Ruijie Reyee RG-RAP Series Access Points ReyeeOS 1.249

Web-based Configuration Guide

Document Version: V1.0
Date: 2023-06-26

Copyright

Disclaimer

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

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

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

Preface

Intended Audience

This document is intended for:

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

Technical Support

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

Conventions

1. GUI Symbols

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

2. Signs

The signs used in this document are described as follows:

Warning

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

Caution

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

Note

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

Specification

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

3. Note

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

Contents

Preface I

1 Fast Internet Access 1

1.1 Configuration Environment Requirements 1

1.1.1 PC 1

1.2 Default Configuration 1

1.3 Login to Eweb 1

1.3.1 Connecting to the Access Point 1

1.3.2 Configuring the IP Address of the Management Client 2

1.3.3 Logging in to the Web Page 2

1.4 Work Mode 3

1.4.1 AP Mode 3

1.4.2 Router Mode 3

1.4.3 Wireless Repeater Mode 3

1.5 Configuration Wizard (Router Mode) 4

1.5.1 Getting Started 4

1.5.2 Configuration Steps 5

1.6 Configuration Wizard (AP Mode) 7

1.6.1 Getting Started 7

1.6.2 Configuration Steps 7

1.7 Configuration Wizard (Wireless Repeater Mode) 8

1.7.1 Getting Started 8

1.7.2 Configuration Steps 8

1.8 Introduction to the Eweb GUI 10

1.8.1 Single Management Webpage 10
1.8.2 Dual Management Webpages 12
2 Network Monitoring 15
2.1 Viewing the Network Information 15
2.2 Adding Network Devices 17
2.2.1 Wired Connection 17
2.2.2 AP Mesh 19
2.3 Managing Network Devices 28
2.4 Configuring Network Planning 30
2.4.1 Configuring Wired VLAN 30
2.4.2 Configuring Wi-Fi VLAN 32
2.5 Troubleshooting Fault Alerts 34
3 Wi-Fi Network Settings 36
3.1 Configuring AP Groups 36
3.1.1 Overview 36
3.1.2 Procedures 36
3.2 Configuring SSID and Wi-Fi Password 38
3.3 Hiding the SSID 39
3.3.1 Overview 39
3.3.2 Configuration Steps 39
3.4 Checking Wireless Clients 40
3.5 Configuring Wi-Fi Band 42
3.6 Configuring Band Steering 42
3.7 Configuring Wi-Fi 6 43

3.8 Configuring Layer-3 Roaming....44
3.9 Configuring AP Isolation....45
3.10 Adding a Wi-Fi Network....46
3.11 Configuring a Guest Wi-Fi....47
3.11.1 Overview....47
3.11.2 Configuration Steps....47
3.12 Configuring Wi-Fi Blacklist or Whitelist....48
3.12.1 Overview....48
3.12.2 Configuration Steps....48
3.13 Optimizing Wi-Fi Network....50
3.13.1 Overview....50
3.13.2 Getting Started....50
3.13.3 Optimizing the Radio Channel....51
3.13.4 Optimizing the Channel Width....52
3.13.5 Optimizing the Transmit Power....53
3.13.6 Configuring the Kick-off Threshold....54
3.13.7 Configuring the Client Limit....55
3.13.8 Configuring the Roaming Sensitivity....55
3.13.9 Configuring WIO....56
3.13.10 Configuring Wi-Fi Roaming Optimization (802.11k/v)....57
3.14 Configuring Healthy Mode....58
3.15 Configuring XPress....59
3.16 Configuring Wireless Schedule....60
3.17 Enabling Reyee Mesh....61

3.18 Configuring AP Load Balancing 61
3.18.1 Overview 61
3.18.2 Configuring Client Load Balancing 62
3.18.3 Configuring Traffic Load Balancing 63
4 Network Settings 65
4.1 Switching Work Mode 65
4.1.1 Work Mode 65
4.1.2 Self-Organizing Network Discovery 65
4.1.3 Configuration Steps 65
4.1.4 Viewing Device Role 67
4.2 Configuring Internet Type 67
4.3 Configuring LAN Port 68
4.4 Configuring Repeater Mode 69
4.4.1 Wired Repeater 69
4.4.2 Wireless Repeater 70
4.5 Creating a VLAN 72
4.6 Configuring Port VLAN 74
4.7 Changing MAC Address 76
4.8 Changing MTU 77
4.9 Configuring DHCP Server 77
4.9.1 DHCP Server 77
4.9.2 Configuring the DHCP Server Function 77
4.9.3 Displaying Online DHCP Clients 79
4.9.4 Displaying the DHCP Static IP Address List 79

4.10 Link Aggregation 80
4.11 Configuring DNS 80
4.12 Hardware Acceleration 81
4.13 Configuring Port Flow Control 81
4.14 Configuring ARP Binding 82
4.15 Configuring LAN Ports 83
5 System Settings 85
5.1 PoE 85
5.2 PoE Settings 85
5.3 Setting the Login Password 86
5.4 Setting the Session Timeout Duration 87
5.5 Setting and Displaying System Time 87
5.6 Configuring Reboot 89
5.6.1 Rebooting the Current Device 89
5.6.2 Rebooting All Devices in the Network 89
5.6.3 Rebooting the Specified Device 90
5.7 Configuring Scheduled Reboot 91
5.7.1 Configuring Scheduled Reboot for the Current Device 91
5.8 Configuring Backup and Import 92
5.9 Restoring Factory Settings 93
5.9.1 Restoring the Current Device to Factory Settings 93
5.9.2 Restoring All Devices to Factory Settings 94
5.10 Performing Upgrade and Checking System Version 94
5.10.1 Online Upgrade 94

5.10.2 Local Upgrade 95
5.11 Switching System Language 95
5.12 Configuring LED Status Control 96
6 Network Diagnosis Tools 97
6.1 Network Check 97
6.2 Network Tools 98
6.3 Alarms 99
6.4 Fault Collection 100
7 FAQs 102
7.1 Login Failure 102
7.2 Factory Setting Restoration 102
7.3 Password Loss 102

1 Fast Internet Access

1.1 Configuration Environment Requirements

1.1.1 PC

- Browser: Google Chrome, Internet Explorer 9.0, 10.0, and 11.0, and some Chromium/Internet Explorer kernel-based browsers (such as 360 Extreme Explorer) are supported. Exceptions such as garble or format error may occur if an unsupported browser is used.
- Resolution: 1024 x 768 or a higher resolution is recommended. If other resolutions are used, the page fonts and formats may not be aligned, the GUI is less artistic, or other exceptions may occur.

1.2 Default Configuration

Table 1-1 Default Web Configuration

Item	Default
IP address	10.44.77.254
Username/Password	A username is not required when you log in for the first time. The default password is **admin**.

1.3 Login to Eweb

1.3.1 Connecting to the Access Point

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

- Wired Connection

Connect a local area network (LAN) port of the access point to the network port of the PC, and set the IP address of the PC. See Configuring the IP Address of the Management Client.

- Wireless Connection

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

1.3.2 Configuring the IP Address of the Management Client

Configure an IP address for the management client in the same network segment as the default IP address of the device (The default device IP address is 10.44.77.254, and the subnet mask is 255.255.255.0.) so that the management client can access the device. For example, set the IP address of the management client to 10.44.77.100.

Caution

- Make sure that the client can access the Eweb system as long as it can ping the access point.
- The IP address of the management client cannot be set to 10.44.77.253, because this IP address is reserved by the device. If the management client uses this IP address, it cannot access the device.

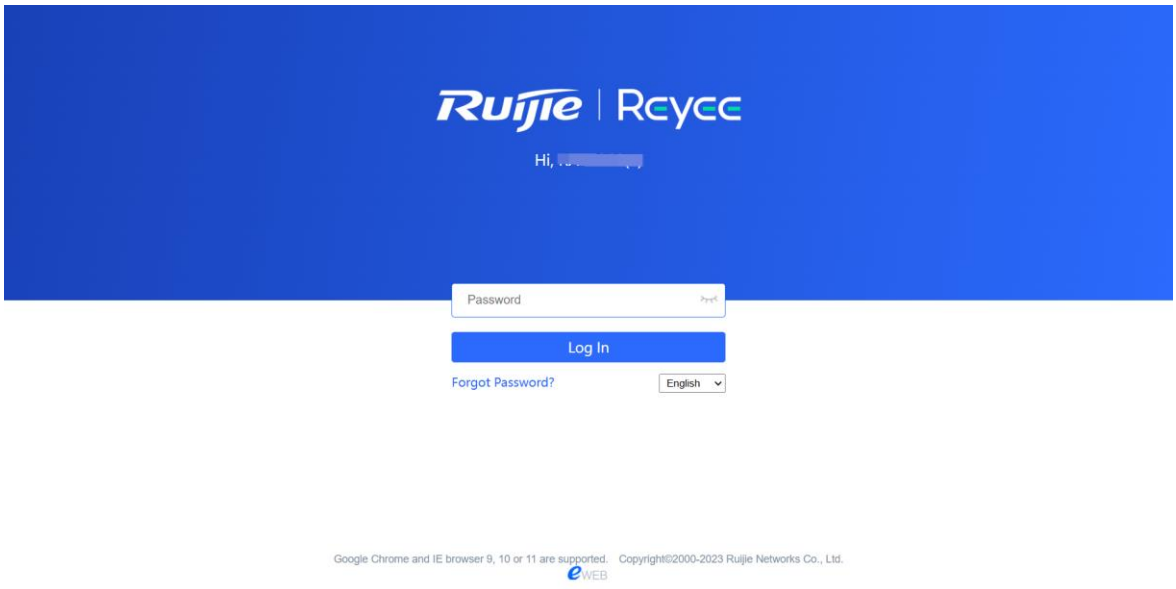
1.3.3 Logging in to the Web Page

(1) Enter the IP address (10.44.77.254 by default) of the access point in the address bar of the browser to open the login page.

Note

If the static IP address of the device is changed, or the device obtains a new dynamic IP address, the new IP address can be used to access the web management system of the device as long as the management client and the device are in the same network segment of a LAN.

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



You can use the default password **admin** to log in to the device for the first time. For security purposes, you are advised to change the default password as soon as possible after logging in, and to regularly update your password thereafter.

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

Caution

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

1.4 Work Mode

The device can work in the router mode, AP mode or wireless repeater mode. The displayed system menu page and function ranges vary with the work mode. The RAP works in the AP mode by default. If you want to switch the work mode, see Switching Work Mode.

1.4.1 AP Mode

The device performs L2 forwarding and does not support the DHCP address pool function. In AP mode, the device often networks with devices supporting the routing function. IP addresses of downlink wireless clients are assigned and managed by the uplink device (supporting the DHCP address pool) of the AP in a unified manner, and the AP only transparently transmits data.

1.4.2 Router Mode

The device supports NAT routing and forwarding. The addresses of wireless clients can be assigned by the AP and wireless network data is routed and forwarded by the AP. NAT is supported in this mode. When an AP works in the router mode, it supports device networking, network-wide configuration, and AP-specific radio functions.

There are three Internet types available: PPPoE, DHCP mode and static IP address mode. You can connect the device to an Ethernet cable or an upstream device.

Caution

After switching to the router mode, the device's LAN IP address will change to 192.168.120.1. Please obtain an IP address automatically for your management client and enter 10.44.77.254 into the address bar of the browser to log in to Eweb again.

1.4.3 Wireless Repeater Mode

The device does not support the routing and DHCP server functions in the wireless repeater mode. IP addresses of the clients are assigned and managed by the primary router. On an available network, the device can be connected to the primary router through wireless connection to expand the Wi-Fi coverage and increase the number of LAN ports and wireless access devices.

1.5 Configuration Wizard (Router Mode)

Upon first login, you can perform quick configuration procedures to configure the Internet type, Wi-Fi network and management password.

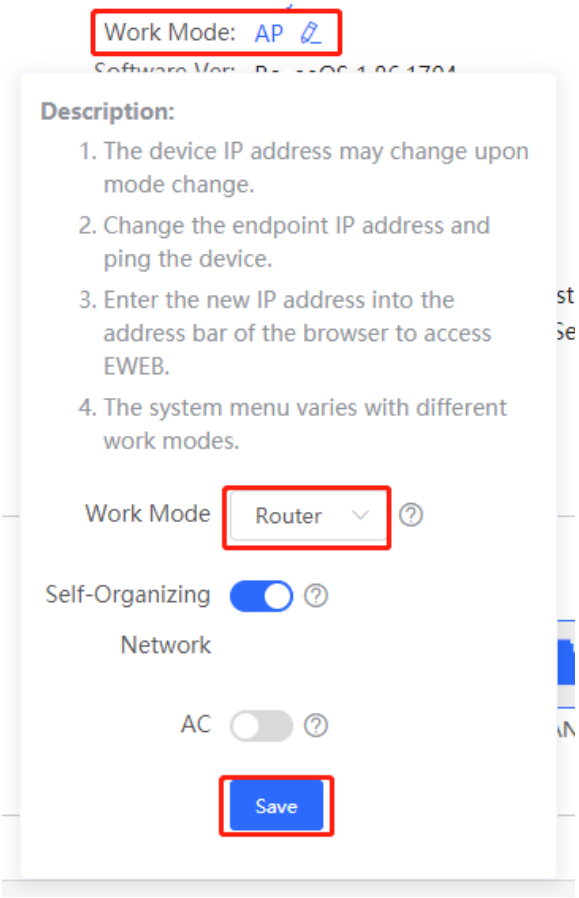
1.5.1 Getting Started

(1) Connect the device to a power supply and connect the port of the device to an upstream device with an Ethernet cable. Or you can connect an Ethernet cable to the device.

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

- Figure out whether the Internet connection type is PPPoE, DHCP mode, or static IP address mode.
- In the PPPoE mode, a username, a password, and possibly a service name are needed.
- In the static IP address mode, an IP address, a subnet mask, a gateway, and a DNS server need to be configured.

(3) The device works in the AP mode by default. If you want to switch the work mode to the router mode, perform the configuration on the work mode setting page. See Switching Work Mode for more details.



1.5.2 Configuration Steps

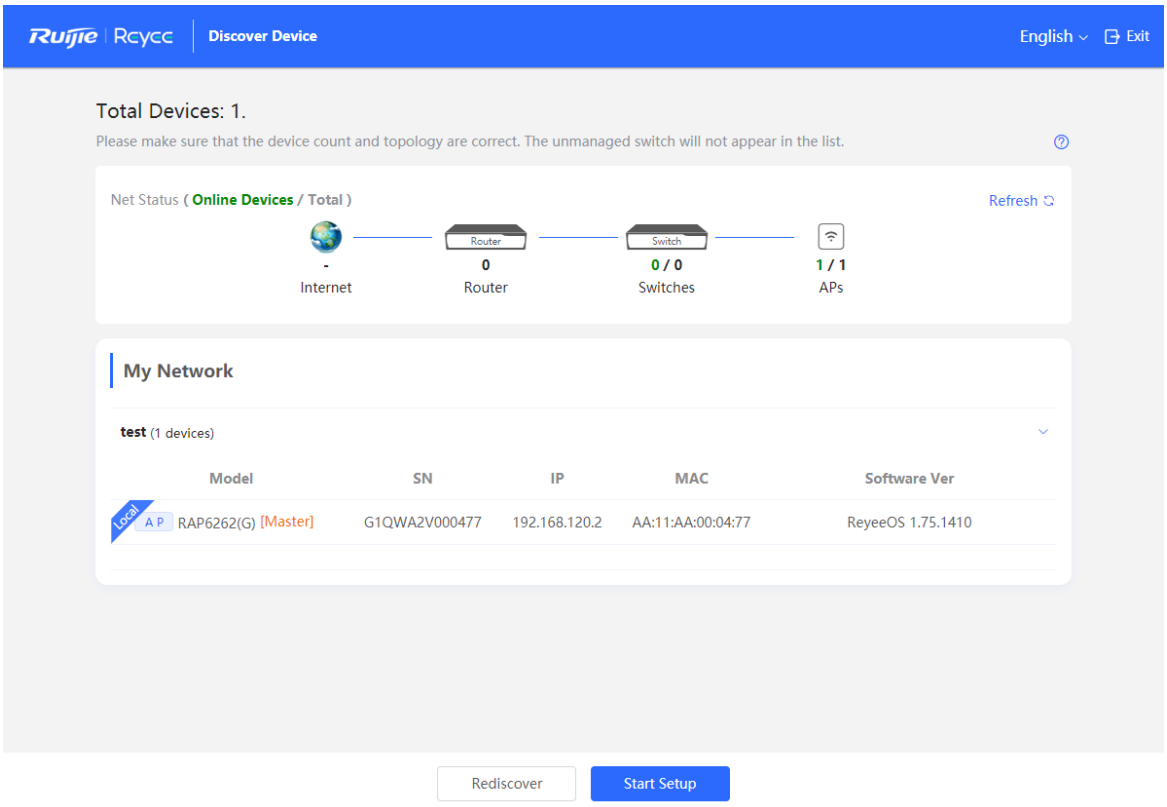
1. Add a Device to Network

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

Note

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

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



2. Creating a Network Project

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

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

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

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

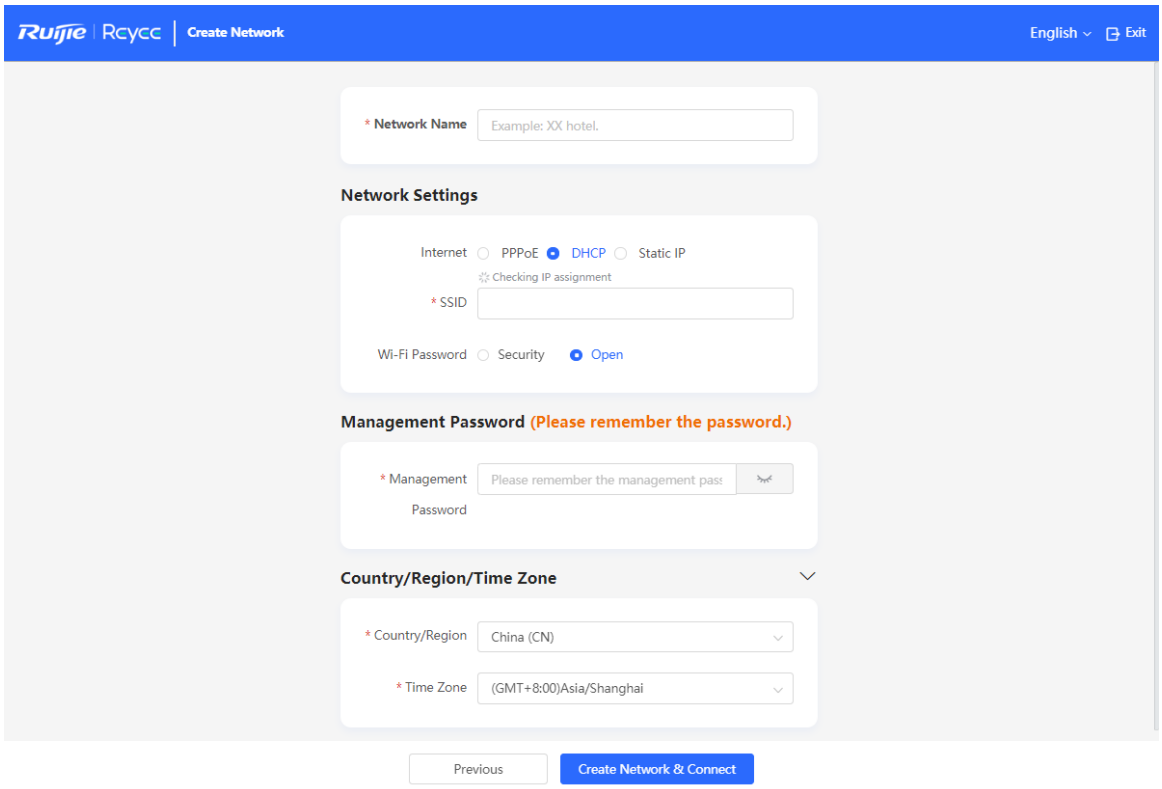
- **Static IP**: Enter the IP address, subnet mask, gateway, and DNS server, and click **Next**.

