Ruijie Reyee Series Access Points

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
- Skype: service_rj@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
boldface font	Commands, command options, and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	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**).

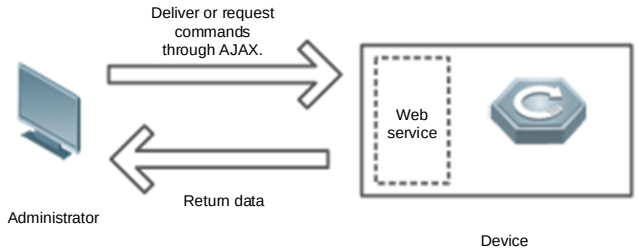
2 Configuration Guide

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



Remarks	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 192.168.120.X. The subnet mask is 255.255.255.0. The default management address of the device is 192.168.120.1. Alternatively, you can set the IP assignment mode to **Obtain an IP address automatically**.

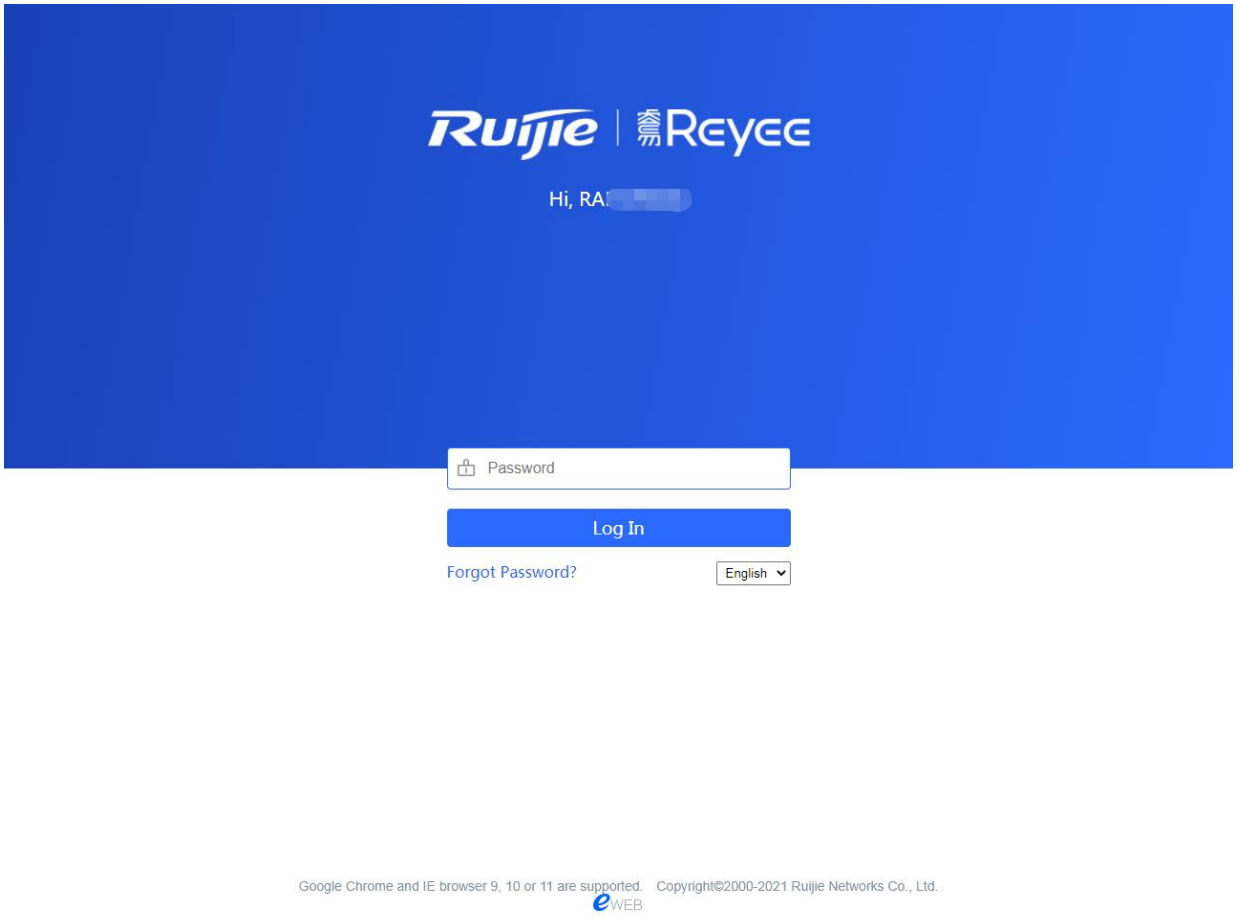
Server requirements:

- 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).

To log into the eWeb management system, open the Google Chrome browser, and enter 192.168.120.1 into the address bar, and press **Enter**.

Figure 2-1-2 Login Page



Enter the password and click **Login**.

2.2 Network Setup

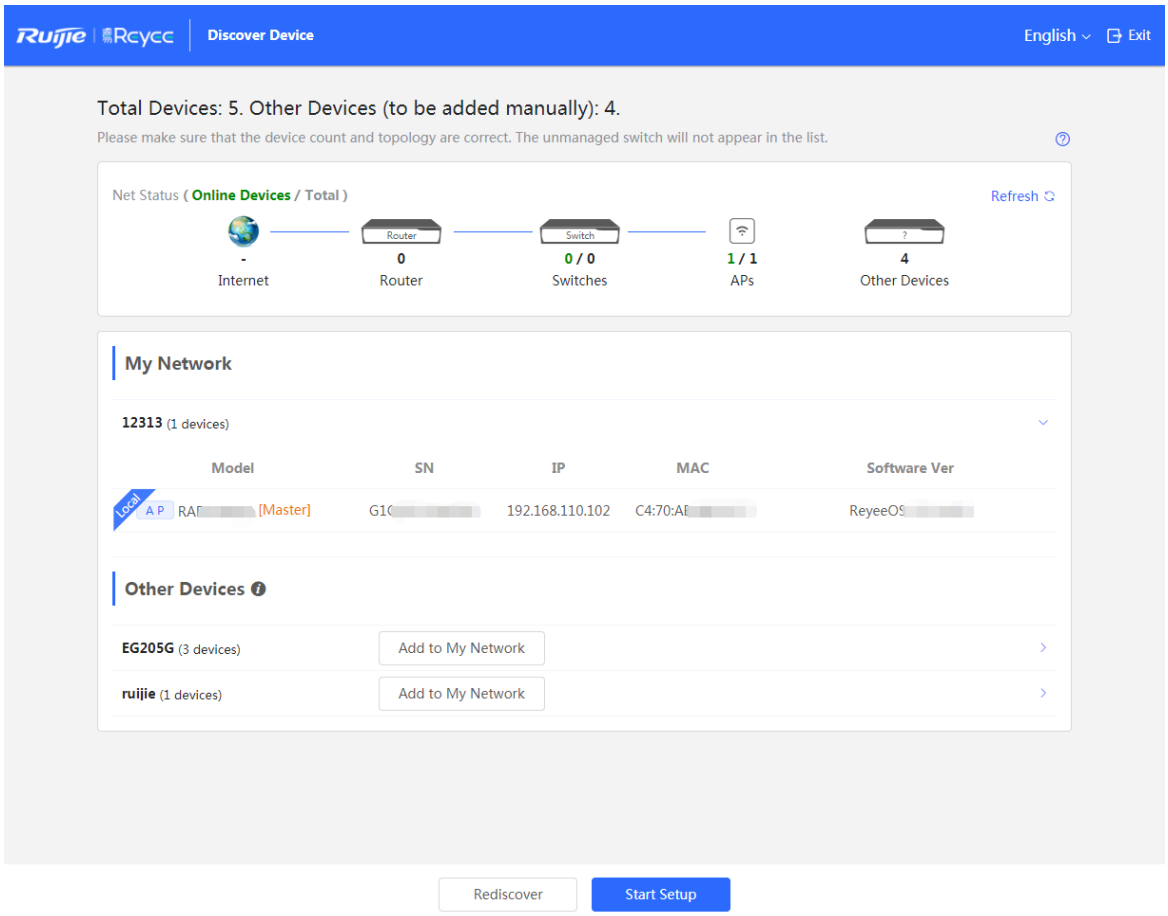
You will enter the **Network Setup** page without login at initial setup.

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.

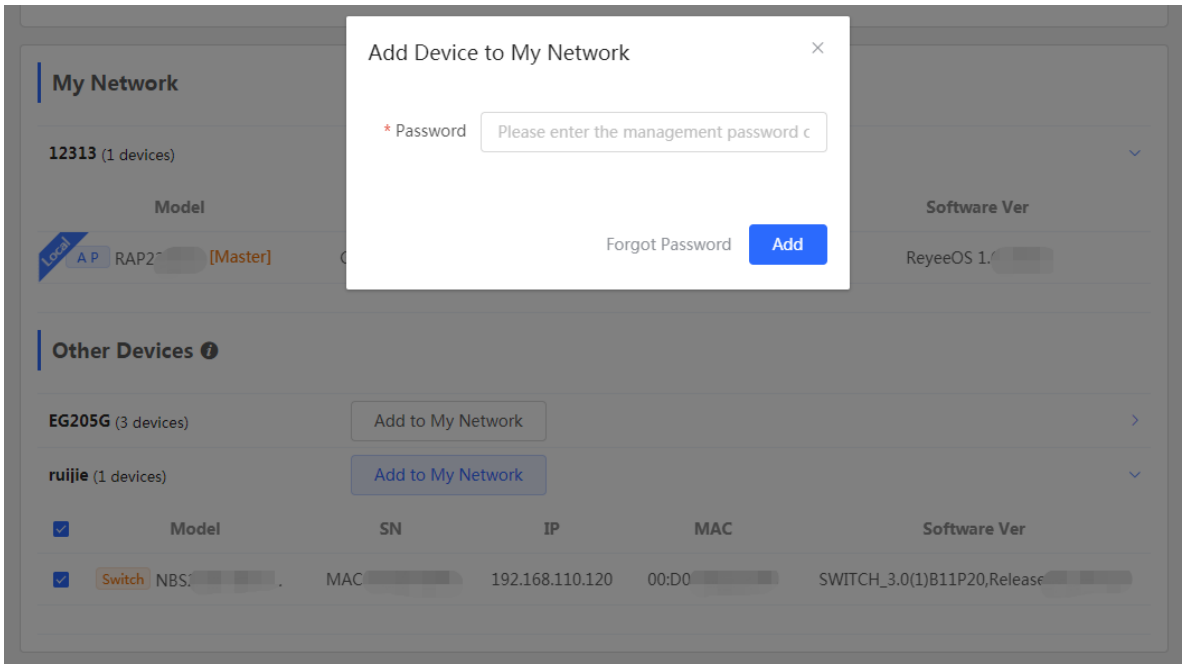
Figure 2-2-1 Discover Device



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

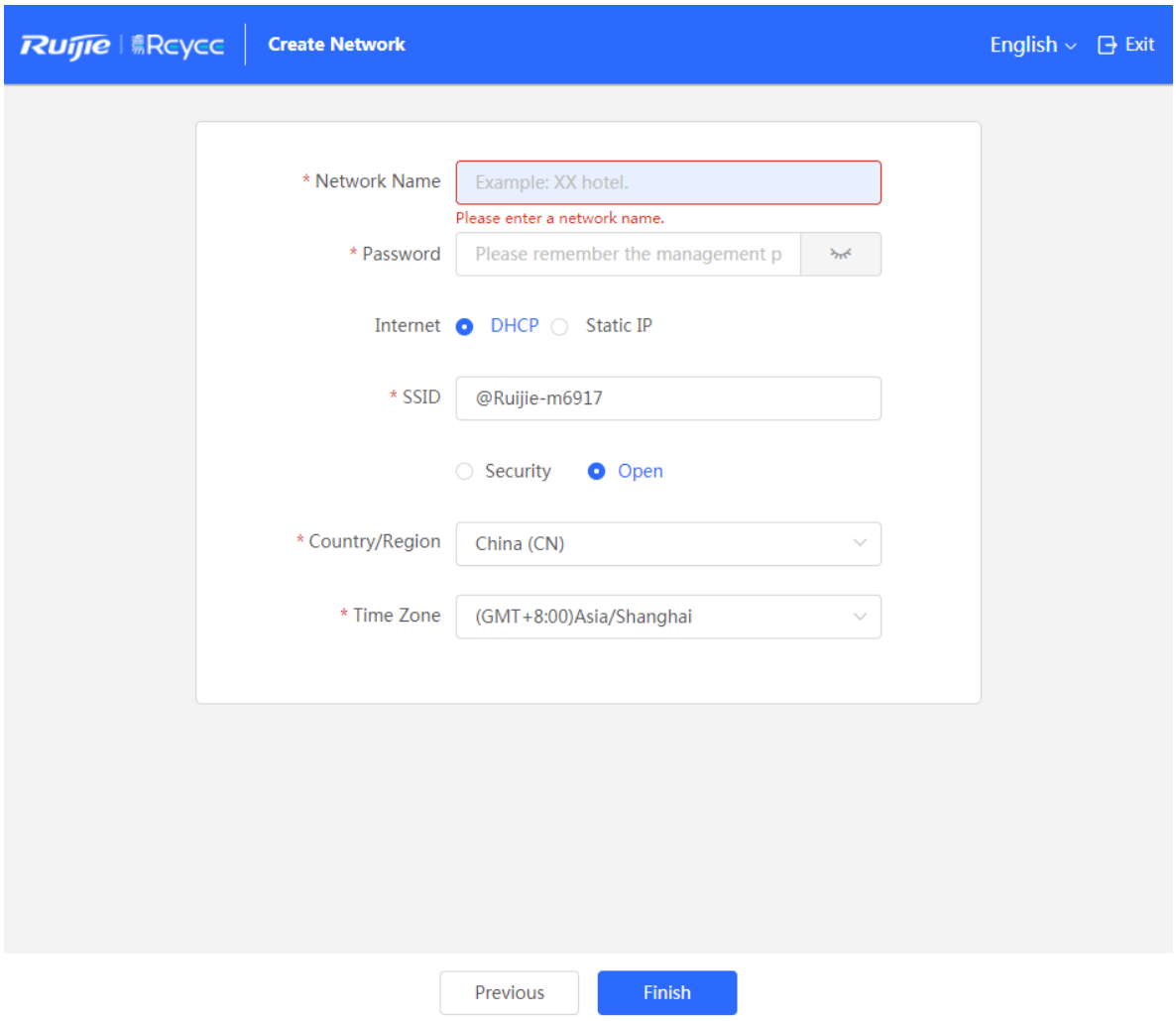


2.2.3 Create Network & Connect

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.

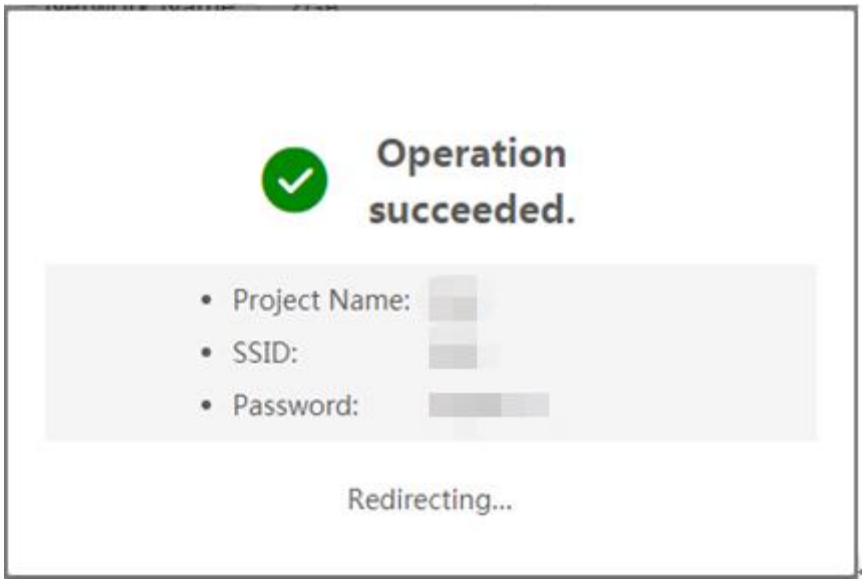
If the device is detected disconnected to Ruijie Cloud, the Ruijie Cloud page will be embedded for you to bind your account after the device accesses the Internet successfully. If the device is already connected to Ruijie Cloud, the eWeb homepage will be displayed after this step.

Figure 2-2-3 Create Network



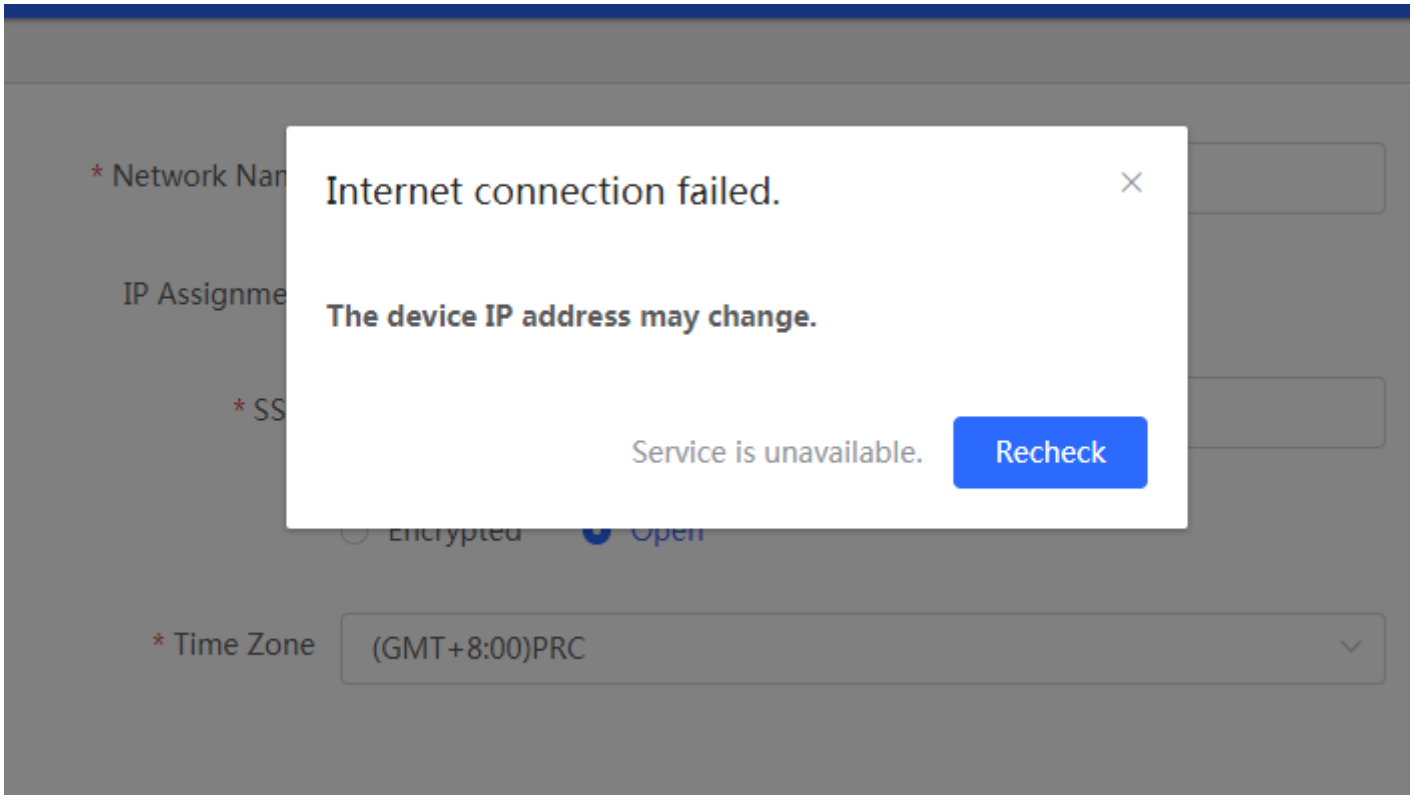
Click **Create Network & Connect**, and it takes about 60 seconds to deliver and activate settings. The following message will appear after Internet connection is set up.

Figure 2-2-4 Connect to Internet



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

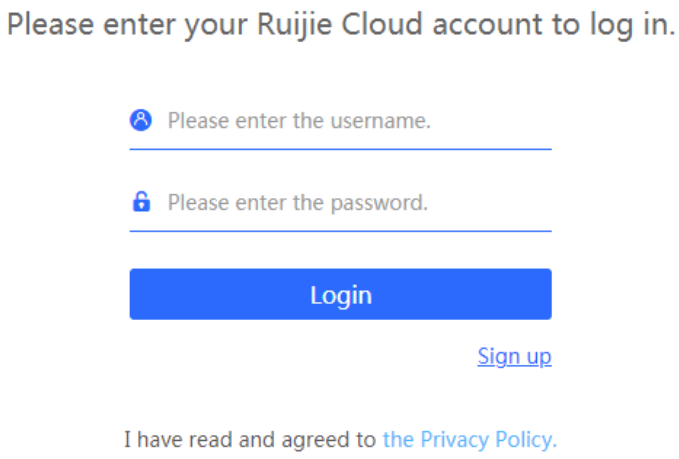
Figure 2-2-5 Failed Connection



2.2.4 Cloud Service

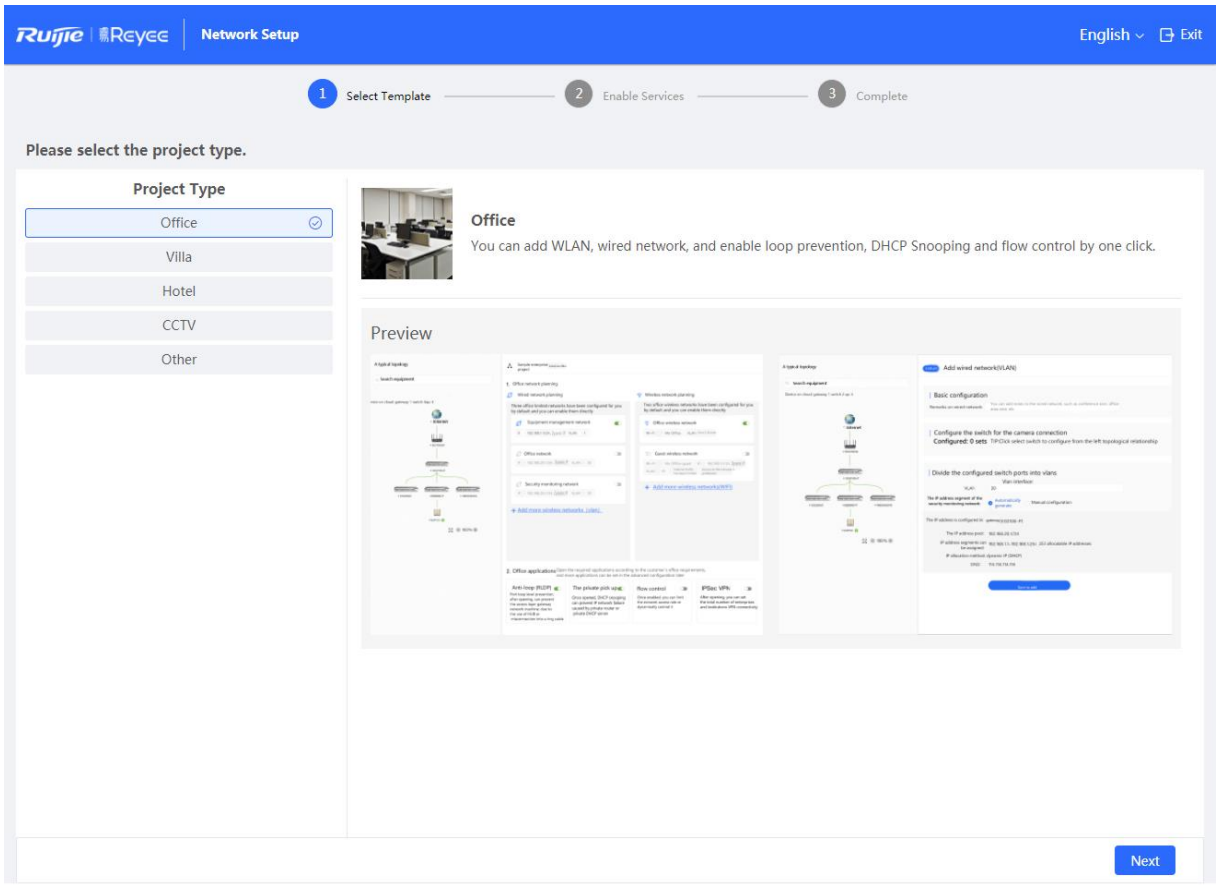
The **Network Setup** module requires a Ruijie Cloud account. If you are a new user, please register an account first at the Ruijie Cloud website.

