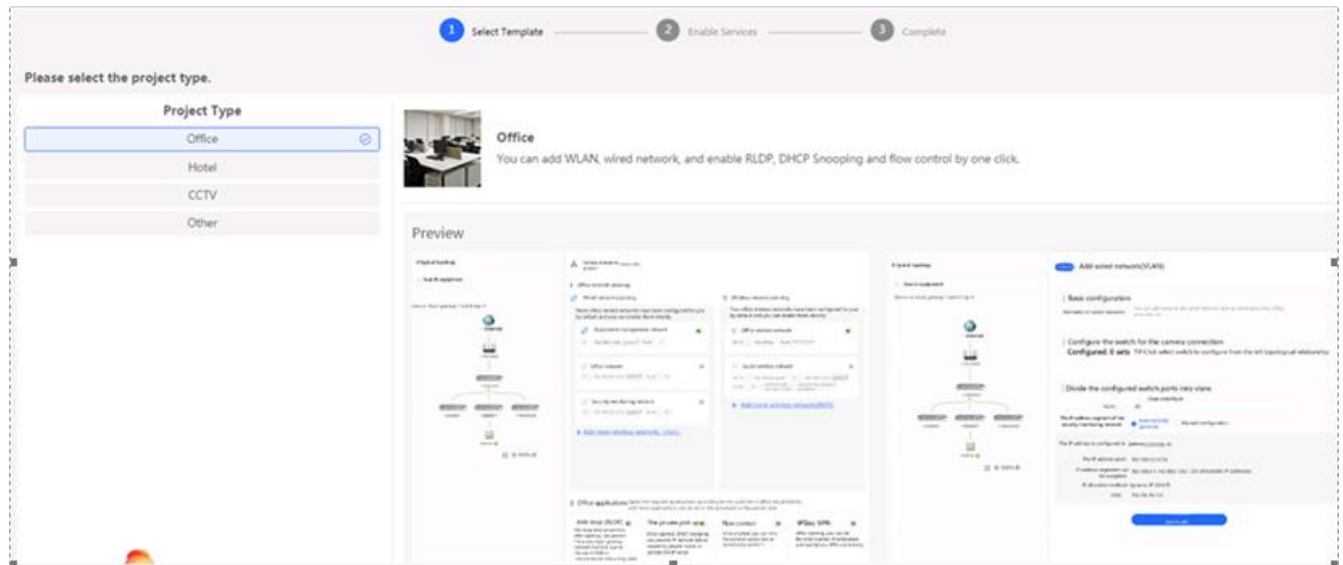
Please enter the password.

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 2-2-7 Select Template



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

Figure 2-2-8 Confirm Device Status

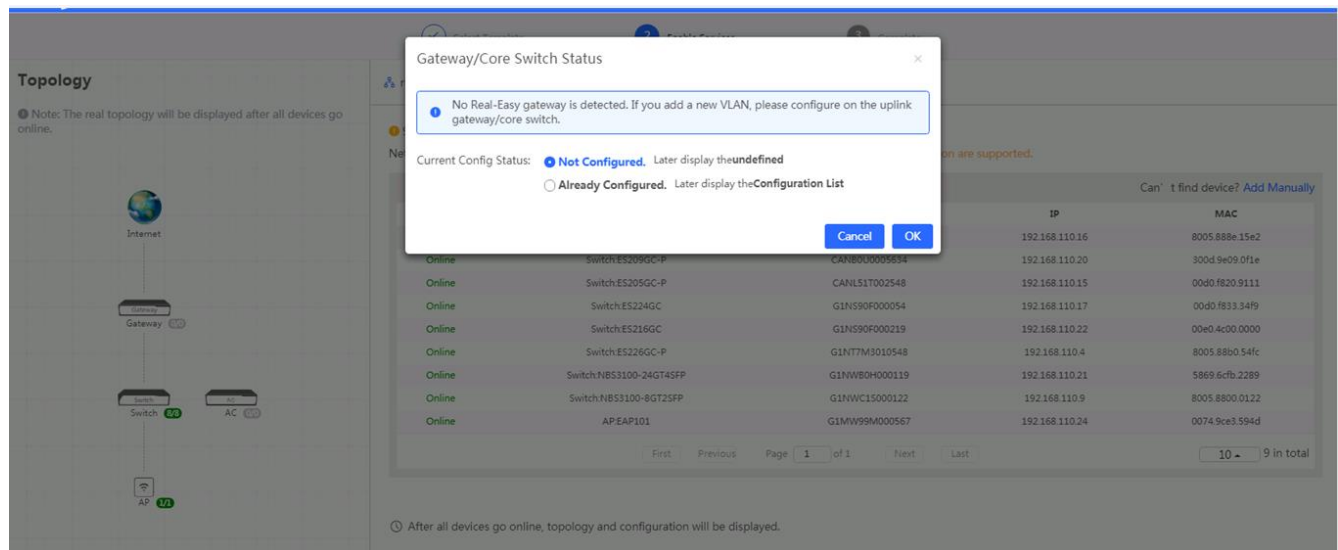
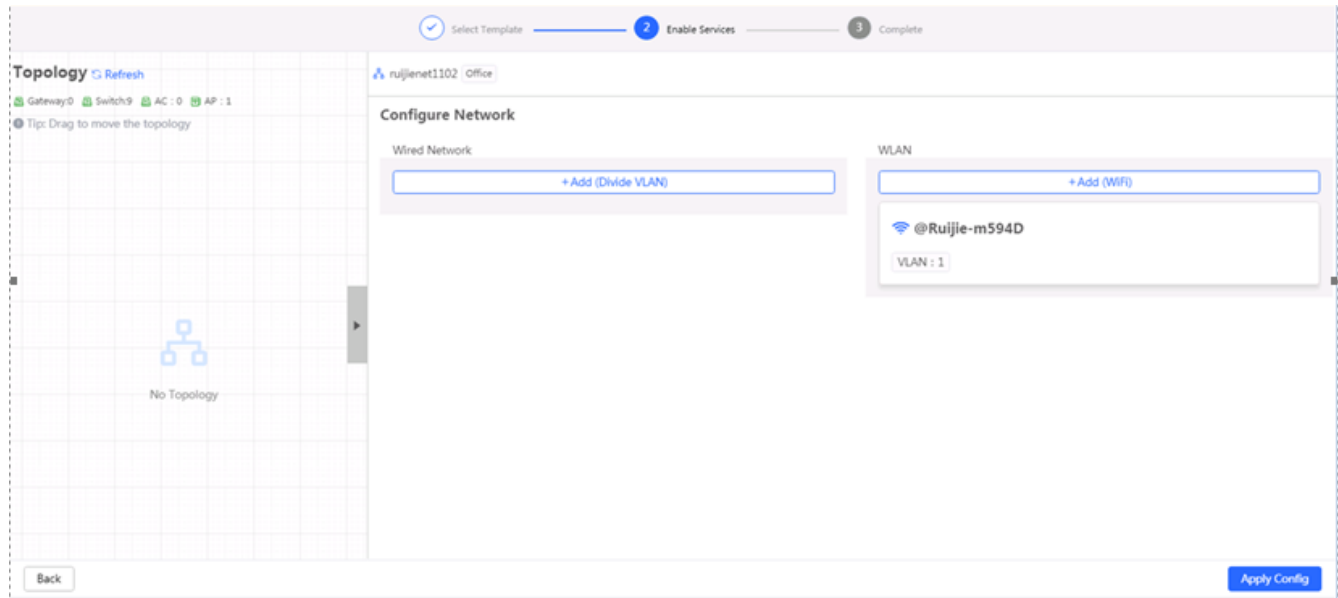
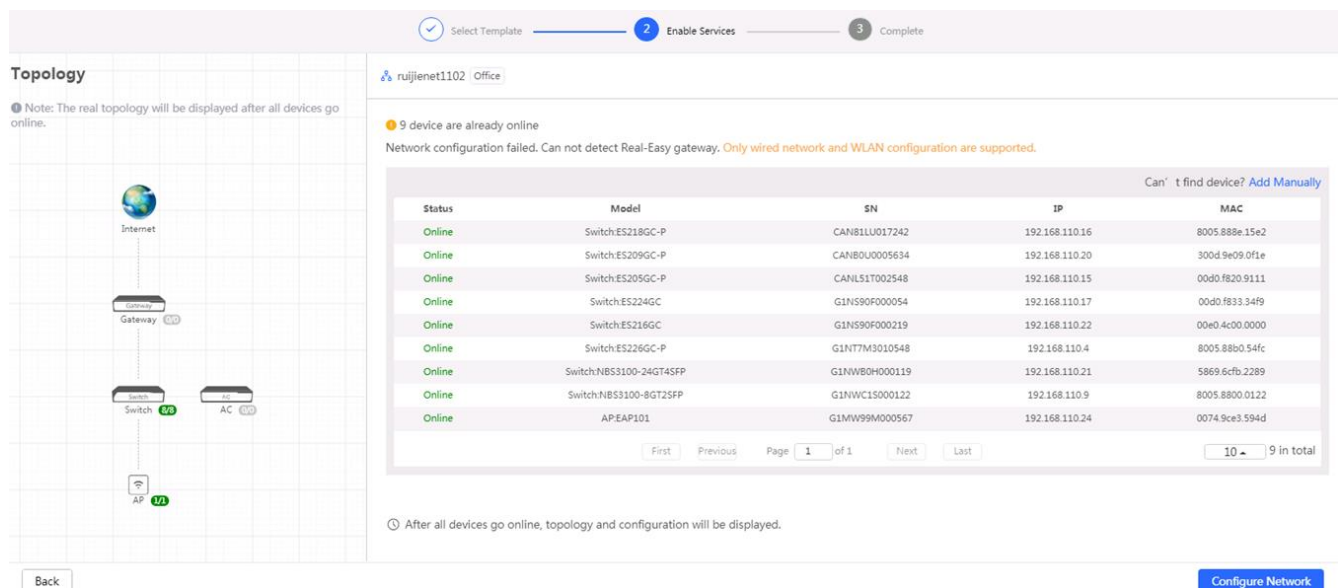


Figure 2-2-9 Enable Services



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

Figure 2-2-10 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 2-3-1 Device Overview

The screenshot displays the configuration page for a Ruijie EG205G router. At the top, the device is identified as a Router with model EG205G. Key information includes Hostname: Ruijie, 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 corner. Below this is a navigation menu with options: Overview (selected), Basics, Security, Behavior, VPN, Advanced, Diagnostics, and System.

The **Overview** section contains three summary cards: Memory Usage at 24%, Online Clients at 5, and Status: Online. The status card also shows Duration: 35Min39Sec and Systemtime: 2020-09-04 13:59:07.

The **Device Details** section lists: Model: EG205G, MAC: 00:74:9C:87:6D:85, Role: Master AC, Hostname: Ruijie, Hardware Ver: 1.00, Software Ver: EG\_3.0(1)B11P30,Release(07210123), SN: H1LA0U100362A, and Work Mode: Router.

The **Interface Details** section shows a legend for Connected (blue) and Disconnected (grey) states. Five interface icons are shown: LAN0 (grey), LAN1/WAN3 (blue, IP 192.168.110.1), LAN2/WAN2 (blue), LAN3/WAN1 (blue), and WAN (blue, IP 172.30.111.17).

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

Figure 2-3-2 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 2-4-1 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 2-4-2 Enable Self-Organizing Network