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

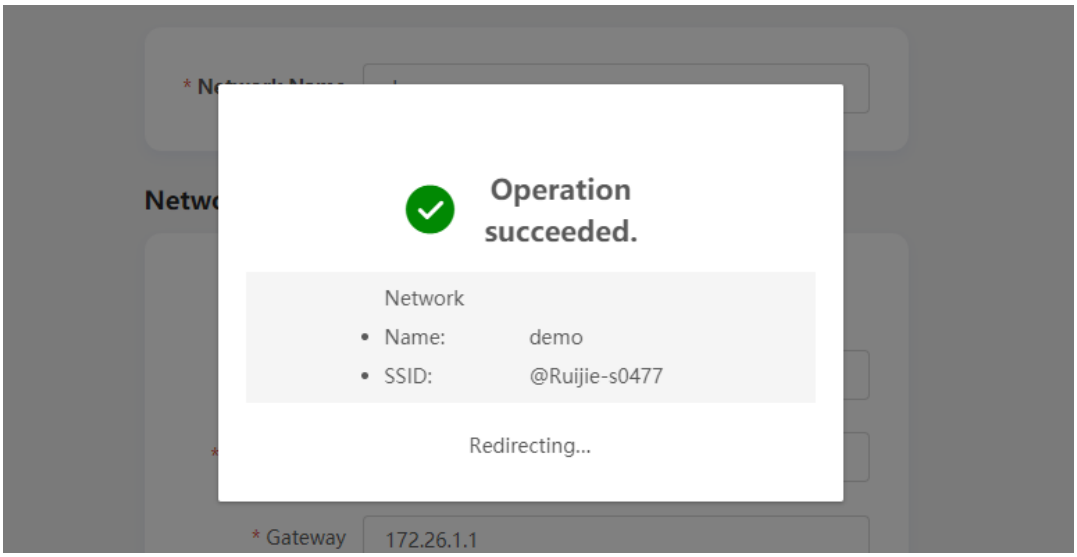
(4) **Management Password**: The password is used for logging in to the management page.

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

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



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



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

Note

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

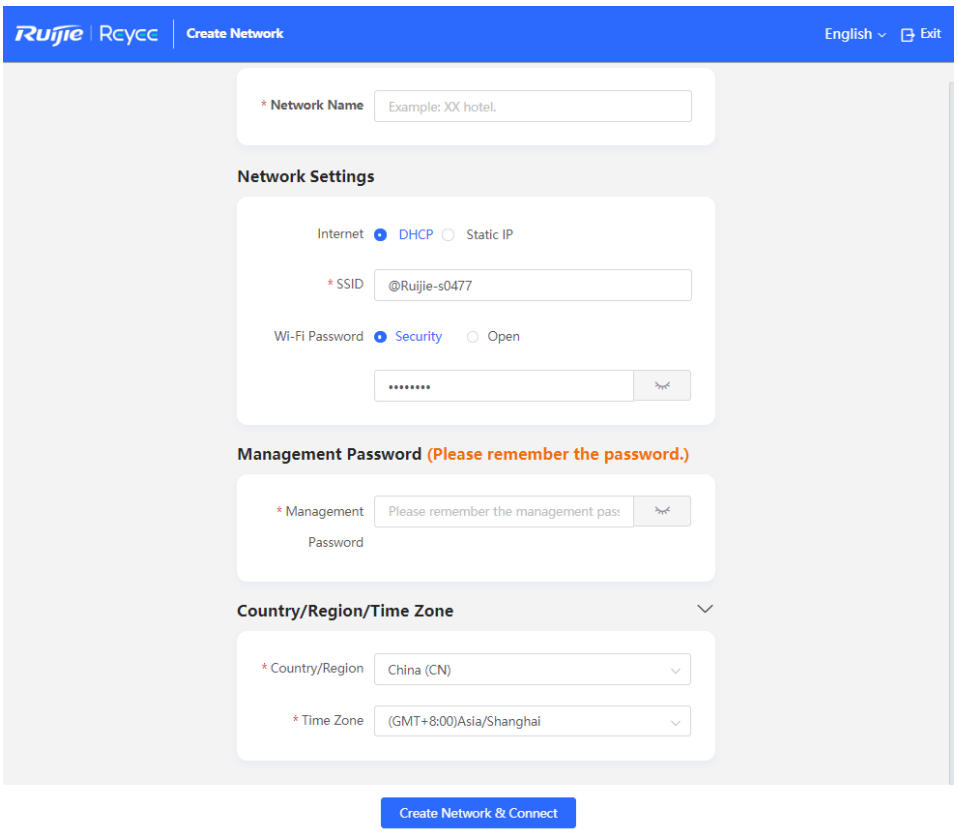
1.6 Configuration Wizard (AP Mode)

1.6.1 Getting Started

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

1.6.2 Configuration Steps

The device obtains the IP address through the DHCP by default. Configure the SSID, Wi-Fi password and management password. The default Internet connection type is DHCP mode. You are advised to use the default value.



1.7 Configuration Wizard (Wireless Repeater Mode)

1.7.1 Getting Started

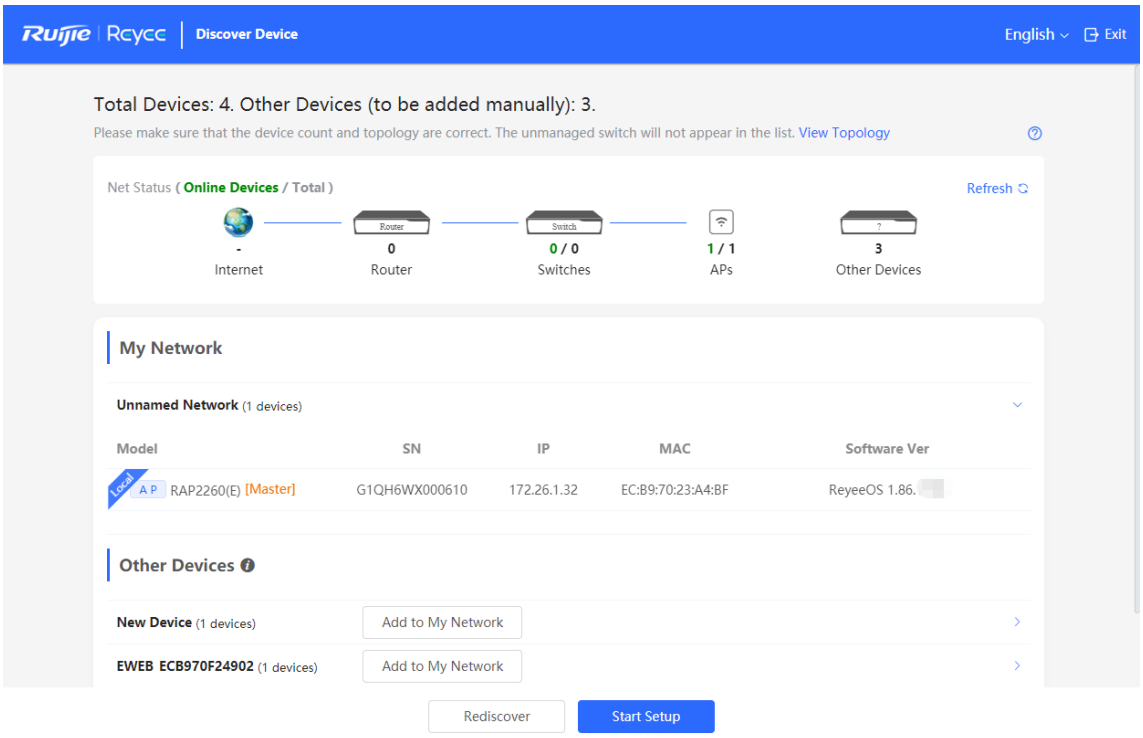
- Before configuring the wireless repeater mode, configure the primary router and test that the primary router can access the Internet.
- Place the device where it can discover at least two-bar Wi-Fi signal of the primary router.

Caution

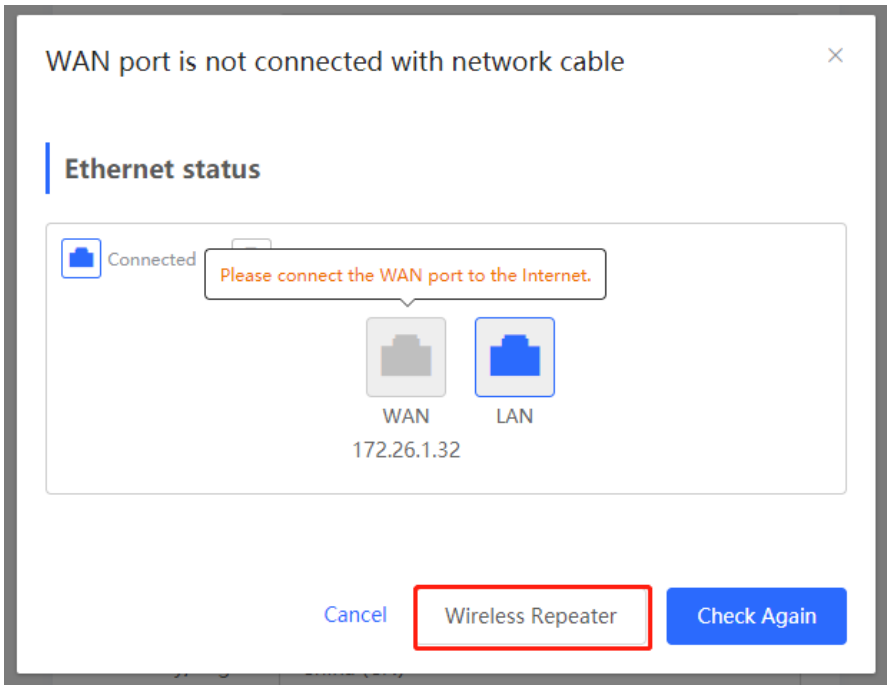
- No Ethernet cable is required in the wireless repeater mode. The wireless network stability can be affected by many factors. Therefore, the wired connection is recommended.

1.7.2 Configuration Steps

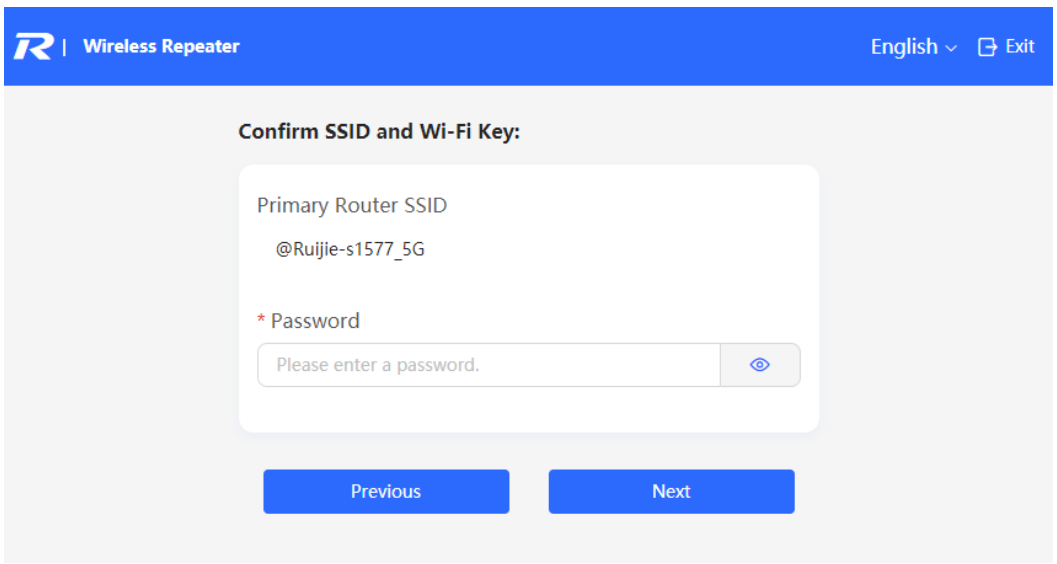
(1) Connect the device to a power supply without connecting an Ethernet cable to the uplink port, and click **Start Setup**.



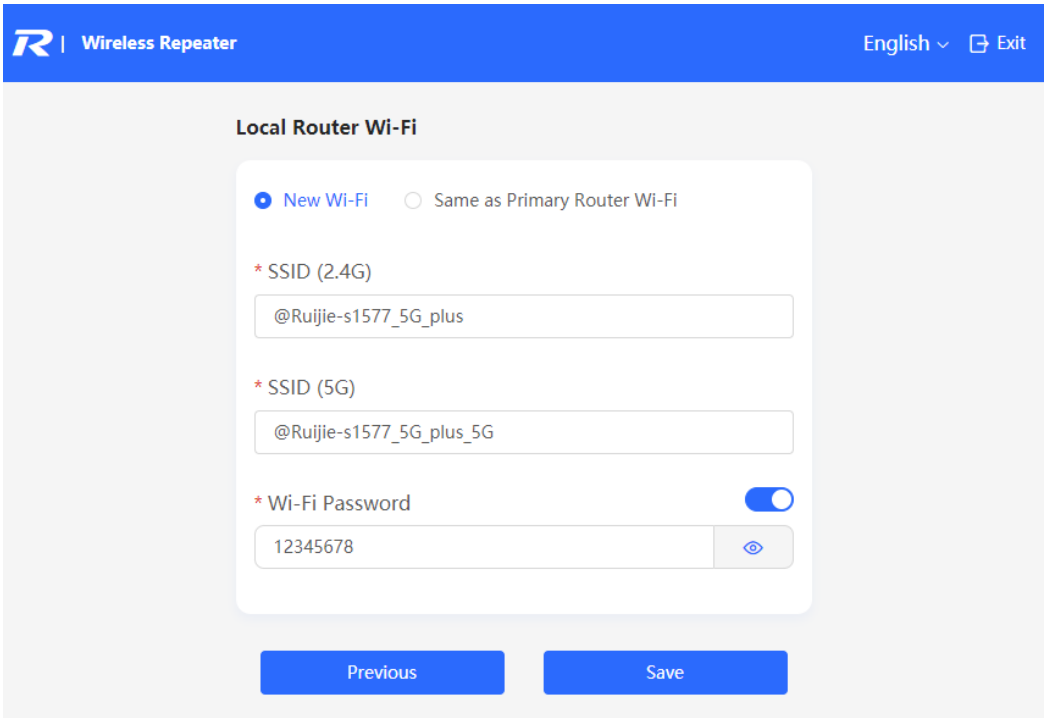
(2) If you see a dialogue box indicating that the Ethernet cable is not connected to the WAN port, click **Wireless Repeater**.



(3) Select the primary router SSID that requires expanding the Wi-Fi coverage, enter the Wi-Fi password of the primary router, and click **Next**.



(4) Set the SSID and password and click **Save**. Then, the Wi-Fi network will be restarted.



1.8 Introduction to the Eweb GUI

To facilitate flexible device management, the Web page displays different system configuration menus in different work modes. For details about the work mode, see Switching Work Mode.

As to the RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models, please refer to Dual Management Webpages.

As to other RAP models, please refer to Single Management Webpage.

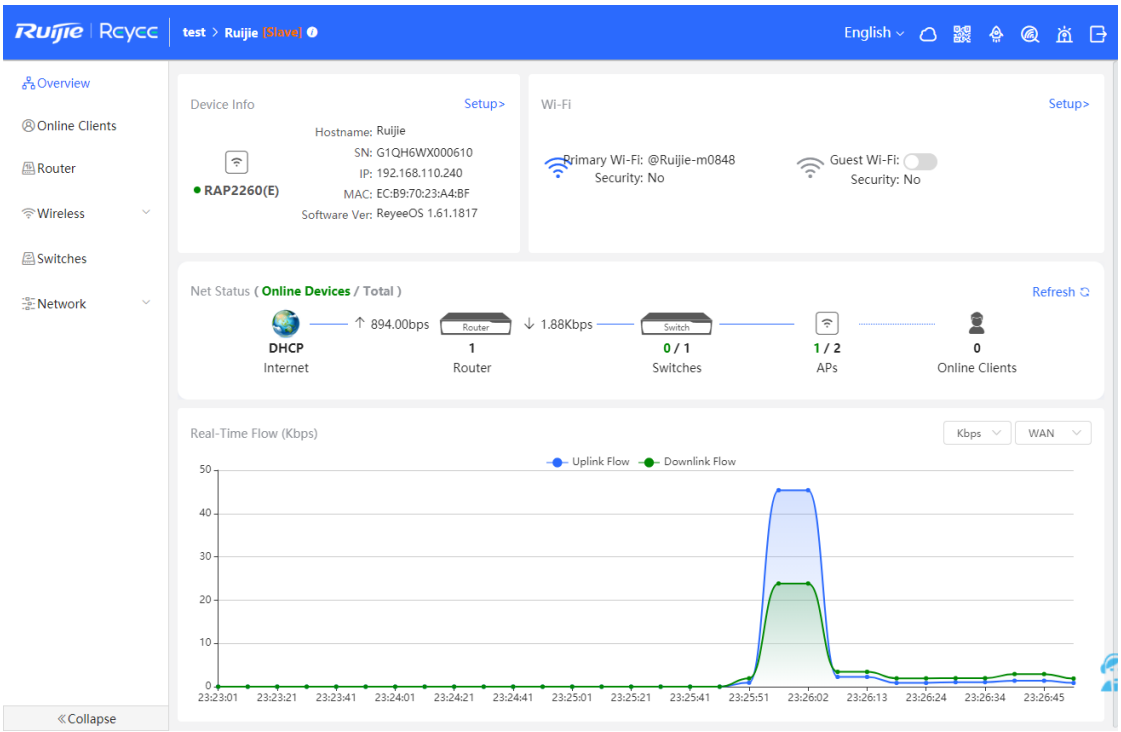
Note

When the self-organizing network is enabled, the Eweb GUI is subject to the master device in the network. If the master device supports the dual management webpages, the slave device also displays the dual management webpages.