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



If the device works in the standalone mode, log in and the account will be bound 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

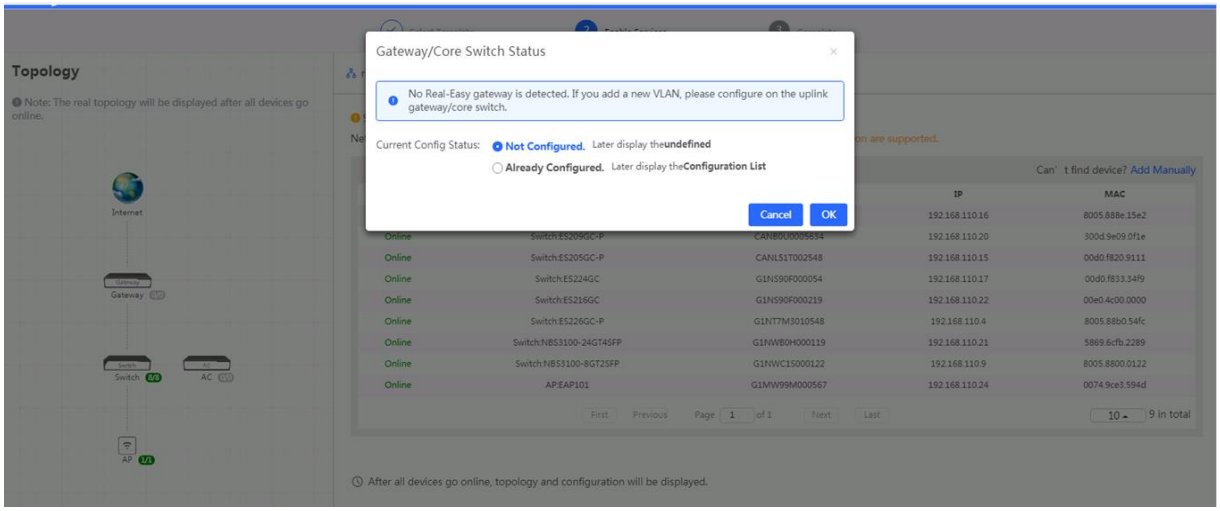
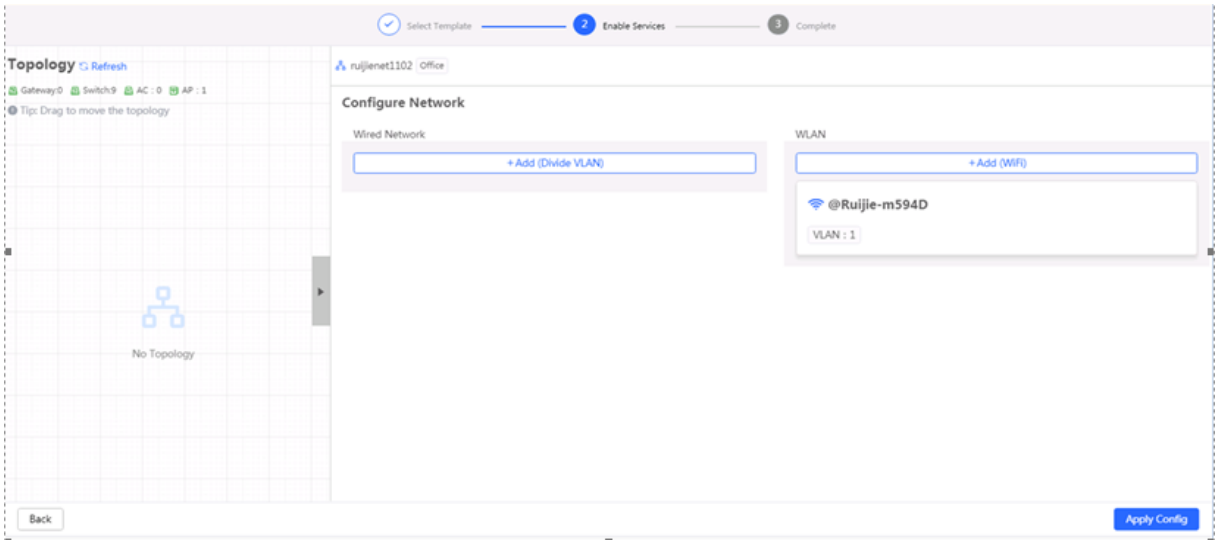
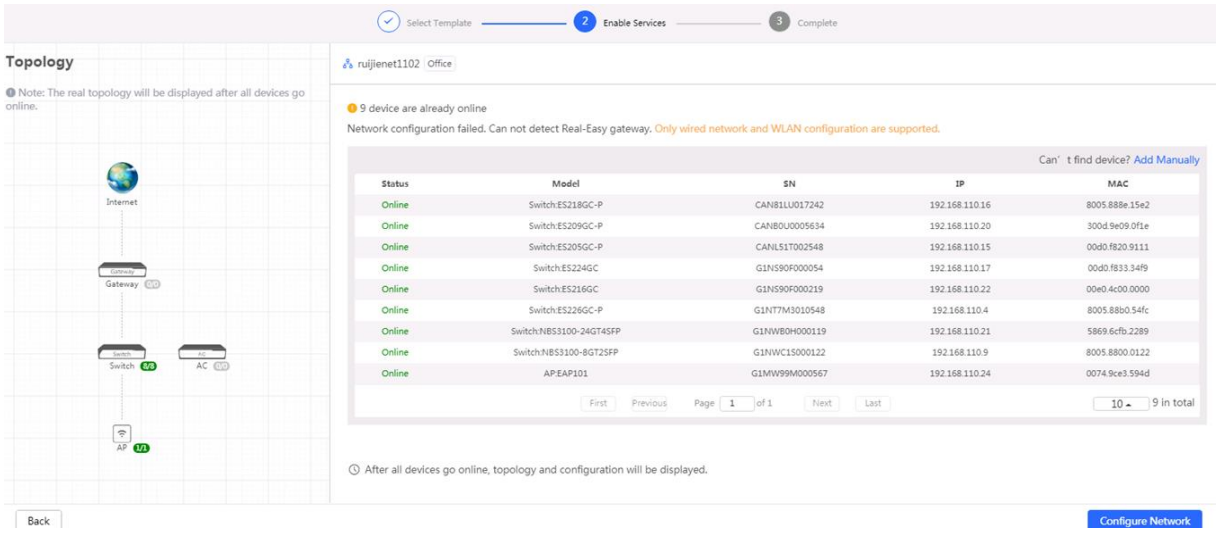


Figure 2-2-9 Enable Services



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

Figure 2-2-10 Complete



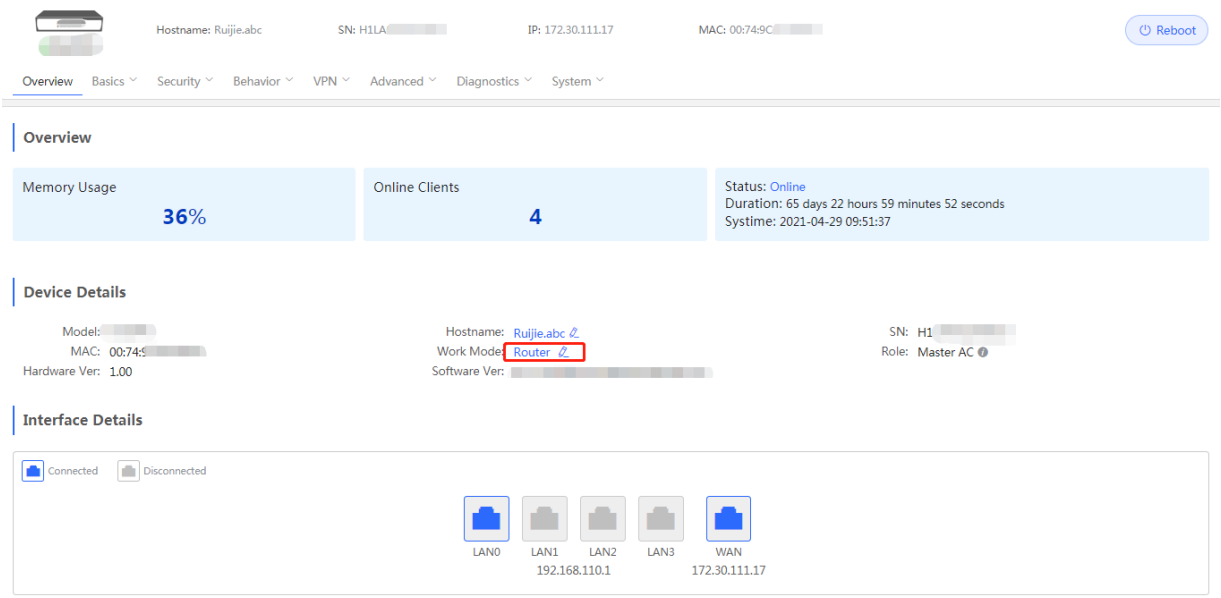
After the above step, click **Ruijie Cloud** to configure the device on Ruijie Cloud. Then exit from Ruijie Cloud and enter the eWeb page again.

Upon the configuration, check the network and wireless settings of each device for consistency.

2.3 Work Mode

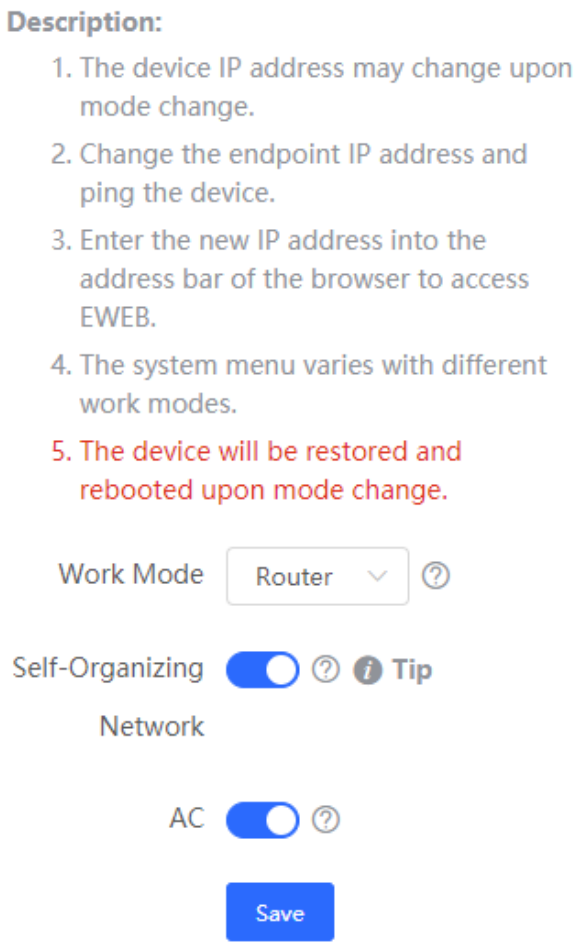
The eWeb menu varies with different work modes. The EG device works in the **Router** mode and the EAP device works in the **AP** mode by default. The work mode is displayed on the **Route > Overview** page.

Figure 2-3-1 Device Overview



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



2.3.1 Router Mode

The **Router** mode indicates NAT forwarding.

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

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

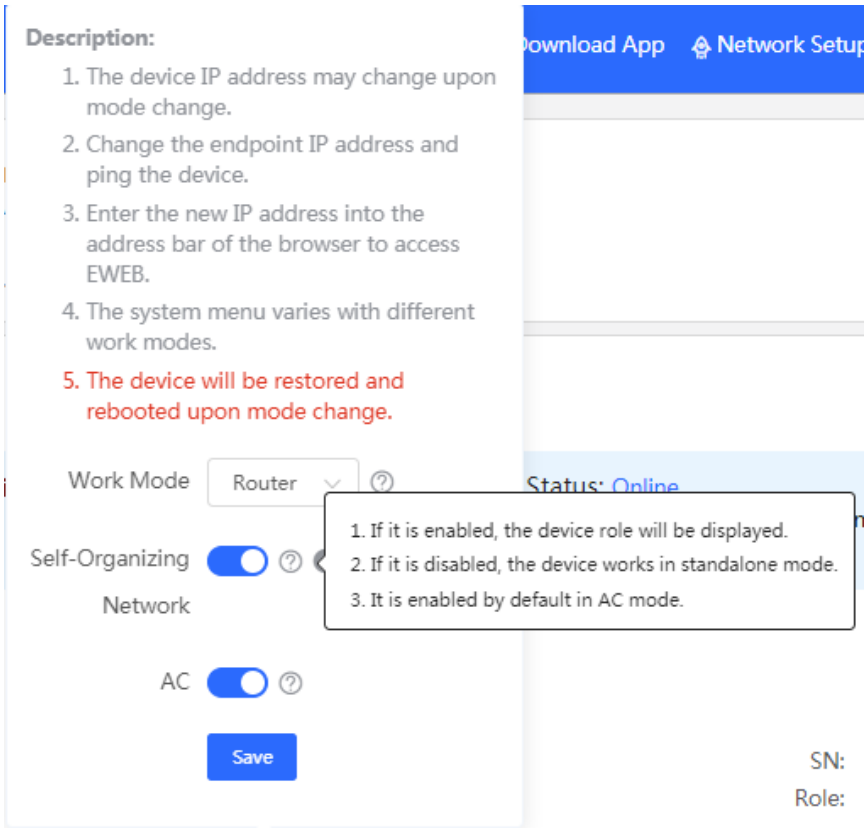
2.3.2 AP Mode

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

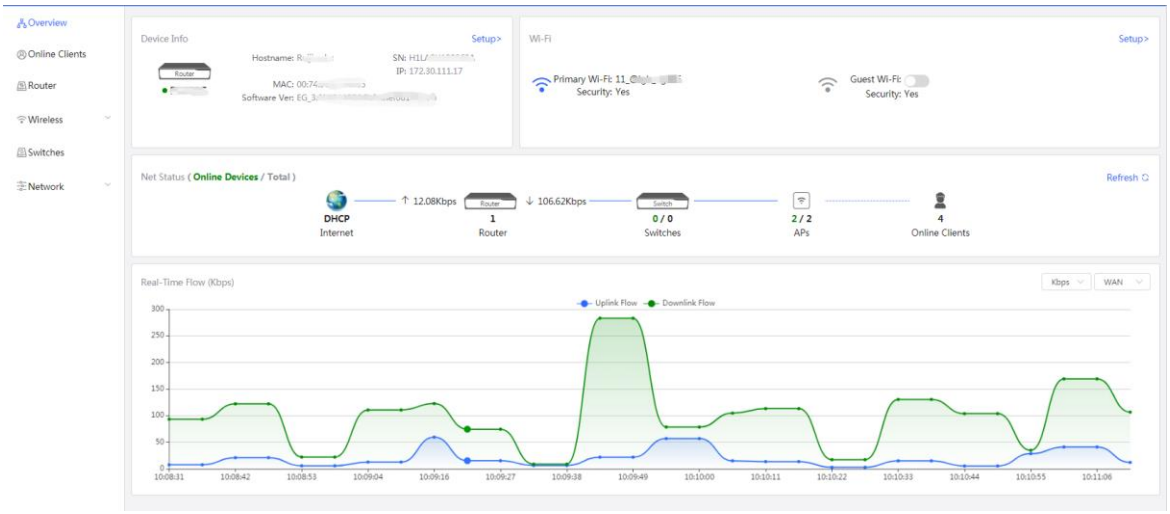


2.4.1 Enable

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.

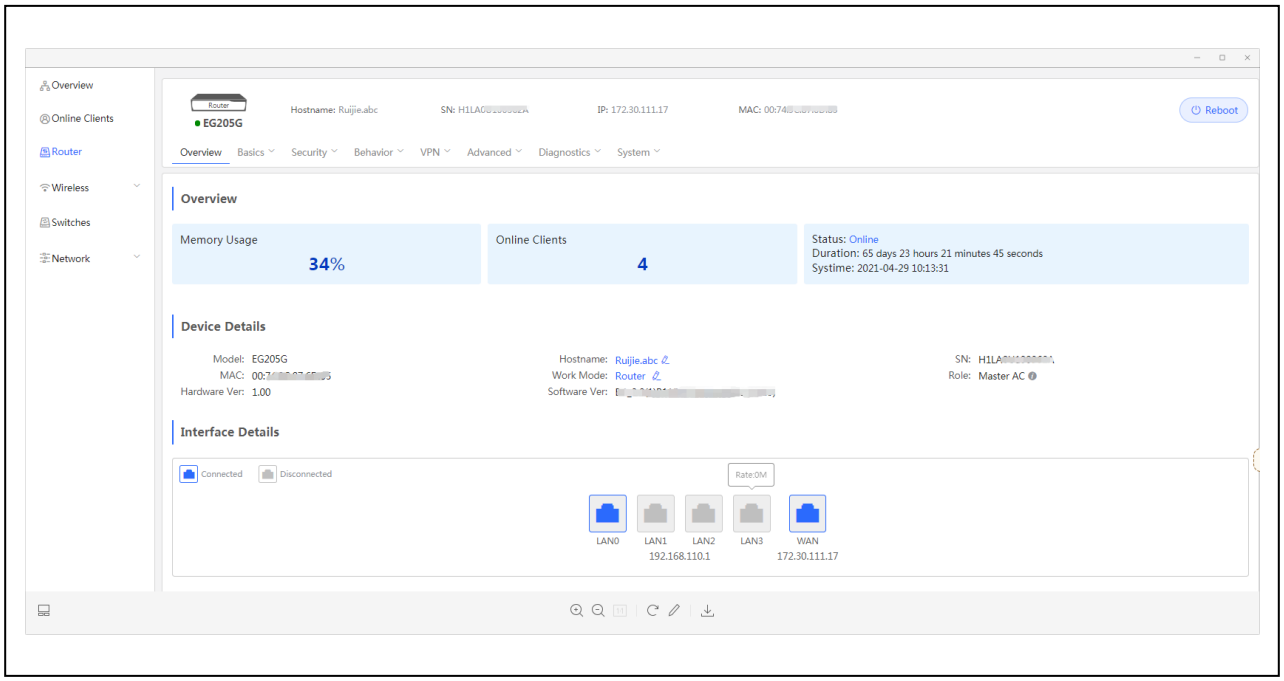
The menu on the left contains all network settings, including wireless management, switch management and system management.