Overview

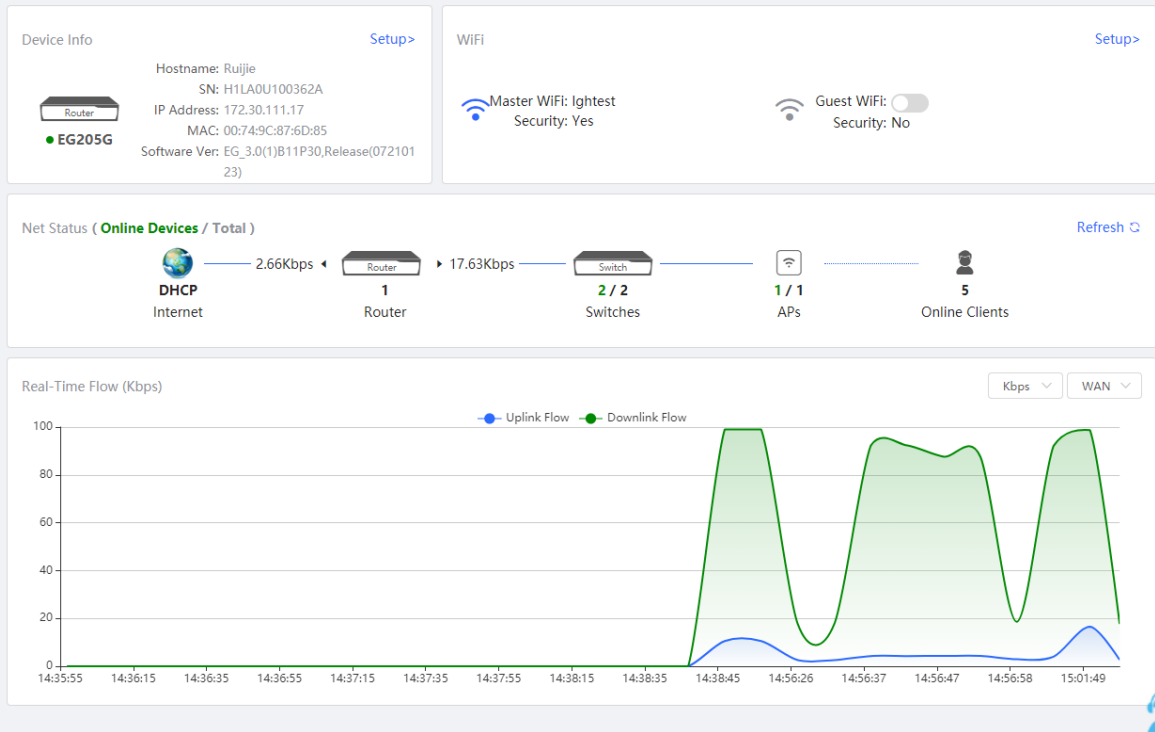
Online Clients

Router

Wireless

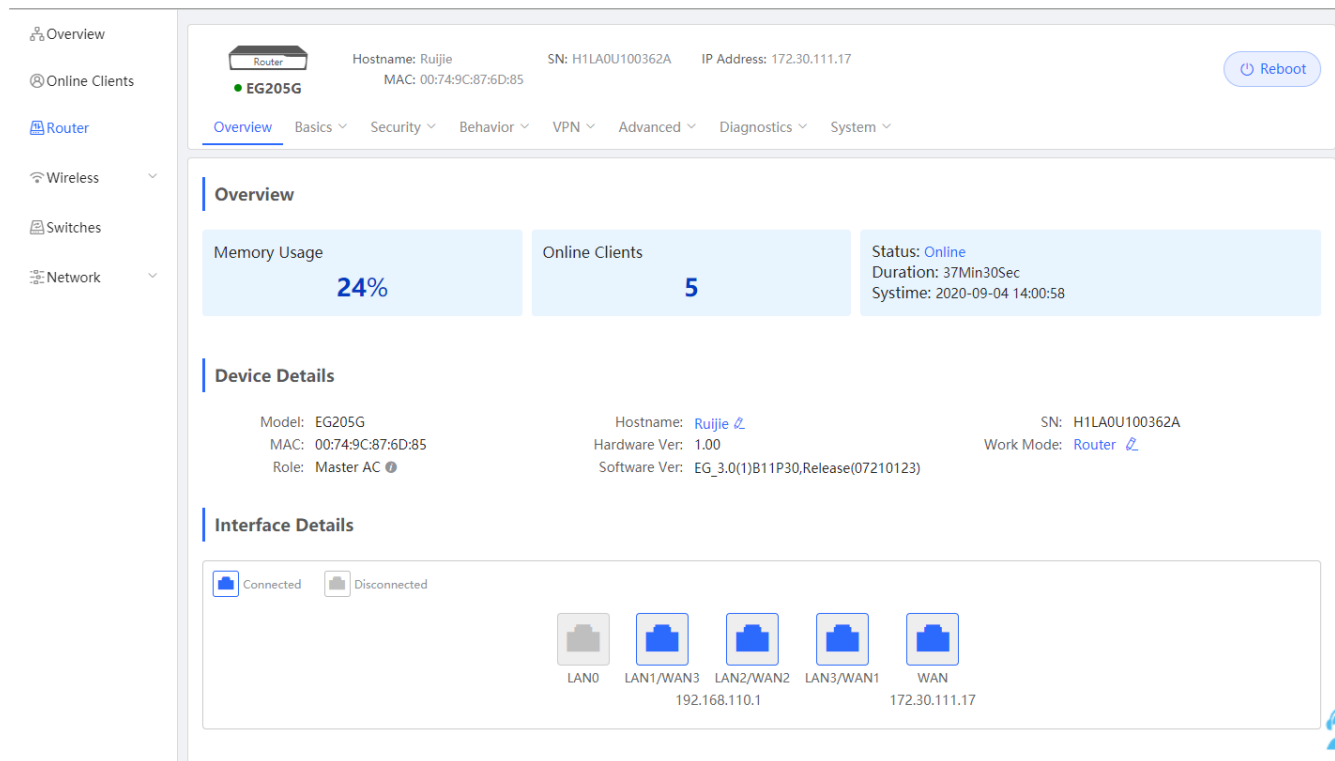
Switches

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**, and a horizontal menu will be displayed.

Figure 2-4-3 Router Menu

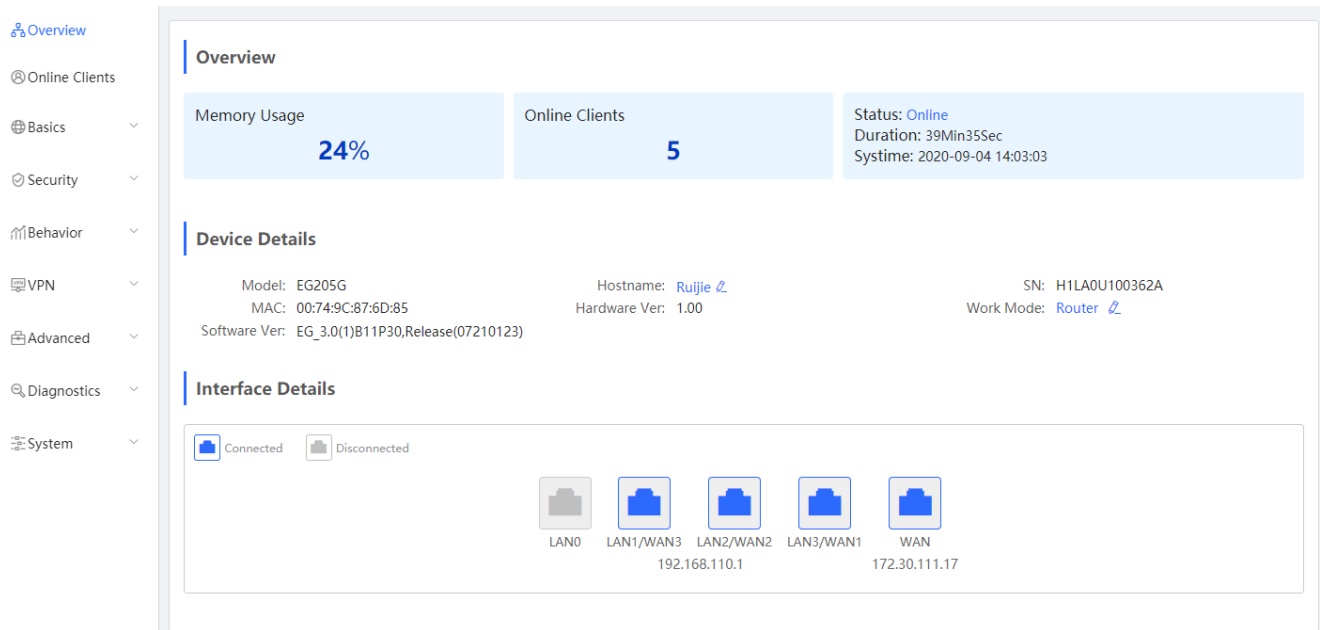


## 2.4.2 Disable

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 2-4-4 Disable Self-Organizing Network

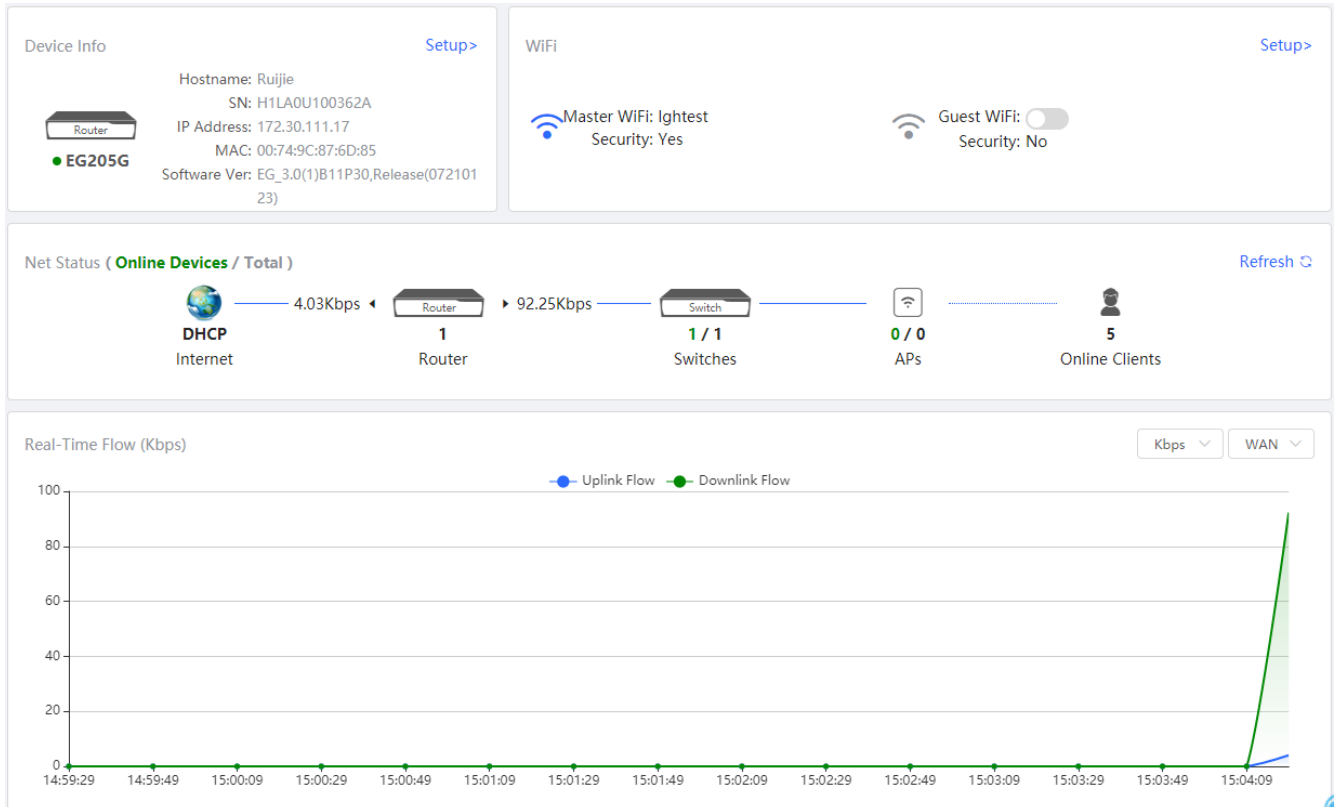


### 3 eWeb Configuration

#### 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 3-2-1 Online Clients

Online Clients
?

There is a delay of 3 minutes. After a client is offline, he will stay in the list for about 3 more minutes.

Online Clients

Refresh
Search

Username	IP Address	MAC	Access Type	Current Rate	Wireless Info	ACL
--	192.168.110.29	8c:ab:8e:a2:21:68	Wired	Up:120.00bps Down:120.00bps	--	<a href="#" style="color: #007bff; font-size: 0.8em;">Add Rule</a>
--	192.168.110.153	00:d0:f8:15:08:48	Wired	Up:1.41Kbps Down:1.18Kbps	--	<a href="#" style="color: #007bff; font-size: 0.8em;">Add Rule</a>
--	192.168.110.61	00:74:9c:87:6d:aa	Wired	Up:80.00bps Down:87.00bps	--	<a href="#" style="color: #007bff; font-size: 0.8em;">Add Rule</a>
R03605	192.168.110.136	c8:5b:76:94:00:3c	Wired	Up:1.32Kbps Down:1.39Kbps	--	<a href="#" style="color: #007bff; font-size: 0.8em;">Add Rule</a>
--	192.168.110.16	00:d0:f8:48:45:88	Wired	Up:768.00bps Down:86.00bps	--	<a href="#" style="color: #007bff; font-size: 0.8em;">Add Rule</a>