1.8.1 Single Management Webpage

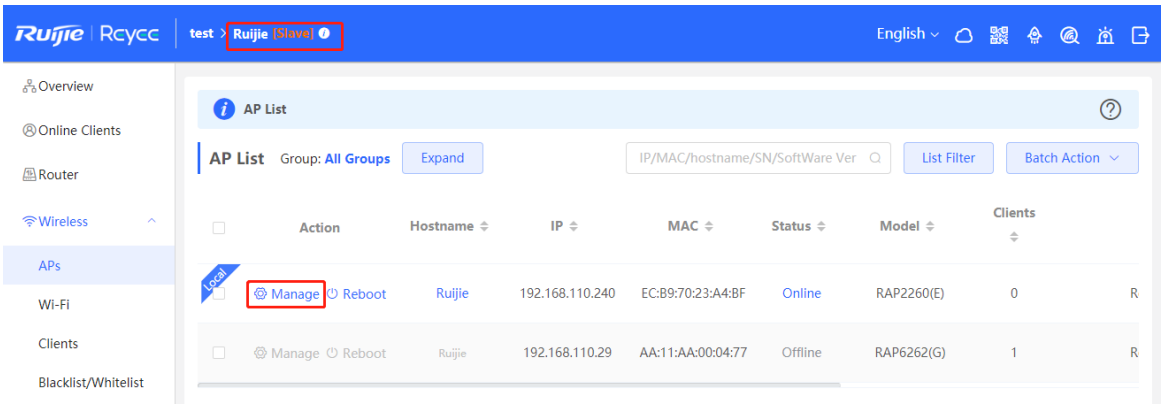
1. Network-wide Management

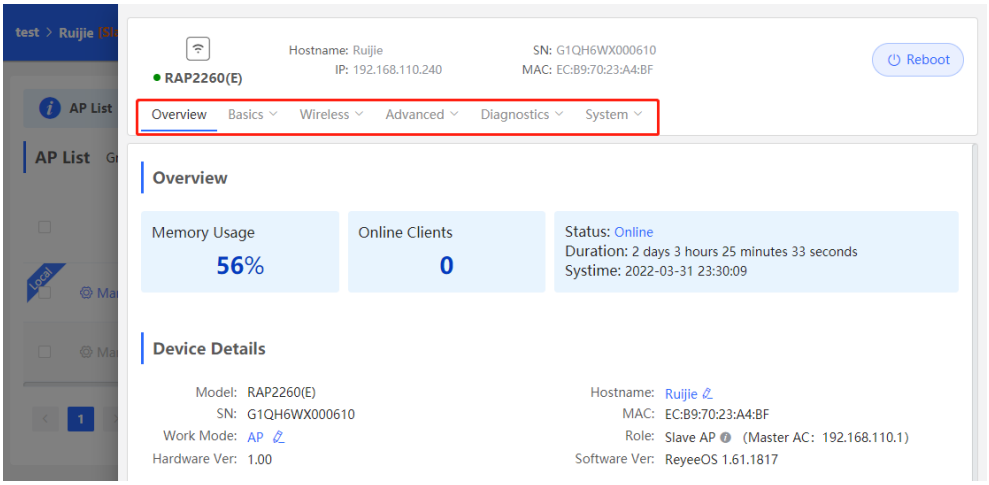
The device works in self-organizing network mode by default. The Web page displays the network-wide management menu on the left side, in which you can check the current status of all devices in the network, and modify network-wide configuration, including global Wi-Fi network management configuration (APs and Wi-Fi), routing management configuration (if routers exist in the network), switch management configuration, and network-wide management configuration (time, password, network-wide reboot, and other system settings).



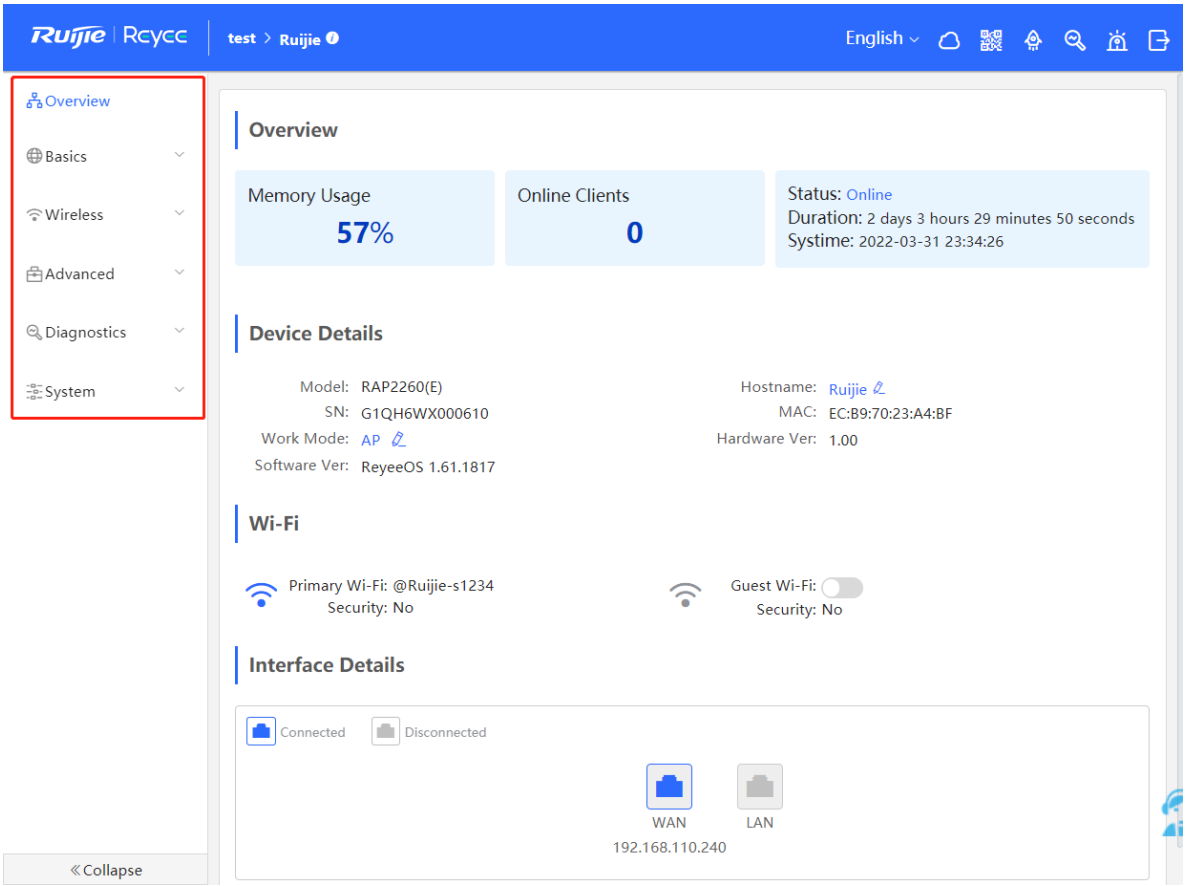
2. Standalone Management

- If a device is in self-organizing network mode, click the name of the currently logged in device or click **Manage** of a specified device in the device list to configure and manage the device.





- If a device is in standalone mode, you can configure and manage only the currently logged in device. The Web page displays the function configuration menu of a single device on the left side.



1.8.2 Dual Management Webpages

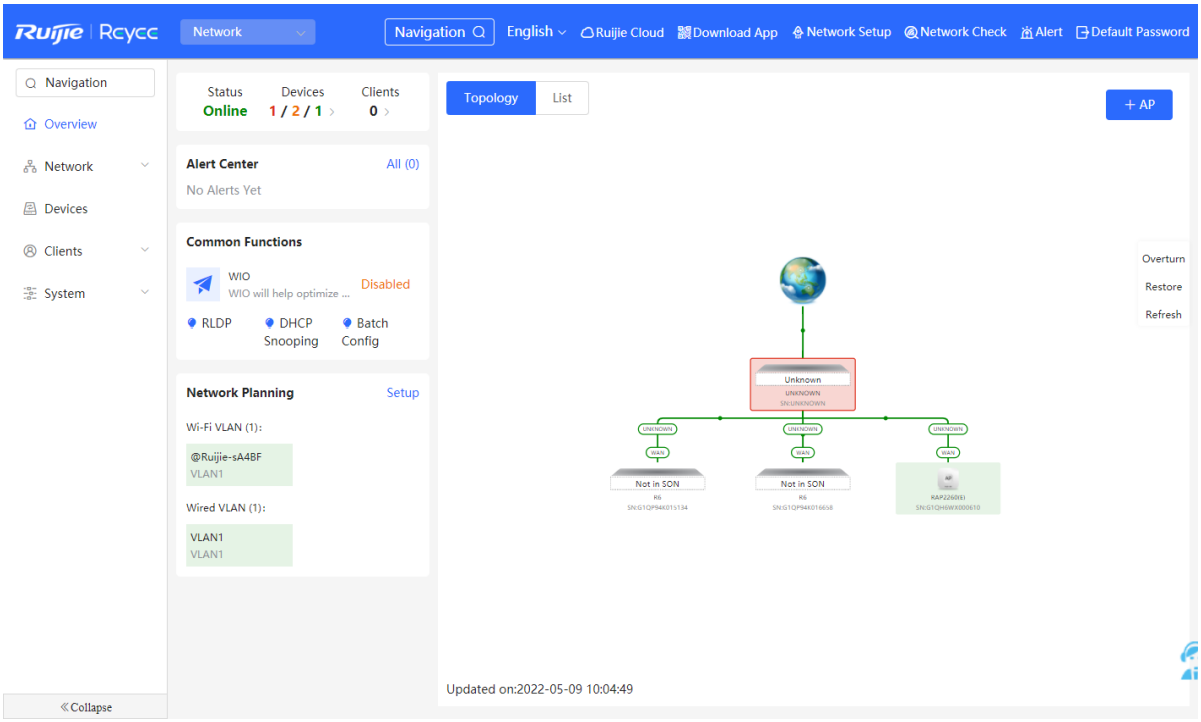
1. Introducing the Management Mode

If the self-organizing network is disabled (The function is enabled by default. See Switching Work Mode for details.), the device works in the local device mode displayed on the Web page.

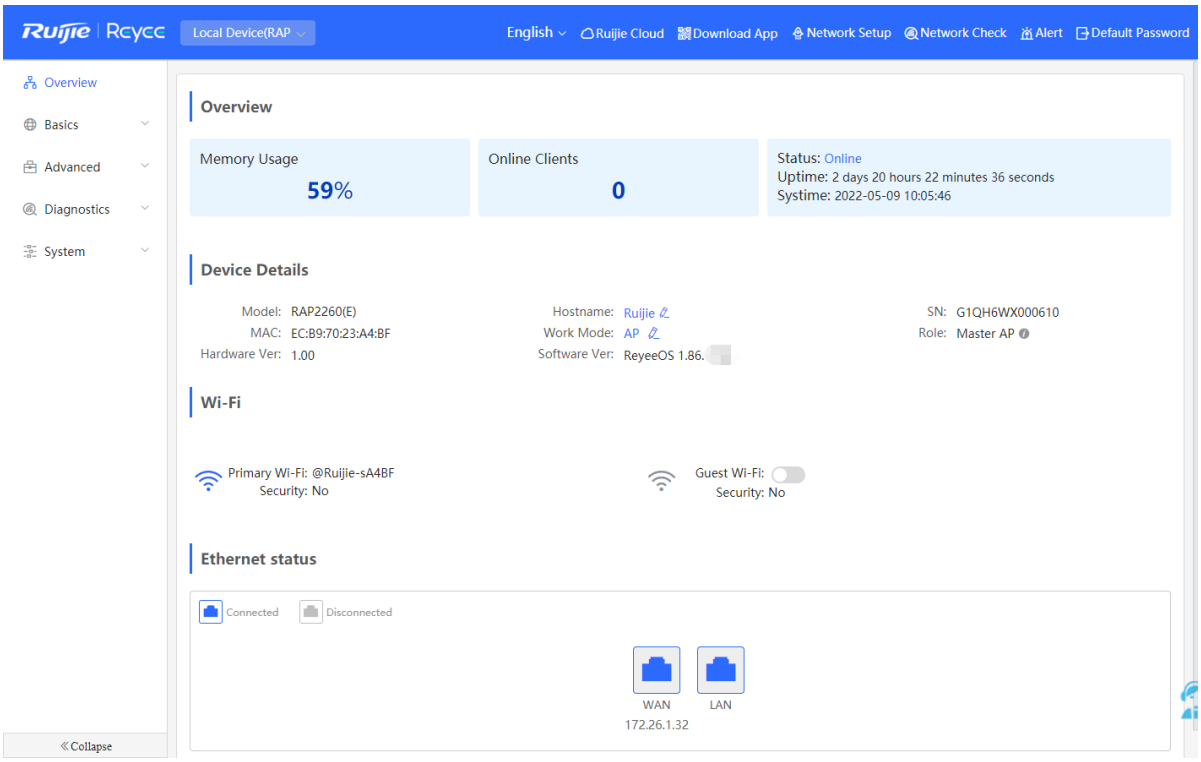
If the self-organizing network is enabled, the device can work in the network mode and the local device mode. The two modes can be switched on the Web page.

- Network mode: View the management information of all devices in the network, and configure all devices based on network management.
- Local Device mode: Only configure the currently logged in devices.

Network mode webpage

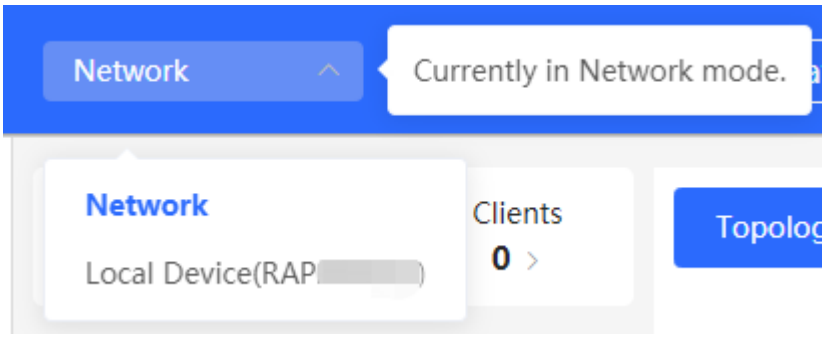


Local Device mode webpage



2. Switching the Management Mode

Click the current management mode in the navigation bar, and select the mode in the drop-down box to switch the work mode of the device.



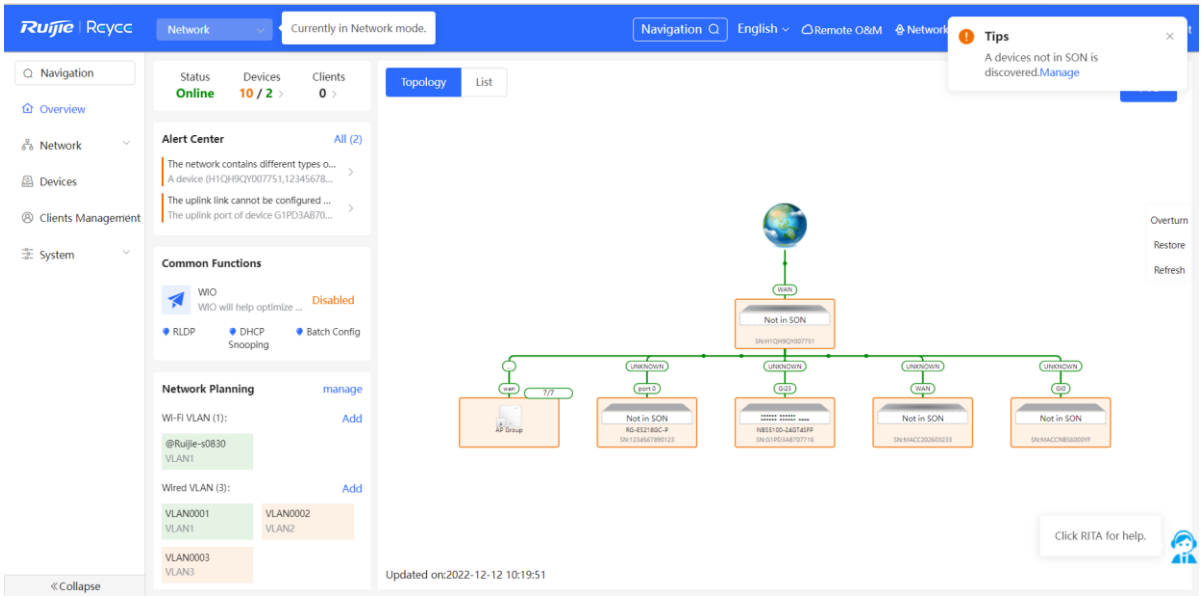
2 Network Monitoring

Note

The functions mentioned in this chapter are only applicable to such models as RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262.

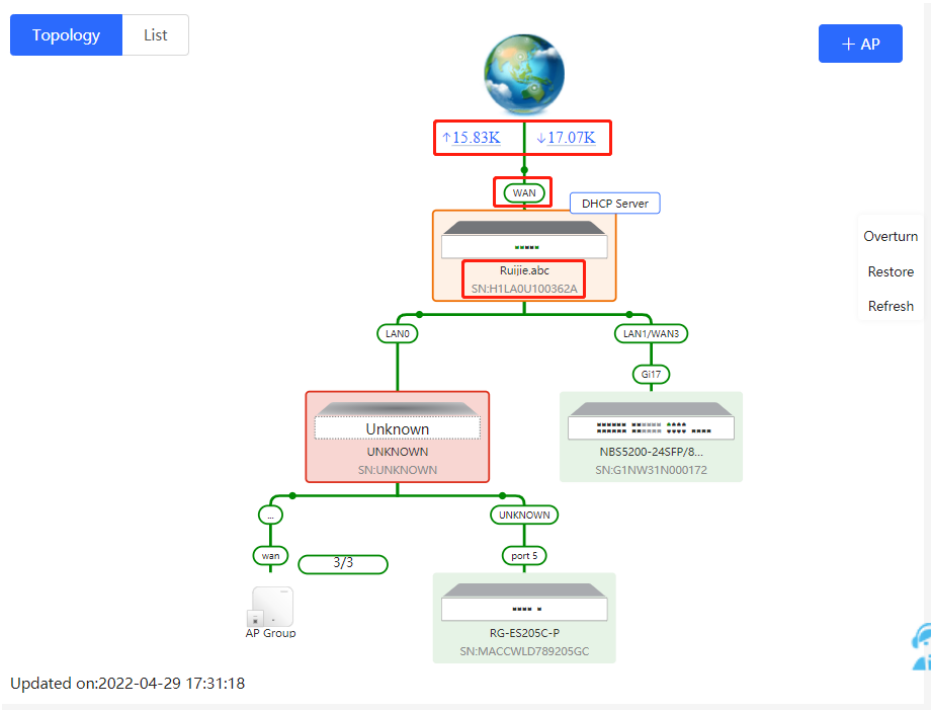
In **Network** mode, select **Overview**.

The **Overview** webpage displays the current network topology, real-time uplink and downlink flow, networking status, and the number of users. The quick access to network and device settings is also provided on the **Overview** webpage. Users can monitor, configure and manage the network status on the current page.