Figure 2-4-2 Enable Self-Organizing Network



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

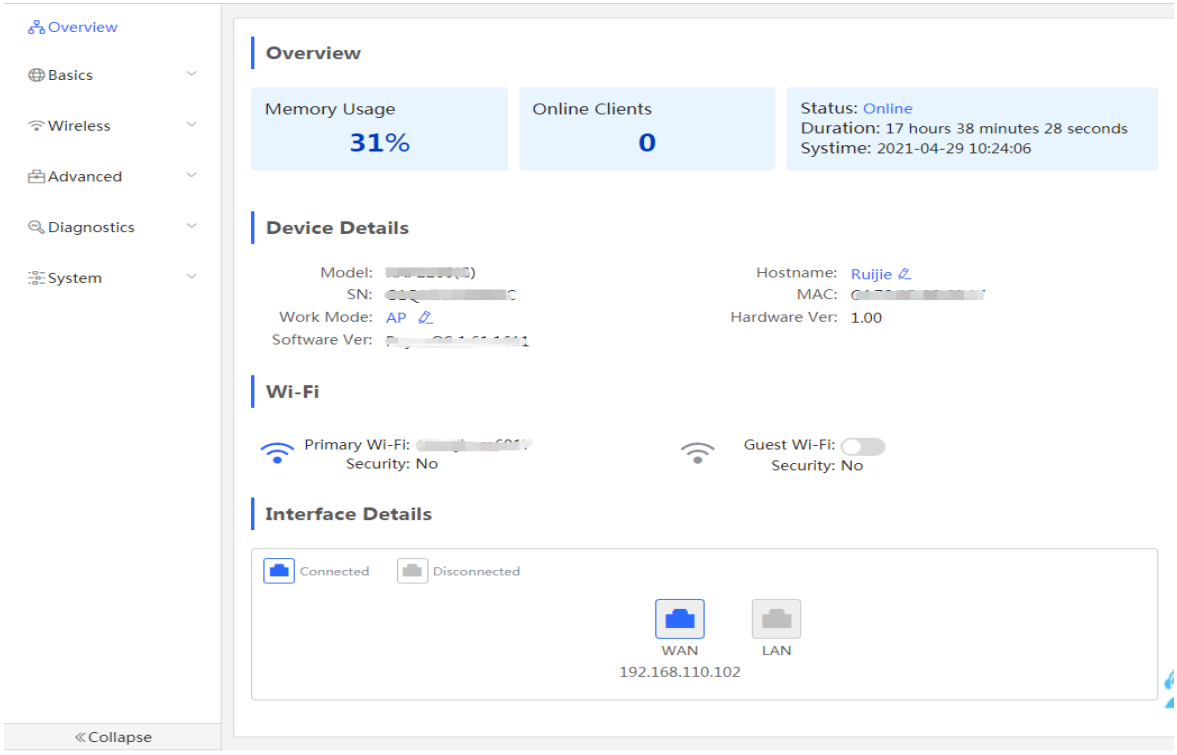


2.4.2 Disable

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

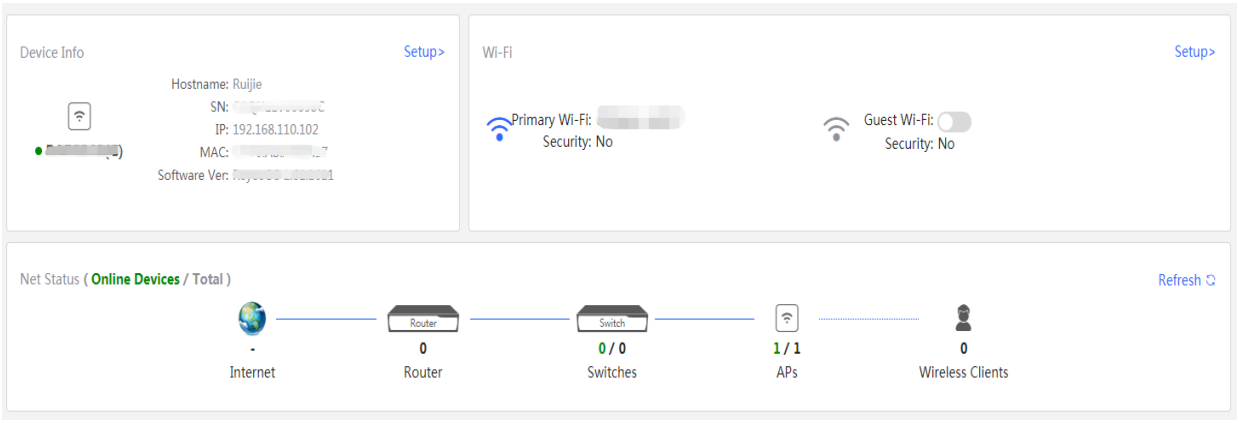


3 eWeb Configuration

3.1 Overview

The **Overview** page displays login device, wireless information and network status.

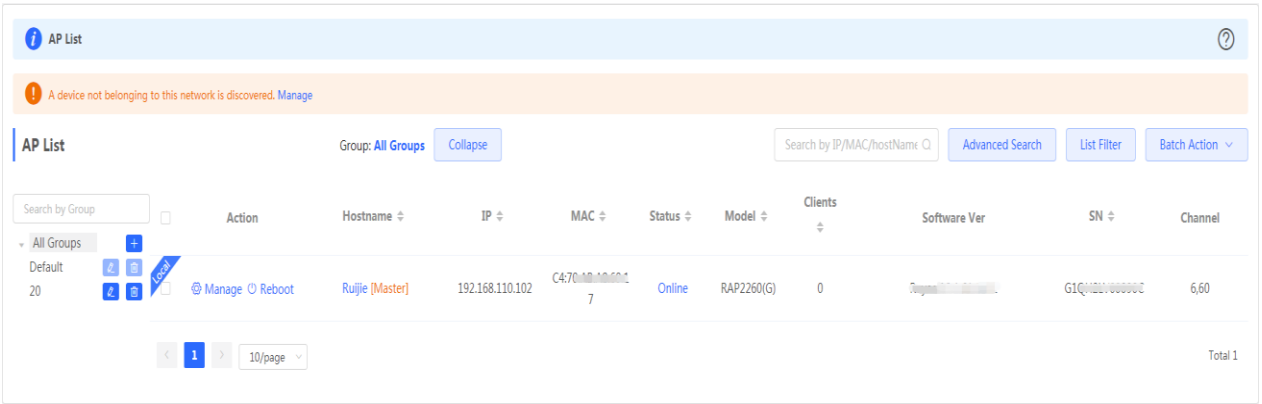
Figure 3-1 Overview



3.2 Basic Wireless

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

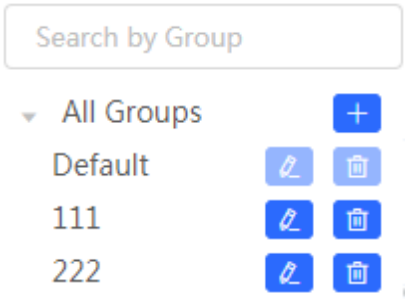
Figure 3-2-1 AP List



A. Group Management

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 3-2-2 Group Management



B. Advanced Search and List Filter

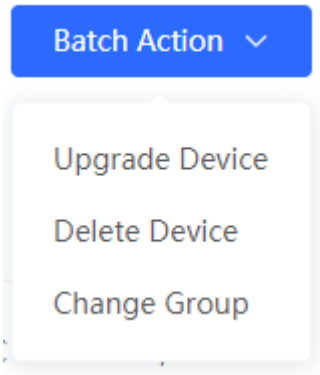
Click **Advanced Search**, and you can search APs by SN, model, software version, MAC address and IP address.

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

C. Batch Action

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

Figure 3-2-3 Batch Action



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

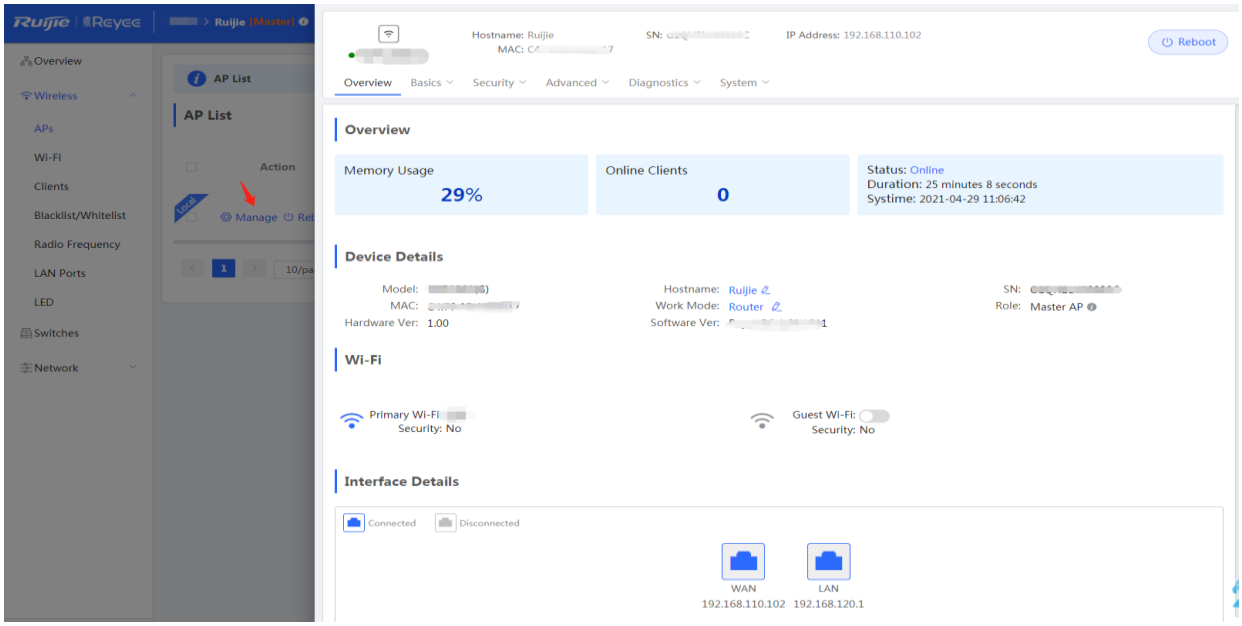
Delete Device: You can delete the devices in batches.

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

3.2.1 Configuration

Figure 3-2-4 Configuration

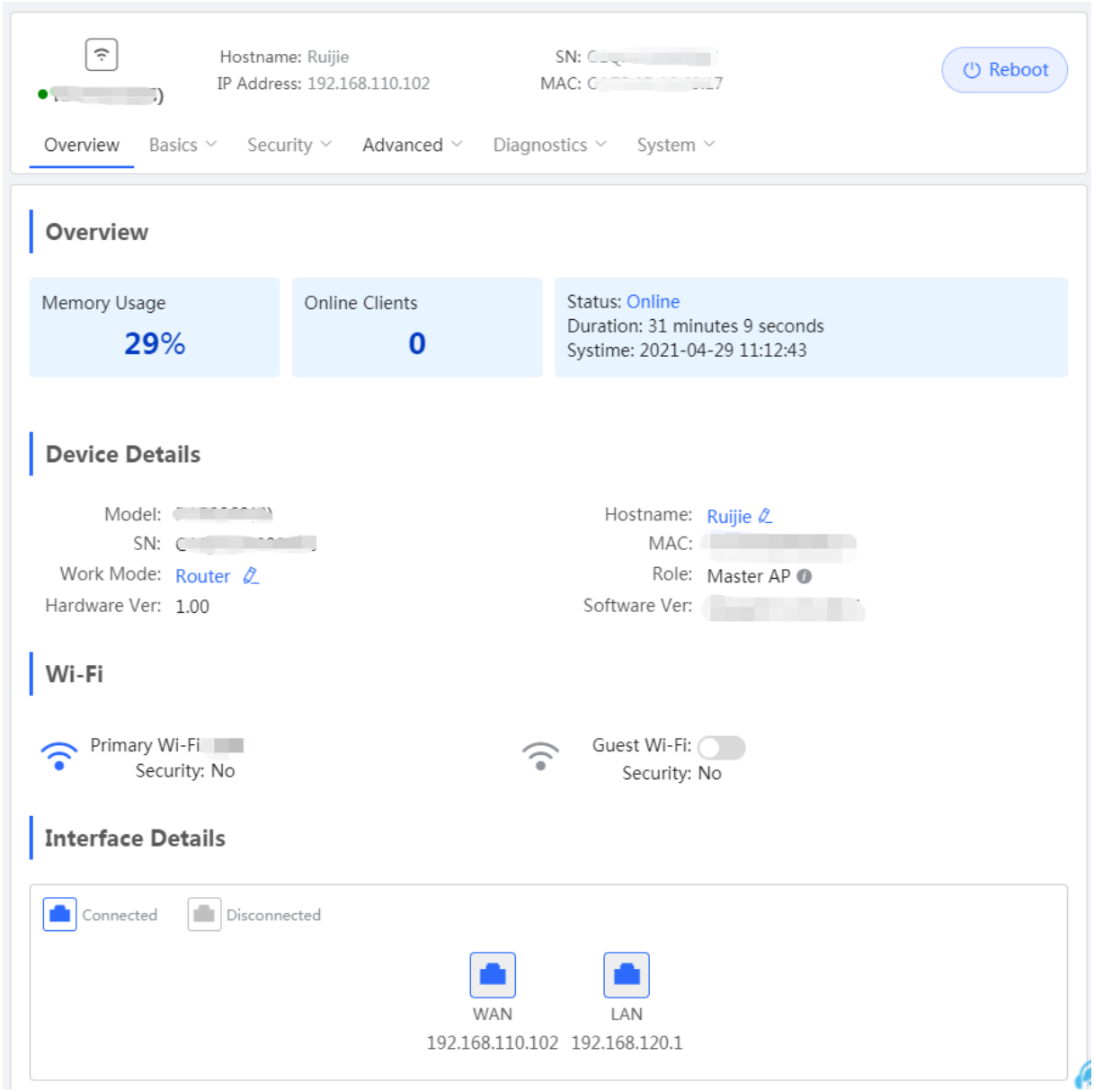
Select the target device and click **Manage** in the **Action** column, and the AP management page will be displayed.



3.2.2 Overview

The **Overview** page displays the information including memory usage, online clients, status, device details, wireless information and interface details.

Figure 3-2-5 Overview

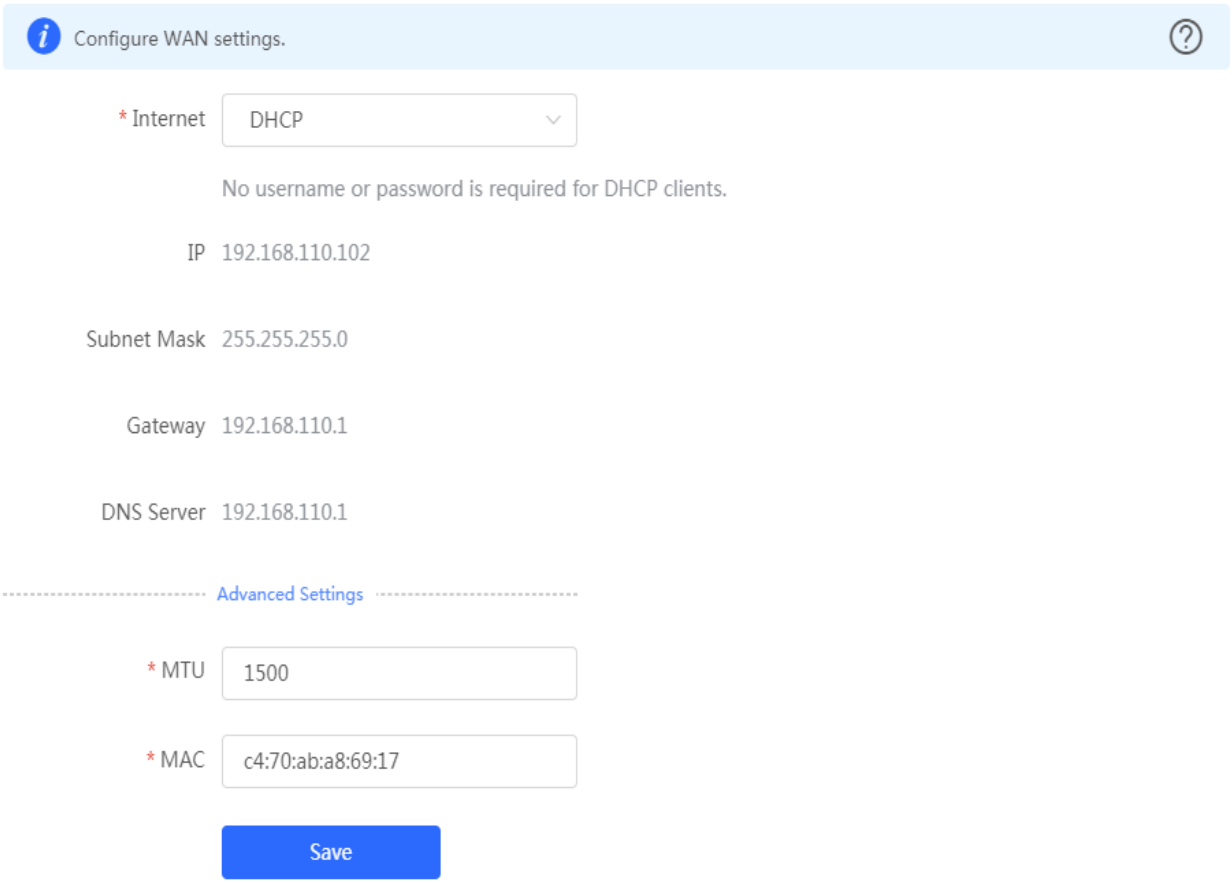


3.2.3 Basics

3.2.3.1 WAN

The **WAN** module allows you to configure WAN settings. WAN settings support multiple lines, and you can configure a specific line as needed.

Figure 3-2-6 WAN Settings



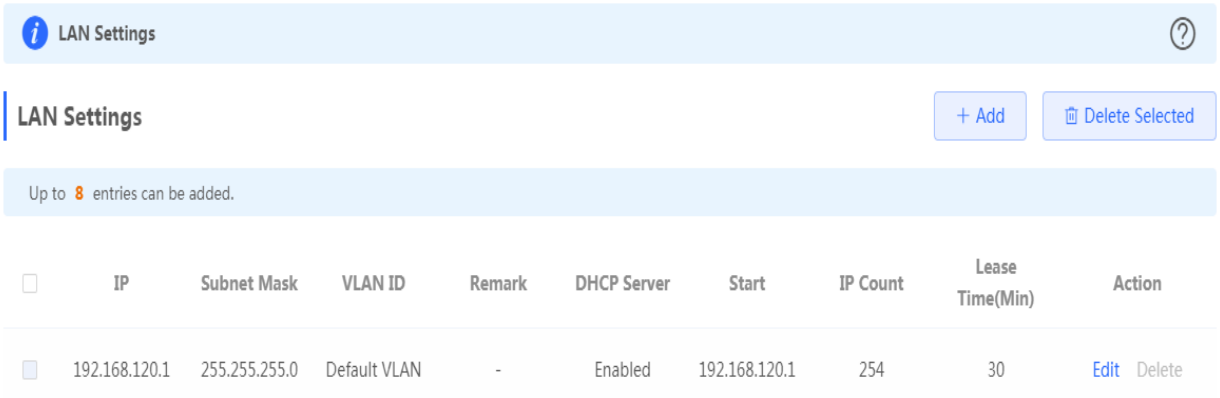
3.2.3.2 LAN

The **LAN** module contains **LAN Settings**, **Port VLAN**, **DHCP Clients** and **Static IP Addresses**.

LAN Settings

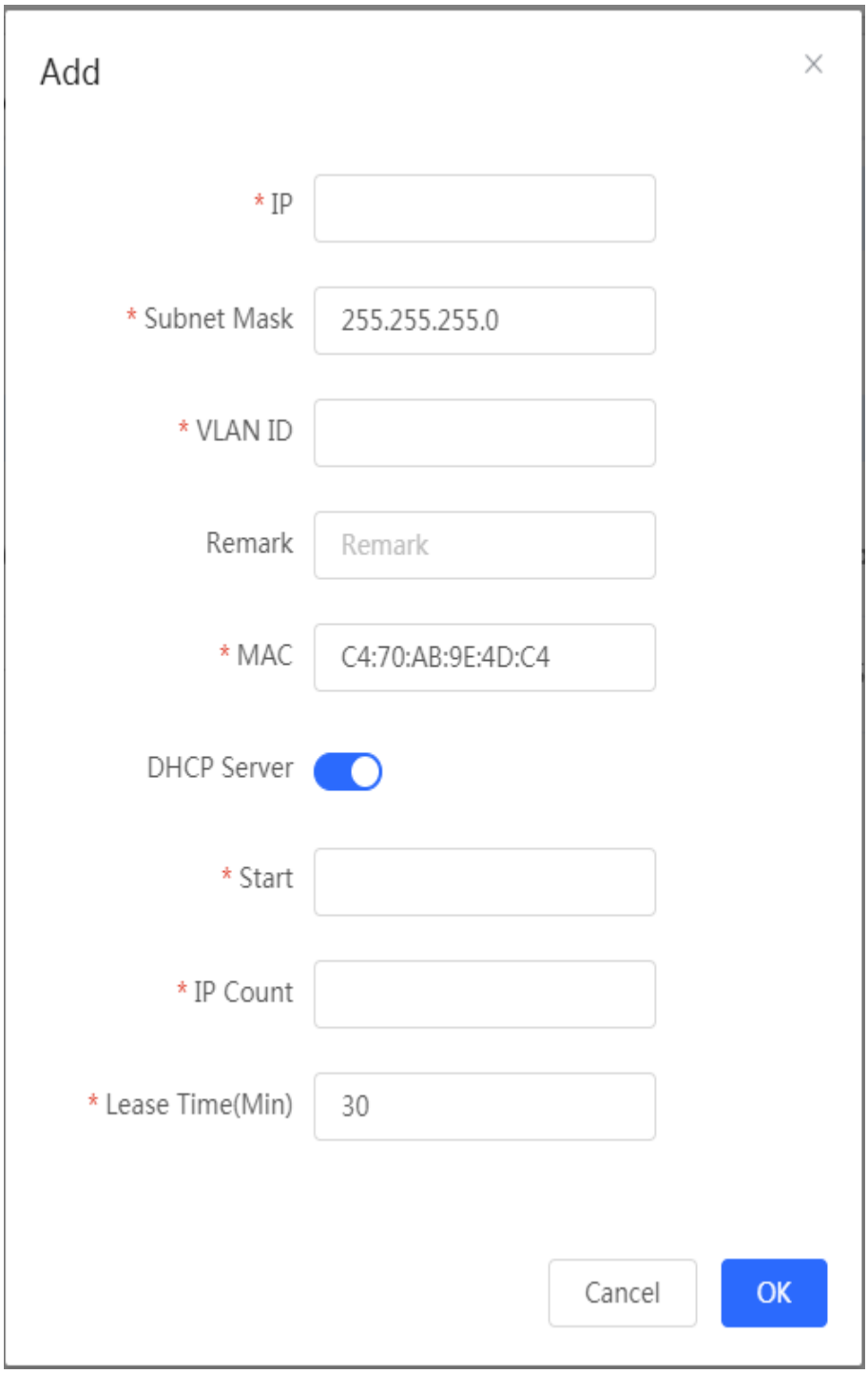
The **LAN** module allows you to set the IP address of the LAN port and DHCP status.

Figure 3-2-7 LAN Settings



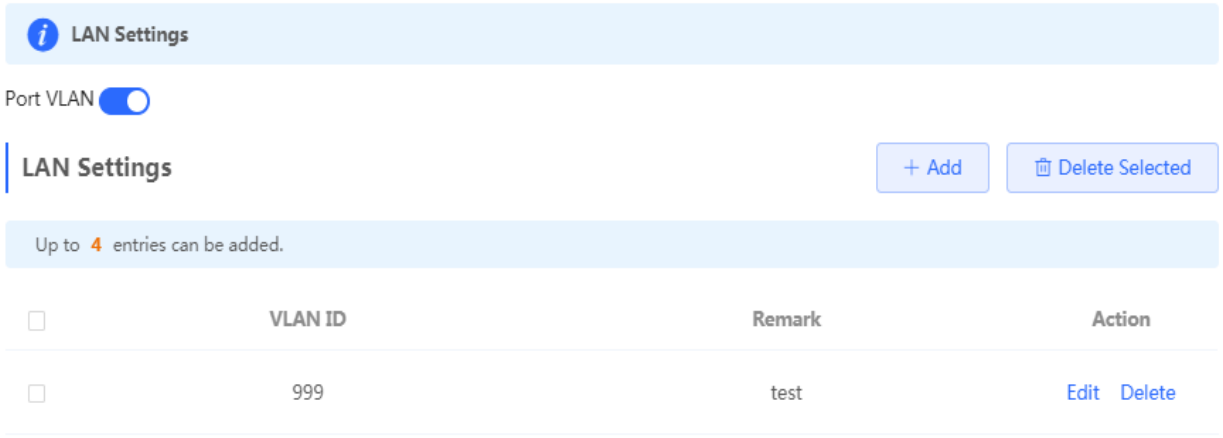
Click **Add** to add a VLAN. In the displayed dialog box, configure settings and click **OK**.