Total 5
10/page
< 1 >
Go to page
1

Figure 3-2-2 Advanced Search

Refresh
Search

IP Address

MAC

Username

Type

All Types
v

Search
Cancel

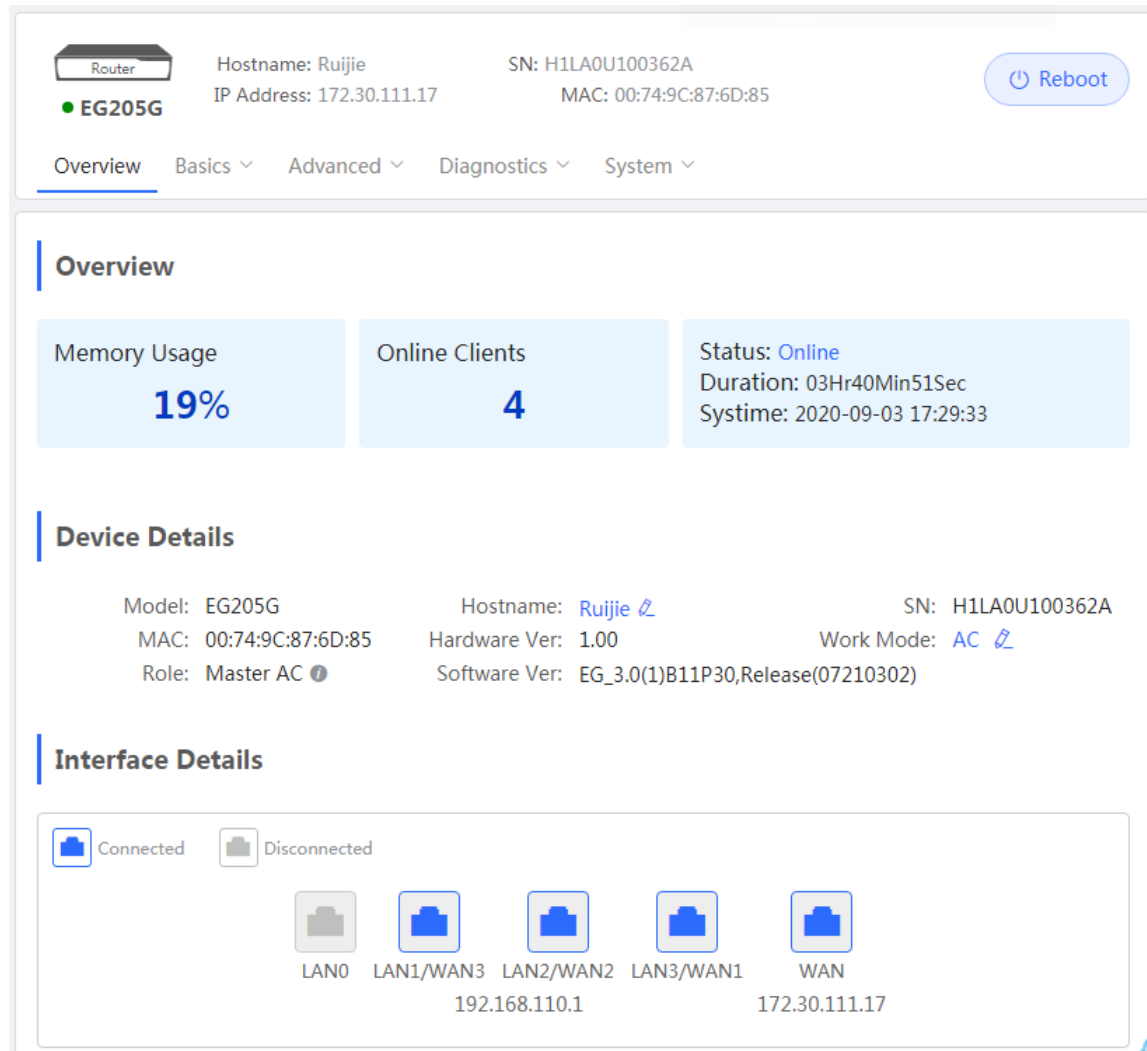
### 3.3 Router

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 3-3-1 Overview



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

Figure 3-3-2 Router Mode

The screenshot displays the eWeb Configuration interface for a Ruijie EG205G router. At the top, the router's status is shown with a 'Reboot' button. The main navigation menu includes Overview, Basics, Security, Behavior, VPN, Advanced, Diagnostics, and System. The Overview section provides a summary of system metrics: Memory Usage at 24%, 5 Online Clients, and a Status of Online with a duration of 35 minutes and 39 seconds. The Device Details section lists the model (EG205G), MAC address (00:74:9C:87:6D:85), role (Master AC), hostname (Ruijie), hardware version (1.00), software version (EG\_3.0(1)B11P30,Release(07210123)), SN (H1LA0U100362A), and work mode (Router). The Interface Details section shows the connection status of various ports: LAN0 is disconnected, while LAN1/WAN3 (192.168.110.1), LAN2/WAN2, LAN3/WAN1, and WAN (172.30.111.17) are all connected.

### 3.3.2 Basics

#### 3.3.2.1 WAN

The **WAN** module allows you to configure WAN settings. There are three IP assignment modes 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 3-3-3 WAN Settings

**WAN Settings** Configure WAN settings. ?

Single Line Dual-Line Three Lines Four Lines

\* IP Assignment

No username or password is required for DHCP clients.

IP Address

Subnet Mask

Gateway

DNS Server

Advanced Settings

Figure 3-3-4 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

Balancing Policy

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

\* WAN Weight

\* WAN1 Weight

\* WAN2 Weight

### 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 3-3-5 LAN Settings

LAN Settings

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 3-3-6 Add IP Address



Add ×

\* IP Address

\* Subnet Mask

\* VLAN ID

Remark

\* MAC

DHCP Server

\* Start

\* IP Count

\* Lease Time(Min)

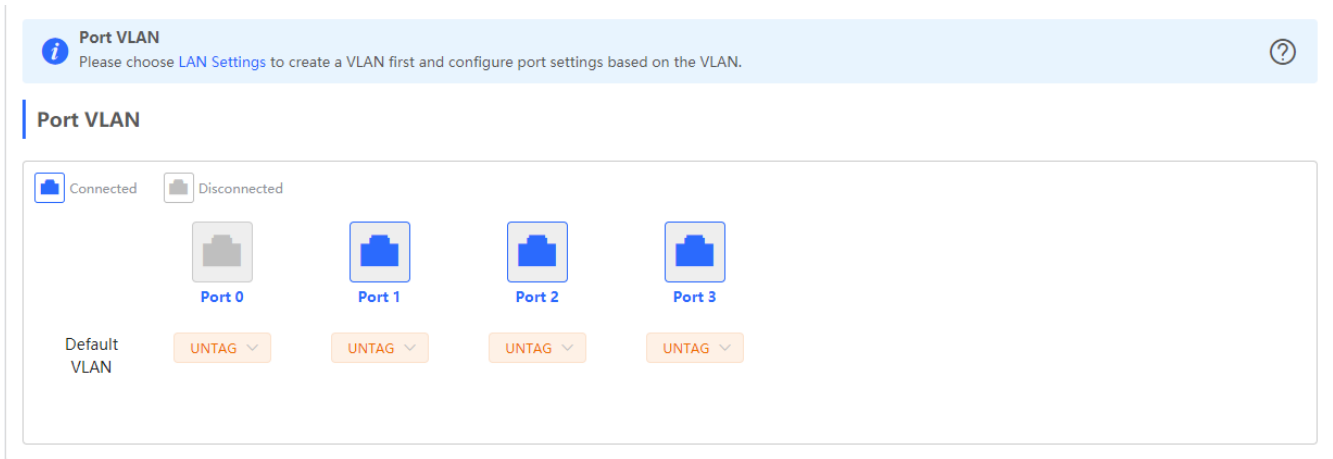
DNS Server - [?](#)

You can click [?](#) in the upper right corner to see description about each configuration item.

### 3.3.2.2.2 Port VLAN

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

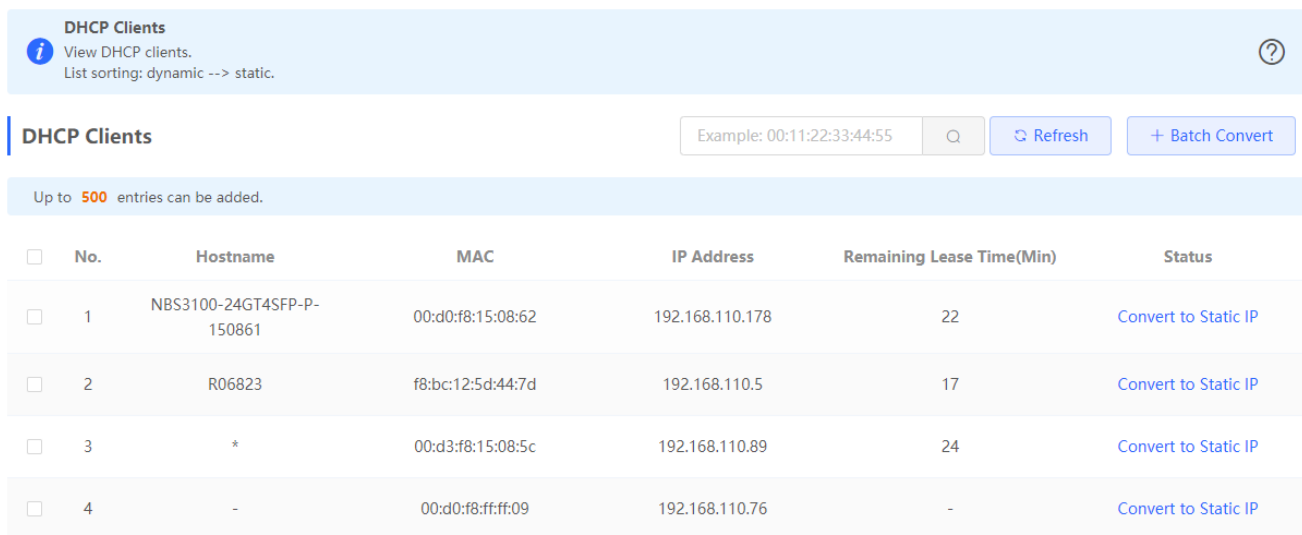
Figure 3-3-7 Port VLAN



### 3.3.2.2.3 DHCP Clients

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

Figure 3-3-8 DHCP Clients

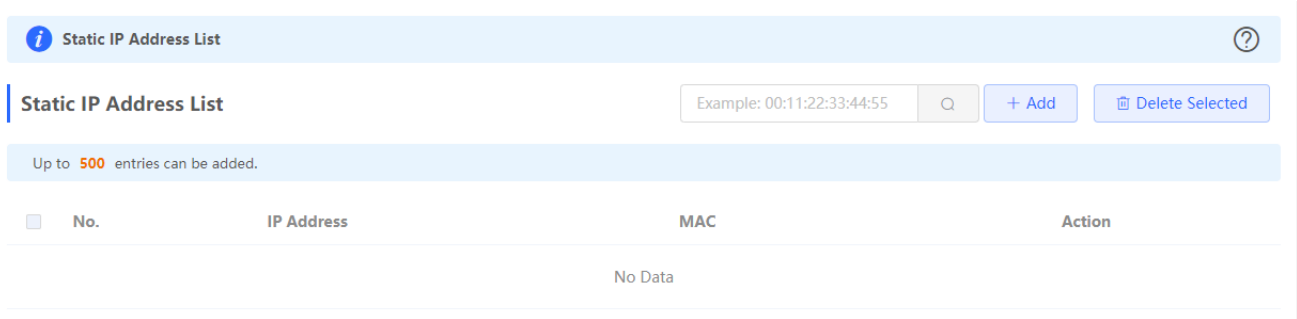


Click **Convert to Static IP** in the **Action** column to convert a DHCP-assigned IP address to a static IP address. Alternatively, select DHCP-assigned IP addresses and click **Batch Convert** to convert more than one IP address.

### 3.3.2.2.4 Static IP Addresses

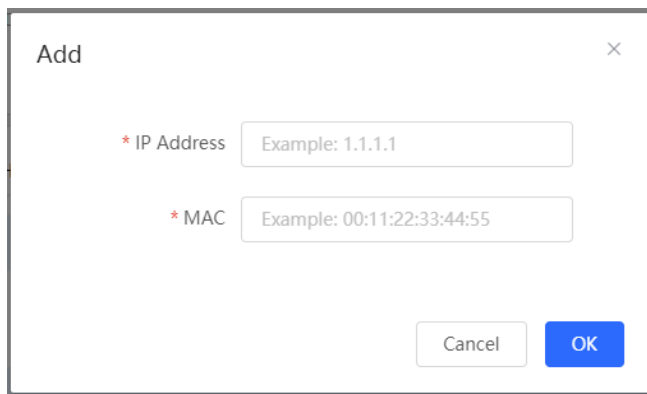
The **Static IP Addresses** module allows you to add, delete and edit static IP addresses.