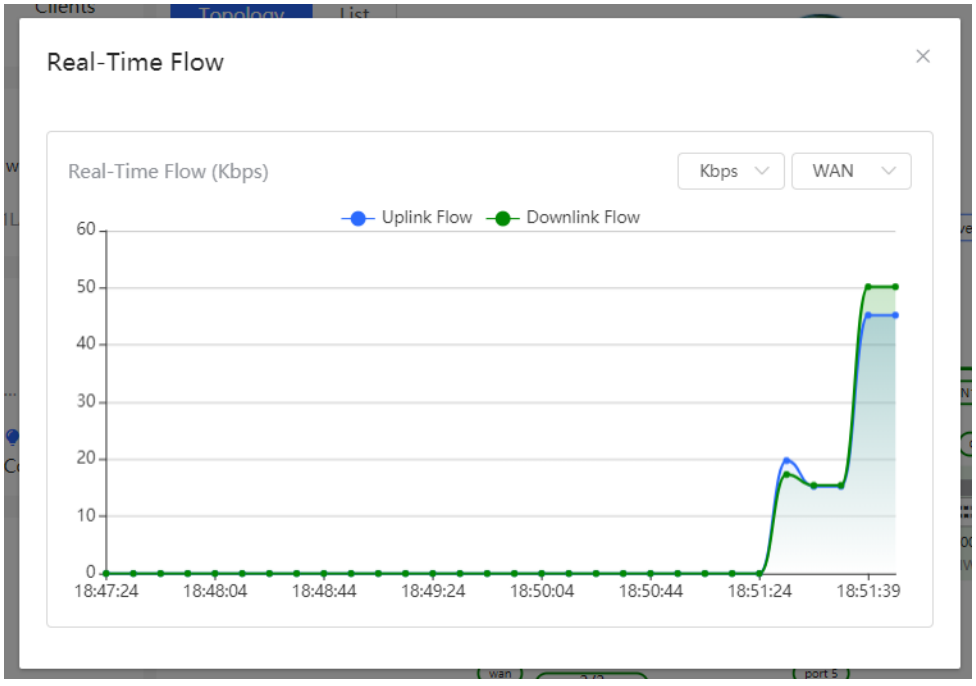


2.1 Viewing the Network Information

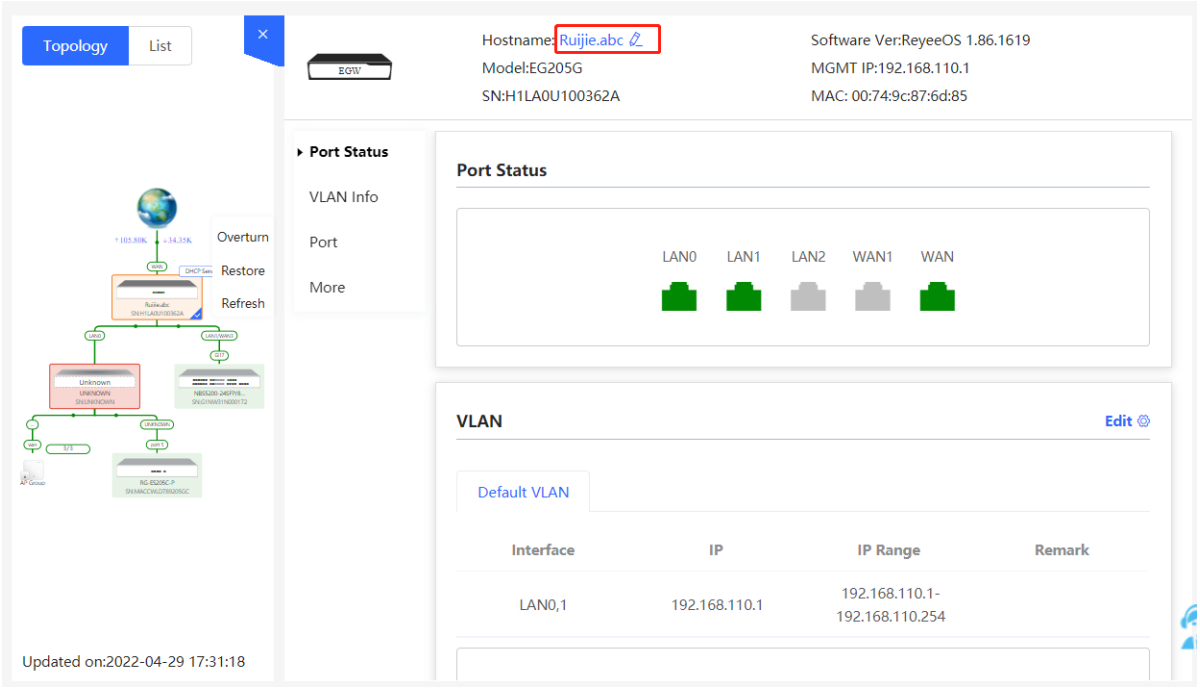
You can view the online device, port ID, device SN as well as the real-time uplink and downlink flow in the network topology.



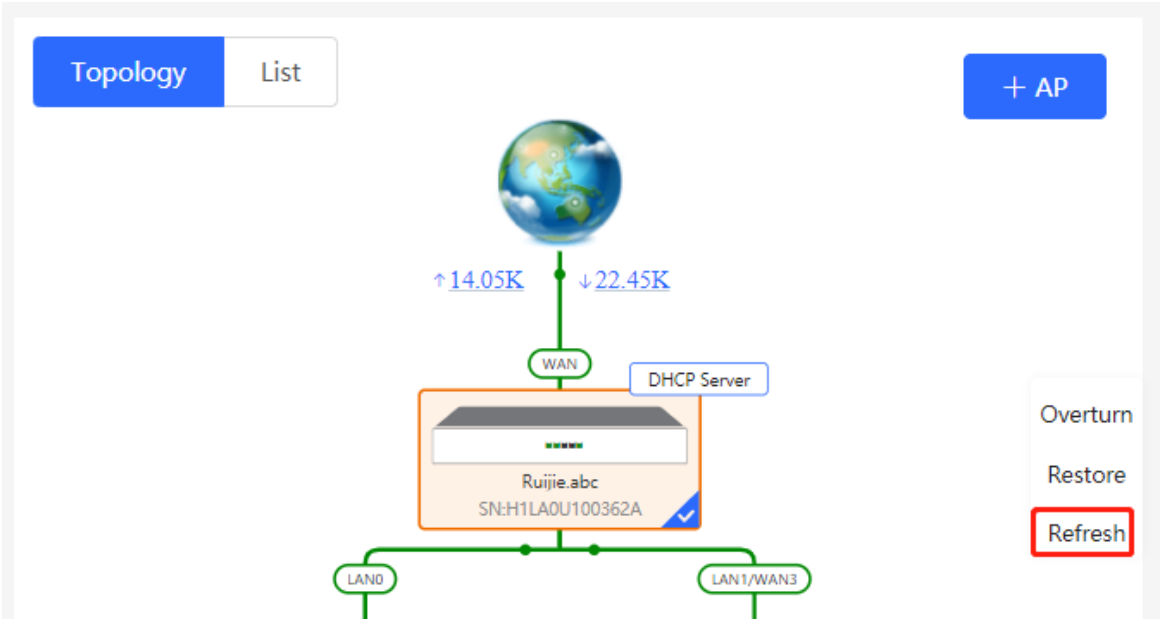
- Click the flow data and view the real-time flow.



- Click the device in the topology to view the operating status and configuration of the device and configure the device functions. The hostname is set to the product model by default. You can click to modify the hostname.



- The update time of the topology is displayed at the bottom left corner. Click **Refresh** to update the topology to the latest status. Please wait for a few minutes for the update.

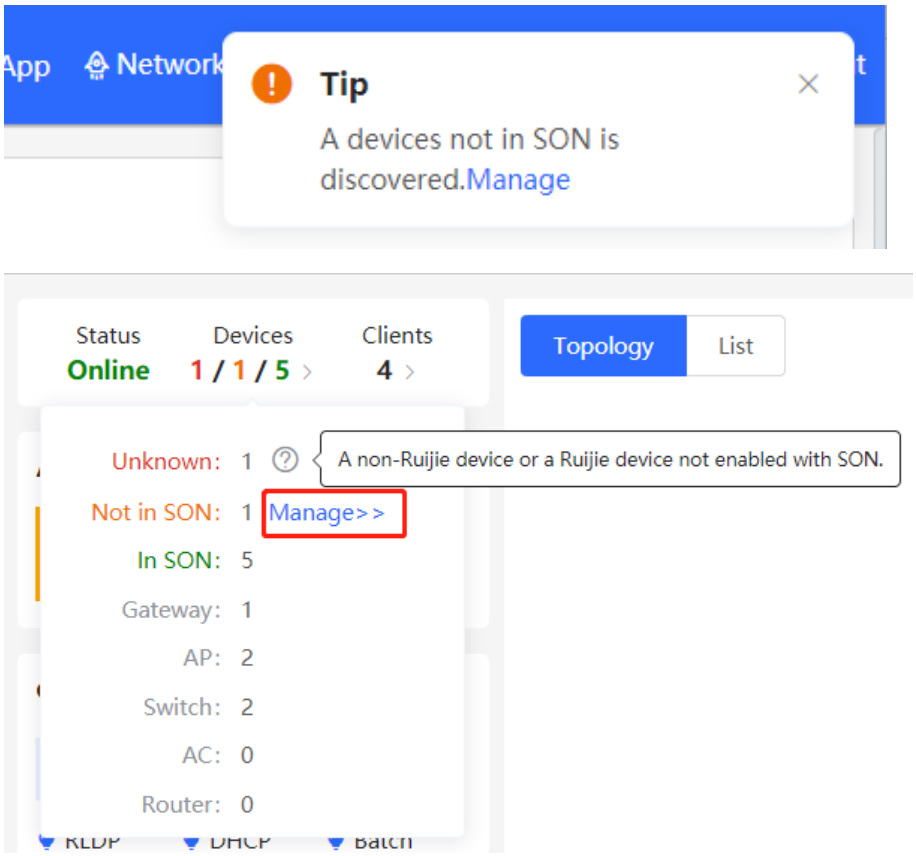


2.2 Adding Network Devices

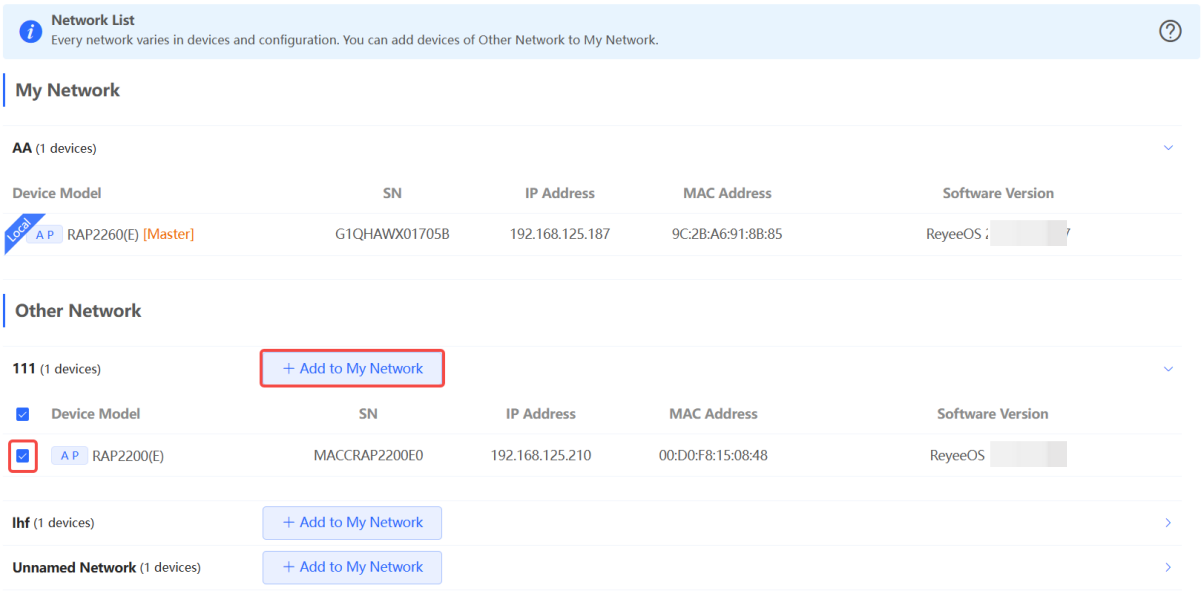
2.2.1 Wired Connection

(1) If a new device is connected to the device in the network through wired connection, a prompt message will pop up, indicating that a device not in SON (Self-Organizing Network) is discovered. The number (in orange)

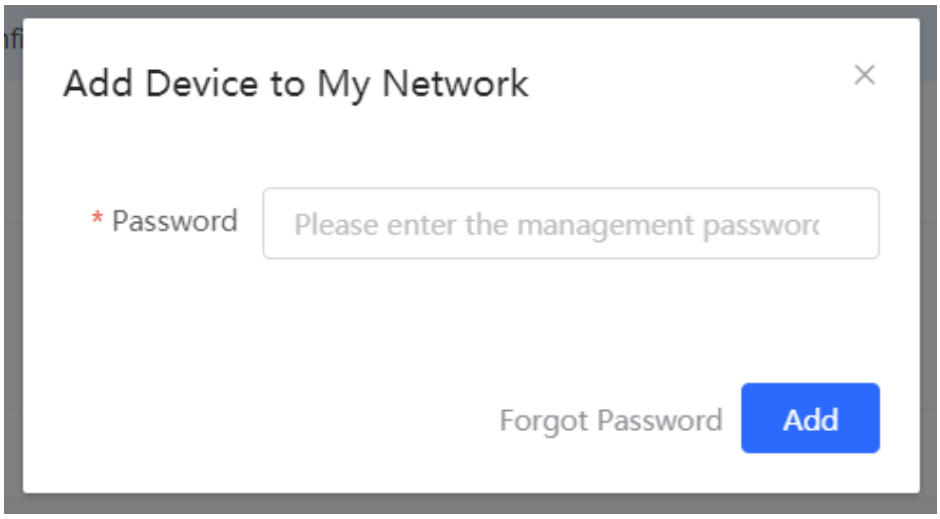
of devices that are not in SON is displayed under the **Devices** at the top left corner of the page. Click **Manage** to add the device to the current network.



(2) Go to the **Network List** page, click **Other Network** to 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. If the device is configured with a password, please enter the management password of the device. If the password is incorrect, the device cannot be added to the network.



2.2.2 AP Mesh

Note

This function is not supported by RG-RAP1200(F), and RG-RAP2200(F).

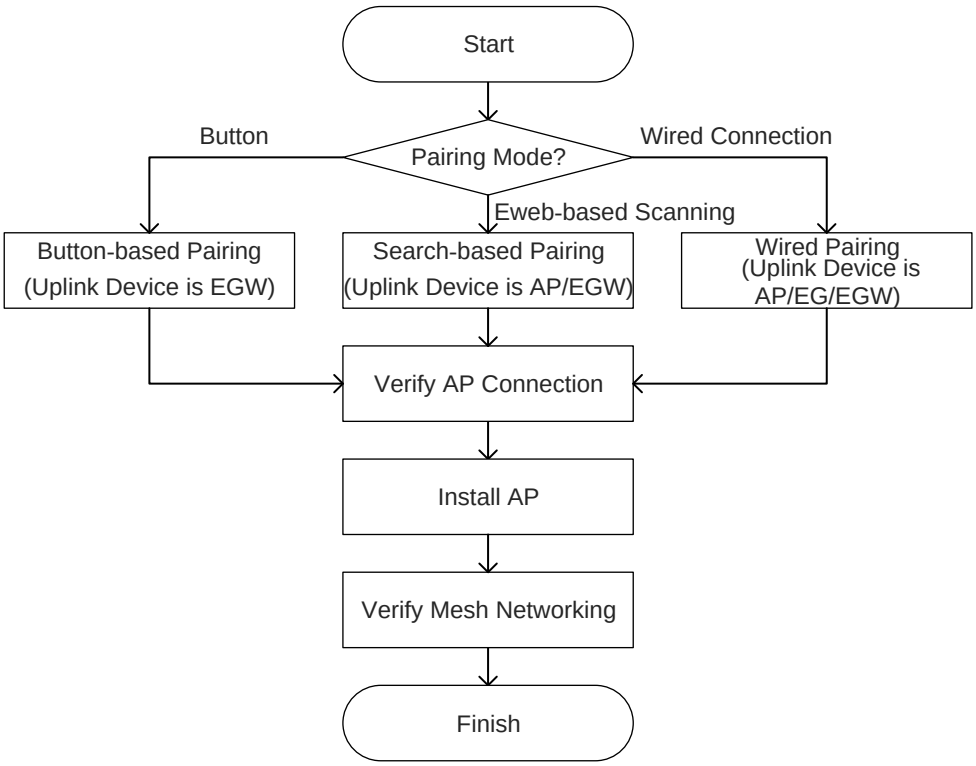
1. Overview

After being powered on and enabled with Mesh (see 3.17 Enabling Reyee Mesh for details), a Mesh-capable new AP can be paired with other Mesh-capable wireless devices on the target network through multiple ways. Then the AP will be synchronized its Wi-Fi configuration with other devices automatically. Mesh networking addresses pain points such as complex wireless networking and cabling. A new AP can be connected to any uplink wireless device among AP, EG router, and EGW router in the following ways:

- Button-based pairing: Short press the Mesh button on the EGW router on the target network to implement fast pairing of the AP with the EGW router.
- Search-based pairing: Log in to the Eweb of a device on the target network. Search and add APs to be paired.
- Wired pairing: Connect the new AP to a wireless device on the target network using an Ethernet cable. The new AP will go online on the target network.

After pairing finishes, the new AP obtains the wireless backhaul information from network-wide neighboring APs. Install the new AP as planned, and it will connect to the optimal neighboring AP.

2. Configuration Procedure



3. Configuration Steps for Button-based Pairing (Uplink Device is an EGW Router)

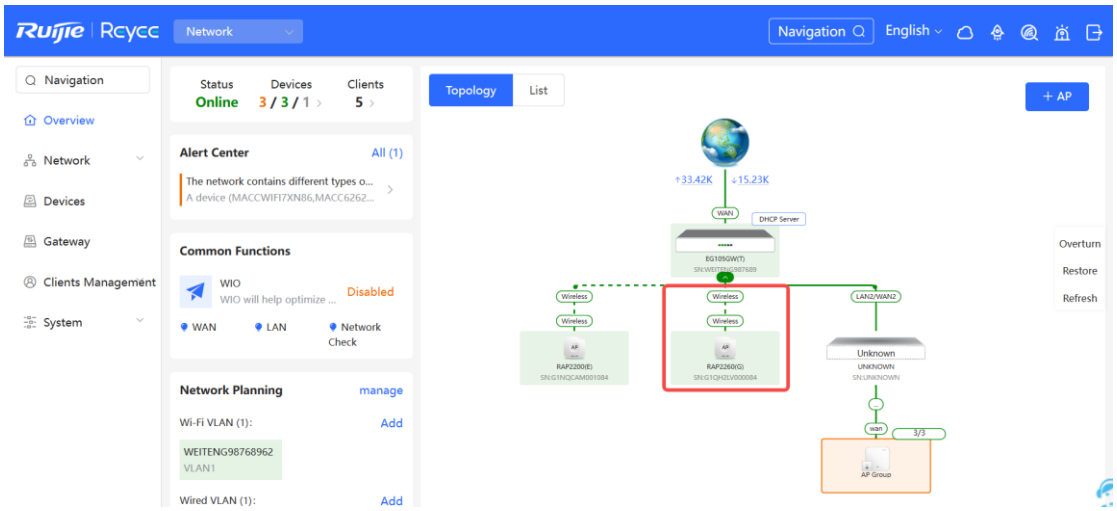
Caution

- Only EG105GW-X and EG105GW(T) support button-based pairing and each router can be paired with up to 15 new APs.
- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh (see Enabling Reyee Mesh for details).
- Place the new AP no more than 2 meters away from the uplink device to ensure that the new AP can receive the Wi-Fi signal from the uplink device. The new AP may fail to be scanned due to the long distance or obstacles between it and the uplink device.

(1) Power on the new AP and place it near the EGW router on the target network.

(2) Press and hold the Mesh button  on the EGW router for no more than two seconds to start pairing. The pairing process takes about one minute.