Figure 3-2-8 Add IP Address



In the AP mode, the Port VLAN function is available on page for the AP supporting Port VLAN.

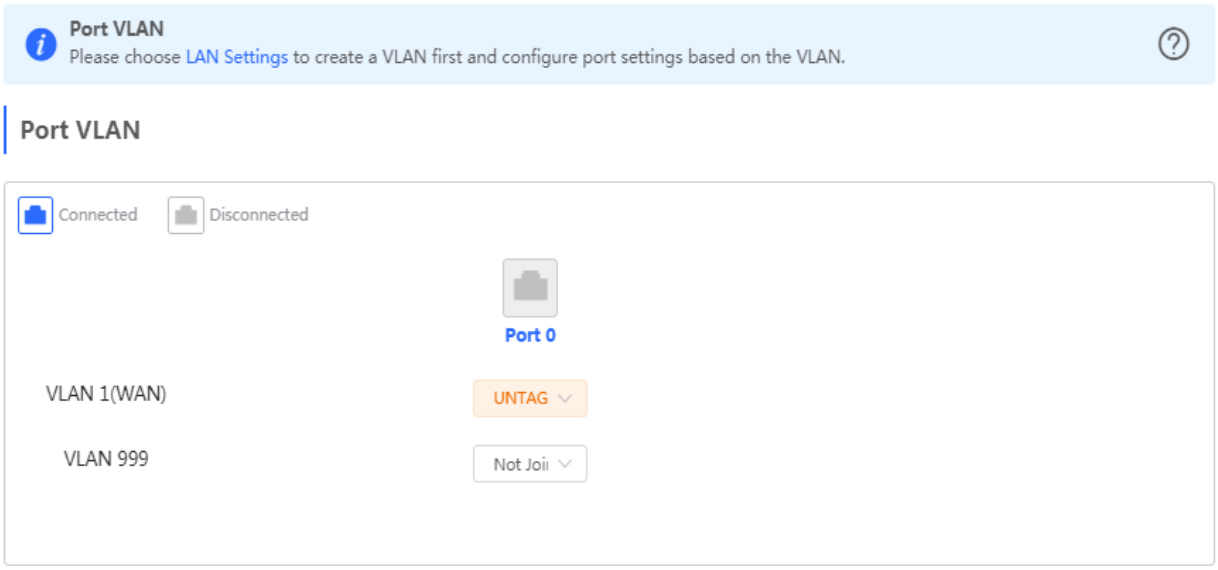
Figure 3-2-9 Port VLAN



Port VLAN

The **Port VLAN** page displays VLAN information. This page is displayed only when the AP is enabled with port VLAN in the AP mode.

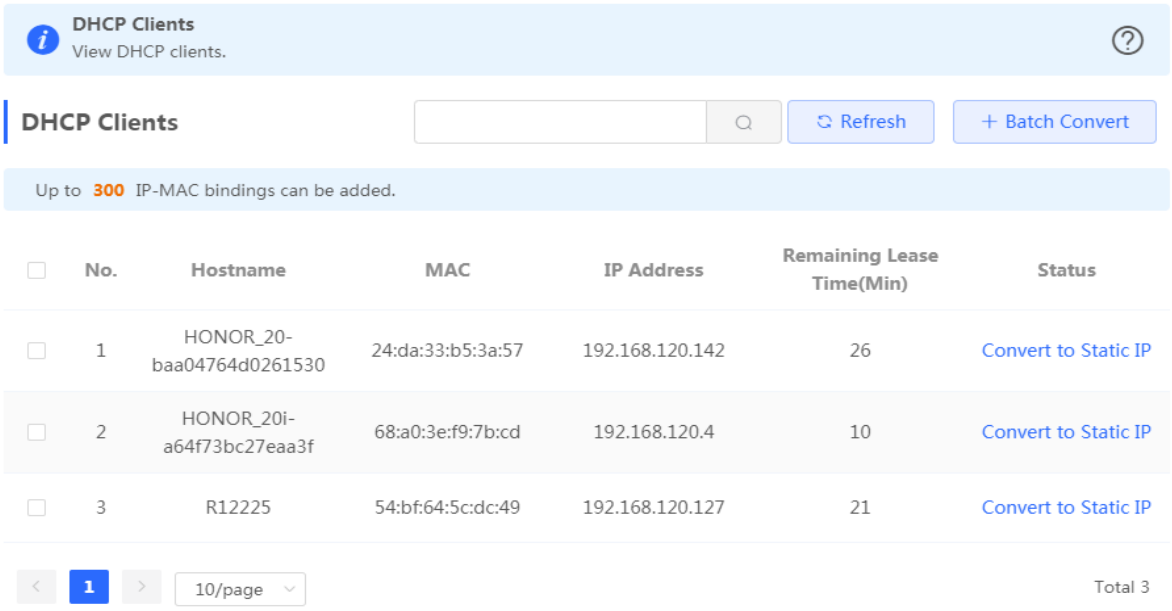
Figure 3-2-10 Port VLAN



DHCP Clients

The **DHCP Clients** page displays DHCP clients. This page is displayed only in the router mode.

Figure 3-2-11 DHCP Clients

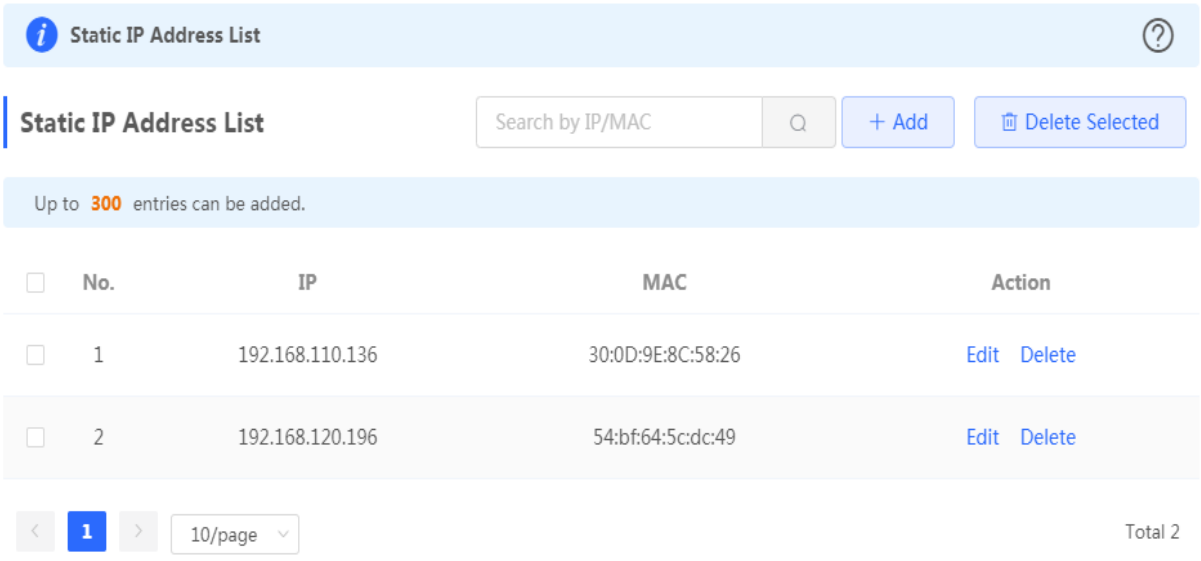


Click **Convert to Static IP** in the **Action** column to convert a DHCP-assigned IP address to a static IP address. Alternatively, select DHCP-assigned IP addresses and click **Batch Convert** to convert more than one IP address.

Static IP Addresses

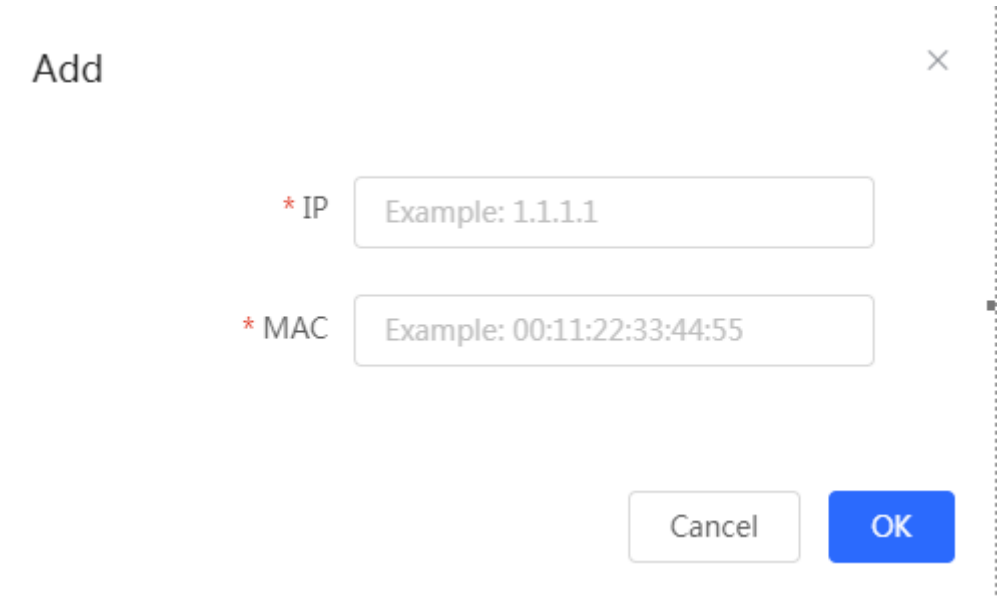
The **Static IP Addresses** module allows you to add, delete and edit static IP addresses. This page is displayed only in the router mode.

Figure 3-2-12 Static IP Addresses



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

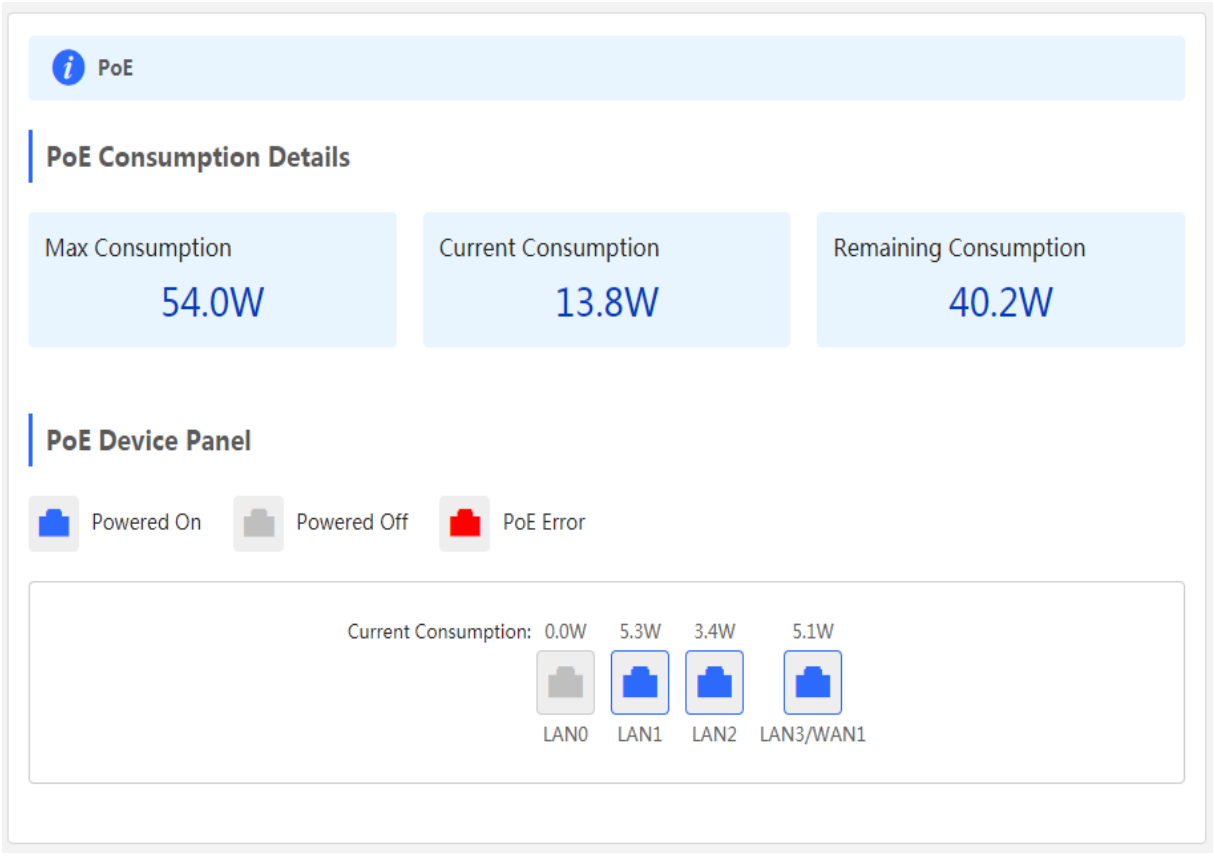
Figure 3-2-13 Add Static IP Address



3.2.3.3 PoE

The **PoE** page displays PoE status and power consumption.

Figure 3-2-14 PoE

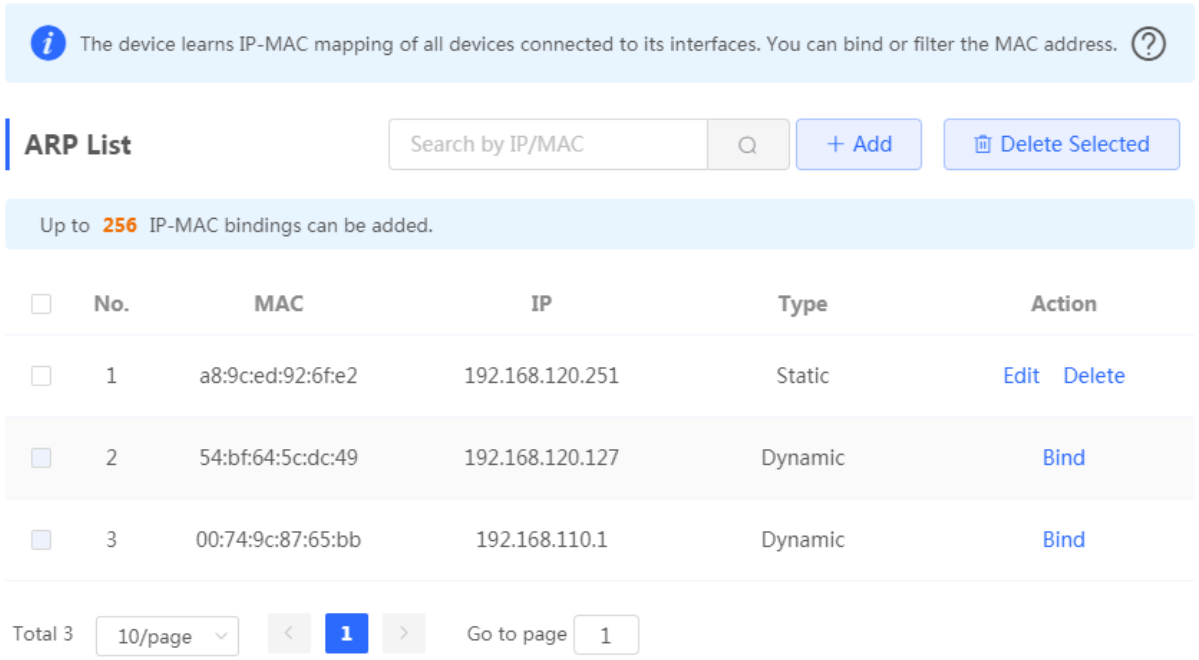


3.2.4 Security

3.2.4.1 ARP List

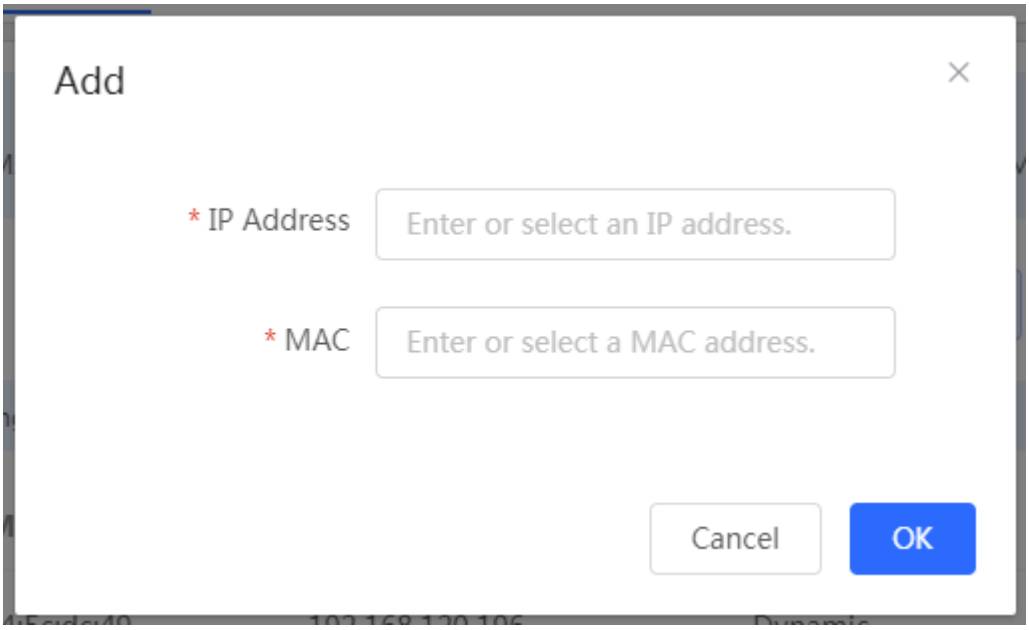
The **ARP List** page displays ARP entries.

Figure 3-2-15 ARP List



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 3-2-16 Add IP-MAC Binding



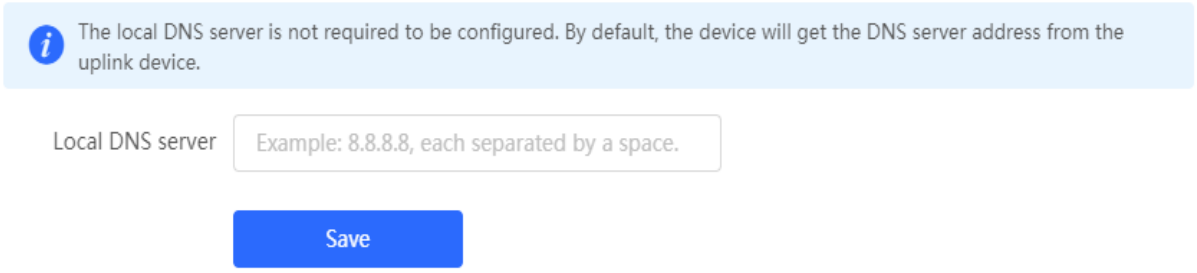
Click **Delete** in the **Action** column. The message "Are you sure you want to delete the entry?" is displayed. In the displayed dialog box, click **OK**. The message "Delete operation succeeded." is displayed.

3.2.5 Advanced

3.2.5.1 Local DNS

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

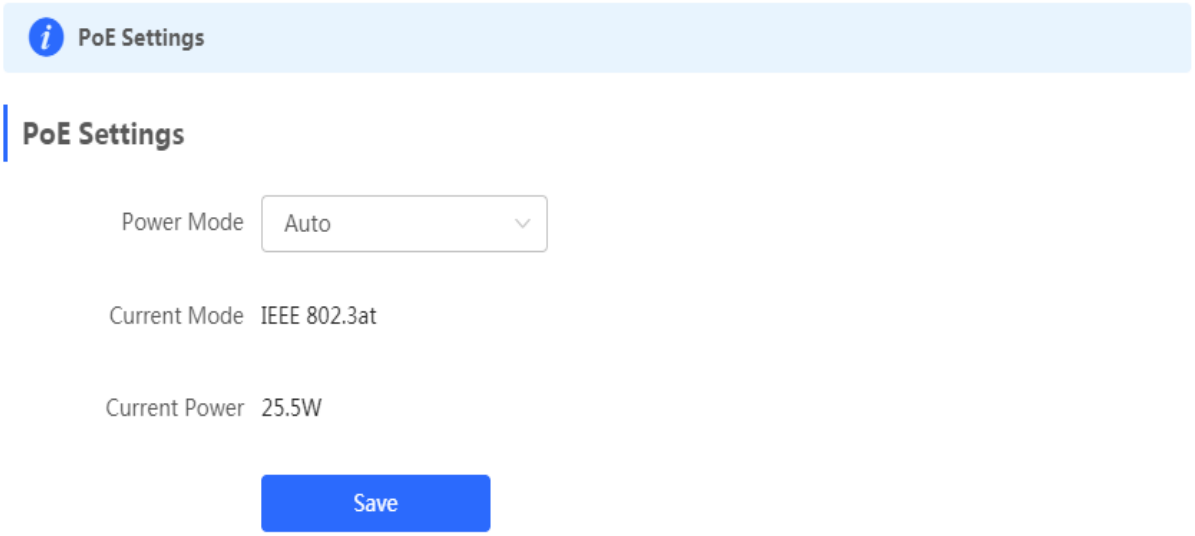
Figure 3-2-17 Local DNS



3.2.5.2 PoE Settings

The **PoE Settings** module allows you to configure the PoE mode.