Figure 3-3-9 Static IP Addresses



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

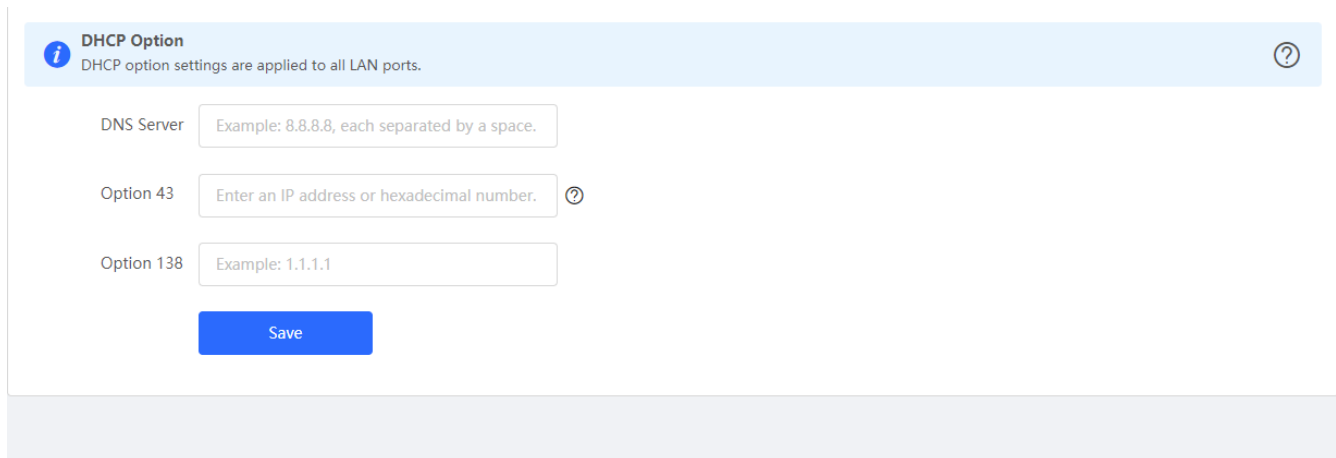
Figure 3-3-10 Add Static IP Address



### 3.3.2.2.5 DHCP Option

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

Figure 3-3-11 DHCP Option



### 3.3.2.2.6 DNS Proxy

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

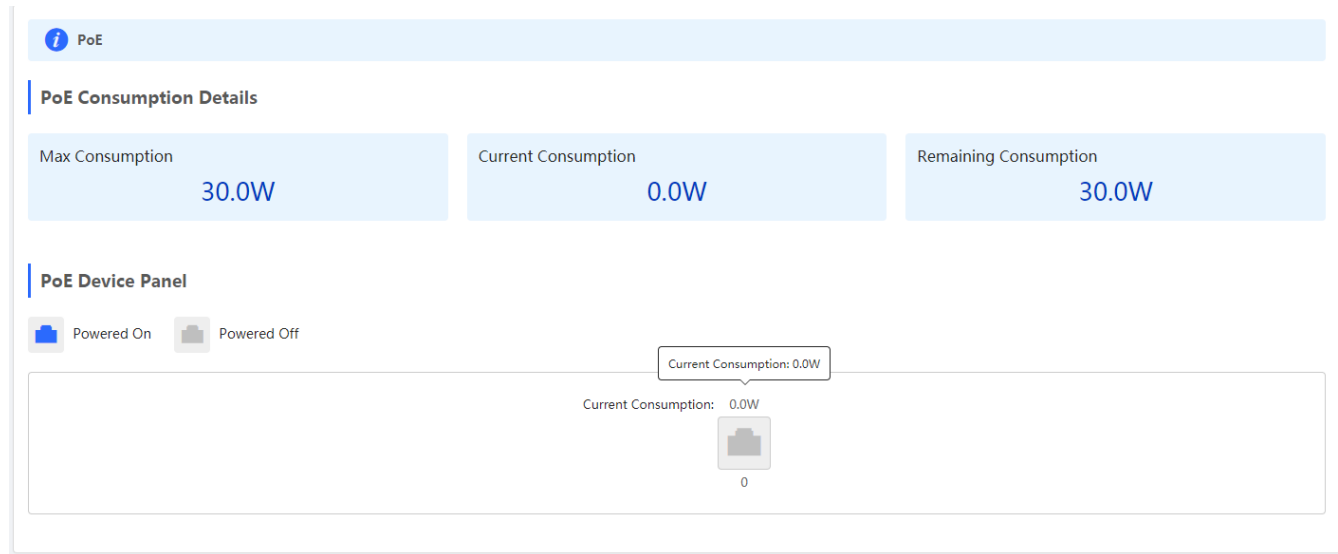
Figure 3-3-12 DNS Proxy



### 3.3.2.3 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 3-3-13 PoE



## 3.3.3 Security

### 3.3.3.1 ARP List

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

Figure 3-3-14 ARP List

**ARP List**

*i* The device learns IP-MAC mapping of all devices connected to its interfaces. You can bind or filter the MAC address. ?

You can cancel IP-MAC binding in batches on the page.

**ARP List** Search by IP/MAC

<input type="checkbox"/>	No.	IP Address	MAC	Status	
<input type="checkbox"/>	1	192.168.110.5	f8:bc:12:5d:44:7d	Bind	Filter
<input type="checkbox"/>	2	172.30.111.56	00:00:12:34:25:26	Bind	Filter
<input type="checkbox"/>	3	172.30.111.246	00:e0:4c:00:00:29	Bind	Filter
<input type="checkbox"/>	4	172.30.111.181	00:23:79:00:23:79	Bind	Filter
<input type="checkbox"/>	5	192.168.110.89	00:d3:f8:15:08:5c	Bind	Filter
<input type="checkbox"/>	6	172.30.111.35	00:e0:4c:00:00:2d	Bind	Filter

Click **Bind** in the **Action** column to bind an IP address with a MAC address. Alternatively, select ARP entries and click **Batch Bind** to bind more than one IP address. You can click [MAC Binding](#) to view static ARP entries.

Click **Filter** in the **Action** column to filter out a MAC address. Alternatively, select ARP entries and click **Batch Filter** to filter out more than one IP address. You can click [MAC Filtering](#) to view filtered MAC addresses.

### 3.3.3.2 MAC Binding

The **MAC Binding** module allows you to add, delete and edit IP-MAC binding entries.

Figure 3-3-15 IP-MAC Binding

**MAC Binding**

*i* 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.

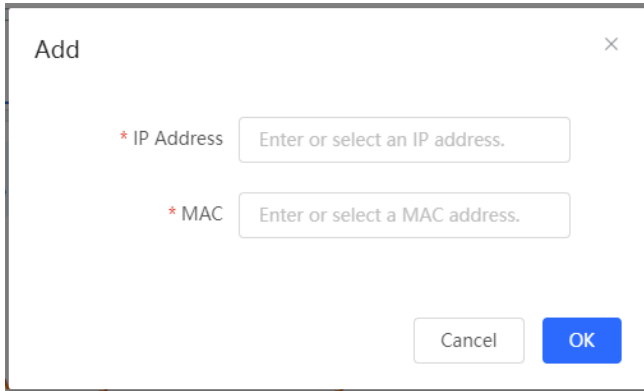
**IP-MAC Binding List**

Up to **256** IP-MAC bindings can be added.

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

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 3-3-16 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.

### 3.3.3.3 MAC Filtering

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

Figure 3-3-17 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

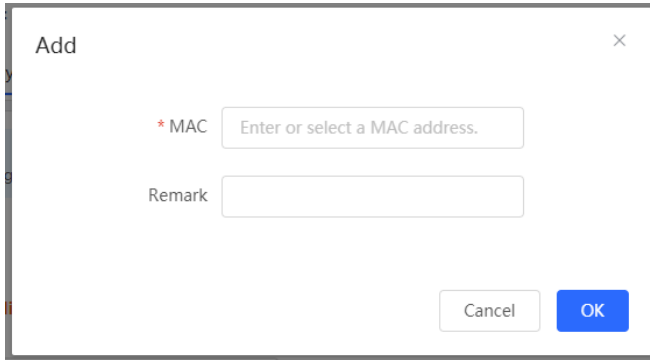
Up to 80 rules can be added.

	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 3-3-18 Add Filtered MAC Address



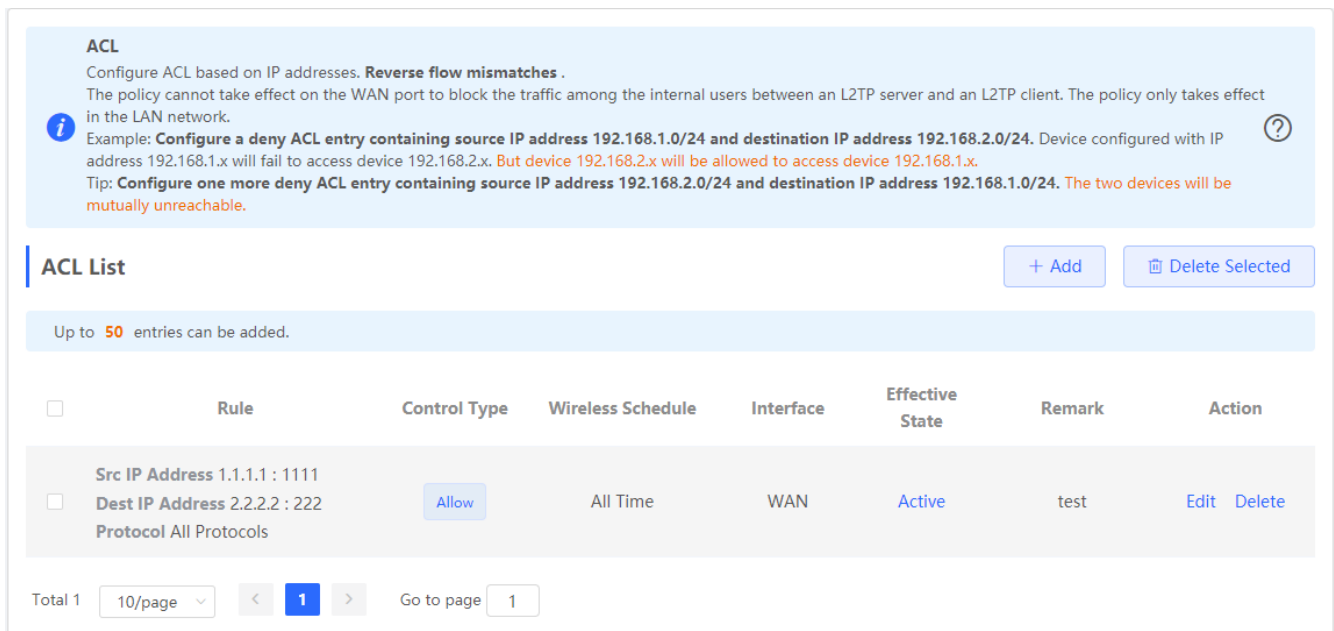
Click **Delete** in the **Action** column. The message "Are you sure you want to delete the entry?" is displayed. In the displayed dialog box, click **OK**. The message "Delete operation succeeded." is displayed.

### 3.3.4 Behavior

#### 3.3.4.1 Access Control

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

Figure 3-3-19 Access Control



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

Figure 3-3-20 MAC-Based ACL

The screenshot shows the 'Add ACL' dialog box with the following configuration:

- Based on:**  MAC,  IP Address
- \* MAC:** Enter a MAC address.
- Control Type:** Allow
- Wireless Schedule:** All Time
- Remark:** Enter the ACL purpose.
- Buttons:** Cancel, OK

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

Figure 3-3-21 IP Address-Based ACL

The screenshot shows the 'Add ACL' dialog box with the following configuration:

- Based on:**  MAC,  IP Address
- Src IP Address: Port:** Net:192.168.1.1/24 : 1-65535
- Dest IP Address: Port:** Net:192.168.1.1/24 : 1-65535
- Protocol Type:** All Protocols
- Control Type:** Allow
- Wireless Schedule:** All Time
- Interface:** WAN
- Remark:** Enter the ACL purpose.
- Buttons:** Cancel, OK

### 3.3.4.2 Time Management

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

Figure 3-3-22 Time List



Time List

+ Add
Delete Selected

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

	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 3-3-23 Add Time Object

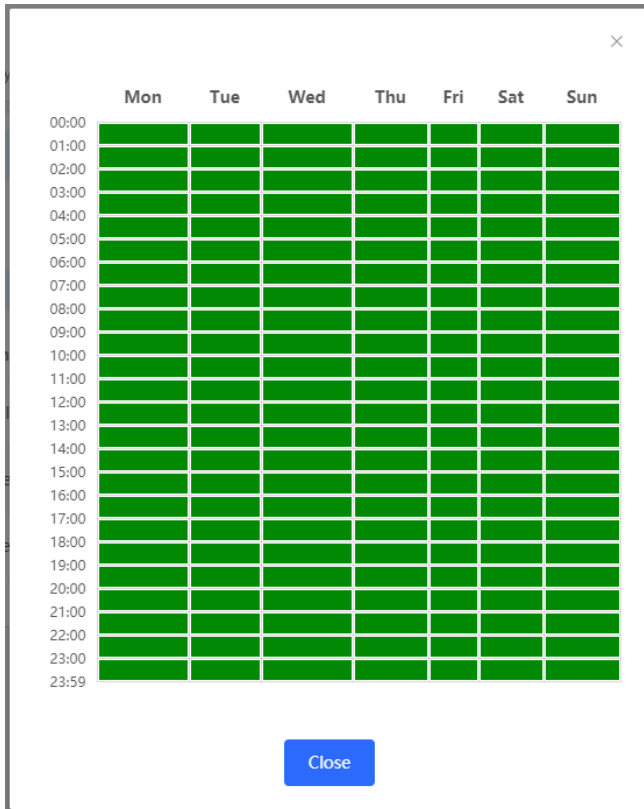
Add Time
×

\* 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 3-3-24 Select Time



	Mon	Tue	Wed	Thu	Fri	Sat	Sun
00:00	Green	Green	Green	Green	Green	Green	Green
01:00	Green	Green	Green	Green	Green	Green	Green
02:00	Green	Green	Green	Green	Green	Green	Green
03:00	Green	Green	Green	Green	Green	Green	Green
04:00	Green	Green	Green	Green	Green	Green	Green
05:00	Green	Green	Green	Green	Green	Green	Green
06:00	Green	Green	Green	Green	Green	Green	Green
07:00	Green	Green	Green	Green	Green	Green	Green
08:00	Green	Green	Green	Green	Green	Green	Green
09:00	Green	Green	Green	Green	Green	Green	Green
10:00	Green	Green	Green	Green	Green	Green	Green
11:00	Green	Green	Green	Green	Green	Green	Green
12:00	Green	Green	Green	Green	Green	Green	Green
13:00	Green	Green	Green	Green	Green	Green	Green
14:00	Green	Green	Green	Green	Green	Green	Green
15:00	Green	Green	Green	Green	Green	Green	Green
16:00	Green	Green	Green	Green	Green	Green	Green
17:00	Green	Green	Green	Green	Green	Green	Green
18:00	Green	Green	Green	Green	Green	Green	Green
19:00	Green	Green	Green	Green	Green	Green	Green
20:00	Green	Green	Green	Green	Green	Green	Green
21:00	Green	Green	Green	Green	Green	Green	Green
22:00	Green	Green	Green	Green	Green	Green	Green
23:00	Green	Green	Green	Green	Green	Green	Green
23:59	Green	Green	Green	Green	Green	Green	Green

Close

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 3-3-25 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 ☑	Edit Delete

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

Figure 3-3-26 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 -----

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

Figure 3-3-27 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 3-3-28 IPSec Connection Status

**IPSec Connection Status** ?

**IPSec Connection Status**

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

### 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 3-3-29 PBR List

**PBR**

Route Priority: PBR > Static Routing > ISP Routing.

**Note:** PBR is more flexible than destination-based routing.

**PBR List**

Up to 30 entries can be added.