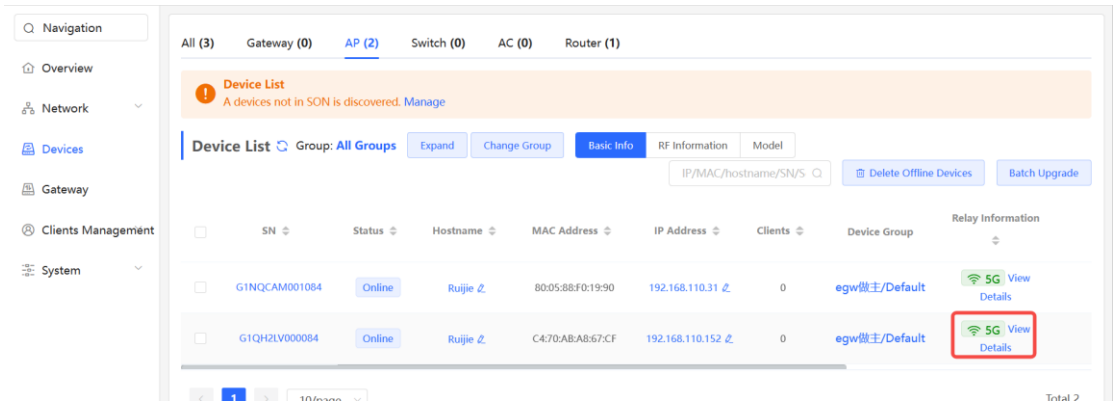
(3) Check the topology on the **Overview** page to make sure that the new AP has connected to the uplink device in wireless mode.



(4) Power off the new AP and install it as planned.

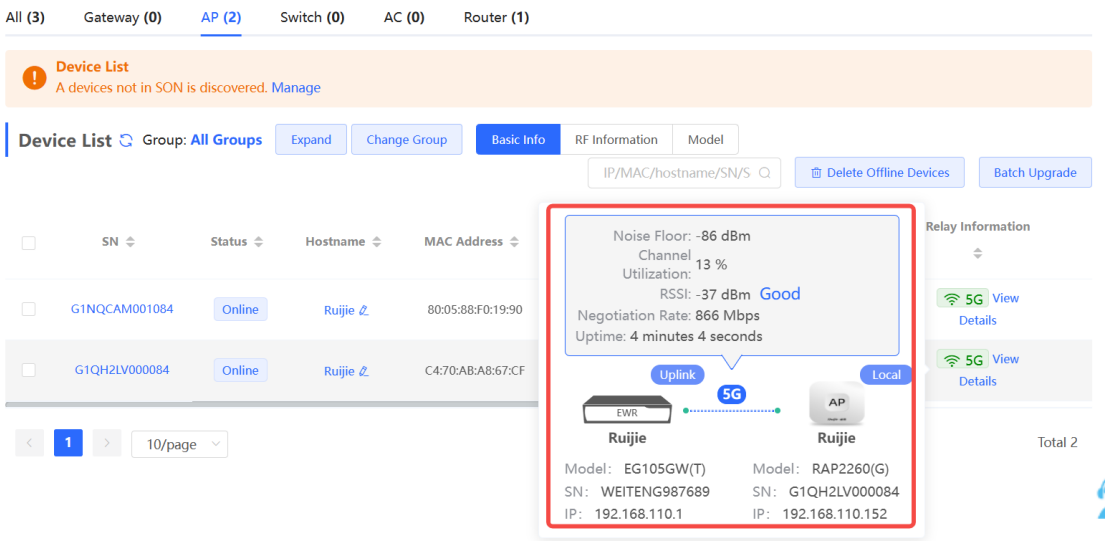
(5) Log in to the Eweb of a device on the target network. In **Network** mode, choose **Devices** > **AP**. Make sure that the new AP is online and the corresponding entry contains icon 

in the **Relay Information** column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.



Click **View Details** following the 

icon to obtain information about the uplink device and RSSI.



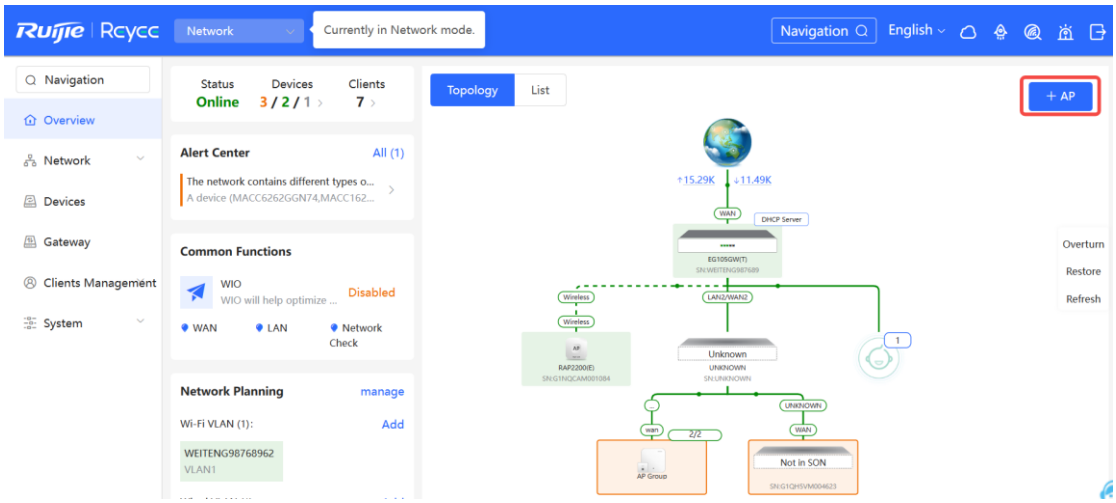
4. Configuration Steps for Search-based Pairing (Uplink Device is an AP or EGW Router)

Caution

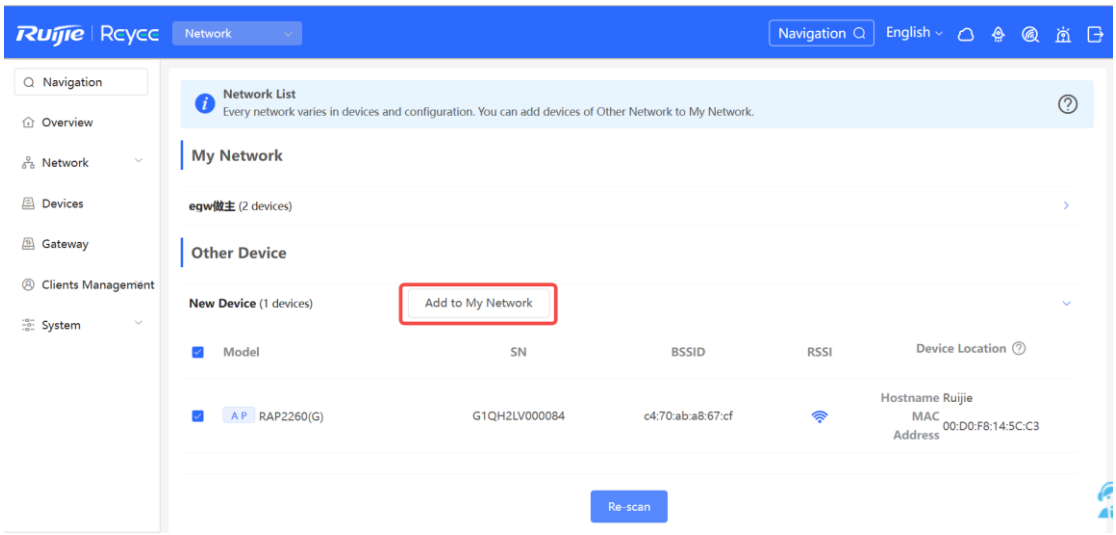
- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh (see Enabling Reyee Mesh for details).
- Place the new AP no more than 2 meters away from the uplink device to ensure that the new AP can receive the Wi-Fi signal from the uplink device. The new AP may fail to be scanned due to the long distance or obstacles between it and the uplink device.

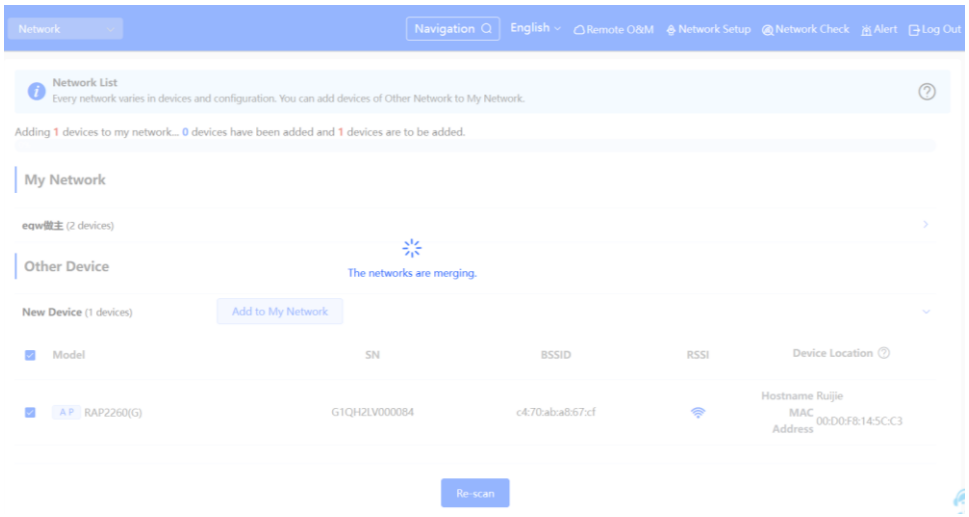
(1) Power on the new AP and place it near the AP or EGW router on the target network.

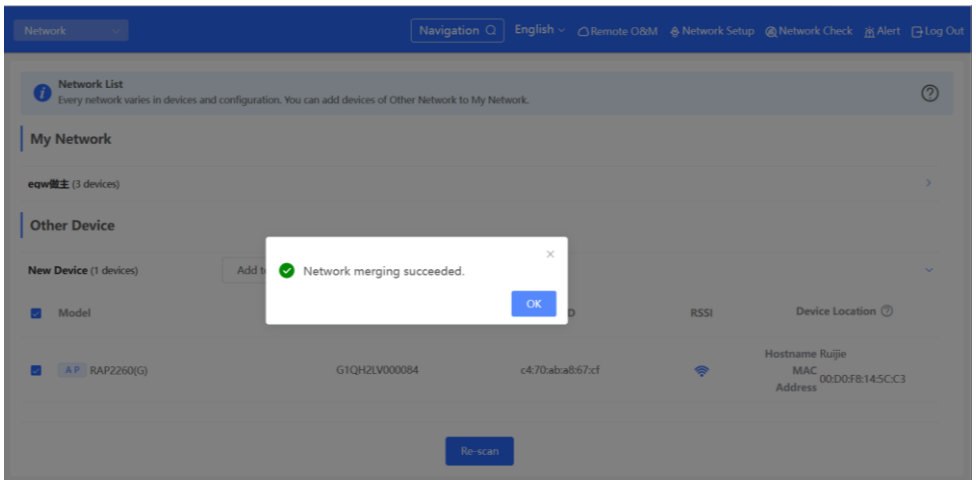
(2) Log in to the Eweb of a device on the target network. In **Network** mode, click **+AP** in the upper right corner of the **Overview** page to scan the APs in other networks not plugged in with Ethernet cables.



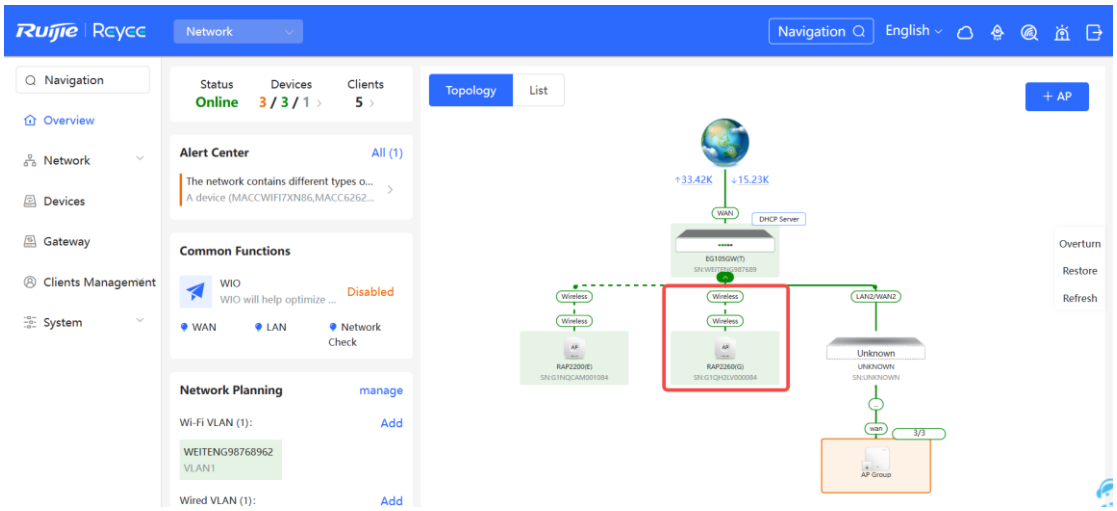
(3) Select the APs to be added and click **Add to My Network**. No more than eight APs are allowed at a time. Wait until network merging finishes.







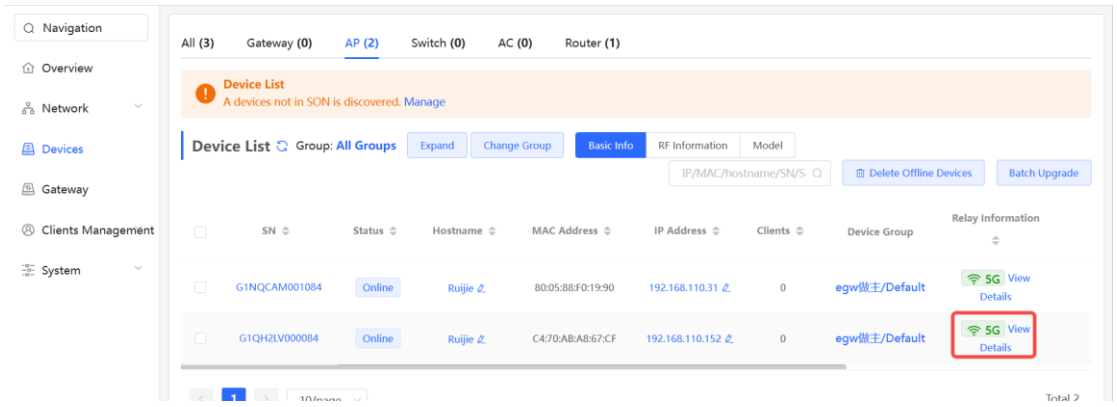
(4) Check the topology on the **Overview** page to make sure that the new AP has connected to the uplink device in wireless mode.



(5) Power off the new AP and install it as planned.

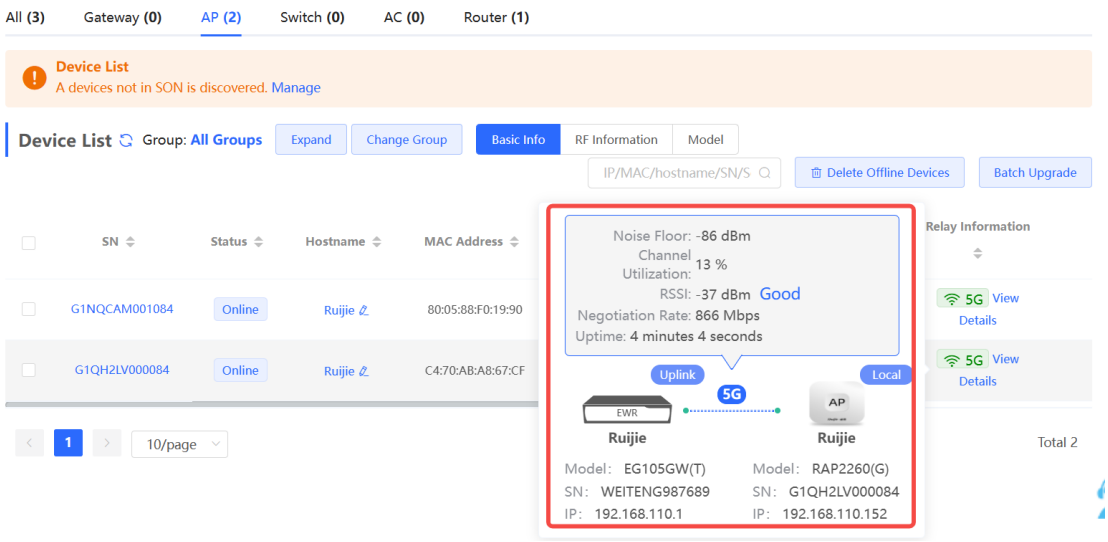
(6) Log in to the Eweb of a device on the target network. In **Network** mode, choose **Devices** > **AP**. Make sure that the new AP is online and the corresponding entry contains icon 

in the **Relay Information** column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.



Click **View Details** following the 

icon to obtain information about the uplink device and RSSI.



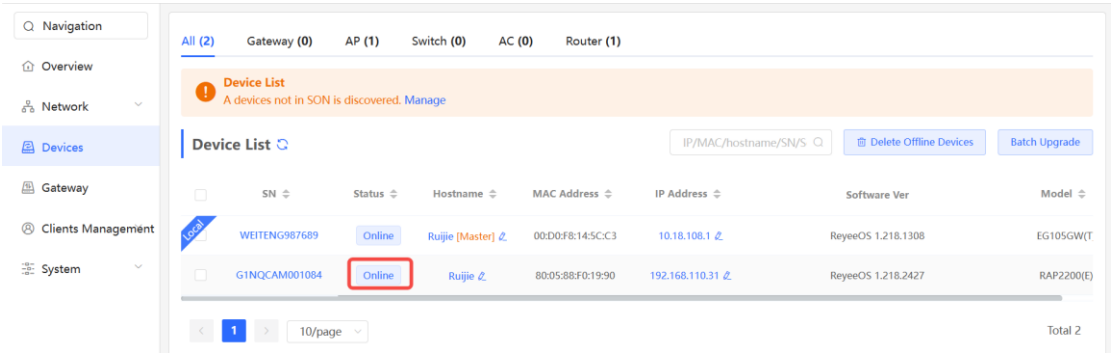
5. Configuration Steps for Wired Pairing (Uplink Device is an AP, EG Router, or EGW Router)

Caution

- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh (see 3.17 Enabling Reyee Mesh for details).

(1) Plug one end of the Ethernet cable to the uplink port of the new AP, and the other end to the downlink port of an AP, EG router, or EGW router on the target network. Mesh networking takes one to three minutes. When the system status LED is steady on, it indicates that Mesh networking finishes.

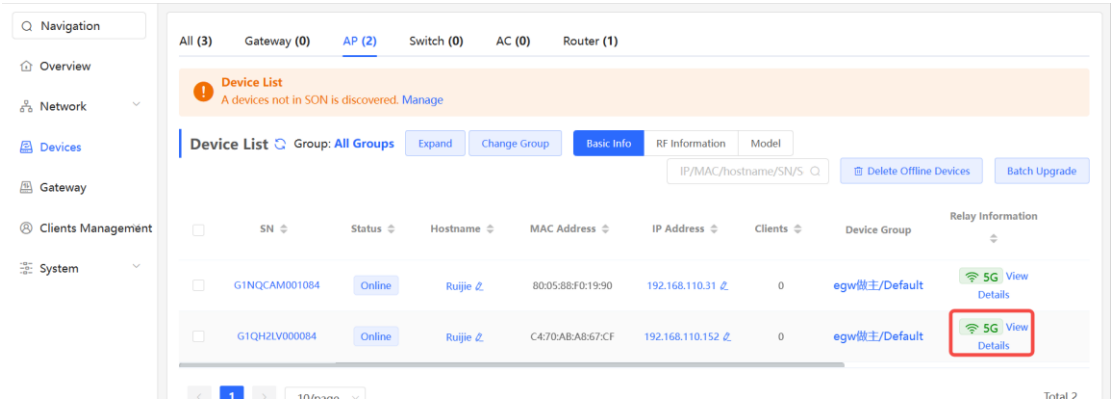
(2) Log in to the Eweb of a device on the target network. In **Network** mode, choose **Devices** and make sure that the new AP is online.