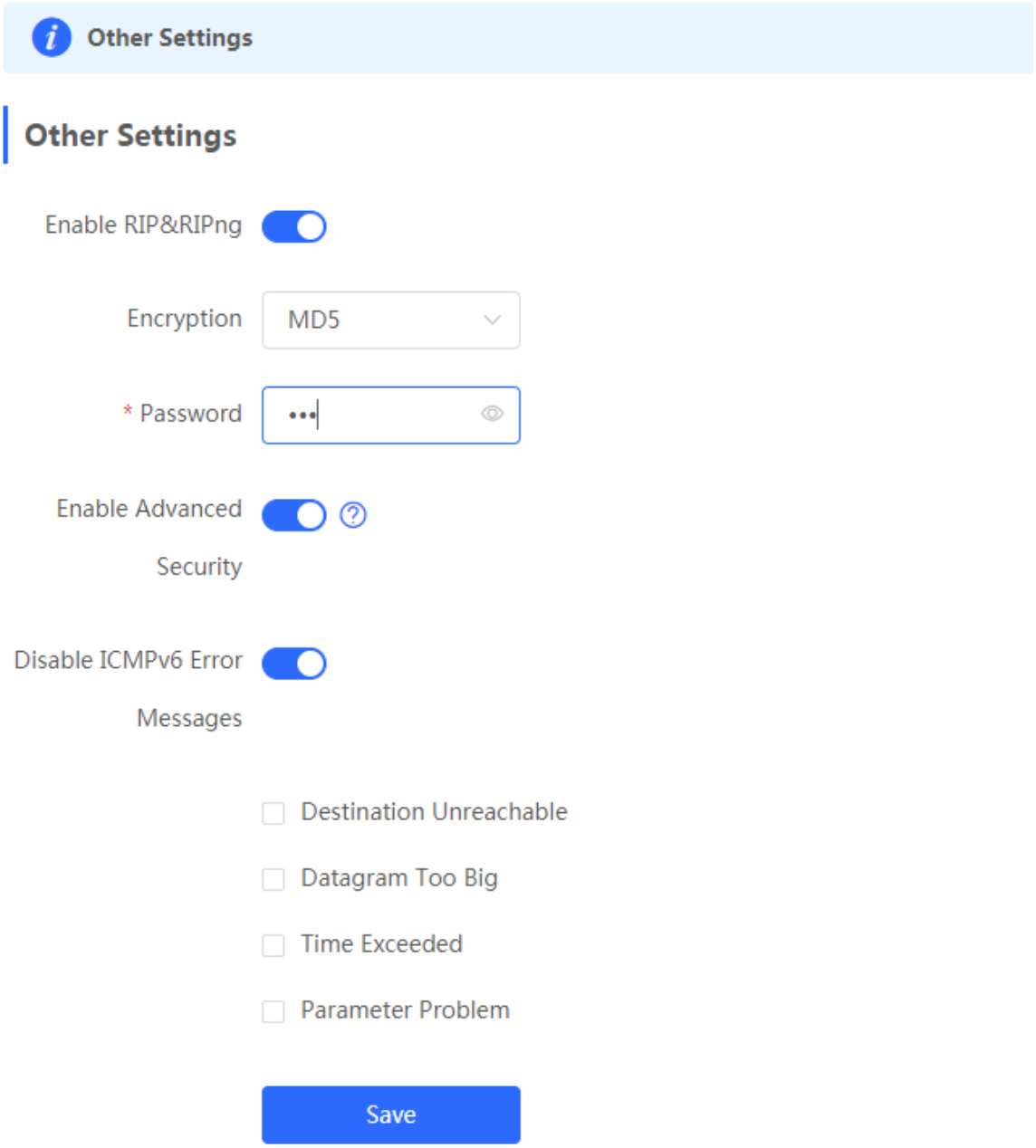
Figure 3-2-18 PoE Settings



3.2.5.3 Other Settings

The **Other Settings** module allows you to perform other settings, such as Enable RIP&RIPng, Enable Advanced and Disable ICMPv6 Error.

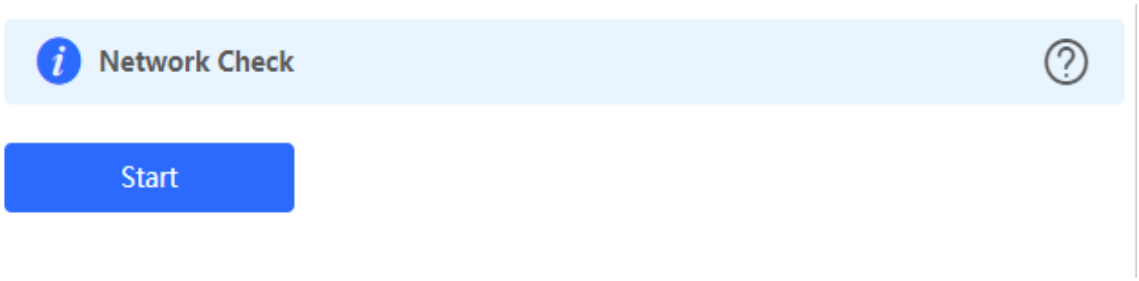
Figure 3-2-19 Other Settings



3.2.6 Diagnostics

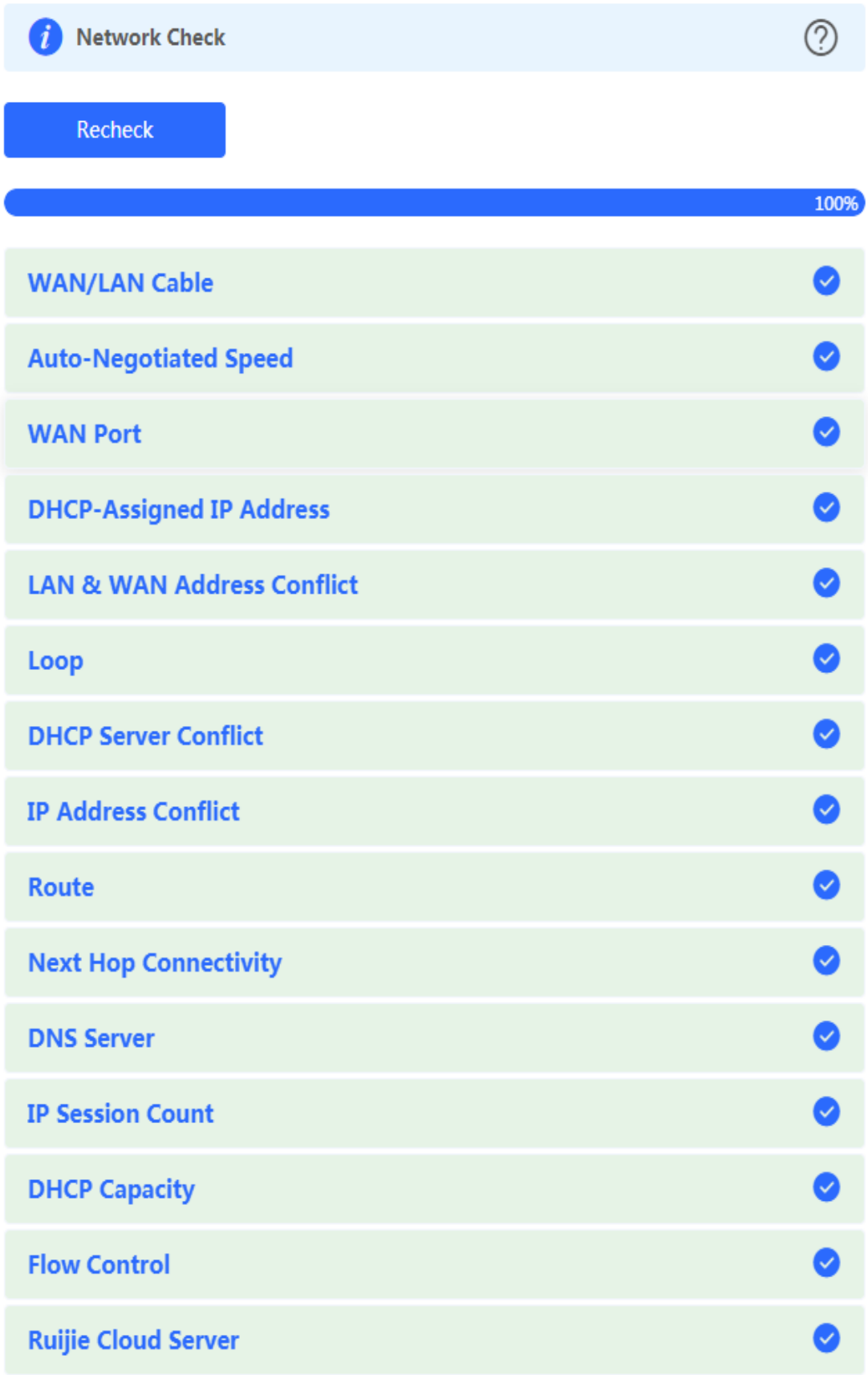
3.2.6.1 Network Check

Figure 3-2-20 Network Check



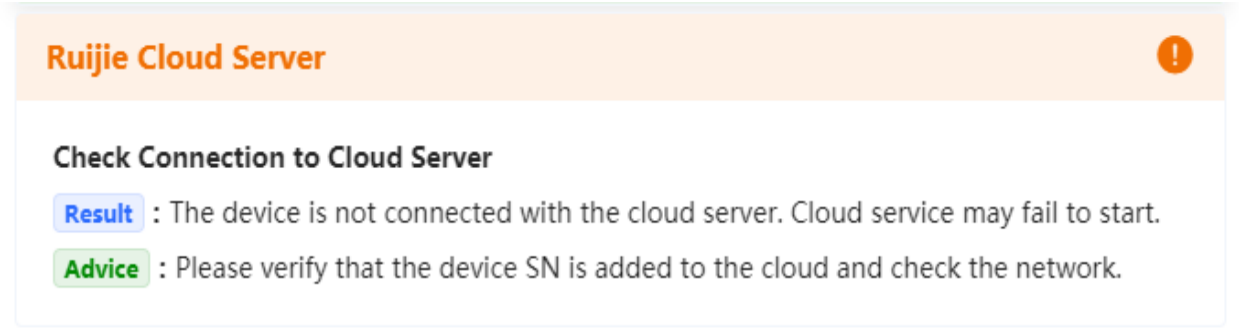
Click **Start**, and click **OK** in the confirmation box. After the test finishes, the result will be displayed.

Figure 3-2-21 Result


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
Flow Control
Ruijie Cloud Server

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

Figure 3-2-22 Issue & Advice

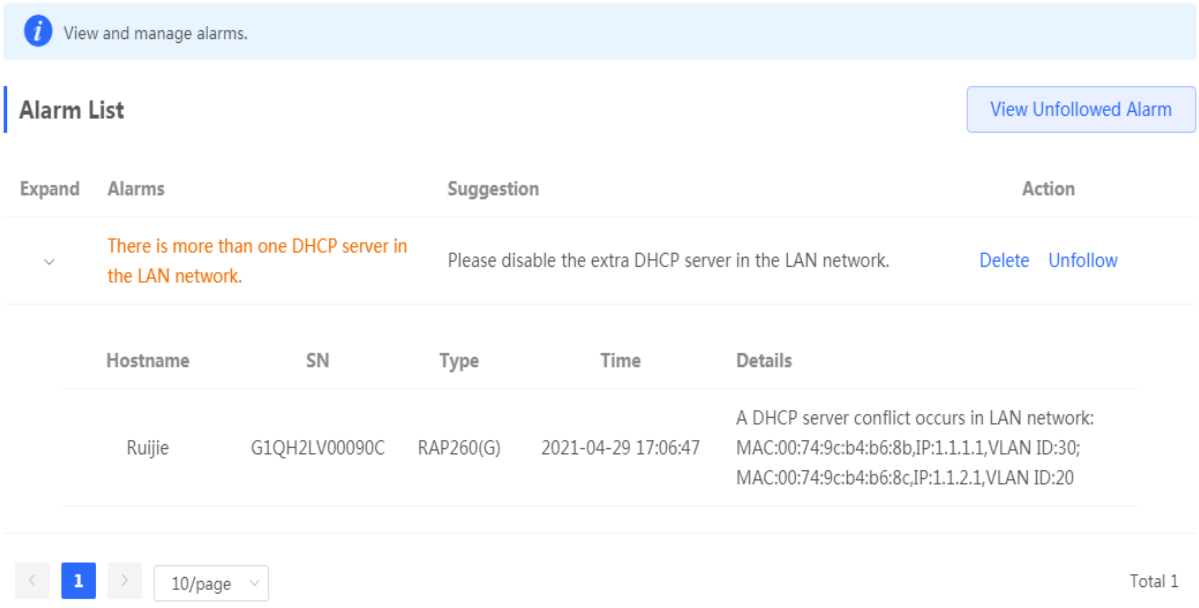


Please fix the problem by taking the suggested action.

3.2.6.2 Alarms

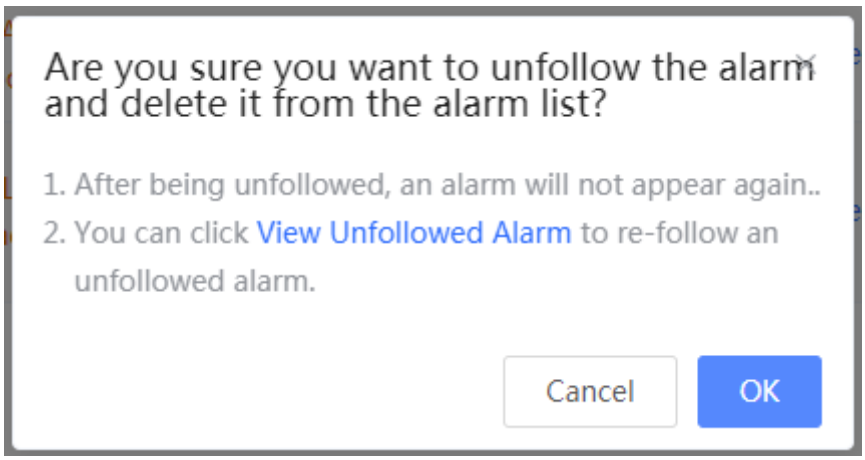
The **Alarms** module allows you to view and manage alarms in the network.

Figure 3-2-23 Alarms



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

Figure 3-2-24 Unfollow Alarm



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

Figure 3-3-25 Re-follow Alarm

3.2.6.3 Network Tools

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

Figure 3-2-26 Ping Test and Result

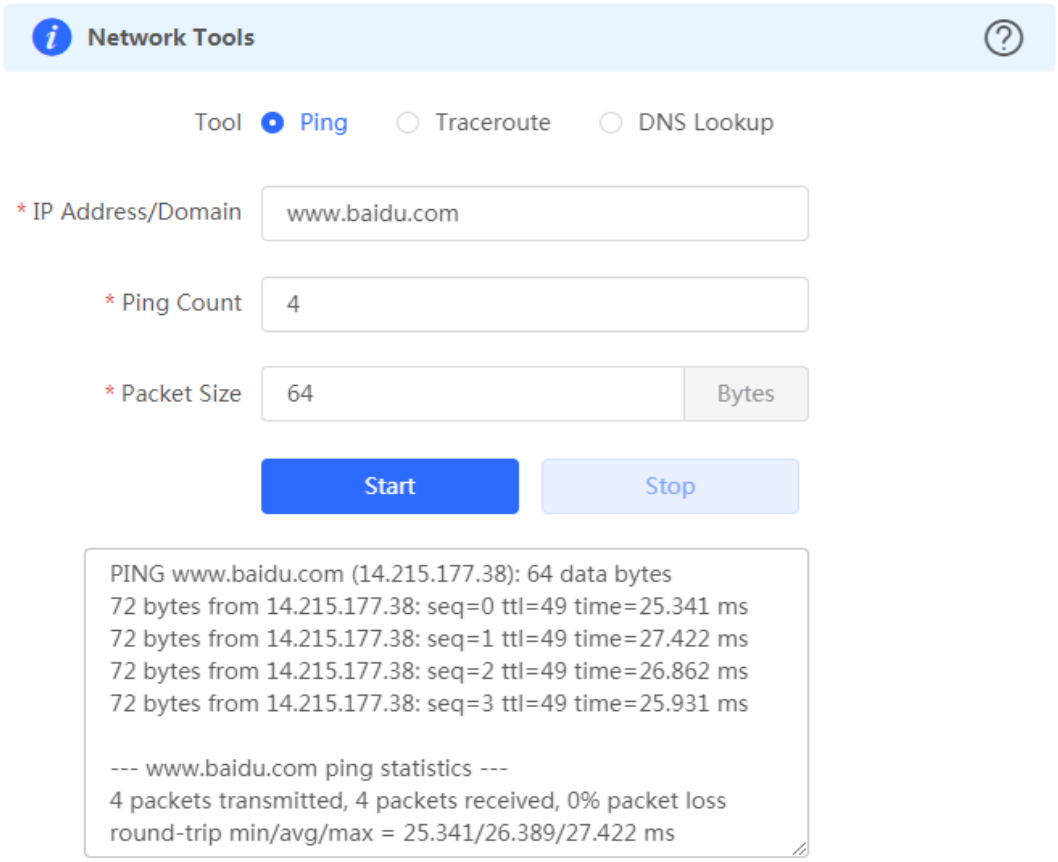


Figure 3-2-27 Traceroute Test and Result

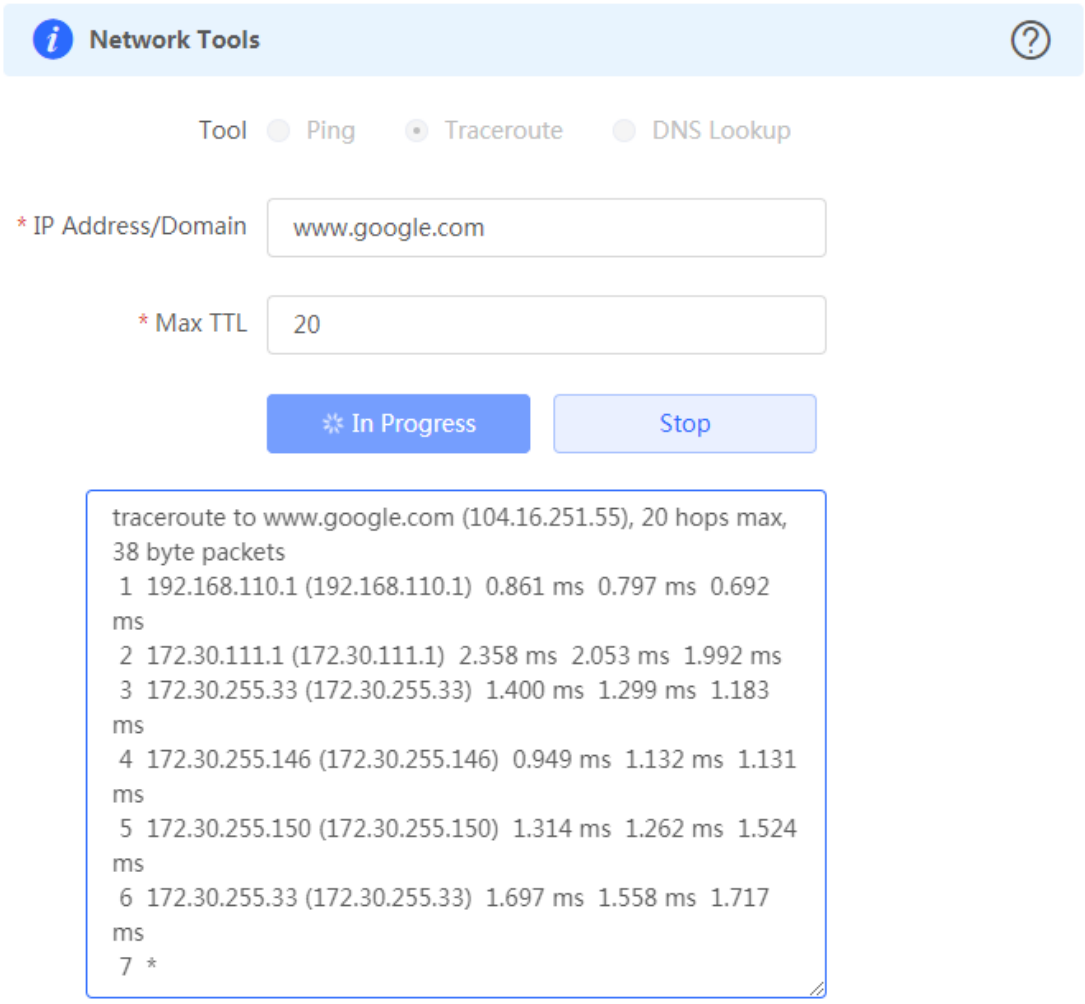
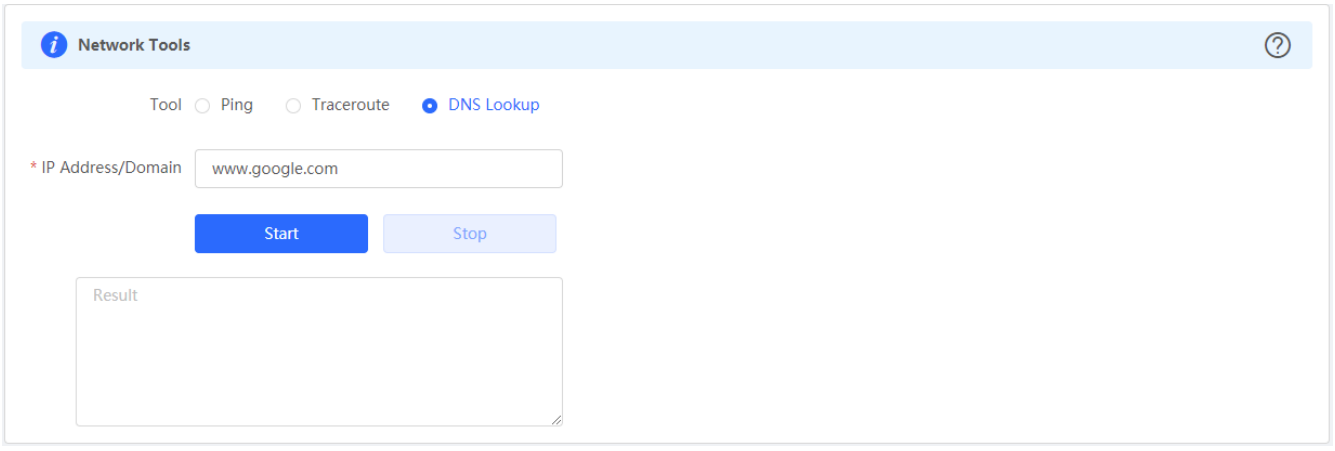


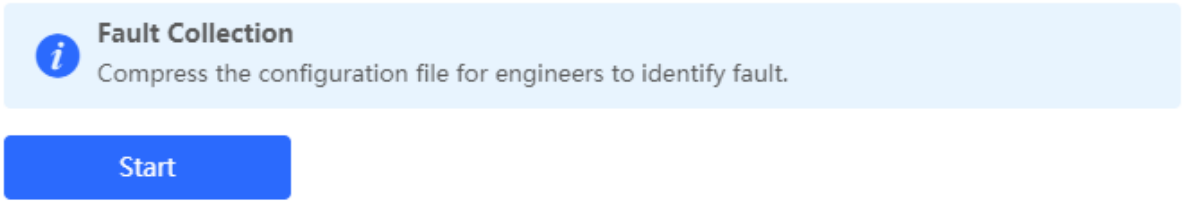
Figure 3-2-28 DNS Lookup Test and Result



3.2.6.4 Fault Collection

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

Figure 3-2-29 Fault Collection

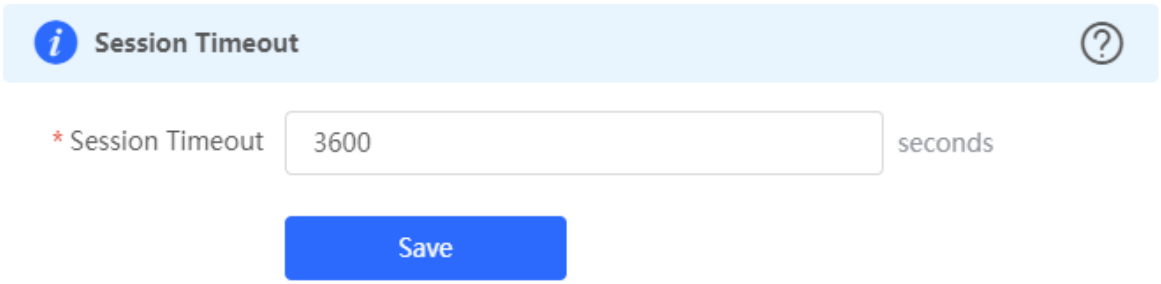


3.2.7 System

3.2.7.1 Session Timeout

The **Session Timeout** module allows you to set the session timeout period.