+ Add Delete Selected

<input type="checkbox"/>	Name	Protocol Type	Src IP Address	Dest IP Address	Src Port Range	Dest Port Range	Outbound Interface	Status	Action
No Data									

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

Figure 3-3-30 Add PBR

Add PBR
×

\* Name

Protocol Type

Src IP/IP Range

Dest IP/IP Range

Outbound Interface

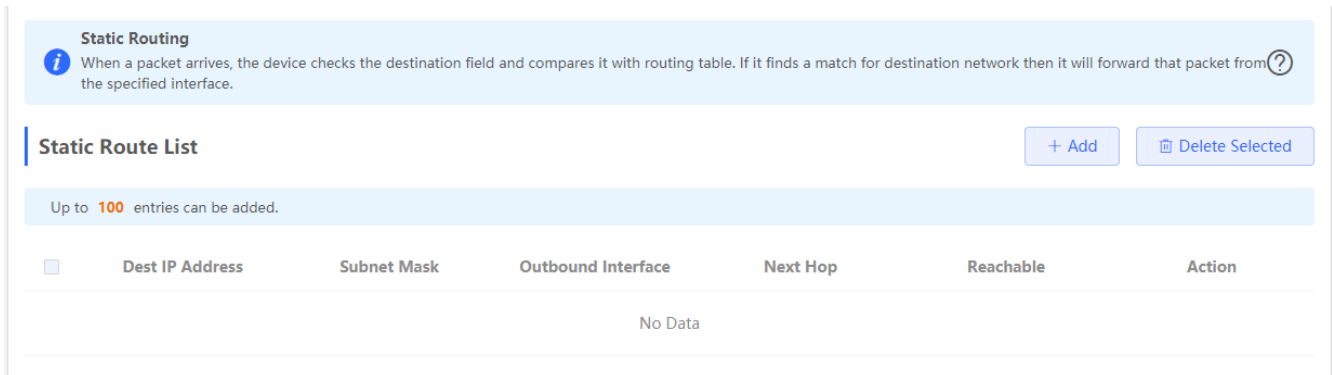
Status

Cancel
OK

### 3.3.6.1.2 Static Routing

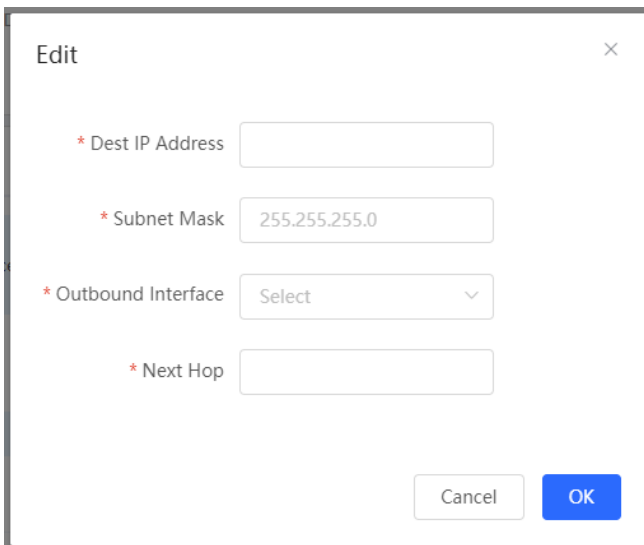
The **Static Routing** module allows you to add, delete and edit static routes.

Figure 3-3-31 Static Route List



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

Figure 3-3-32 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 3-3-33 Smart Flow Control

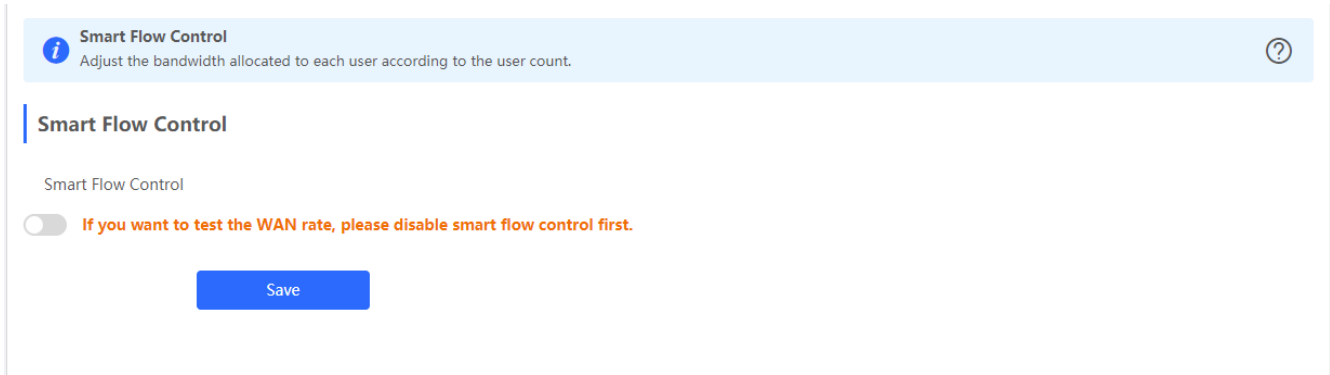
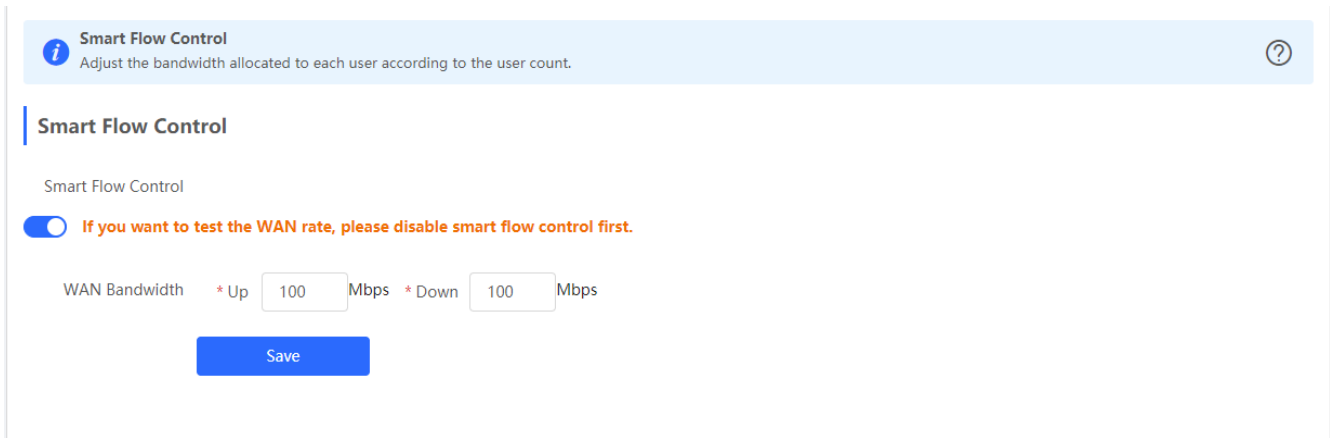


Figure 3-3-34 Enable Smart Flow Control

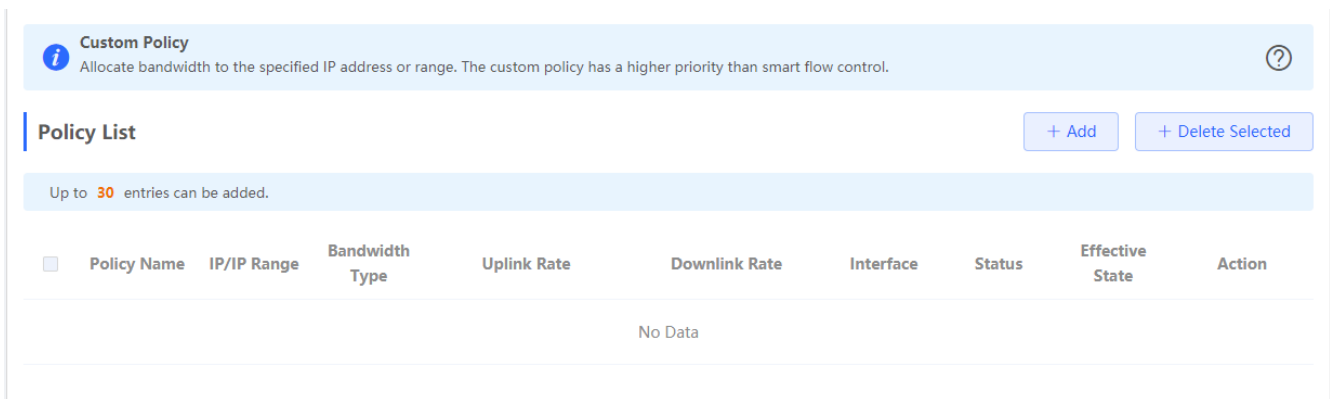


If there is more than one WAN port, **WAN Bandwidth** settings of each port will be displayed accordingly.

### 3.3.6.2.2 Custom Policy

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

Figure 3-3-35 Custom Flow Control Policy



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

Figure 3-3-36 Add Flow Control Policy

Add
×

\* Policy Name

\* IP/IP Range

Bandwidth Type Share ▾

Uplink Rate \* CIR  \* PIR  Kbps

Downlink Rate \* CIR  \* PIR  Kbps

Interface WAN ▾

Status

Cancel
OK

### 3.3.6.3 Session Limit

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

Figure 3-3-37 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.

	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 3-3-38 Add Session Limit Policy



Add
×

\* Name

\* Start IP Address

\* End IP Address

\* Session Count Limit

Status

### 3.3.6.4 Port Mapping

#### 3.3.6.4.1 Port Mapping

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

Figure 3-3-39 Port Mapping List

i Port Mapping
?

**Port Mapping List**
+ Add
Delete Selected

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 3-3-40 Add Port Mapping Policy

Add
✕

\* Name

Protocol

External IP Address

\* External Port/Range

\* Internal IP Address

\* Internal Port/Range

### 3.3.6.4.2 NAT-DMZ

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

Figure 3-3-41 NAT-DMZ Rule List

i **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 3-3-42 Add NAT-DMZ Rule

The 'Add Rule' dialog box includes the following elements:

- Name:** A text input field with an asterisk indicating it is required.
- Dest IP Address:** A text input field with an asterisk and the example text 'Example: 1.1.1.1'.
- Outbound Interface:** A dropdown menu currently showing 'WAN'.
- Status:** A toggle switch that is currently turned on.
- Buttons:** 'Cancel' and 'OK' buttons located at the bottom right.

### 3.3.6.5 Local DNS

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

Figure 3-3-43 Local DNS

The 'Local DNS server' configuration page contains the following elements:

- Information Icon:** A blue circle with a white 'i'.
- Section Header:** 'Local DNS server'.
- Note:** 'The local DNS server is not required to be configured. By default, the device will get the DNS server address from the uplink device.'
- Input Field:** 'Local DNS server' with the placeholder text 'Example: 8.8.8.8, each separated by a space.'
- Button:** A blue 'Save' button.

### 3.3.7 Diagnostics

#### 3.3.7.1 Network Check

Figure 3-3-44 Network Check

The 'Network Check' configuration page contains the following elements:

- Information Icon:** A blue circle with a white 'i'.
- Section Header:** 'Network Check'.
- Button:** A blue 'Start' button.
- Help Icon:** A question mark icon in a circle on the right side of the header bar.

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

Figure 3-3-45 Result

**i** Network Check
?

Recheck

100%

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 3-3-46 Issue & Advice

**WAN/LAN Cable**
**i**

**Check WAN Cable**

**Result** : OK

**Check LAN Cable**

**Result** : The LAN cable is unplugged. Internet access may fail.

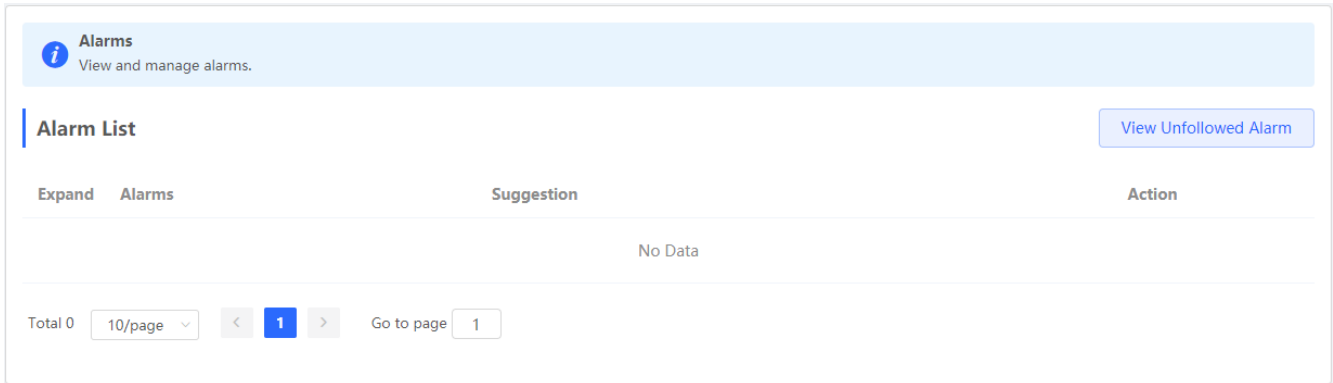
**Advice** : Please verify that the device is plugged into the LAN port properly and check the cable and plug.

Please fix the problem by taking the suggested action.