(3) Unplug the Ethernet cable, power off the new AP, and install it as planned.

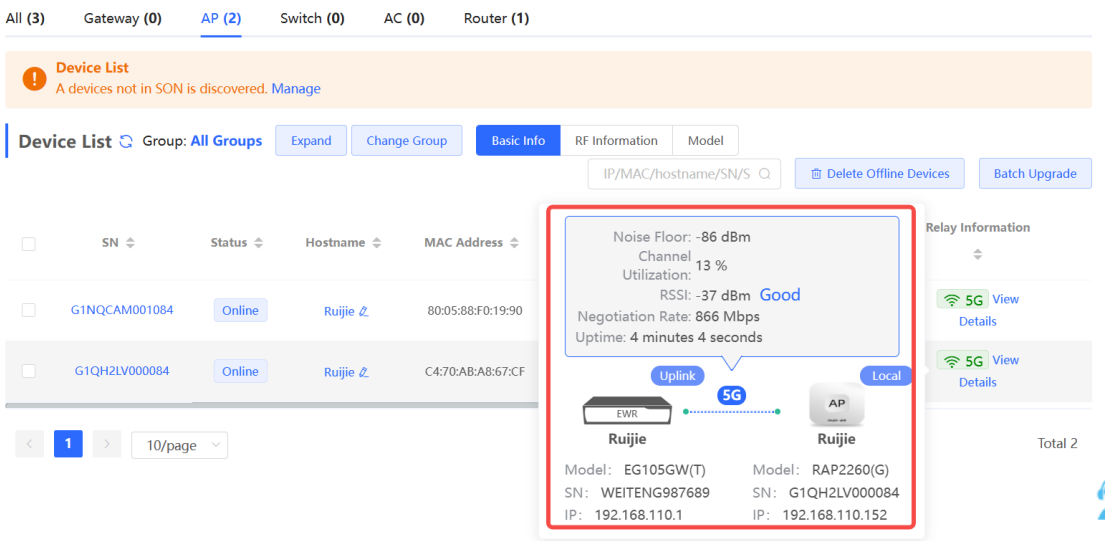
(4) Log in to the Eweb of a device on the target network. In **Network** mode, choose **Devices** > **AP**. Make sure that the new AP is online and the corresponding entry contains icon 

in the **Relay Information** column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.



Click **View Details** following the 

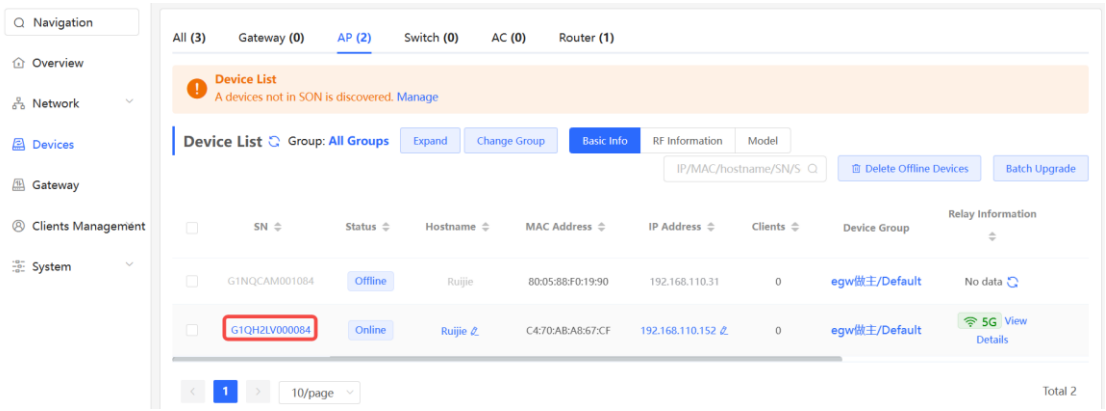
icon to obtain information about the uplink device and RSSI.



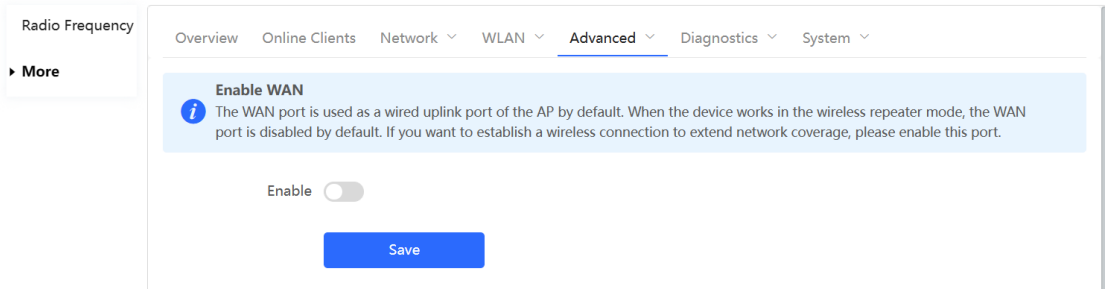
6. Enabling WAN Port

The WAN port works as the wired uplink port of the AP by default. For the AP added to the target network through Mesh pairing, the WAN port is disabled by default. If you want to connect the Mesh AP to other downlink device in wired mode to expand the network, enable this port.

(1) Log in to the Eweb of a device on the target network. In **Network** mode, choose **Devices** > **AP** and click the serial number of the Mesh AP with the WAN port to be enabled.



(2) Choose **More** > **Advanced** > **Enable WAN**, toggle on **Enable**, and click **Save**.

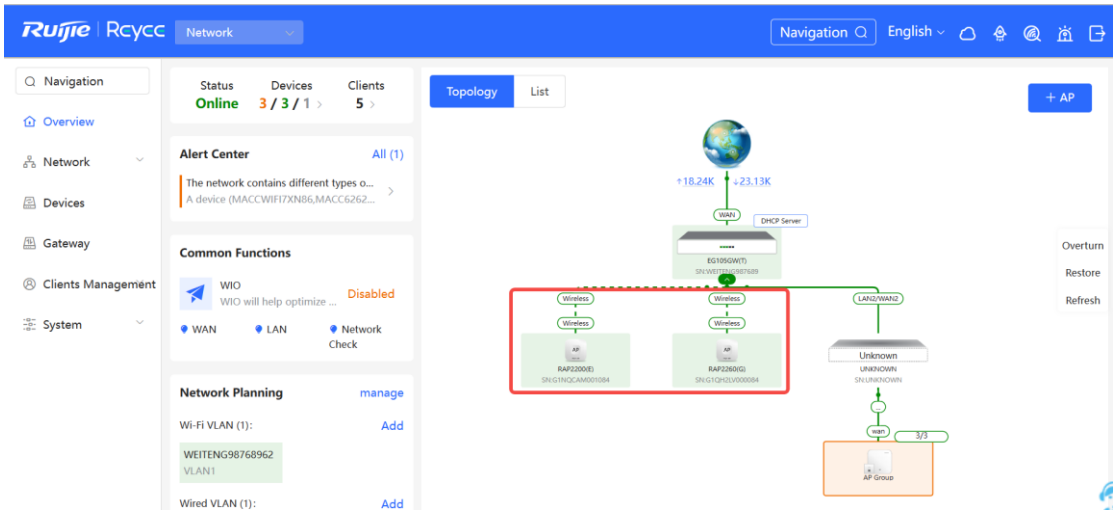


7. Querying Mesh APs and Mesh Details

(1) Log in to the Eweb of a device on the target network.

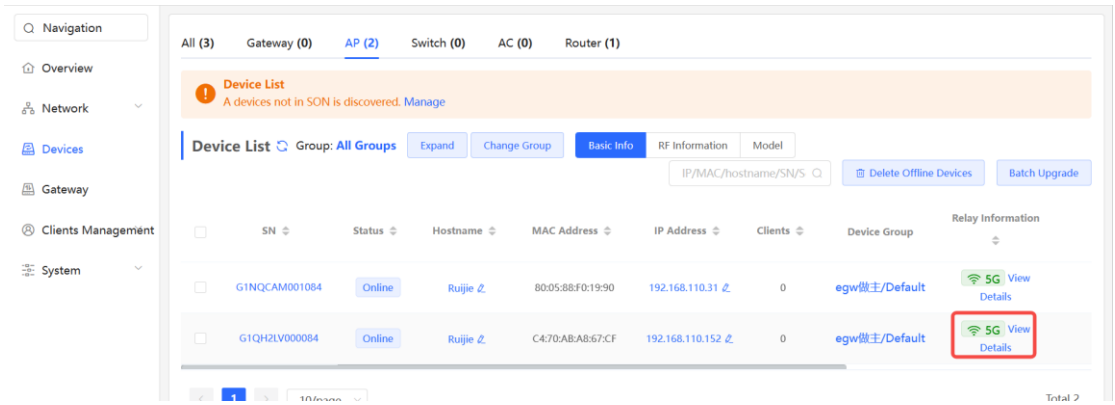
(2) Query Mesh APs.

- Method 1: In **Network** mode, check the topology on the **Overview** page. The AP that connects to the uplink device in wireless mode is a Mesh AP.



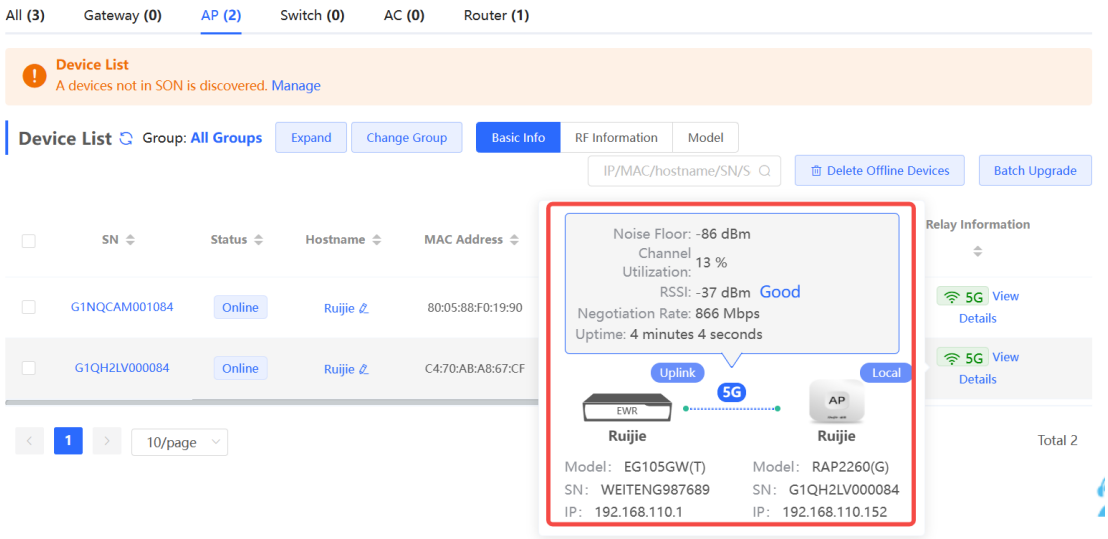
- Method 2: In **Network** mode, choose **Devices** > **AP**. If an entry contains icon 

in the **Relay Information** column, the corresponding AP is a Mesh AP.



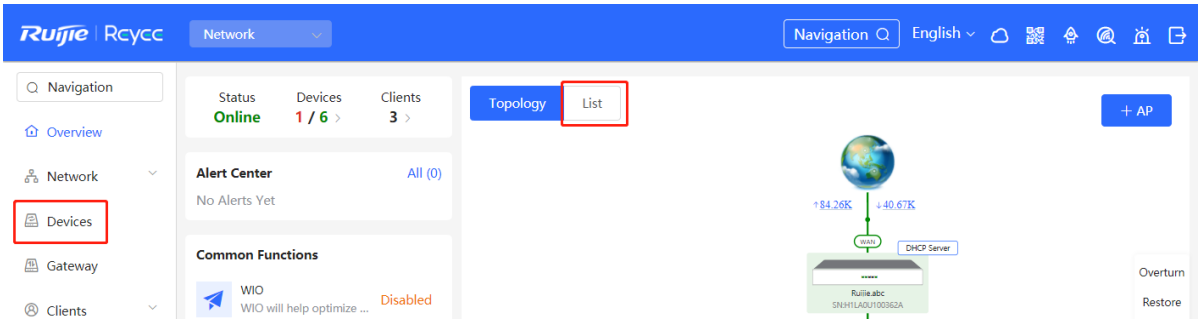
(3) Query Mesh networking details.

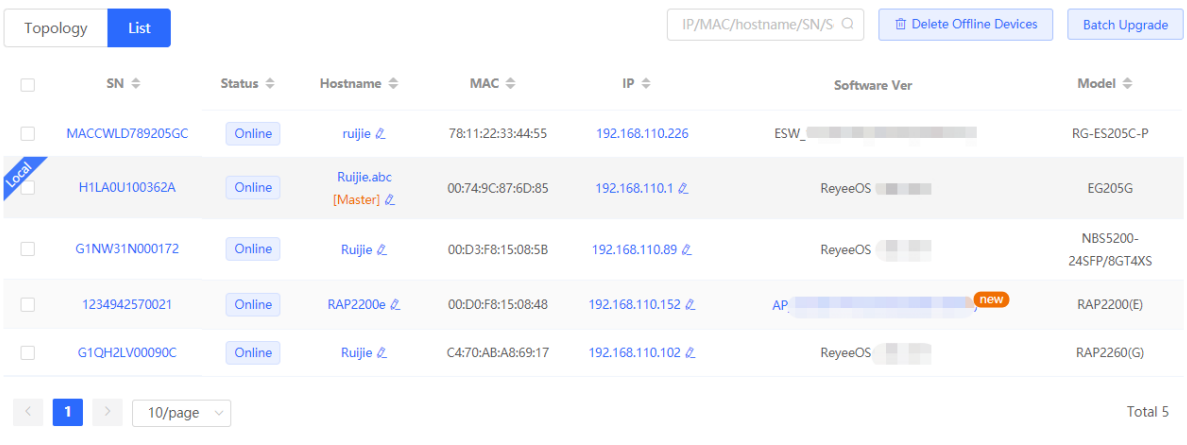
In **Network** mode, choose **Devices** > **AP**. Select the target AP, and click **View Details** in the **Relay Information** column to obtain the Mesh networking details.



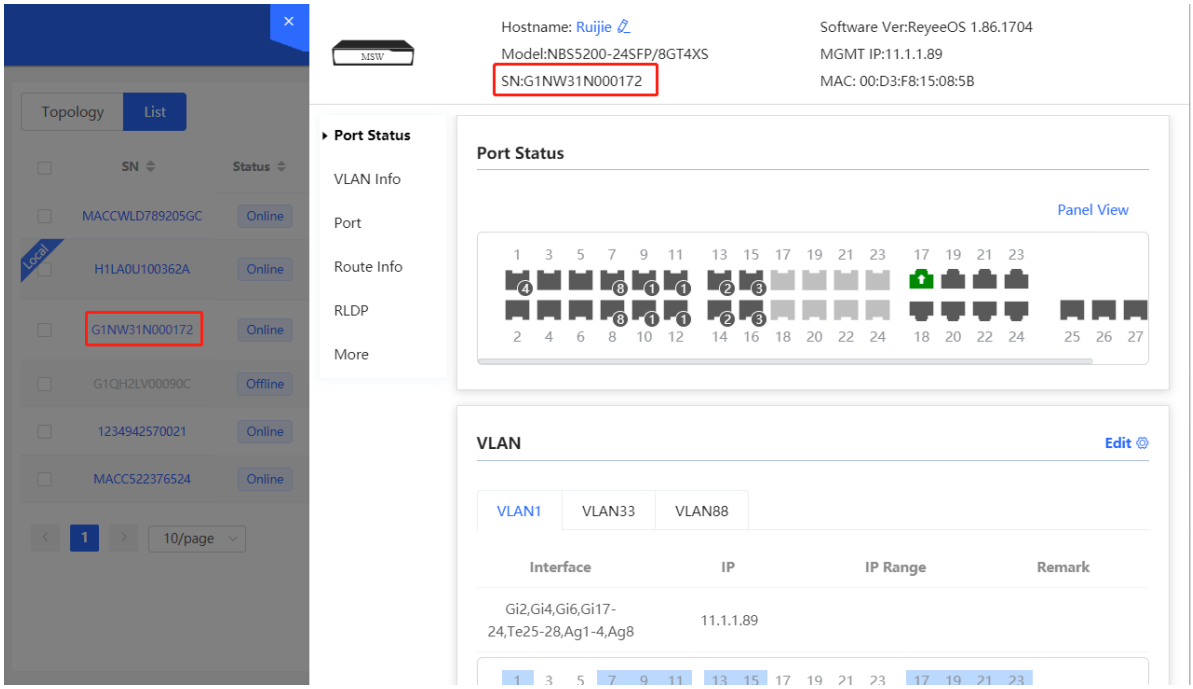
2.3 Managing Network Devices

Click **List** at the top left corner of the topology or click **Devices** in the menu bar to switch to the device list view, and view the information of all devices in the self-organizing network (SON). You can perform configurations and management on all devices by logging in to only one device in the network.

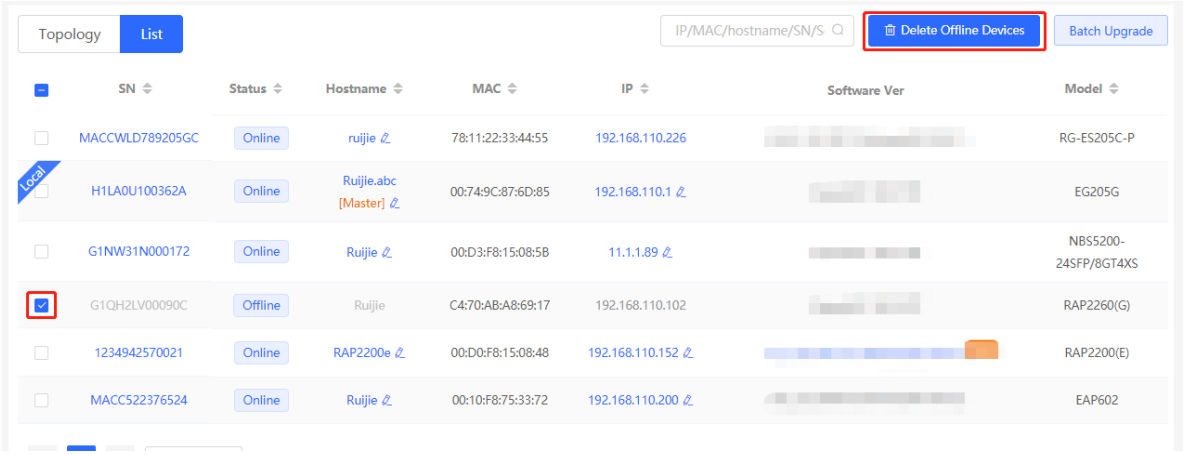




- Click **SN** to configure the specified device.