Figure 3-2-30 Session Timeout

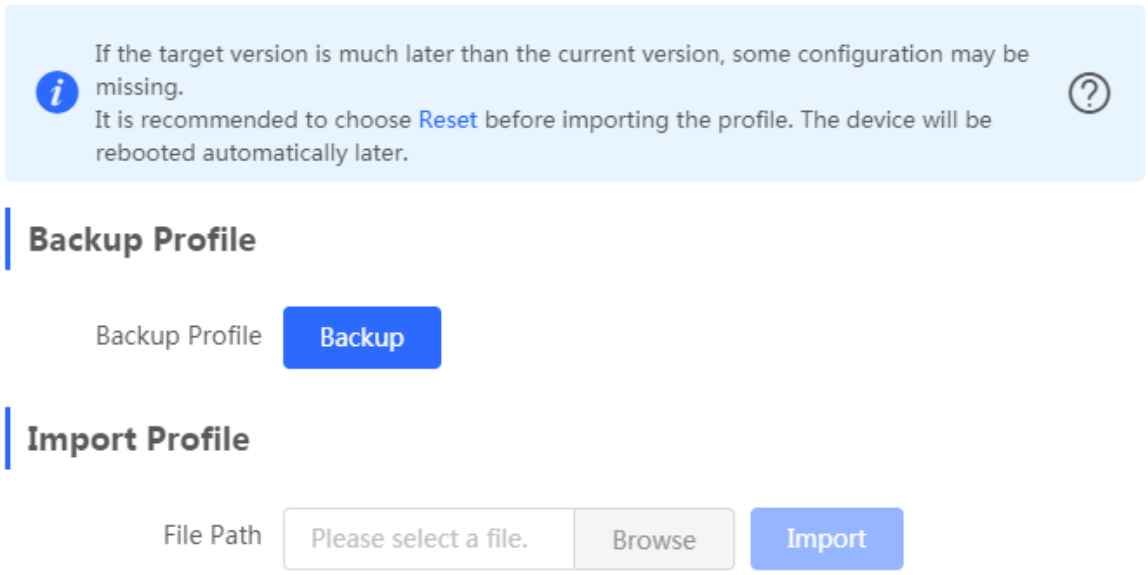


3.2.7.2 Backup & Import & Reset

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.

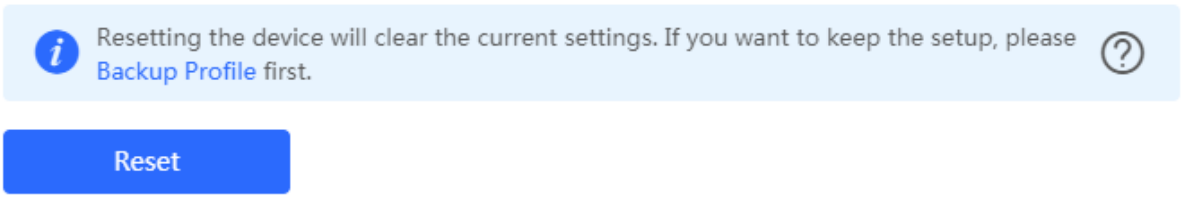
Figure 3-2-31 Backup & Import



Restore

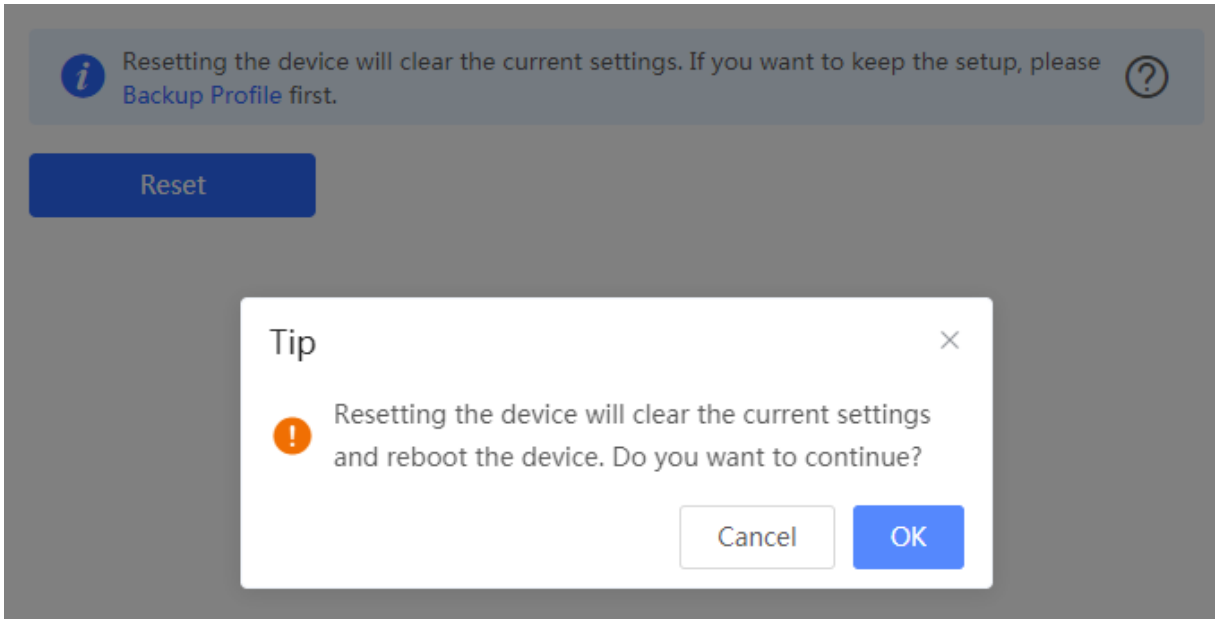
The **Restore** module allows you to restore the device to factory settings.

Figure 3-2-32 Restore



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

Figure 3-2-33 Confirm Restore



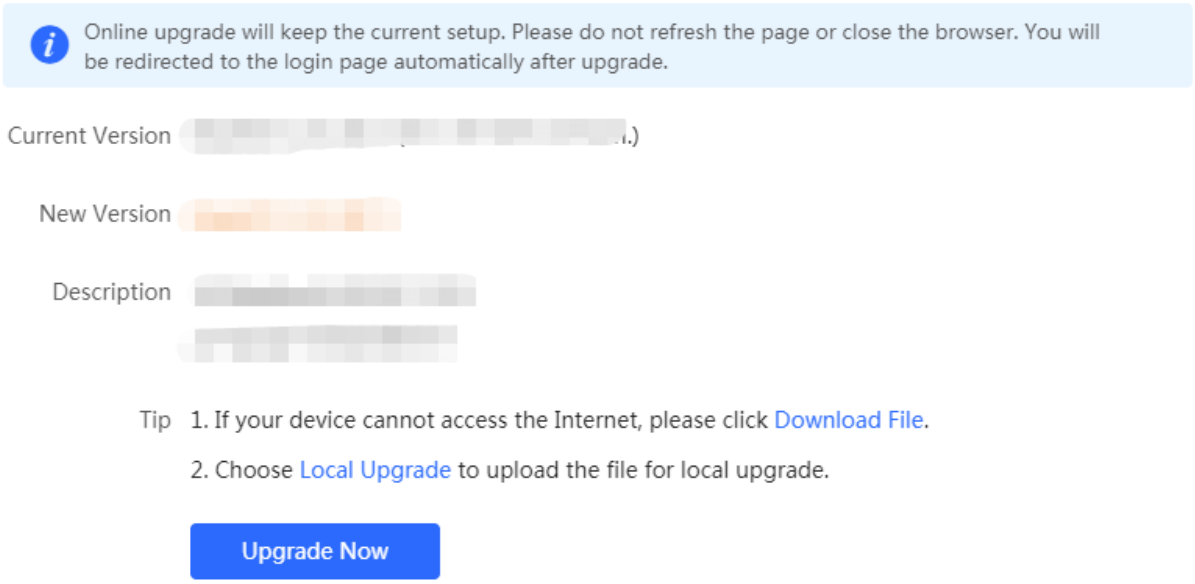
Click **OK** to restore all default values. This function is recommended when the network configuration is incorrect or the network environment is changed.

3.2.7.3 Upgrade

Online Upgrade

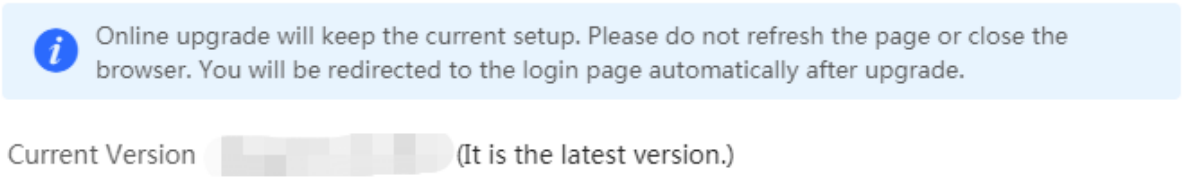
Click **Upgrade Now**. The device downloads the upgrade package from the network, and upgrades the current version. The upgrade operation retains configuration of the current device. Alternatively, you can select **Download File** to the local device and import the upgrade package on the **Local Upgrade** page.

Figure 3-2-34 Online Upgrade



If there is no available new version, the device displays a prompt indicating that the current version is the latest.

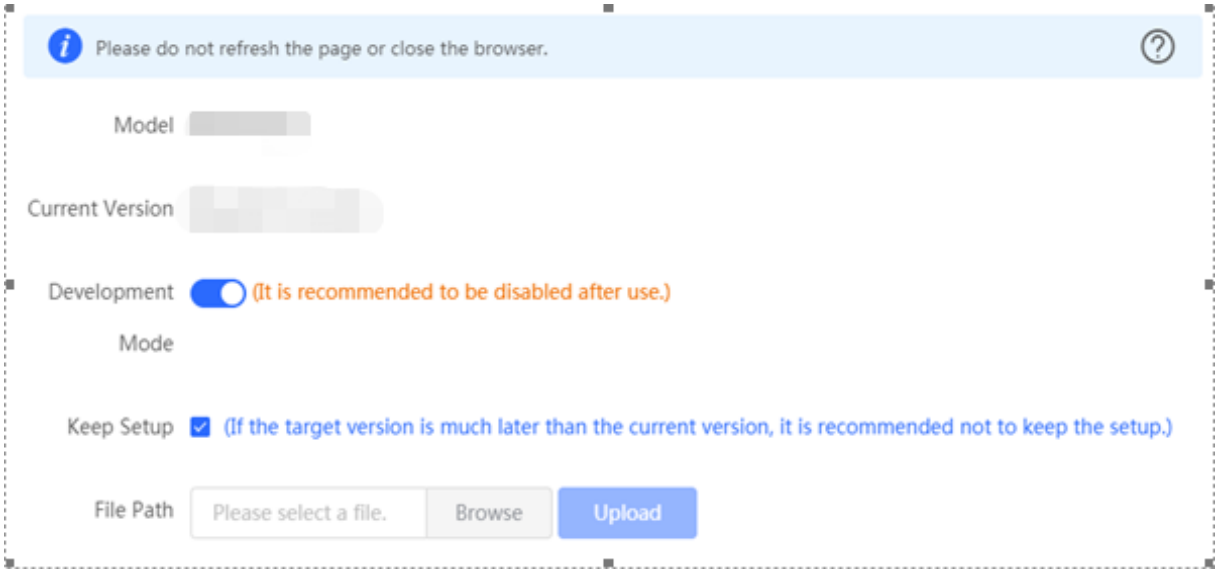
Figure 3-2-35 Upgrade Prompt



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.

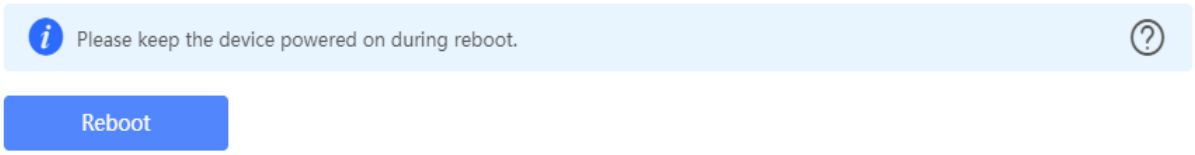
Figure 3-2-36 Local Upgrade



3.2.7.4 Reboot

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

Figure 3-2-37 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.

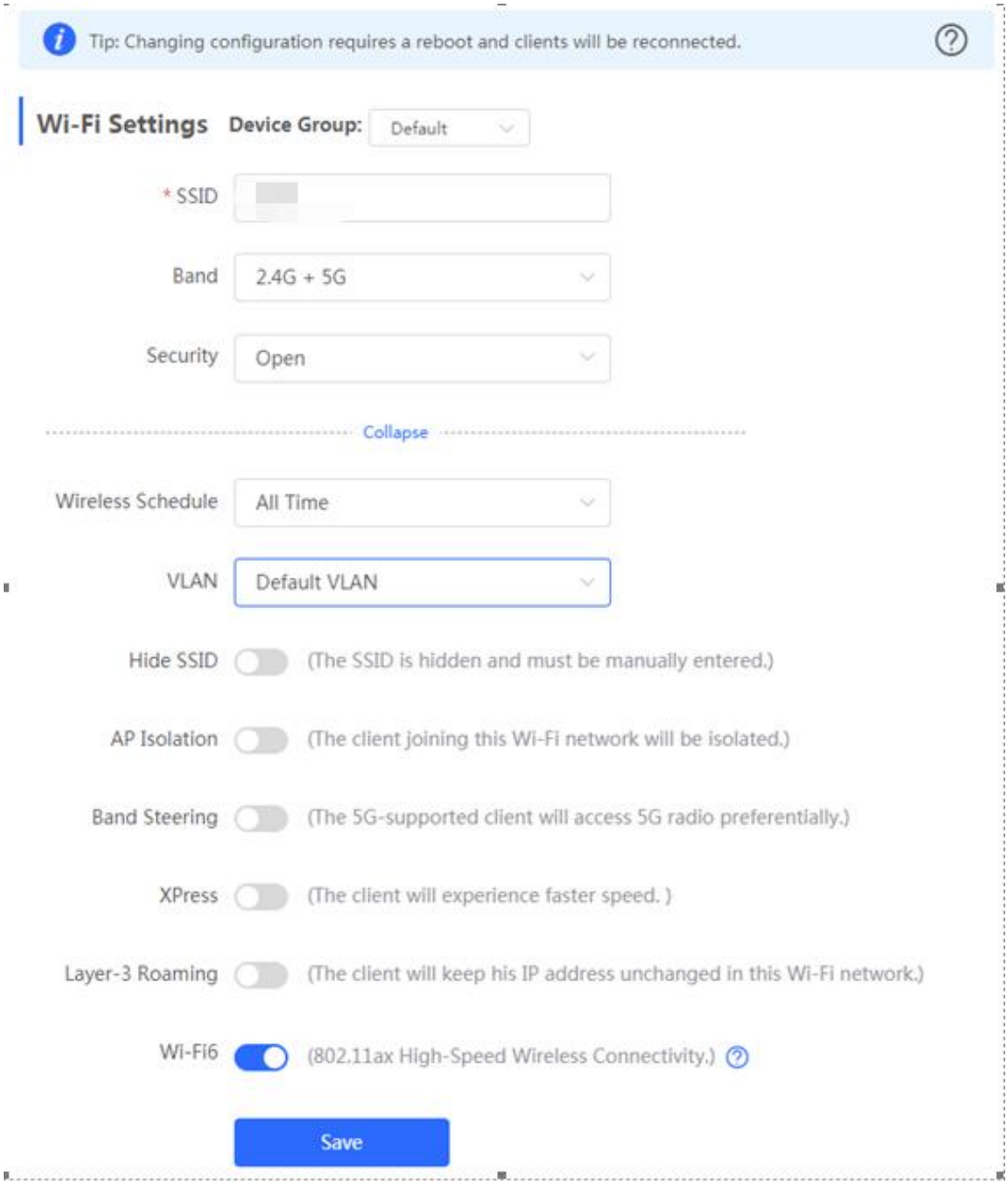
3.3 WiFi

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

3.3.1 WiFi Settings

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

Figure 3-3-1 WiFi Settings



3.3.2 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 3-3-2 Guest WiFi

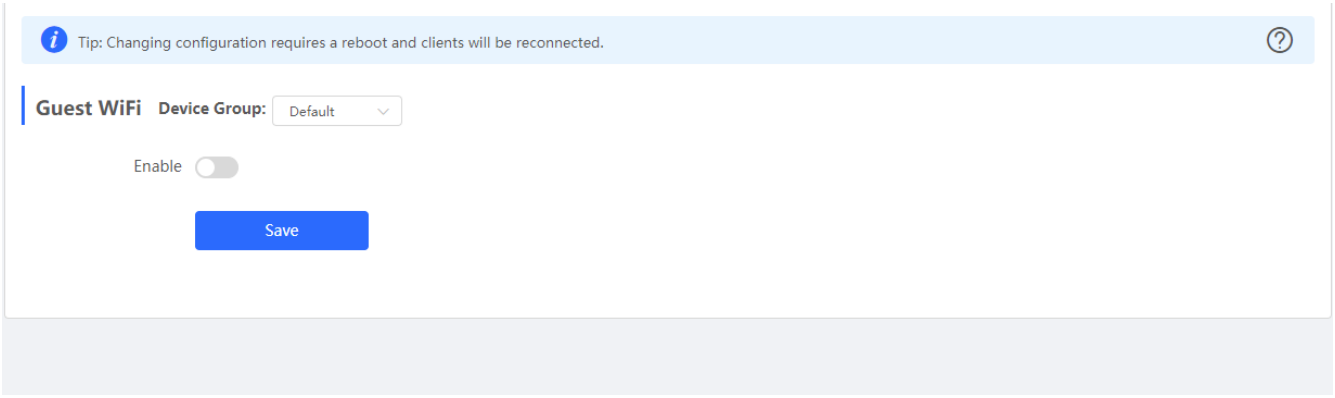
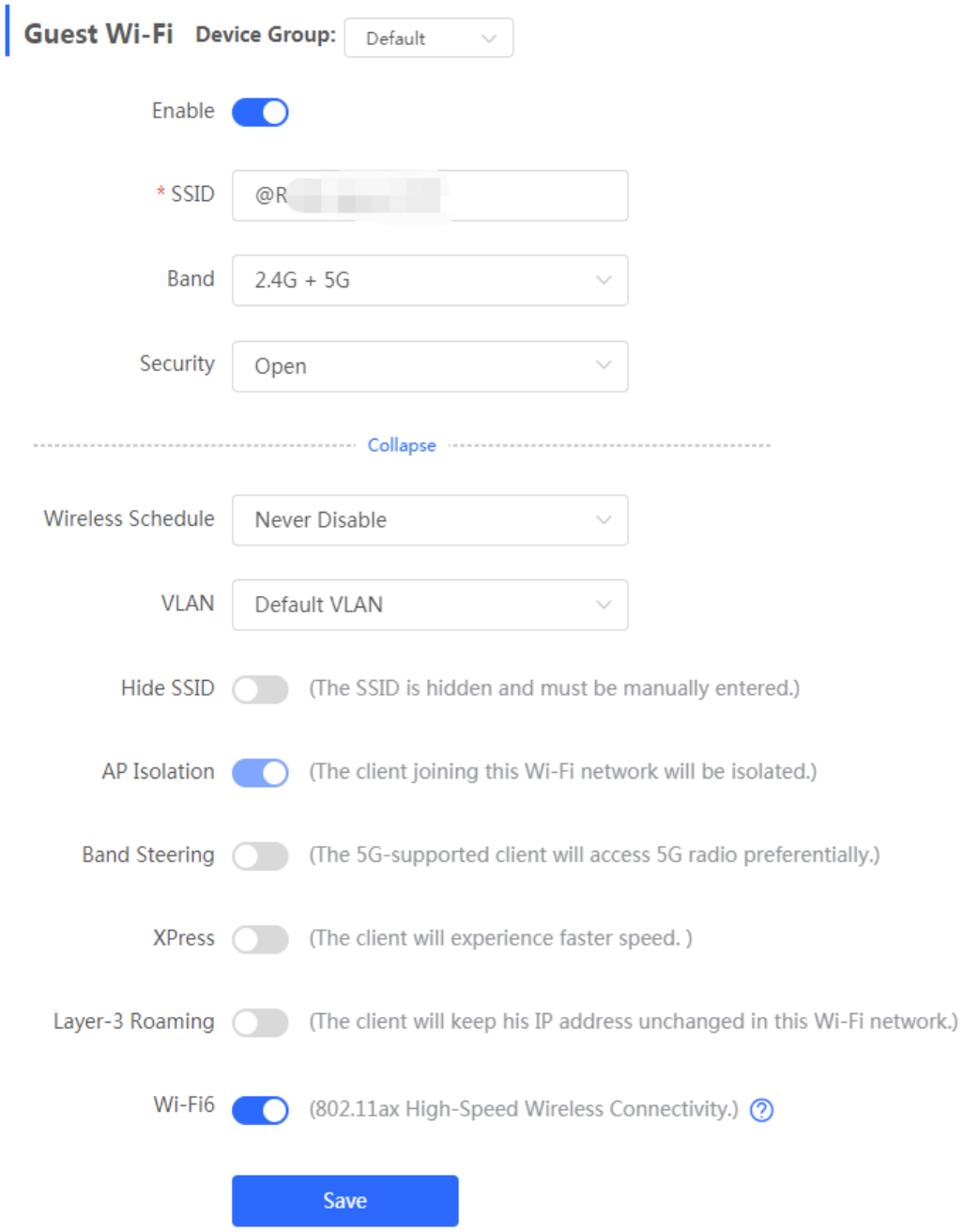