### 3.3.7.2 Alarms

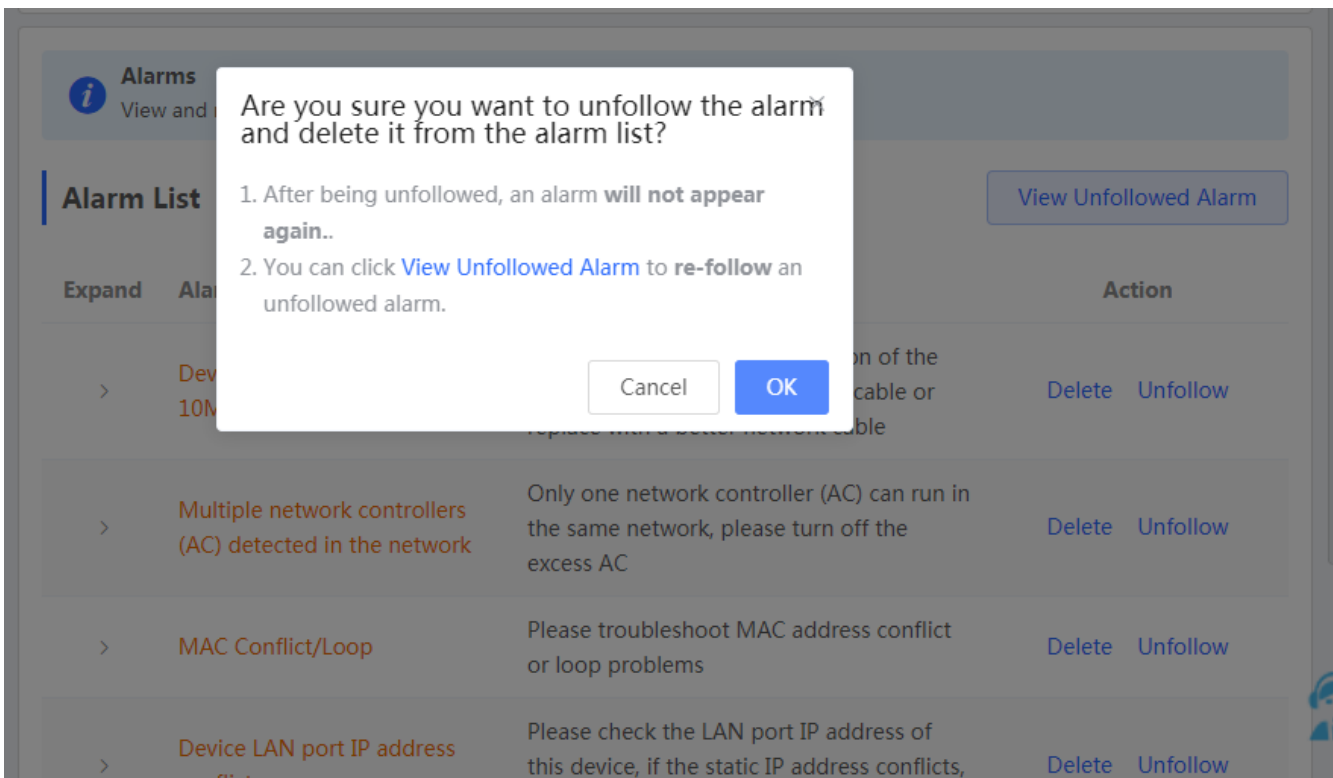
The **Alarms** module allows you to view and manage alarms in the network.

Figure 3-3-47 Alarms



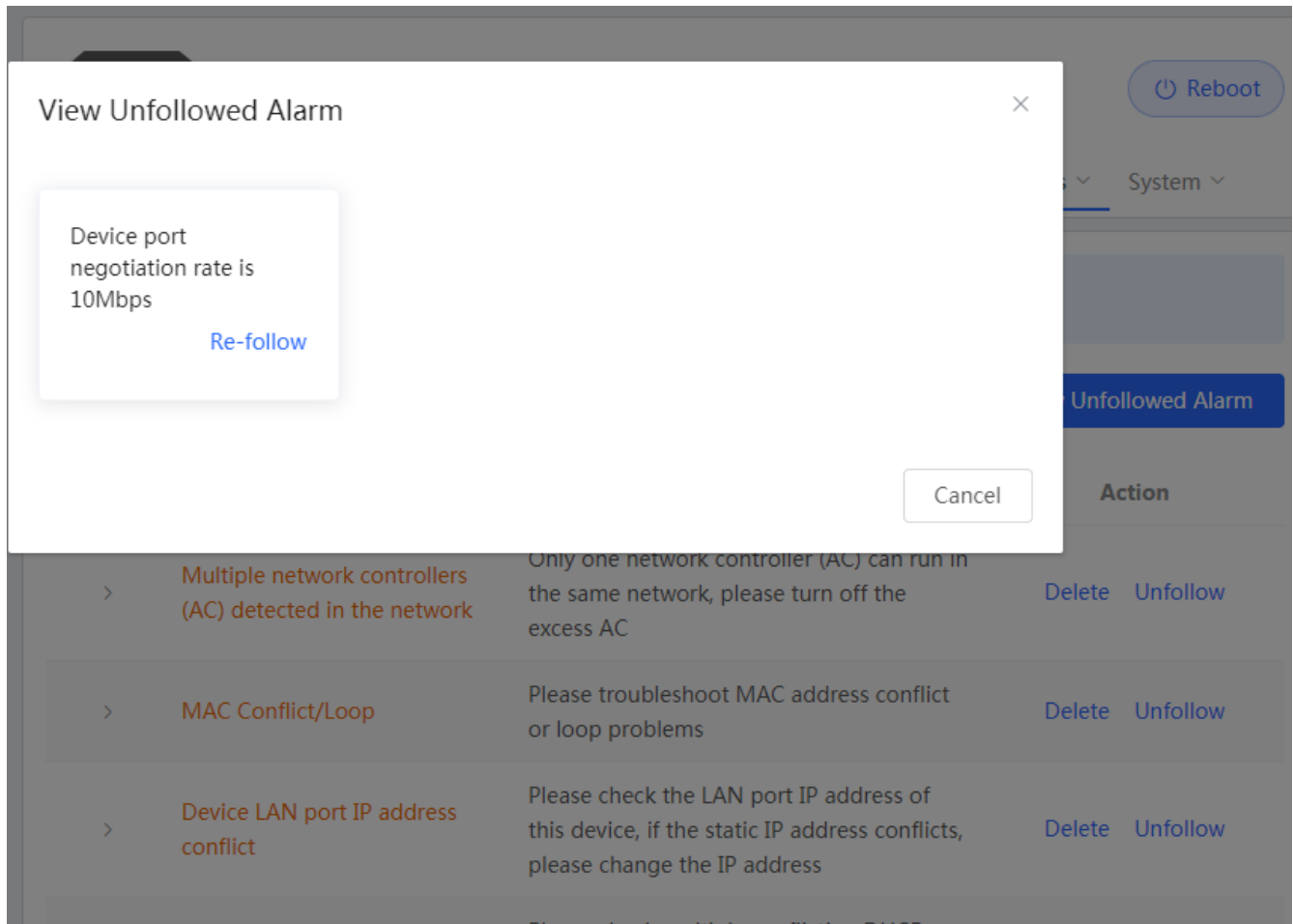
Click **Unfollow** in the **Action** column to unfollow an alarm. In the confirmation box, click **OK**.

Figure 3-3-48 Unfollow Alarm



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

Figure 3-3-49 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 3-3-50 Ping Test and Result

**Network Tools** ⓘ

Tool  Ping  Traceroute  DNS Lookup

\* IP Address/Domain

\* Ping Count

\* Packet Size  Bytes

Result

Figure 3-3-51 Traceroute Test and Result

**Network Tools** ⓘ

Tool  Ping  Traceroute  DNS Lookup

\* IP Address/Domain

\* Max TTL

Result

Figure 3-3-52 DNS Lookup Test and Result

**Network Tools** ⓘ

Tool  Ping  Traceroute  DNS Lookup

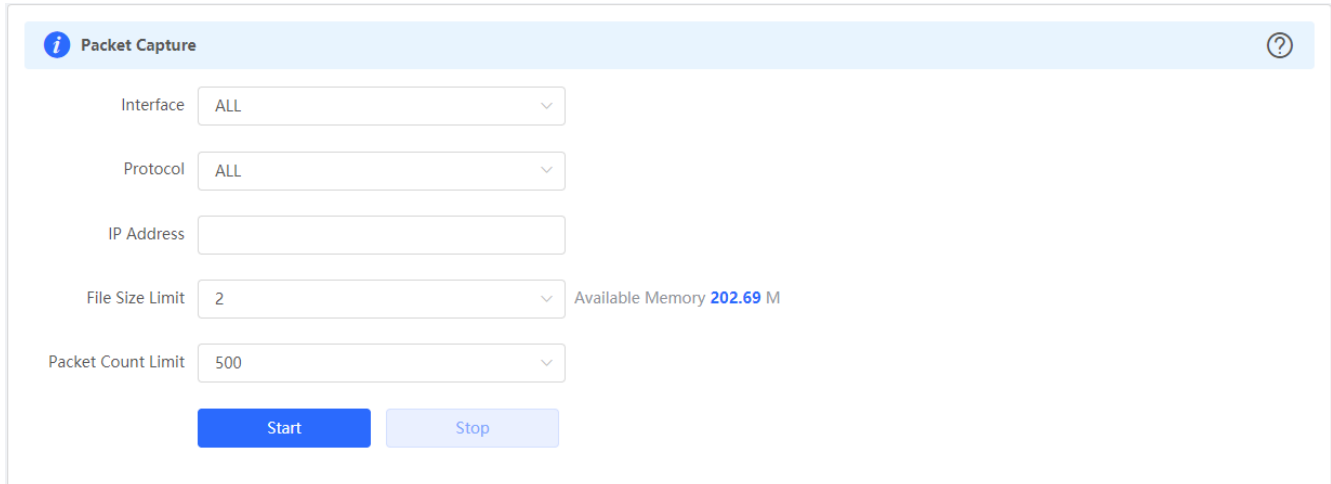
\* IP Address/Domain

Result

### 3.3.7.4 Packet Capture

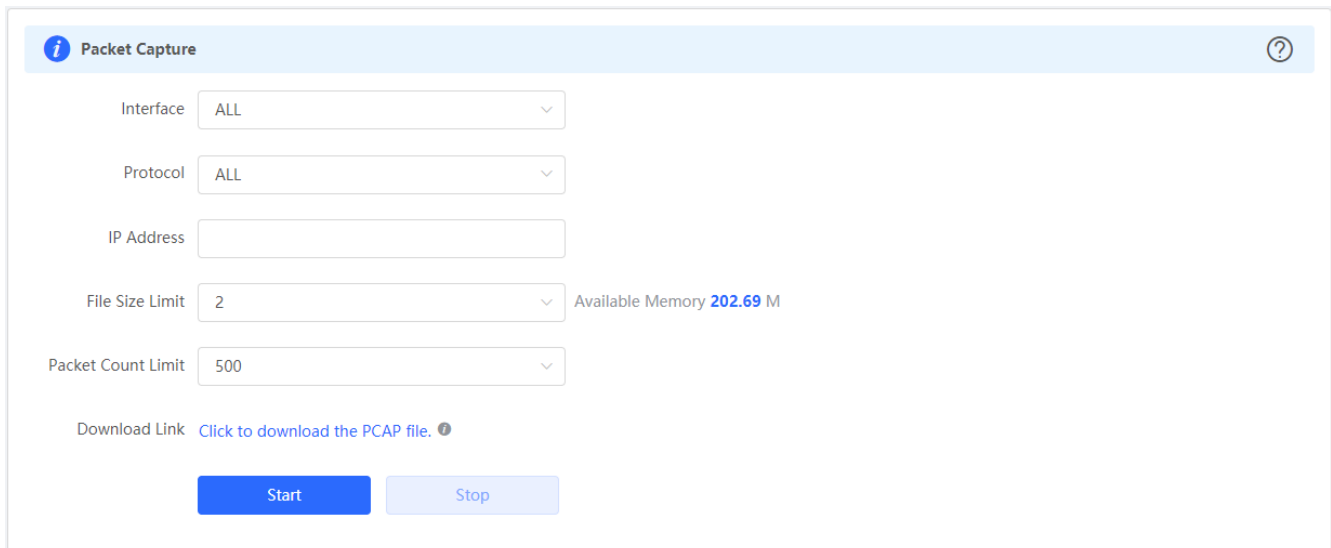
The **Packet Capture** module allows you to perform packet capture and download the result for troubleshooting.

Figure 3-3-53 Packet Capture



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

Figure 3-3-54 Start Packet Capture



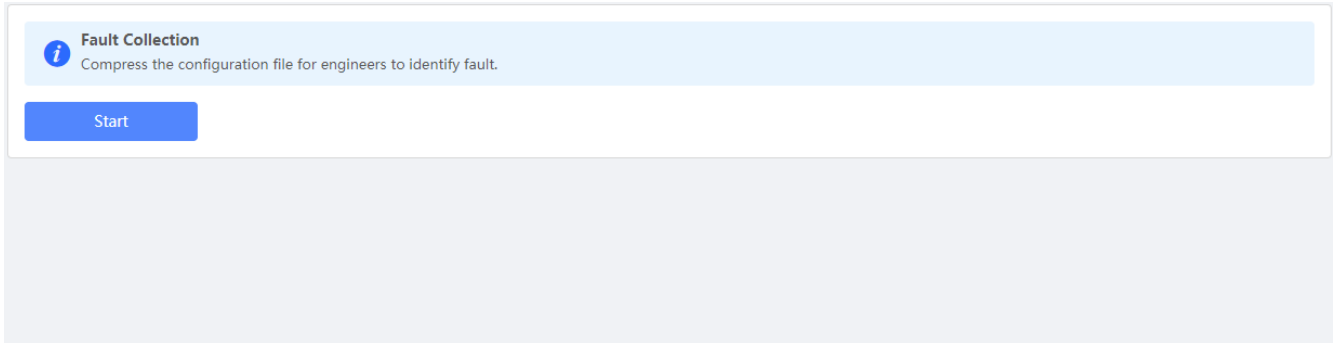
Click to download the packet capture result in the PCAP format.