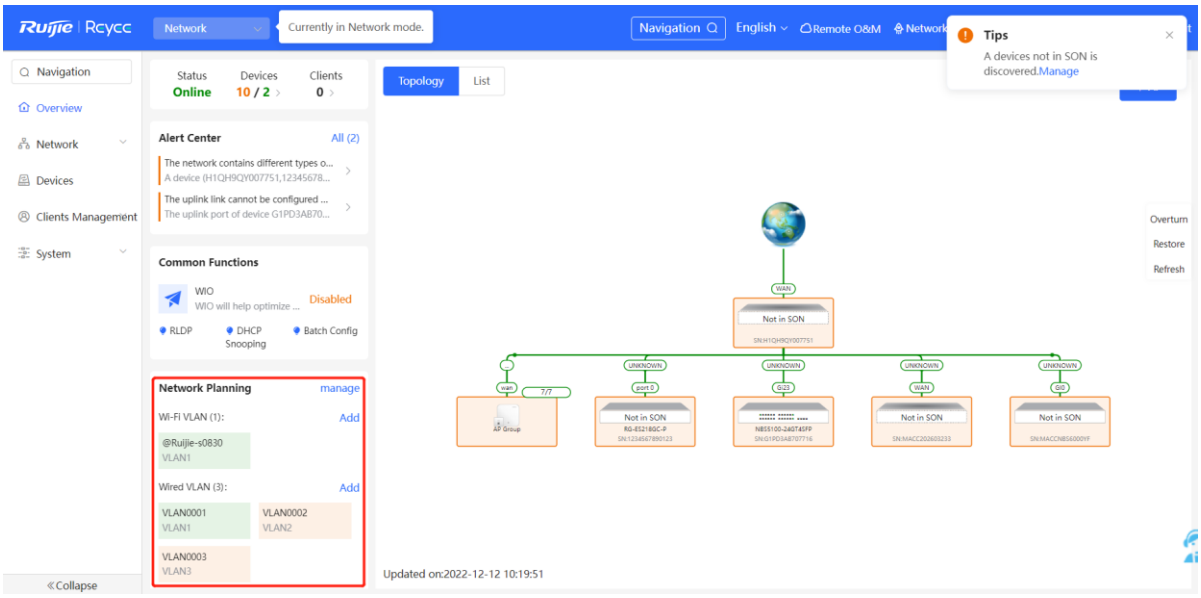


- Select the offline device and click **Delete Offline Devices** to remove the device from the list and the topology.

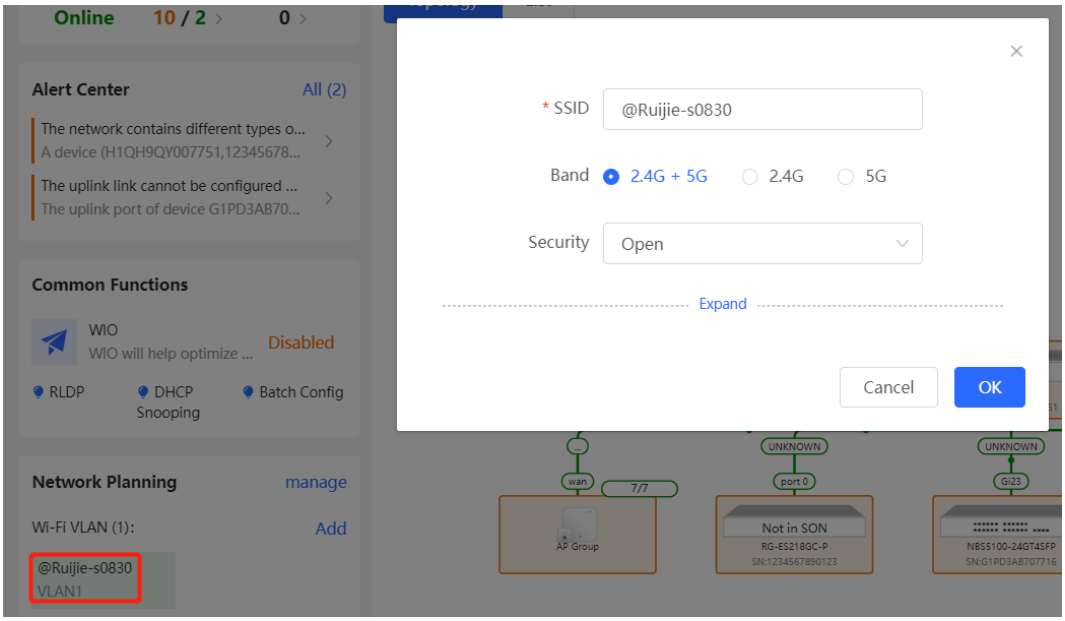


2.4 Configuring Network Planning

The **Overview** page displays the configuration of **Network Planning** at the bottom left corner, including **Wi-Fi VLAN** and **Wired VLAN**.



- Click **manage** to go to the **Network Planning** page for configuration (**Network** > **Network Planning**). You can add or edit the **Network Planning** configuration for the live network.
- Click **Add** to configure **Wi-Fi VLAN** or **Wired VLAN** for the live network.
- Click the SSID to edit the Wi-Fi configuration. For details, see Chapter 3 Wi-Fi Network Settings.



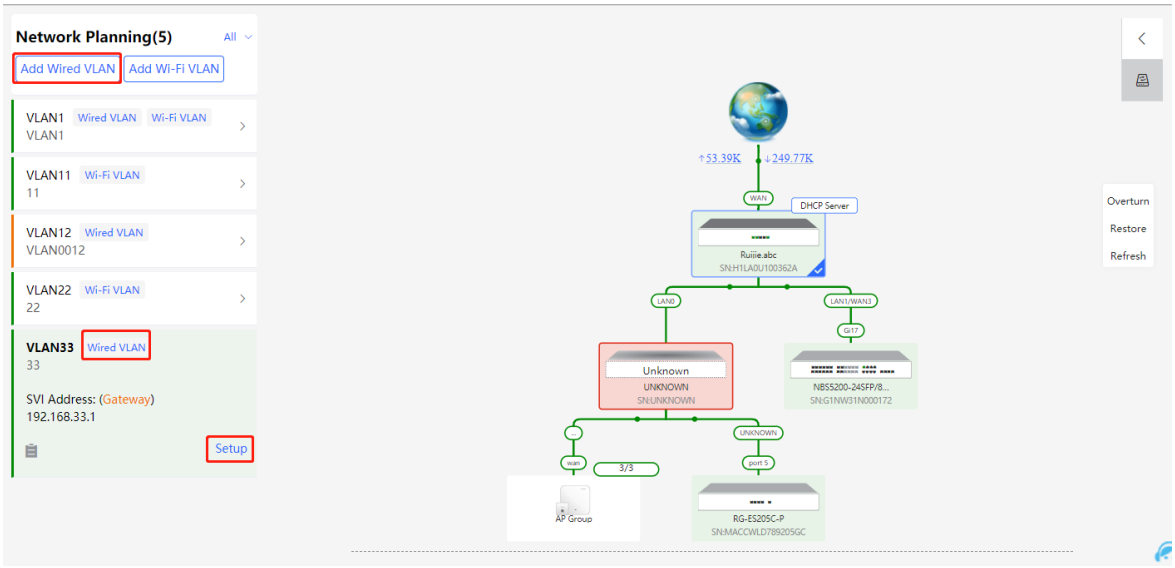
2.4.1 Configuring Wired VLAN

(1) Go to the **Wired VLAN** page for configuration.

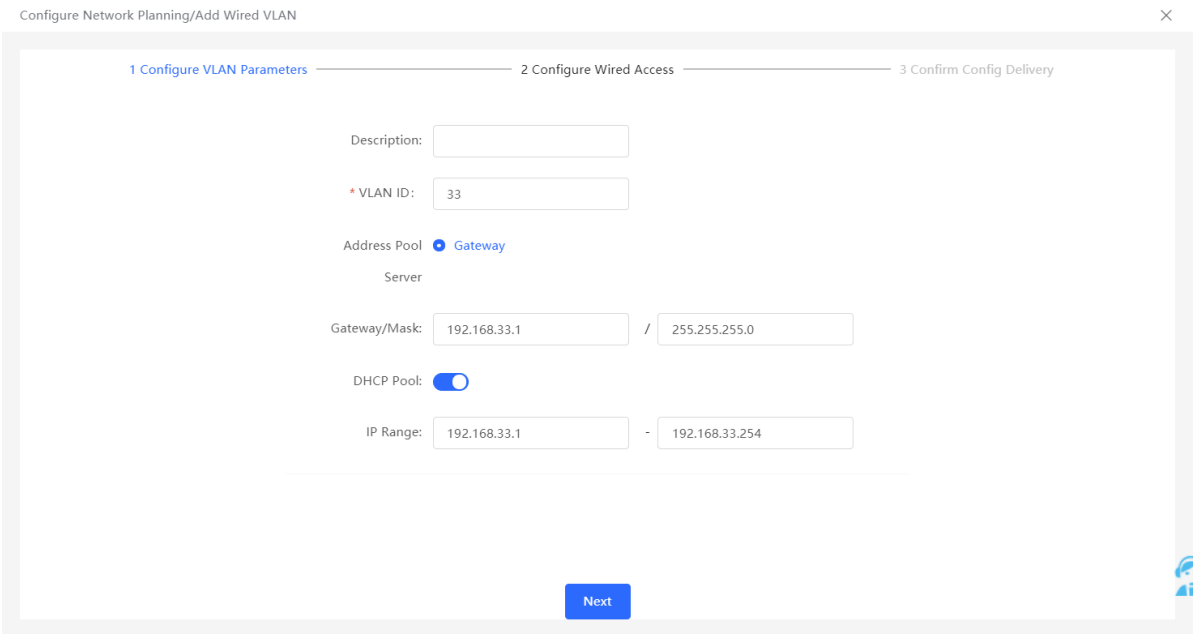
- Method 1: Click **Add** beside **Wired VLAN** in the **Network Planning** area on the **Overview** page to add the

wired VLANs.

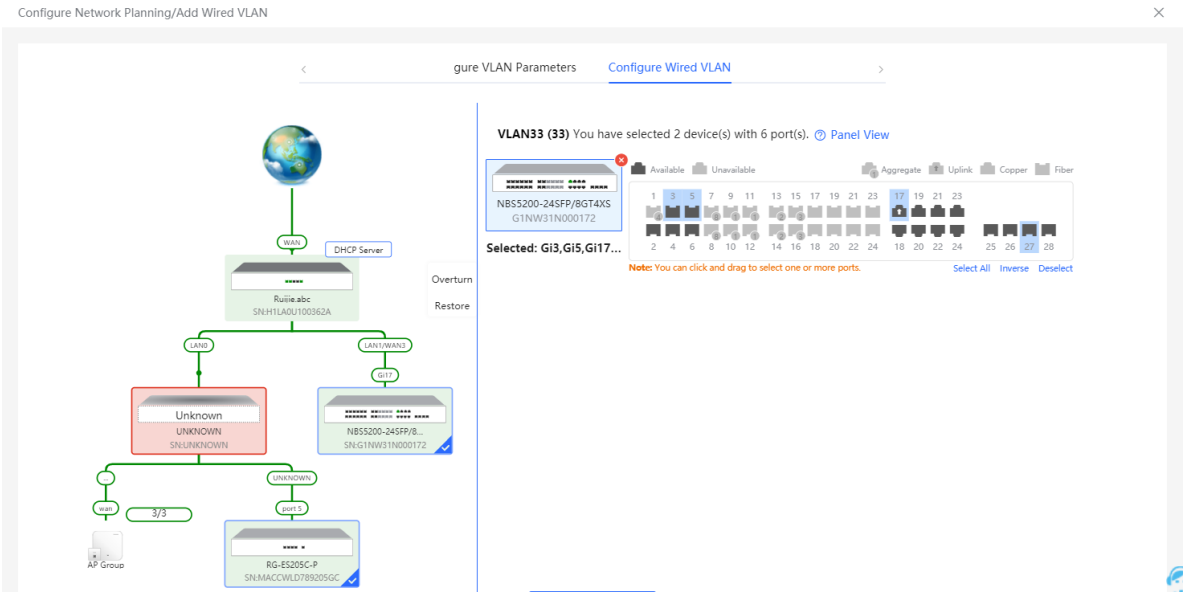
- Method 2: Click **manage** in the **Network Planning** area on the **Overview** page to go to the **Network Planning** page for configuration (**Network** > **Network Planning**). Click **Add Wired VLAN** to add the wired VLANs to the live network or select the available wired VLANs. Click **Setup** to configure the wired VLANs.



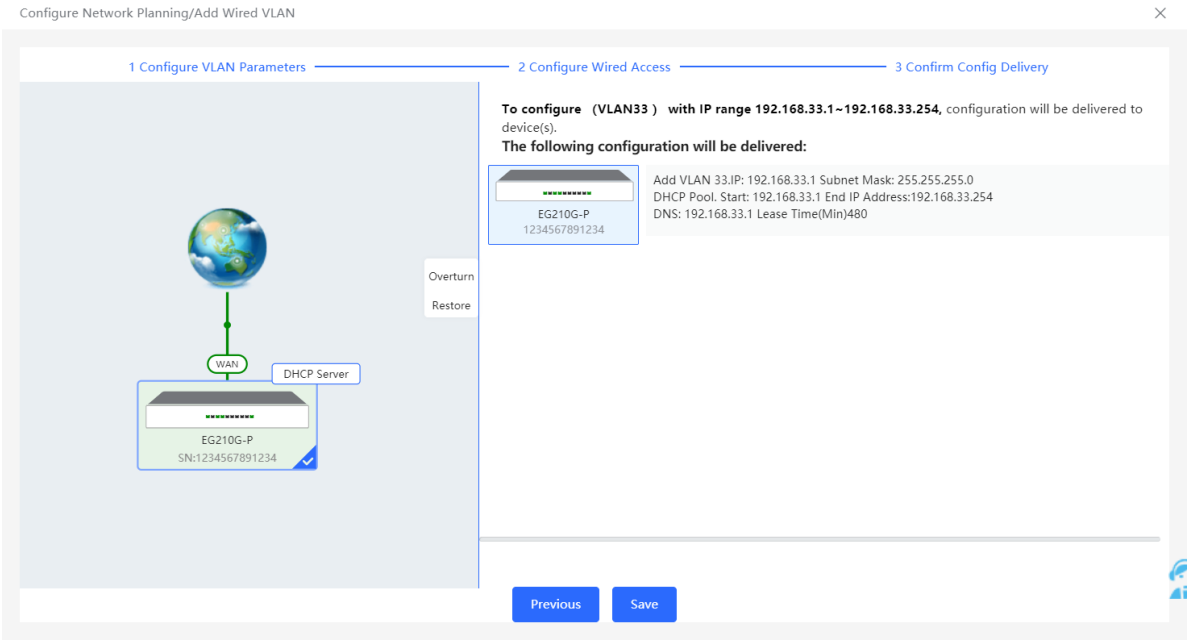
(2) Configure the VLAN ID, address pool server, and DHCP pool. The gateway is configured as the address pool server by default to assign IP addresses to clients. If an access switch exists in the network, you can select the access switch as the address pool server. Click **Next** after VLAN parameters are configured.



(3) Select the target switch in the topology and all member ports in the VLAN, and click **Next**.



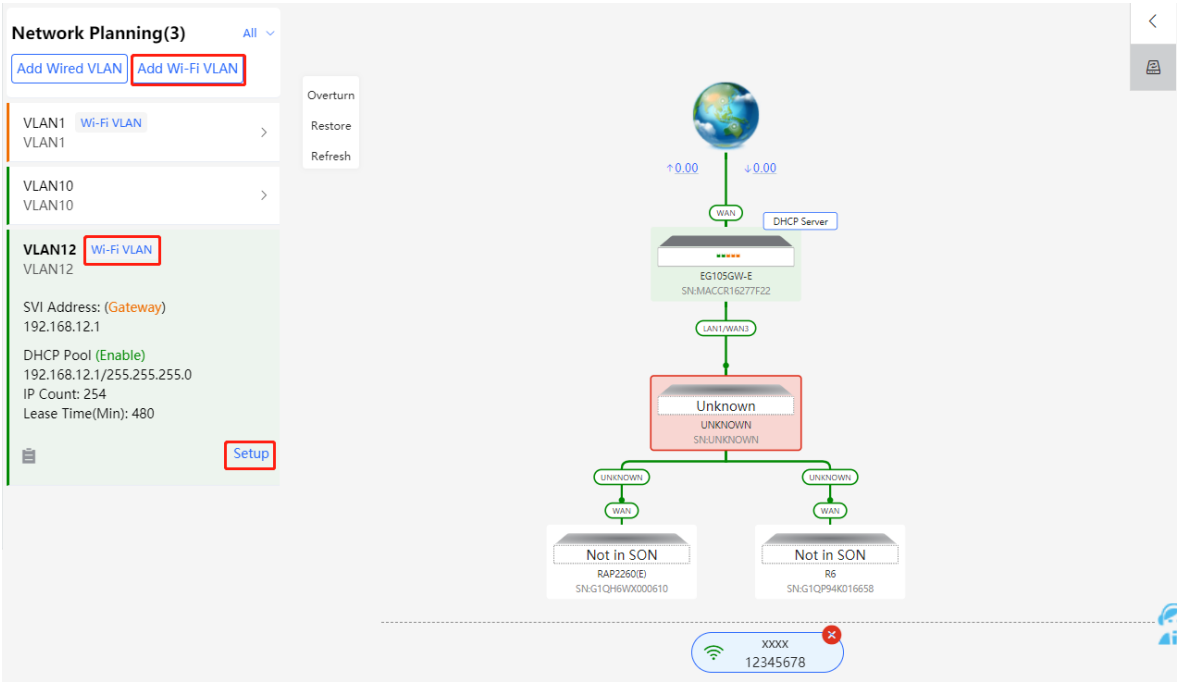
(4) Please confirm the delivered configurations and click **Save**. The configurations will take effect after a few minutes.



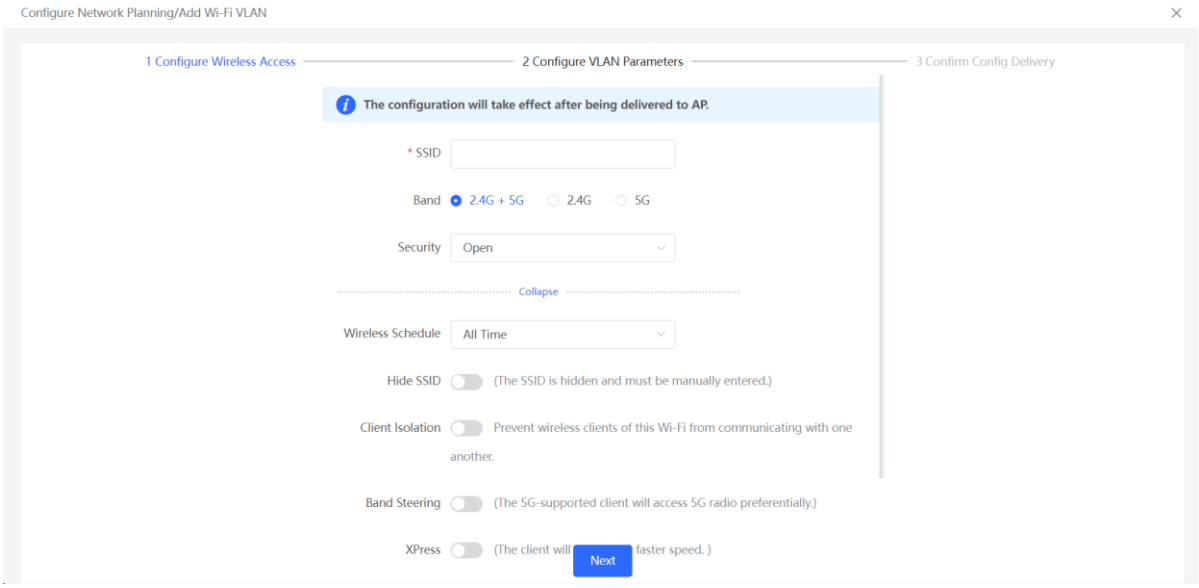
2.4.2 Configuring Wi-Fi VLAN

(1) Go to the **Wired VLAN** page for configuration.