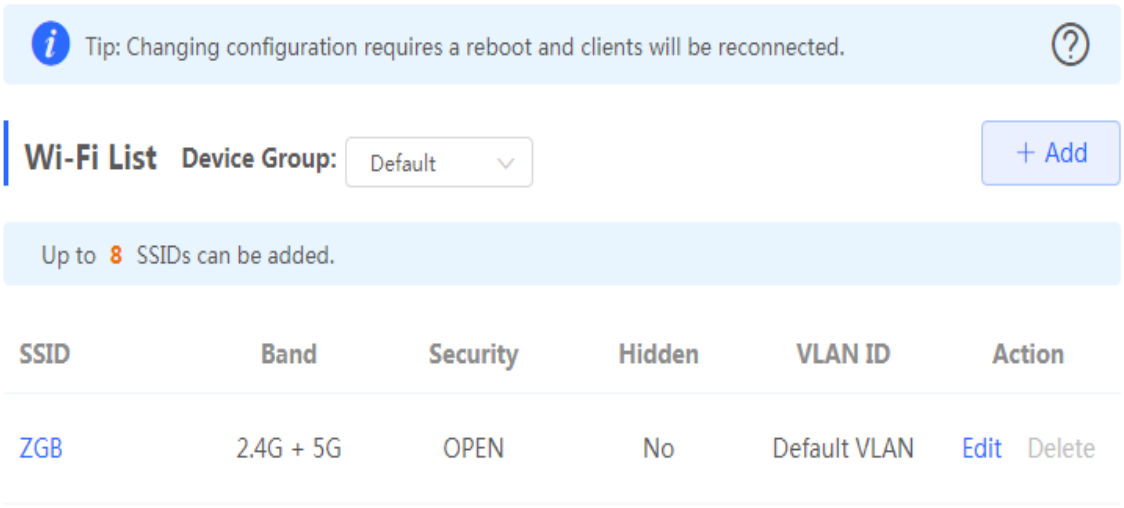
Figure 3-3-3 Enable Guest WiFi



3.3.3 WiFi List

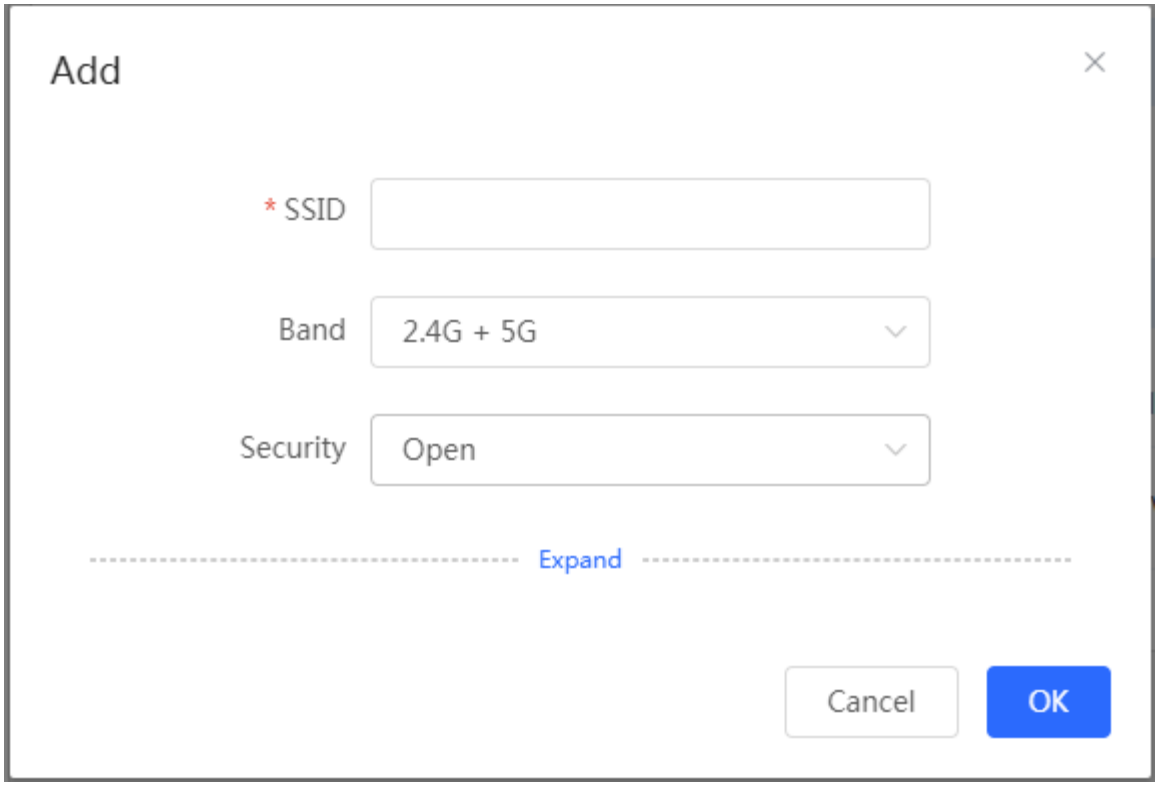
The **WiFi List** displays all WiFi networks. The primary WiFi is also listed here and cannot be deleted.

Figure 3-3-4 WiFi List



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

Figure 3-3-5 Add WiFi

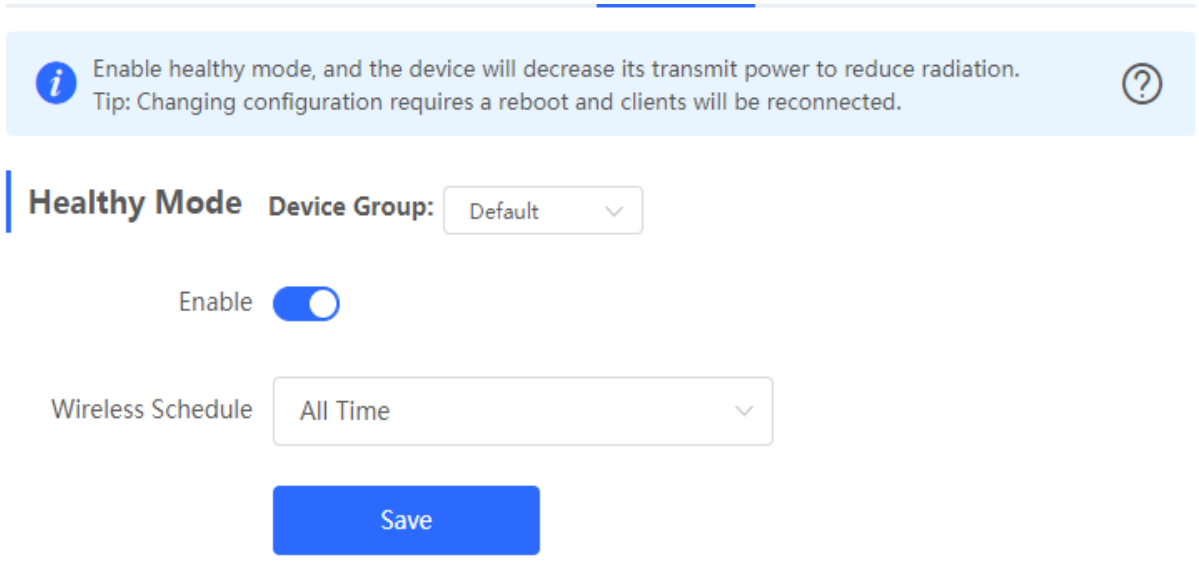


You can click in the upper right corner to see description about each configuration item.

3.3.4 Healthy Mode

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

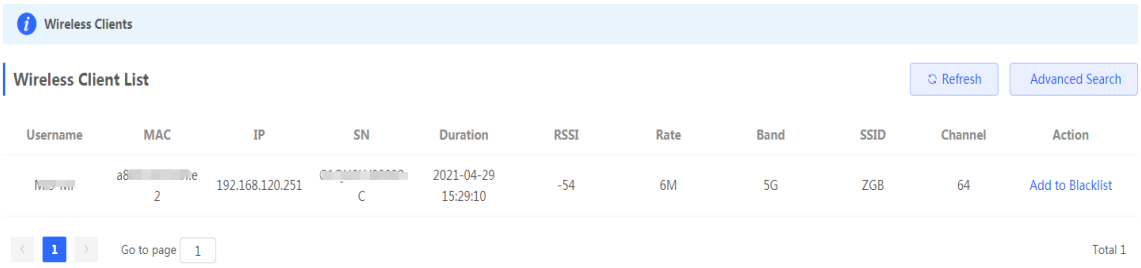
Figure 3-3-6 Healthy Mode



3.4 Wireless Clients

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

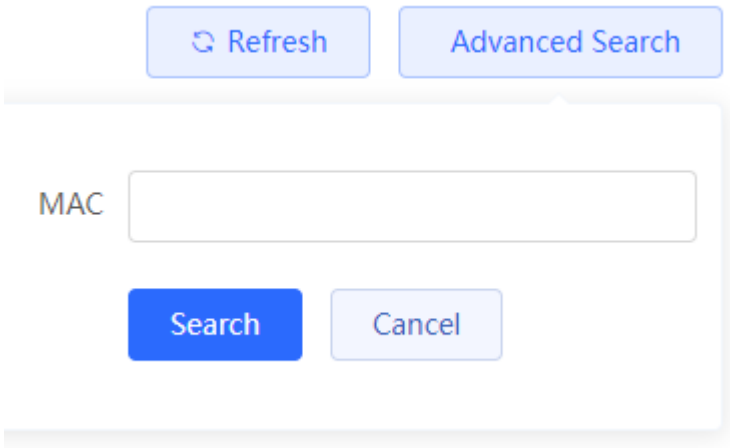
Figure 3-4-1 Wireless Client List



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 3-4-2 Advanced Search

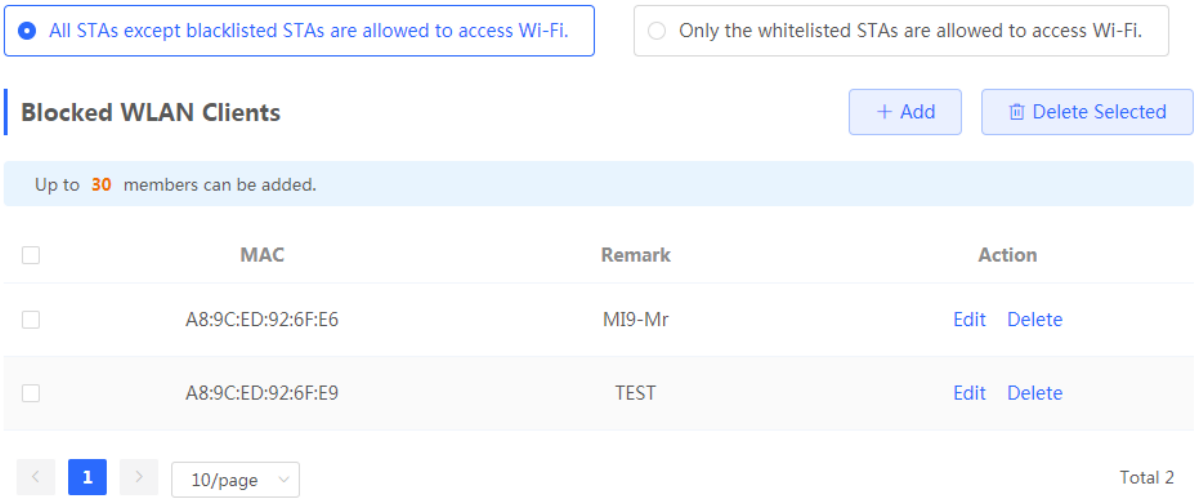


3.5 Blacklist/Whitelist

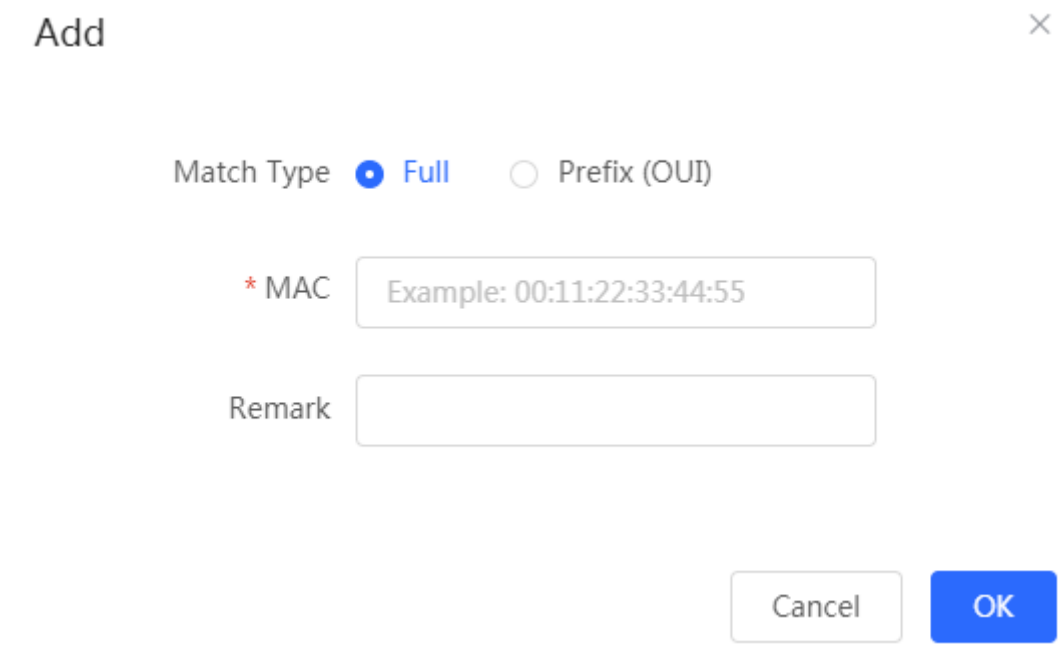
The **Blacklist/Whitelist** module allows you to configure wireless global or SSID-based client blacklist and whitelist. Blacklist and whitelist can achieve full match or prefix match (OUI).

3.5.1 Global Blacklist/Whitelist

Figure 3-5-1 Global Blacklist/Whitelist



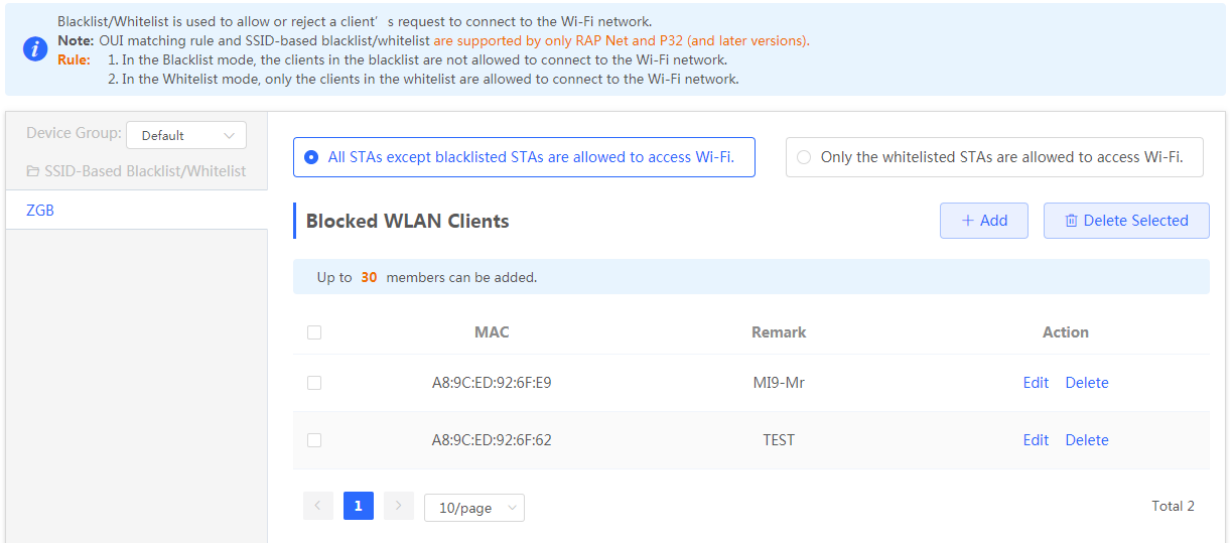
Click **Add** to add a blacklisted or whitelisted client. In the displayed dialog box, configure settings and click **OK**.



3.5.2 SSID-based Blacklist/Whitelist

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

Figure 3-5-2 SSID-based Blacklist/Whitelist



3.6 Radio Frequency

The **Radio Frequency** module allows you to configure the RF parameters.

Figure 3-6-1 Radio Frequency Page without Wireless Function

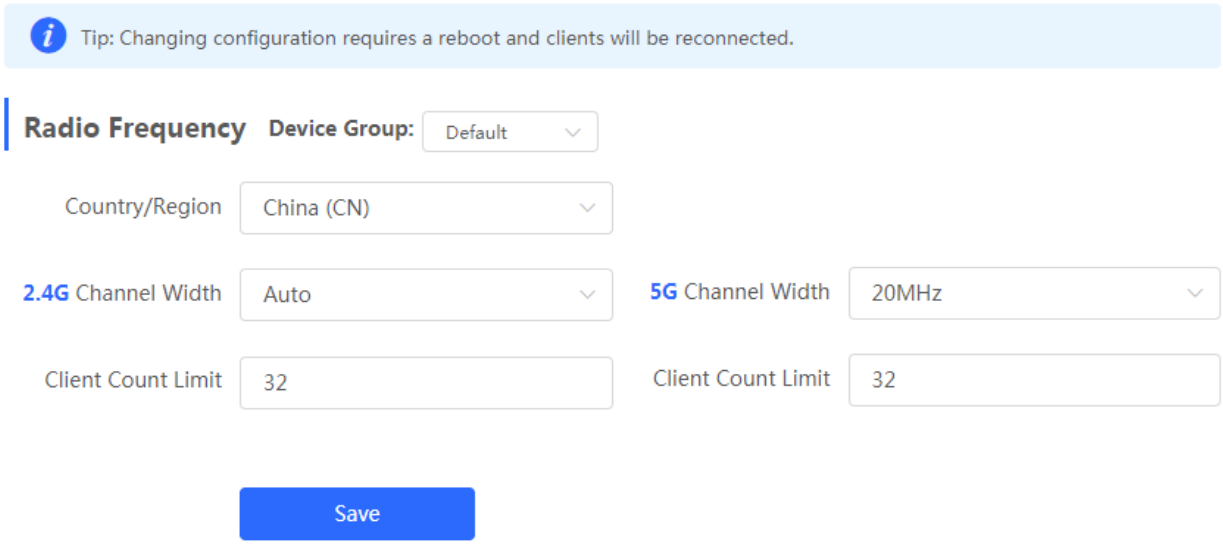
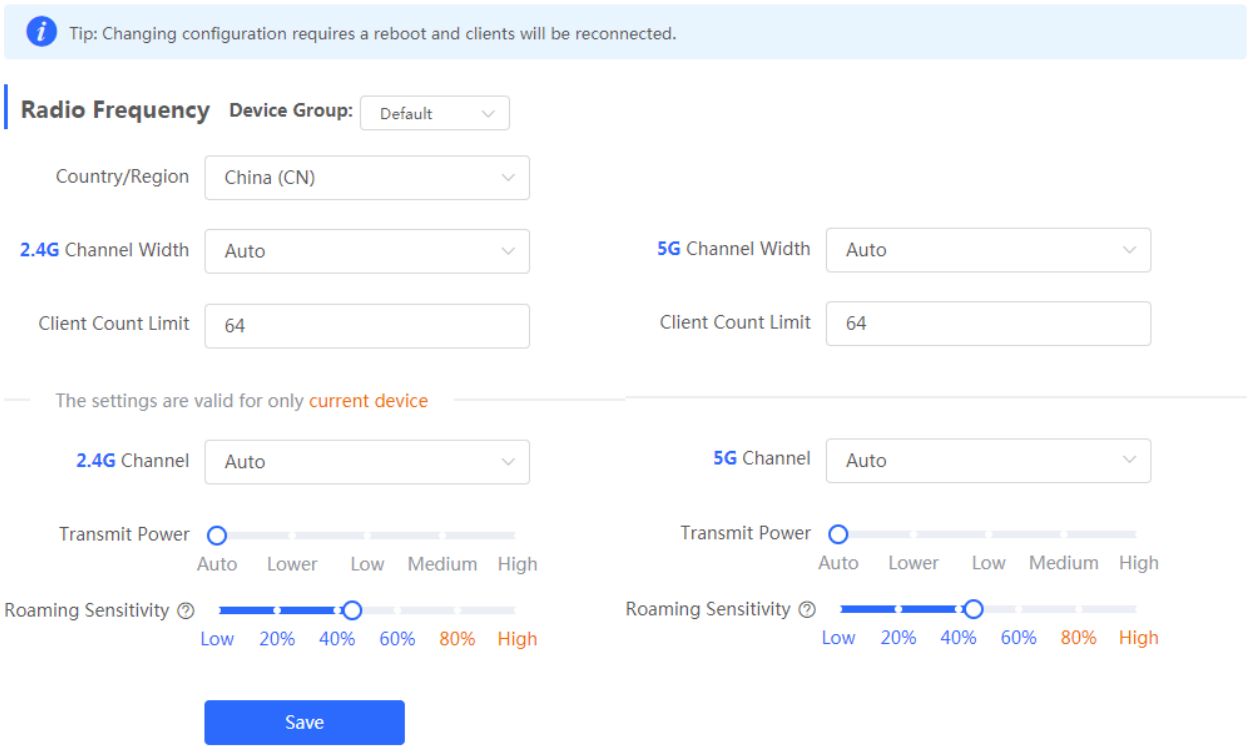