### 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 3-3-55 Fault Collection



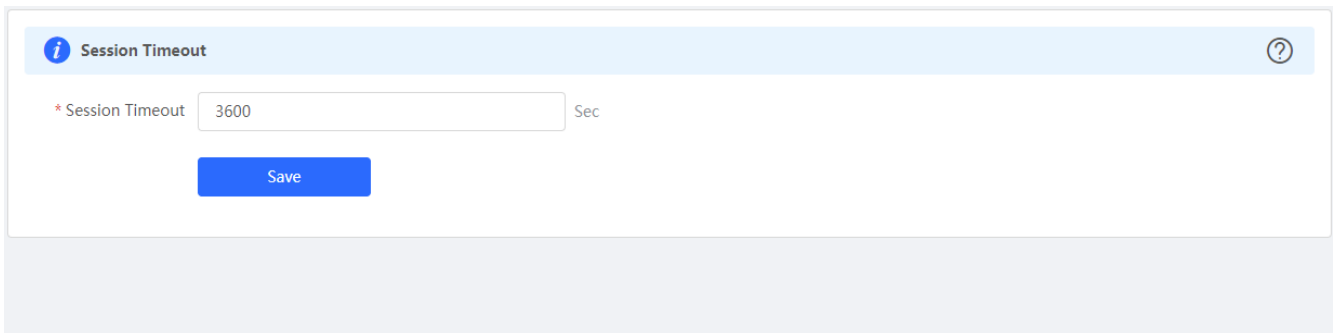


### 3.3.8 System

#### 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.

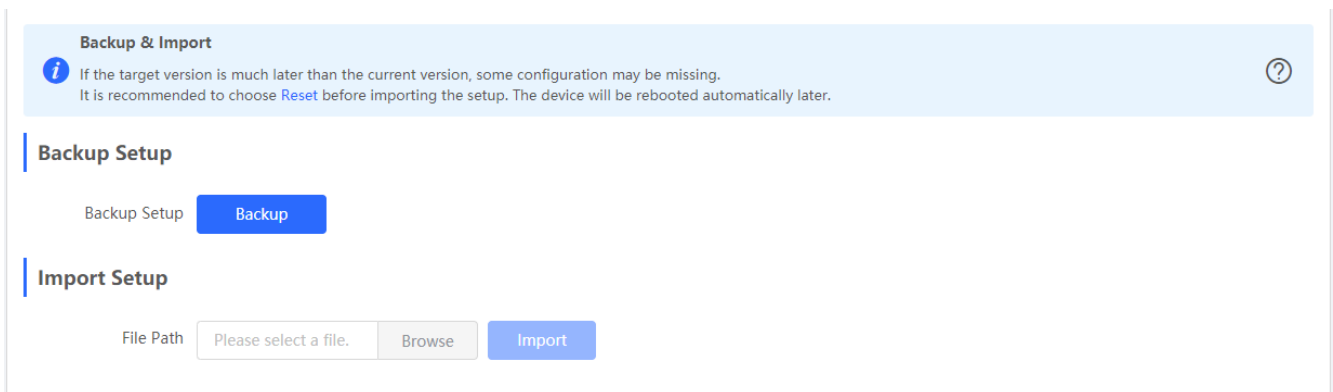
Figure 3-3-56 Session Timeout



#### 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.

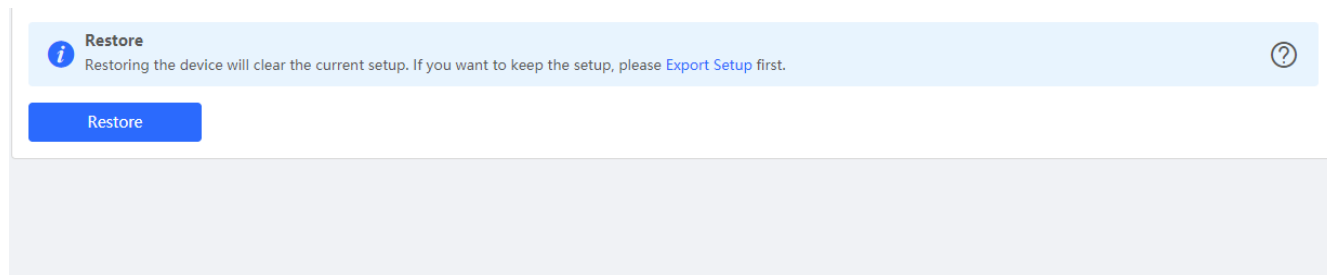
Figure 3-3-57 Backup & Import



### 3.3.8.3 Restore

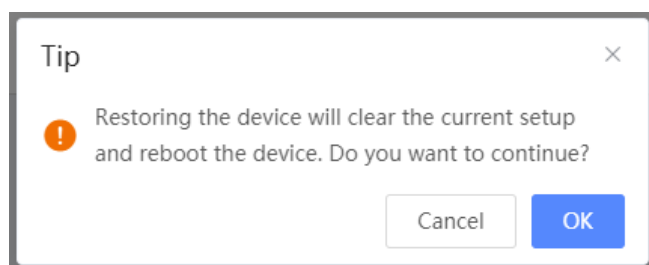
The **Restore** module allows you to restore the device to factory settings.

Figure 3-3-58 Restore



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

Figure 3-3-59 Confirm Restore

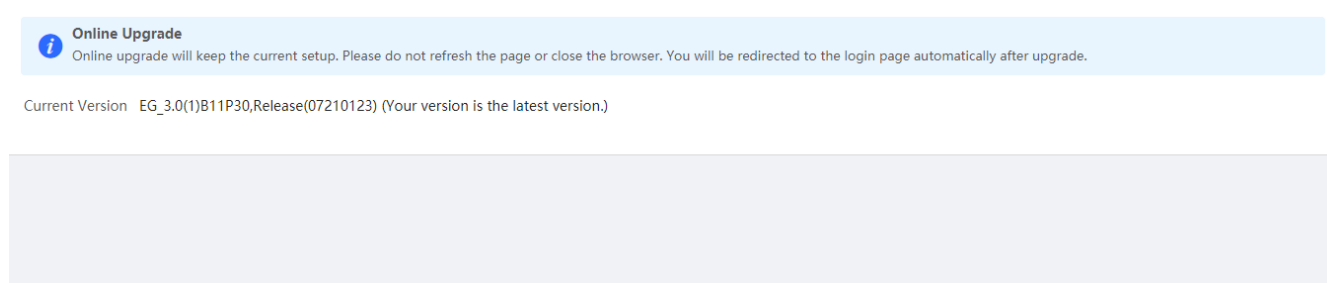


Click **OK** to restore all default values. This function is recommended when the network configuration is incorrect or the network environment is changed..

### 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.

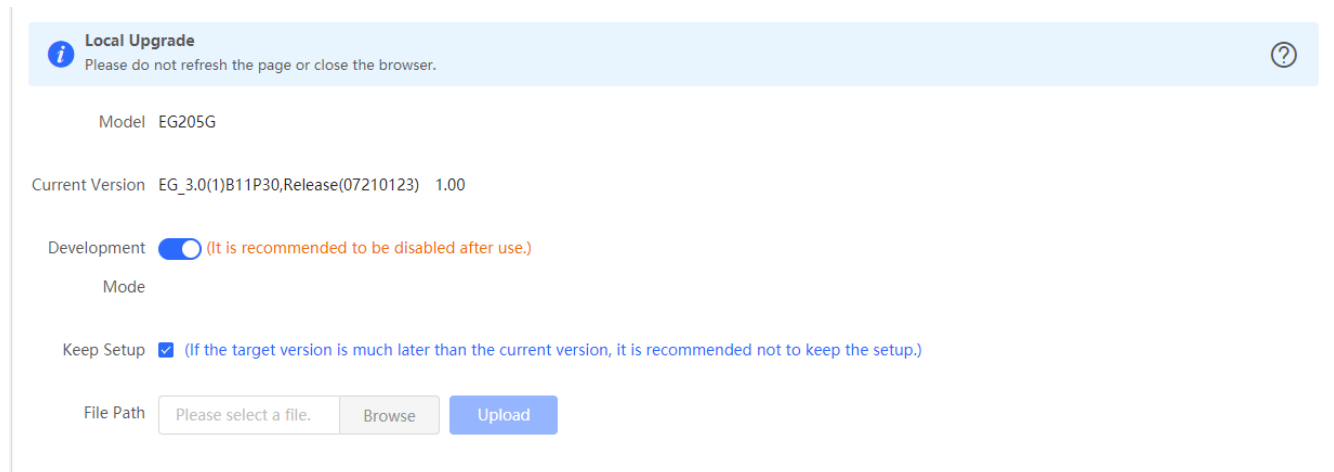
Figure 3-3-60 Online Upgrade



### 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 3-3-61 Local Upgrade

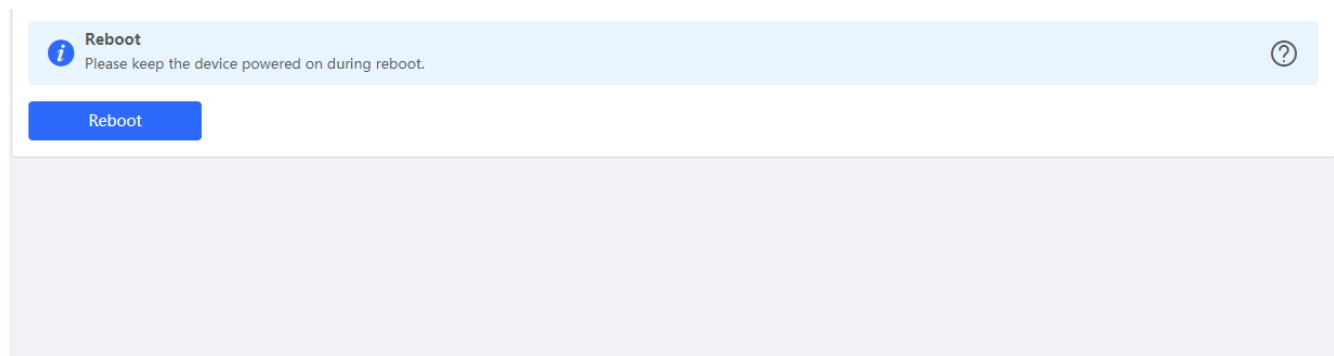


The screenshot shows the 'Local Upgrade' configuration page. At the top, there is a light blue header bar with an information icon (i) on the left and a help icon (?) on the right. Below the header, the text reads 'Please do not refresh the page or close the browser.' The main content area displays the following information: 'Model EG205G', 'Current Version EG\_3.0(1)B11P30,Release(07210123) 1.00', 'Development' with a toggle switch turned on and a note '(It is recommended to be disabled after use.)', 'Mode', and 'Keep Setup' with a checked checkbox and a note '(If the target version is much later than the current version, it is recommended not to keep the setup.)'. At the bottom, there is a 'File Path' section with a text input field containing 'Please select a file.', a 'Browse' button, and an 'Upload' button.

### 3.3.8.6 Reboot

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

Figure 3-3-62 Reboot



The screenshot shows the 'Reboot' configuration page. At the top, there is a light blue header bar with an information icon (i) on the left and a help icon (?) on the right. Below the header, the text reads 'Please keep the device powered on during reboot.' The main content area features a single blue 'Reboot' button. The rest of the page is a light gray area.

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 3-3-63 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

Day  Mon  Tue  Wed  Thu  Fri  Sat  Sun

Time 03 : 00

[Save](#)

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

**AP List** ?

Group: **All Groups** [Expand](#) [Advanced Search](#) [List Filter](#) [Batch Action](#) ▼

<input type="checkbox"/>	Action	Hostname	IP Address	MAC	Status	Model	Clients	Software Ver
<input type="checkbox"/>	<a href="#">Manage</a> <a href="#">Reboot</a>	Ruijie	192.168.110.200	00:10:F8:75:33:72	Online	EAP602	0	AP_3.0(1)B2P32,Release(07210117)

Total 1 10/page < 1 > 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

## AP List

Search by Group

▼ All Groups +

Default  

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

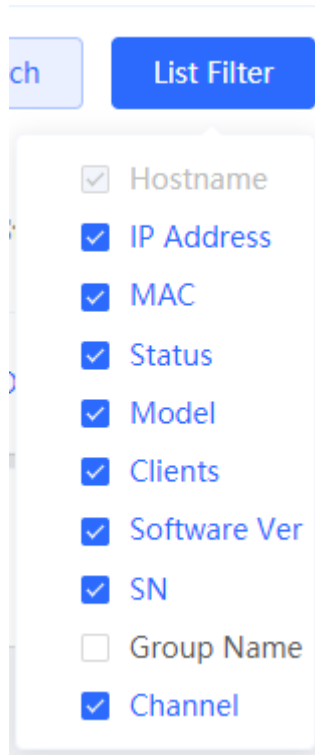
Ver

MAC

Status  ▼

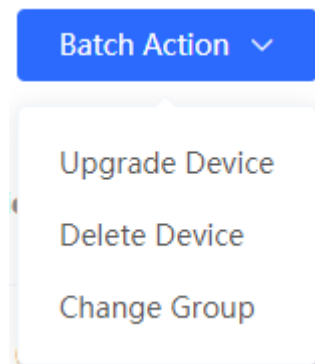
Click **List Filter**, and you can select columns to be displayed in the list.

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.