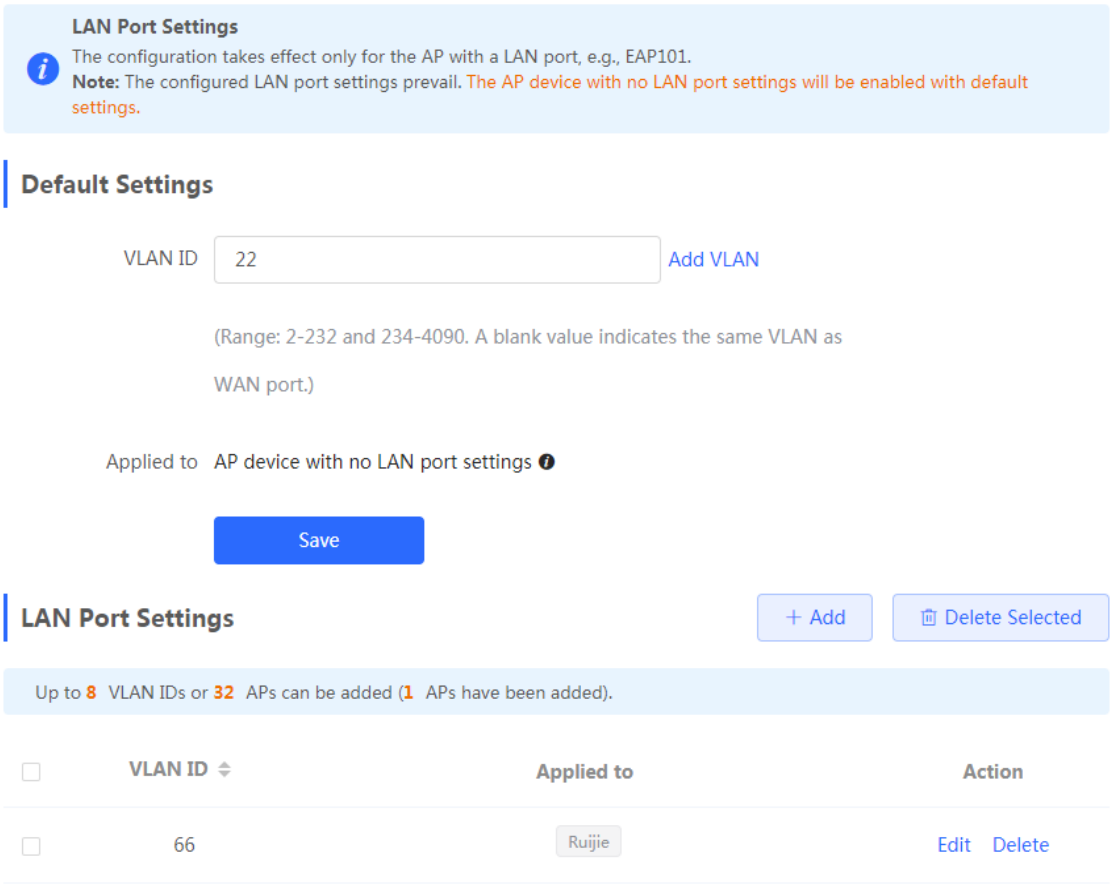
Figure 3-6-2 Radio Frequency Page with Wireless Function



3.7 LAN Ports

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

Figure 3-7-1 LAN Ports



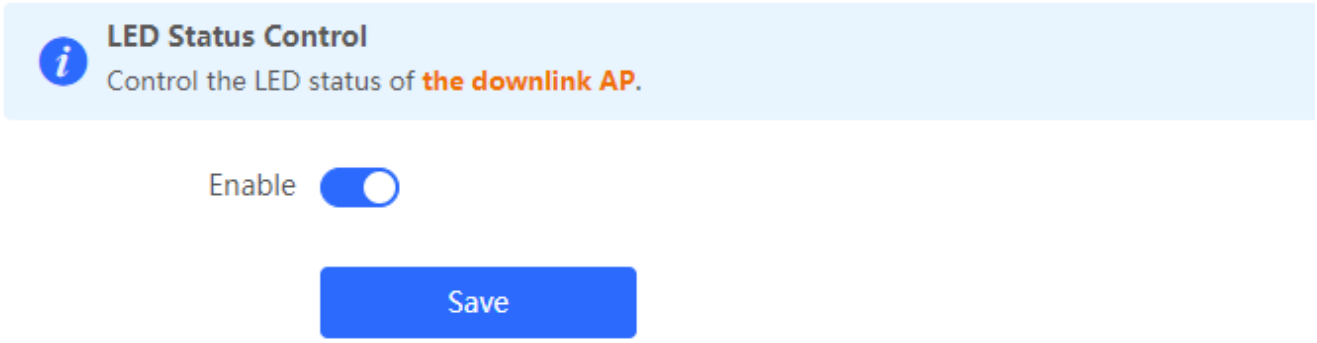
Click **Add** to add a LAN port. In the displayed dialog box, configure settings and click **OK**.

Figure 3-7-2 Add LAN Port

3.8 LED

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

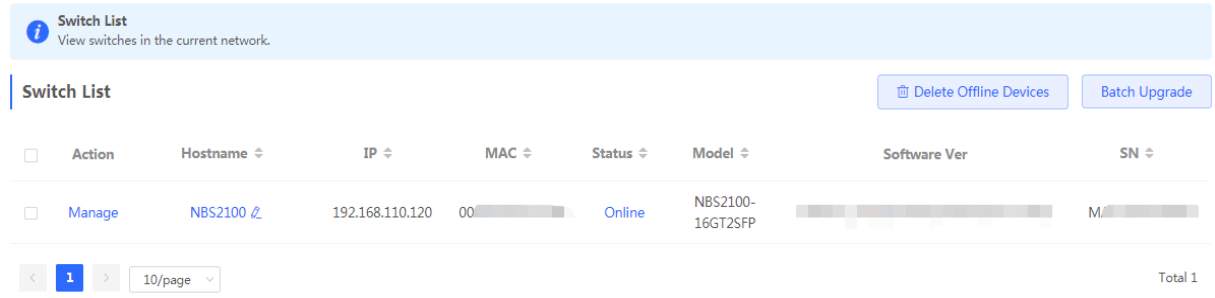
Figure 3-8-1 LED



3.9 Switches

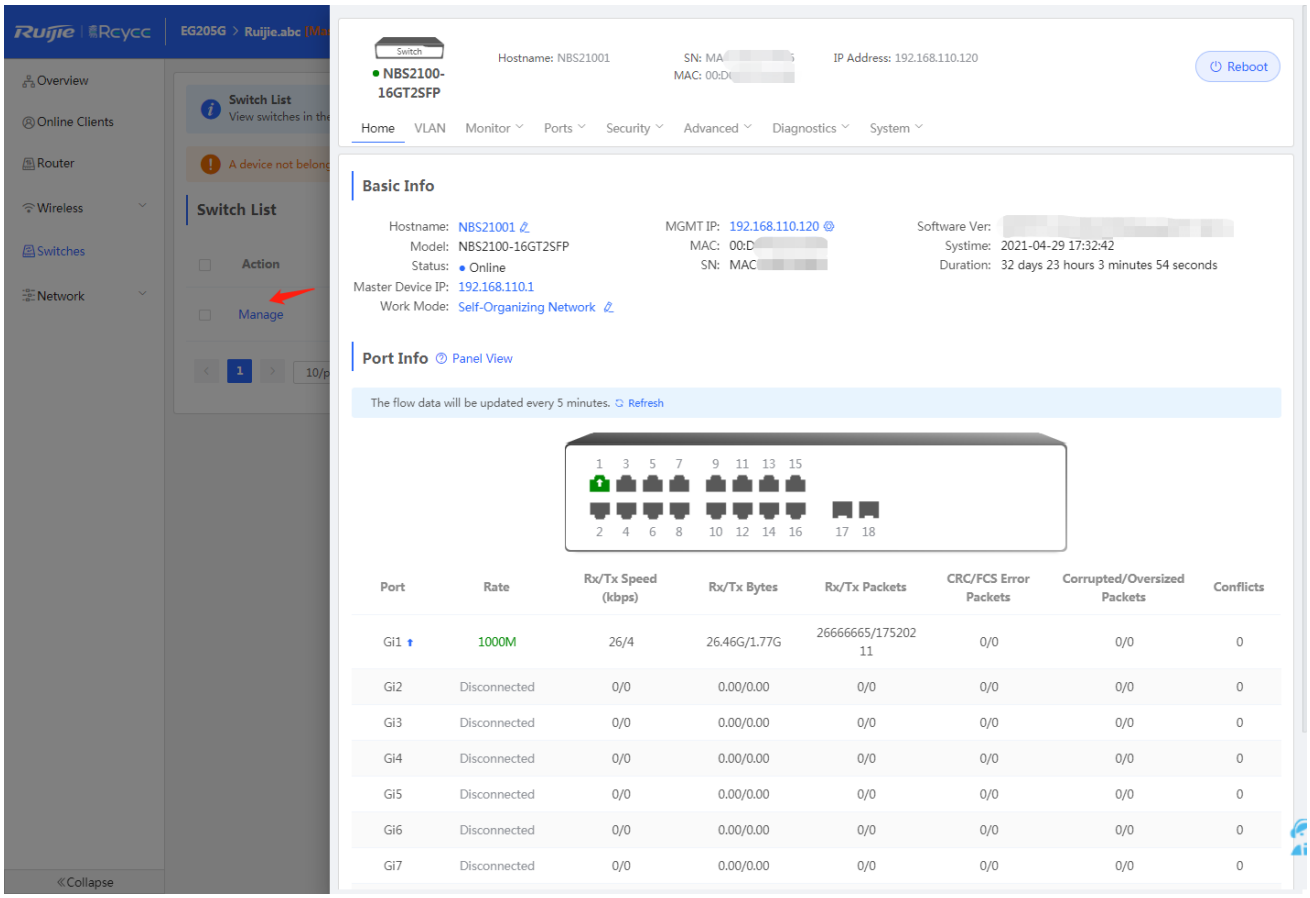
The **Switches** page displays all switches in the current network.

Figure 3-9-1 Switch List



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

Figure 3-9-2 Switch Management



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

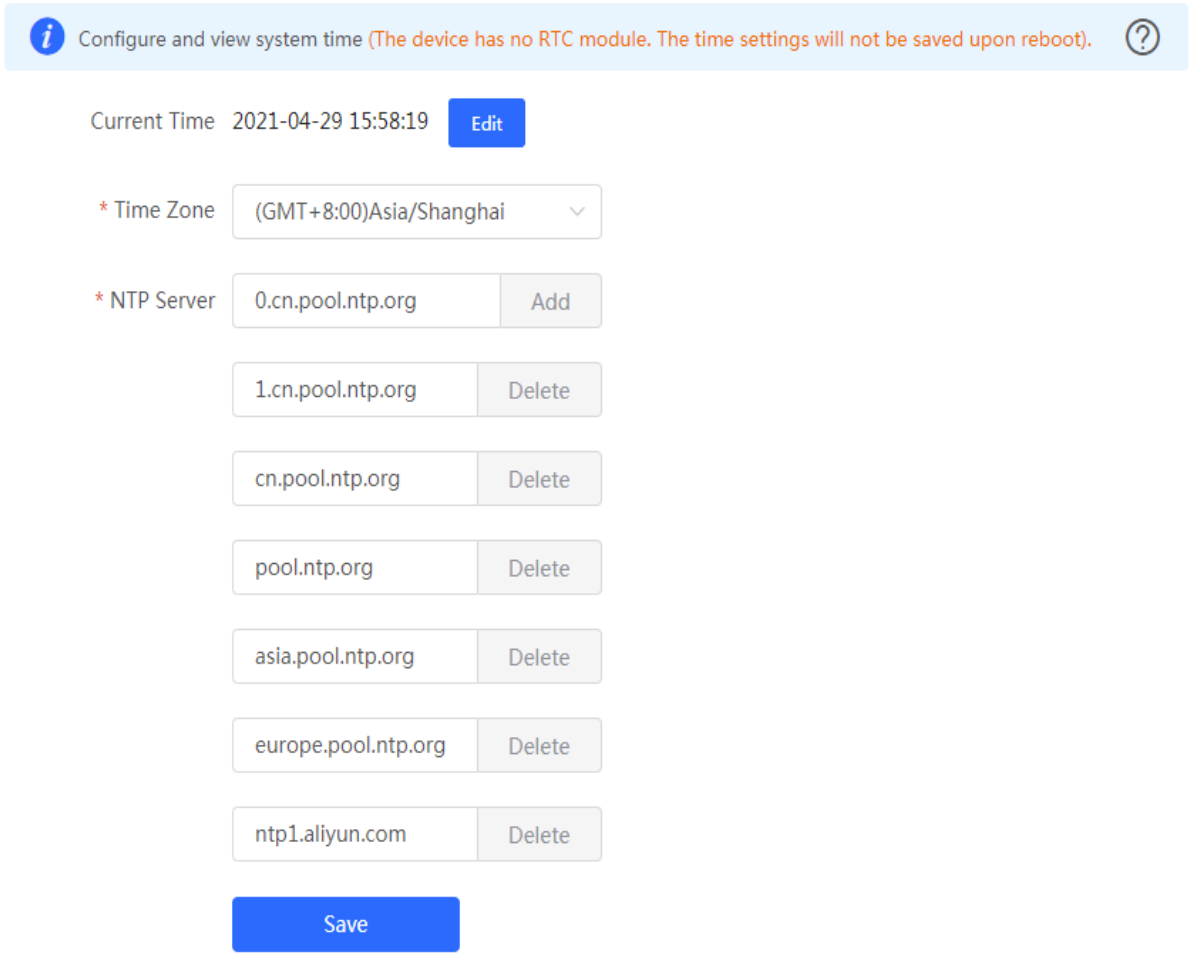
3.10 System

3.10.1 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 3-10-1 System Time



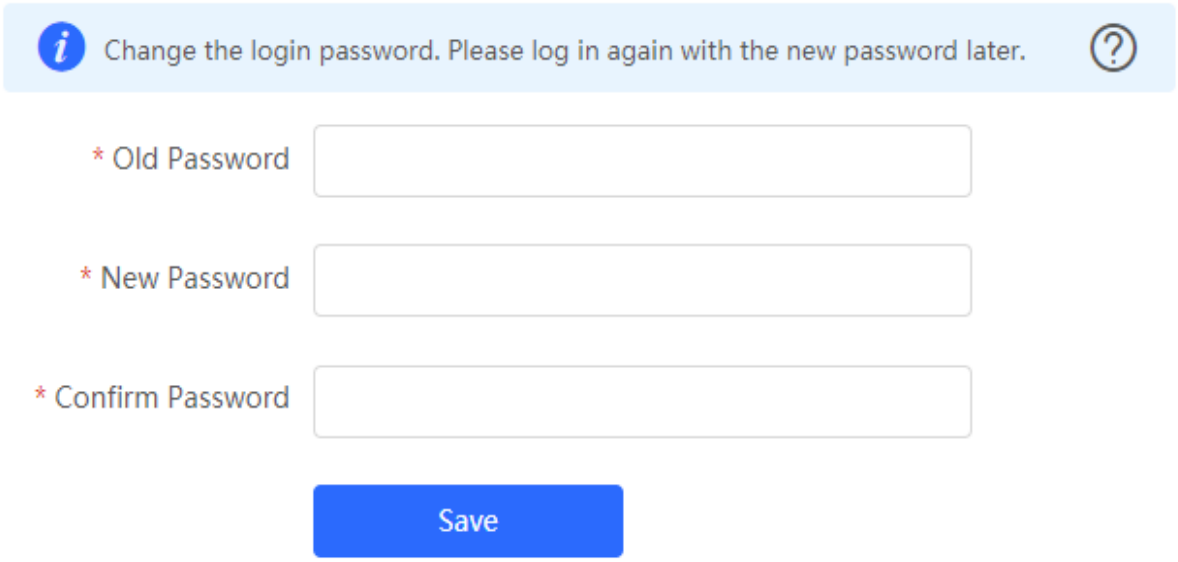
Click **Edit** to modify the system time.

Figure 3-10-2 Edit Time

3.10.2 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.

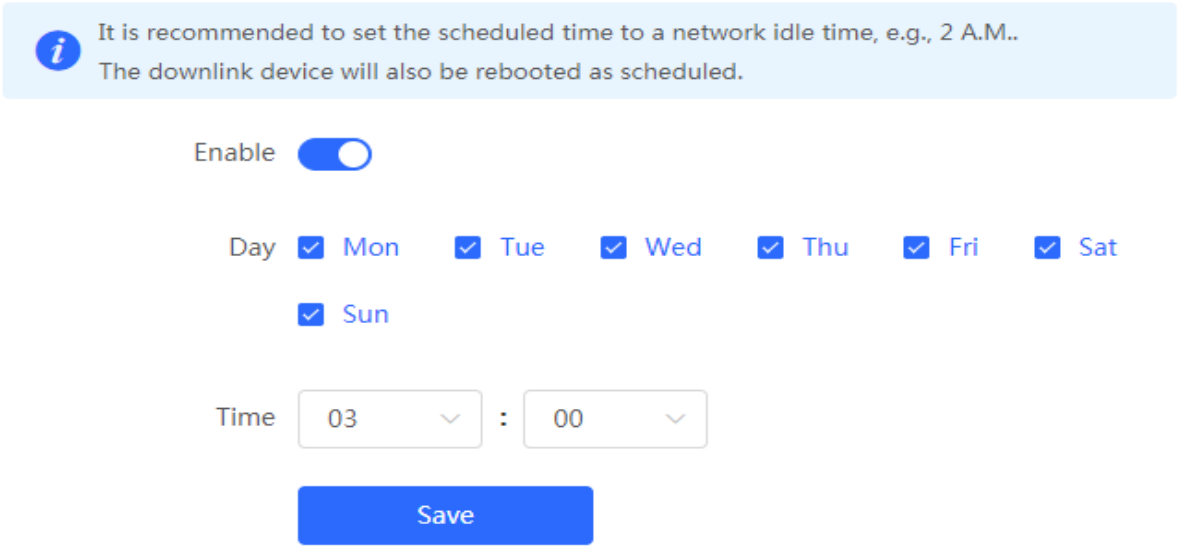
Figure 3-10-3 Device Password



3.10.3 Scheduled Reboot

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

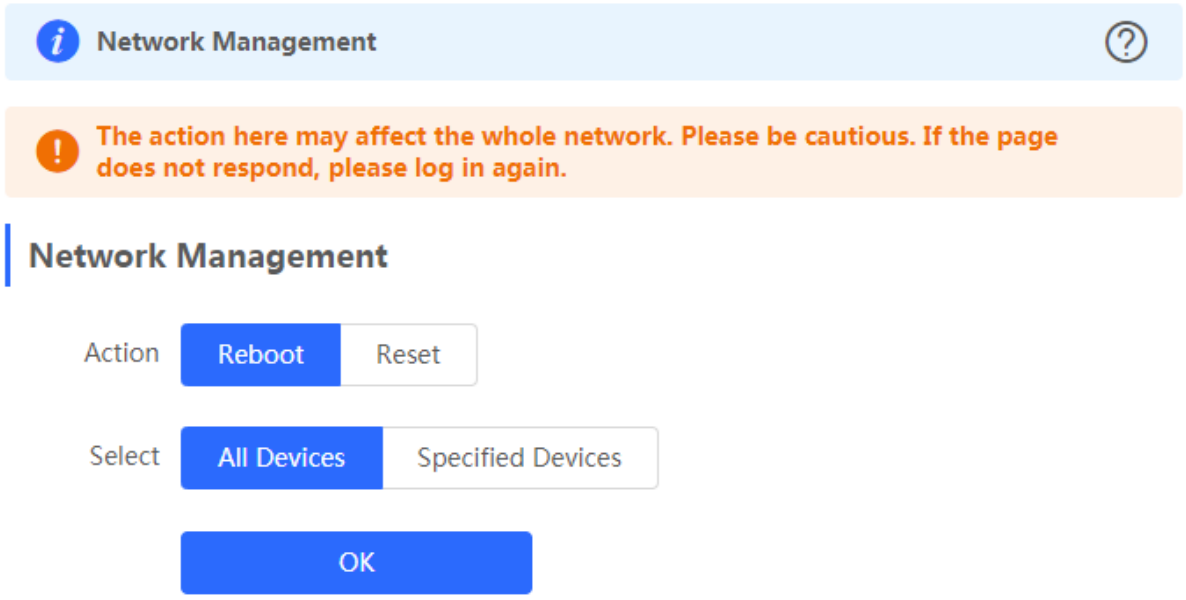
Figure 3-10-4 Scheduled Reboot



3.10.4 Reboot & Reset

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

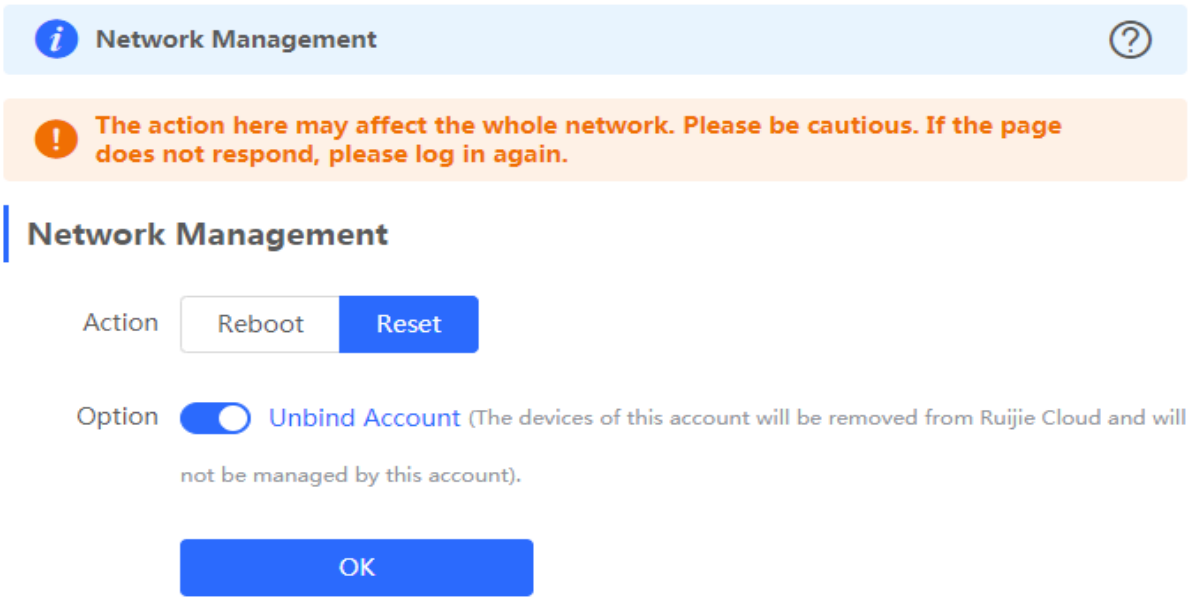
Figure 3-10-5 Reboot



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

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 3-10-6 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 Ruijie Cloud and will not be managed by this account).
OK

3 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 192.168.120.1 and the subnet mask is 255.255.255.0, set the IP address of the PC to 192.168.120.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. The device automatically restores the factory settings. After the restoration, the default factory IP address is 192.168.120.1. You can access the eWeb management system of the factory device without password.