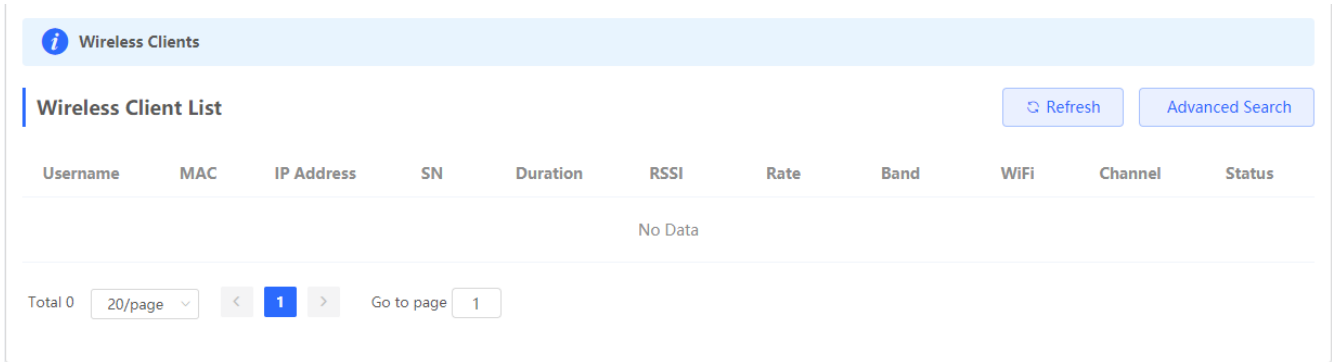
**Change Group:** You can move the devices from one group to another. The devices will be applied with the new group settings.

### 3.4.2 Clients

#### 3.4.2.1 Clients

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

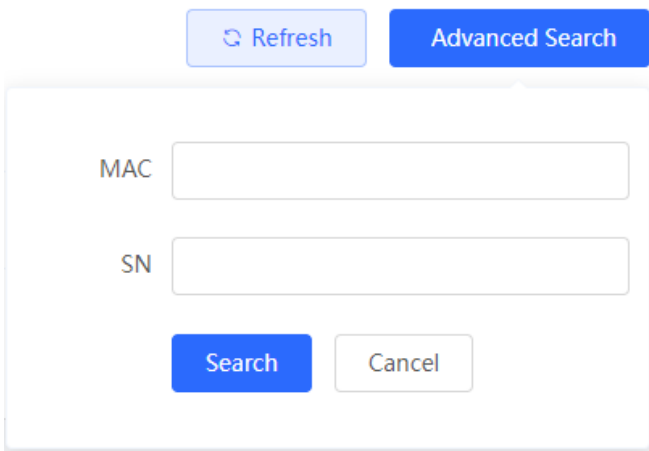
Figure 3-4-6 Wireless Client List



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



#### 3.4.2.2 Blacklist/Whitelist

The **Blacklist/Whitelist** module allows you to configure client blacklist and whitelist.

Figure 3-4-8 Blacklist/Whitelist

Blacklist Mode  Whitelist Mode

**i** All STAs except blacklisted STAs are allowed to access WiFi. ?

**Blacklist** + Add Delete Selected

Up to 30 members can be added.

<input type="checkbox"/>	MAC	Remark	Action
<input type="checkbox"/>	00:11:22:33:44:55	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 ×

\* MAC

Remark

### 3.4.3 Advanced

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

Figure 3-4-10 Advanced Settings (EG Device)

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

**Advanced** Device Group:

Country/Region

2.4G Channel Width  5G Channel Width

Client Count Limit  Client Count Limit

Only the AP supports power and roaming sensitivity settings.

Figure 3-4-11 Advanced Settings (AP)



**i** Tip: Changing configuration requires a reboot and will force online clients to go offline. ?

**Advanced** Device Group:

Country Code

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

Power  Power

Roaming Sensitivity  Roaming Sensitivity

### 3.4.4 WiFi

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

#### 3.4.4.1 WiFi Settings

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

Figure 3-4-12 WiFi Settings

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

**WiFi Settings** Device Group:

\* SSID

Band

Security

\* WiFi Password

---

Expand

### 3.4.4.2 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 3-4-13 Guest WiFi

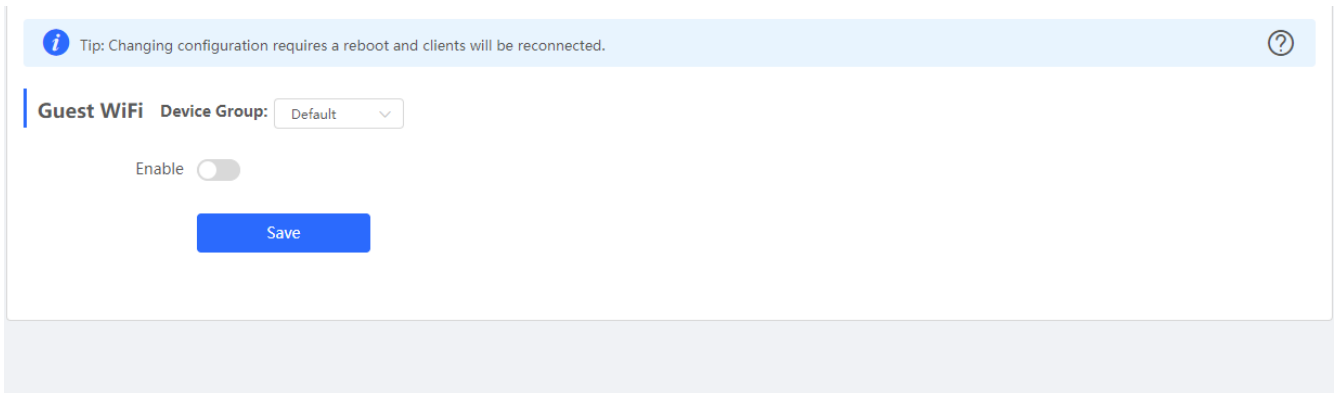
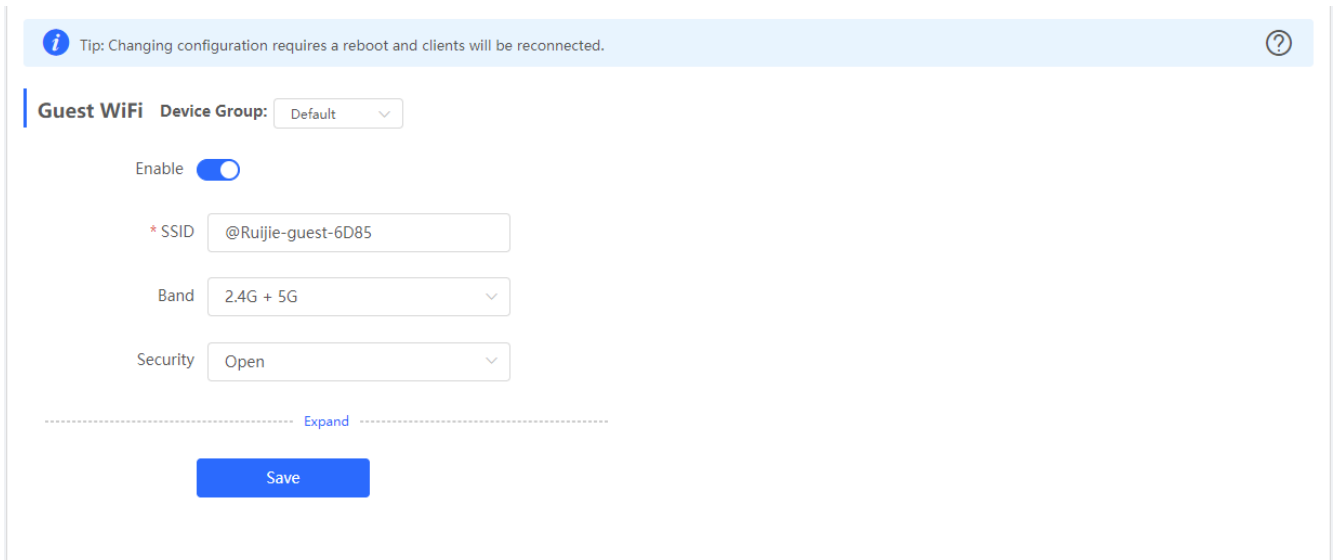


Figure 3-4-14 Enable Guest WiFi



### 3.4.4.3 WiFi List

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

Figure 3-4-15 WiFi List

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

**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 3-4-16 Add WiFi

**Add** ×

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

\* SSID

Band 2.4G + 5G ▼

Security Open ▼

..... [Expand](#) .....

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

### 3.4.4.4 Healthy Mode

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

Figure 3-4-17 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 LAN Ports

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

Figure 3-4-18 LAN Ports

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 ?

Save

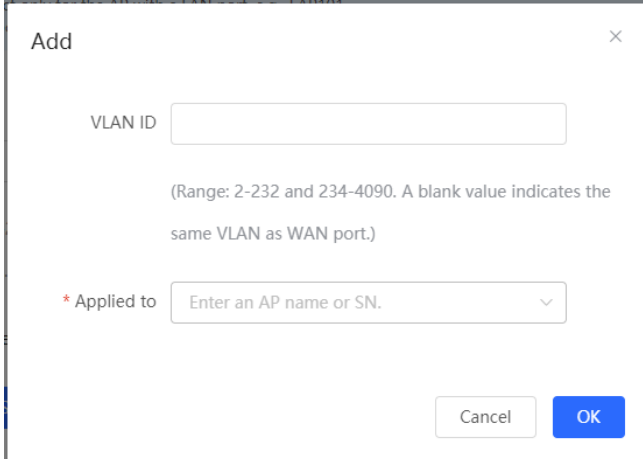
**LAN Port Settings** + Add Delete Selected

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

	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 3-4-19 Add LAN Port

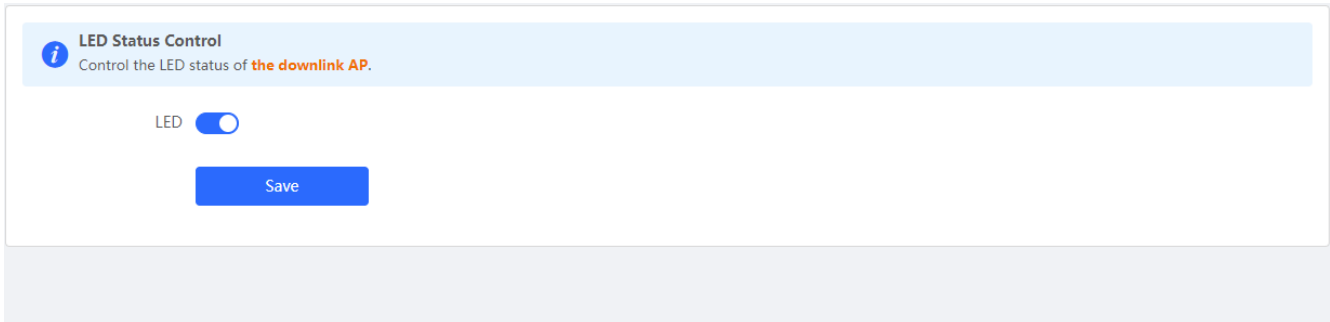


The image shows a dialog box titled "Add" with a close button (X) in the top right corner. It contains a text input field for "VLAN ID". Below the input field is a note: "(Range: 2-232 and 234-4090. A blank value indicates the same VLAN as WAN port.)". There is also a dropdown menu labeled "\* Applied to" with the placeholder text "Enter an AP name or SN.". At the bottom of the dialog are two buttons: "Cancel" and "OK".

### 3.4.6 LED

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

Figure 3-4-20 LED



The image shows a configuration page for "LED Status Control". At the top, there is a blue header bar with an information icon (i) and the text "LED Status Control" and "Control the LED status of the downlink AP.". Below the header, there is a toggle switch for "LED" which is currently turned on. At the bottom of the configuration area is a blue "Save" button.

### 3.4.7 DHCP Security

The **DHCP Security** module allows you to enable IP check and ARP check to filter out invalid IP packets and ARP packets.

Figure 3-4-21 DHCP Security

**7 DHCP Security**
?

IP Check

ARP Check

**Save**

**Trusted DHCP Server** + Add   Delete Selected

Up to 8 entries can be added.

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

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

**Security VLAN** + Add   Delete Selected

Up to 8 entries can be added.

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

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

### 3.4.8 Network Security

The **Network Security** module allows you to limit the rate of ARP packets, broadcast packets and multicast packets.

Figure 3-4-22 Network Security

**i Network Security**  
Limit packet rate and ensure RF resources.
?

Rate Limiting

\* ARP Rate Limit  Packets/Sec

\* Broadcast Rate Limit  Packets/Sec

\* Multicast Rate Limit  Packets/Sec

**Save**

### 3.5 Switches

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

Figure 3-5-1 Switch List

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

Switch List

Delete Offline Devices
Batch Upgrade

	Action	Hostname	IP Address	MAC	Status	Model	Software Ver	SN
<input type="checkbox"/>	Manage	<a href="#">ruijie</a>	192.168.110.16	00:D0:F8:48:45:88	Online	RG-ES226GC-P	ESW_1.0(1)B1P3,Release(07190916)	MACCCTCFVHUG 1
<input type="checkbox"/>	Manage	<a href="#">NBS2100</a>	192.168.110.120	00:D0:F8:22:16:86	Online	NBS2100-16GT2SFP	SWITCH_3.0(1)B11P20,Release(07171423)	MACC992570066

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

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

Figure 3-5-2 Switch Management

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.

Figure 3-6-1 System Time

### 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

\* 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
europa.pool.ntp.org	Delete
rdate.darkorb.net	Delete

[Save](#)

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

### 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**

*i* 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 Reboot **Reset**

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

**OK**

## 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).