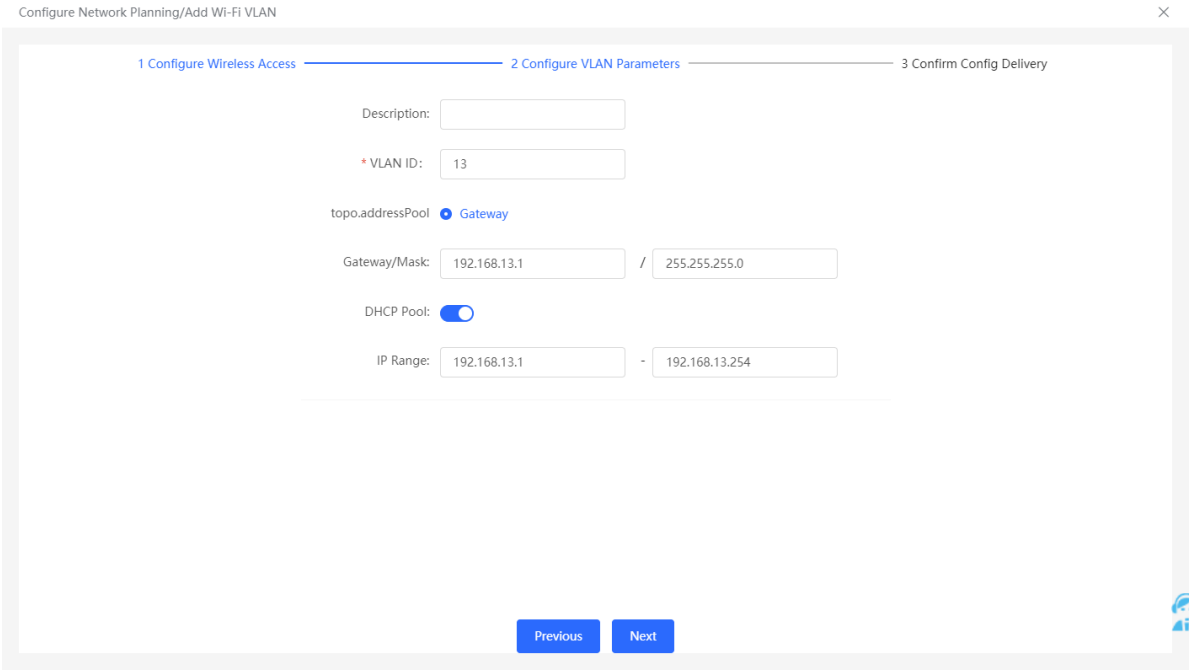
- Method 1: Click **Add** beside **Wi-Fi VLAN** in the **Network Planning** area on the **Overview** page to add the Wi-Fi VLANs.
- Method 2: Click **manage** in the **Network Planning** area on the **Overview** page to go to the **Network Planning** page for configuration (**Network** > **Network Planning**). Click **Add Wi-Fi VLAN** to add the Wi-Fi VLANs to the live network or select the available Wi-Fi VLANs. Click **Setup** to configure the Wi-Fi VLANs.



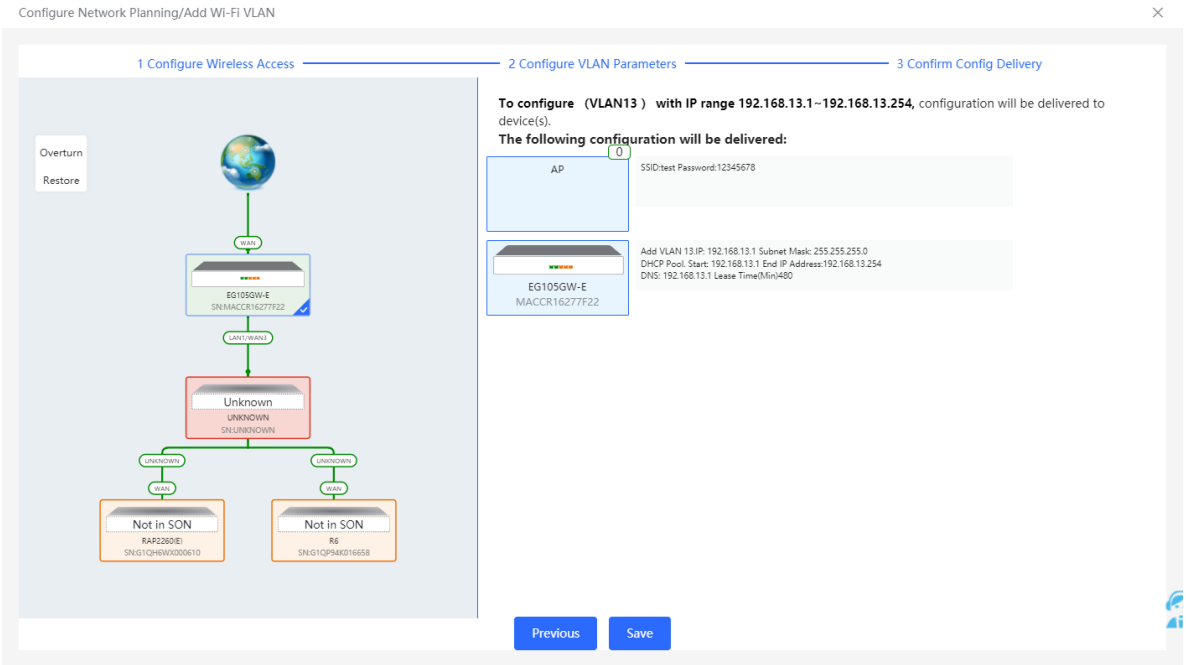
(2) Configure the SSID, Wi-Fi password and band. Click **Expand** to expand the advanced settings and set the parameters. Then, click **Next**.



(3) Configure the VLAN ID, address pool server and DHCP pool. The gateway is configured as the address pool server by default to assign IP addresses to clients. If an access switch exists in the network, you can select the access switch as the address pool server. Click **Next** after VLAN parameters are configured.

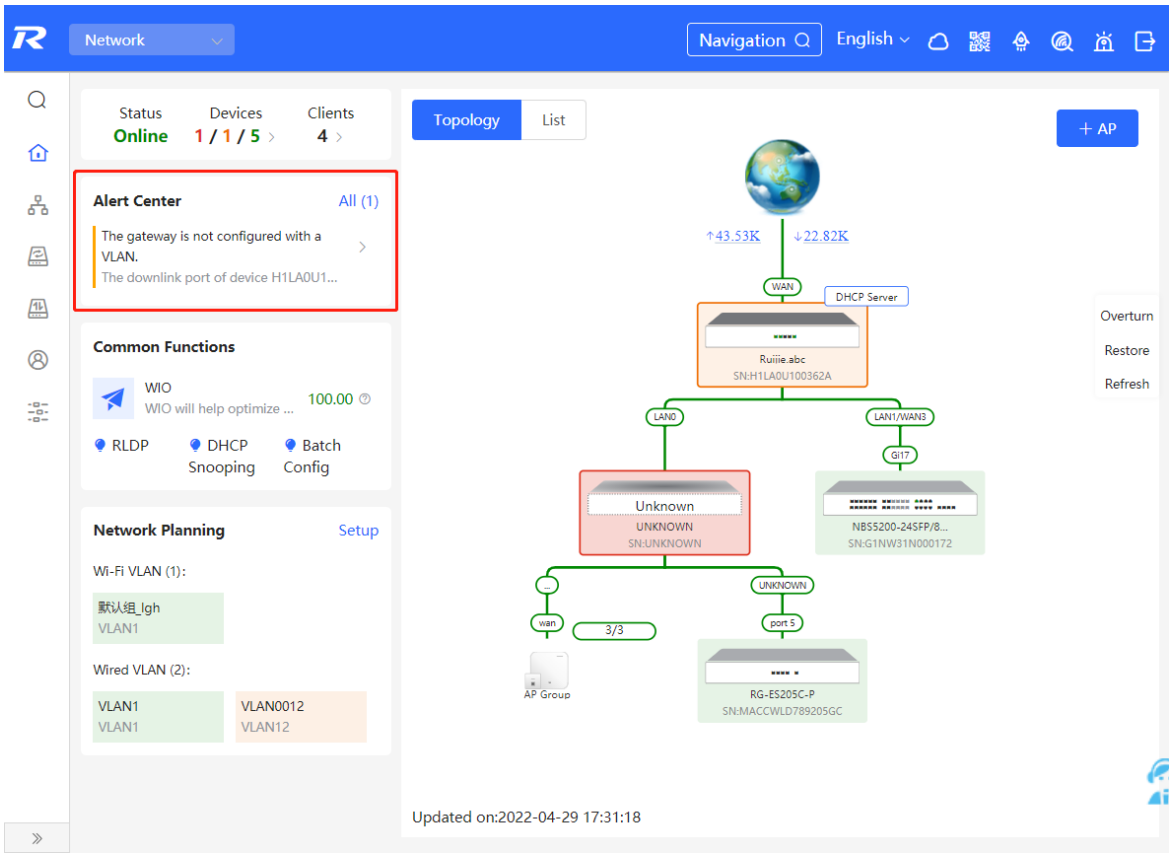


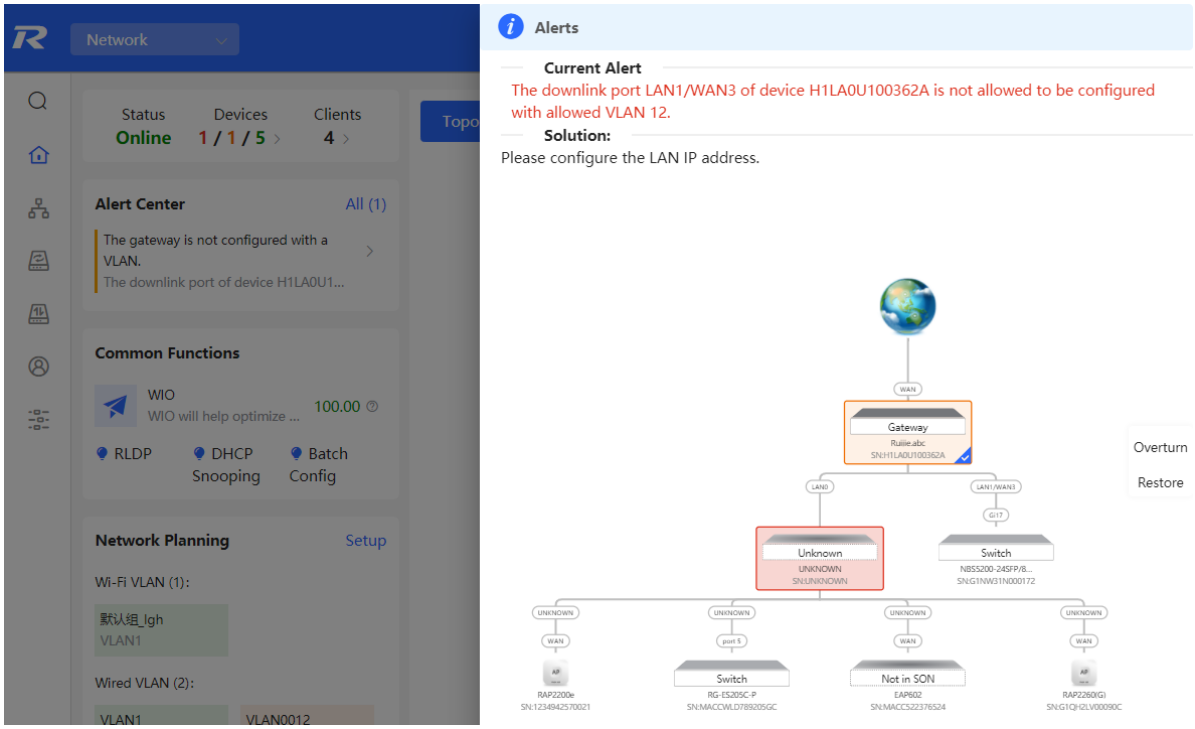
(4) Please confirm the delivered configurations and click **Save**. The configurations will take effect after a few minutes.



2.5 Troubleshooting Fault Alerts

The **Overview** page displays the fault alerts and handling suggestions if faults occur in the network. Click the fault alert in **Alert Center** to view the faulty device, fault details and handling suggestions, and troubleshoot device faults by referring to the handling suggestions.


Network
Navigation
English
Status
Online
Devices
1 / 1 / 5
Clients
4
Alert Center
All (1)
The gateway is not configured with a VLAN.
The downlink port of device H1LA0U1...
Common Functions
WIO
WIO will help optimize ...
100.00
RLDP
DHCP Snooping
Batch Config
Network Planning
Setup
Wi-Fi VLAN (1):
默认组_lgh
VLAN1
Wired VLAN (2):
VLAN1
VLAN1
VLAN0012
VLAN12
Topology
List
+ AP
↑43.53K
↓22.82K
WAN
DHCP Server
Ruijie.abc
SN:H1LA0U100362A
LAN0
LAN1/WAN3
Gi17
Unknown
UNKNOWN
SN:UNKNOWN
NBS5200-24SFP/8...
SN:G1NW31N000172
UNKNOWN
wan
3/3
port 5
AP Group
RG-ES205C-P
SN:MACCWLD789205GC
Overturn
Restore
Refresh
Updated on:2022-04-29 17:31:18


Network
Status
Online
Devices
1 / 1 / 5
Clients
4
Alert Center
All (1)
The gateway is not configured with a VLAN.
The downlink port of device H1LA0U1...
Common Functions
WIO
WIO will help optimize ...
100.00
RLDP
DHCP Snooping
Batch Config
Network Planning
Setup
Wi-Fi VLAN (1):
默认组_lgh
VLAN1
Wired VLAN (2):
VLAN1
VLAN0012
Alerts
Current Alert
The downlink port LAN1/WAN3 of device H1LA0U100362A is not allowed to be configured with allowed VLAN 12.
Solution:
Please configure the LAN IP address.
Gateway
Ruijie.abc
SN:H1LA0U100362A
Unknown
UNKNOWN
SN:UNKNOWN
Switch
NBS5200-24SFP/8...
SN:G1NW31N000172
Switch
RG-ES205C-P
SN:MACCWLD789205GC
Not in SON
EAP602
SN:MACC522376524
Overturn
Restore

3 Wi-Fi Network Settings

Note

Wi-Fi network settings covers the Wi-Fi settings of the currently logged in devices and the management of all wireless devices in the network. In Network mode, the Wi-Fi network settings are synchronized to all wireless devices in the network. You can configure device groups to limit the synchronization range. For details, see Configuring AP Groups.

3.1 Configuring AP Groups

3.1.1 Overview

After the self-organizing network is enabled, the device can act as the master AP/AC to perform batch configuration and management on the downlink APs in groups. Group the APs before the configurations are delivered.

Note

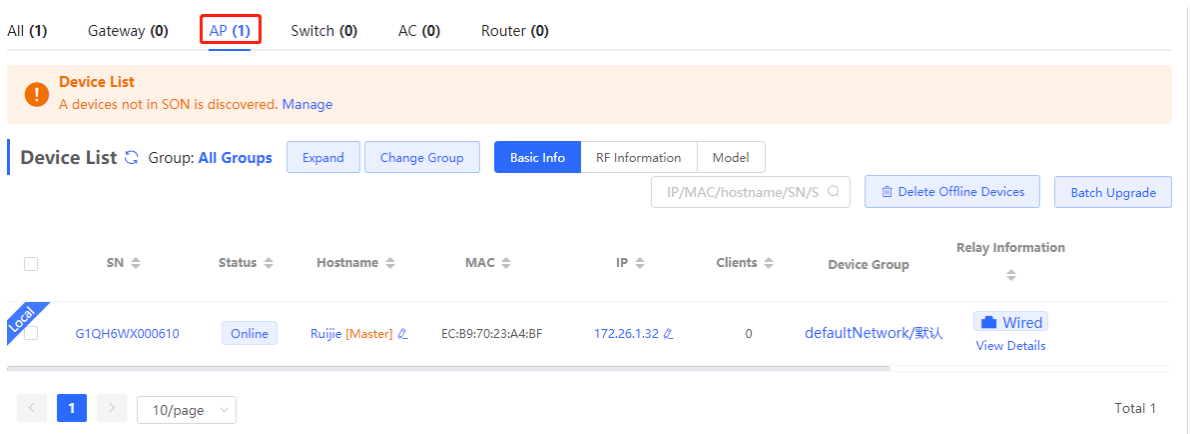
If you specify a group when setting up a wireless network, the corresponding configuration will take effect on the wireless devices in the specified group.

3.1.2 Procedures

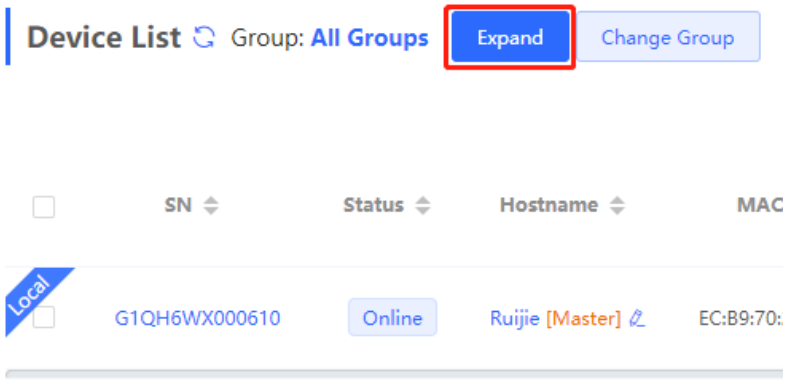
For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Network** mode, choose **Devices** > **AP**

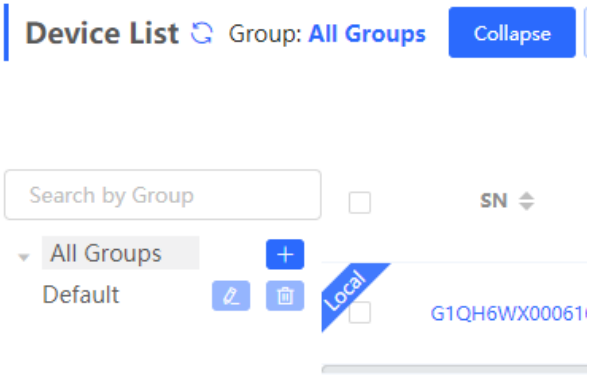
For other RAP models, choose **WLAN** > **APs**

(1) View the information of all APs in the current network, including the basic information, RF information and models. You can click **SN** to configure the device.

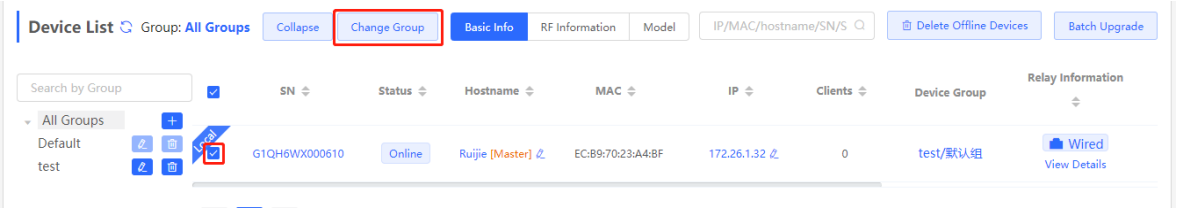


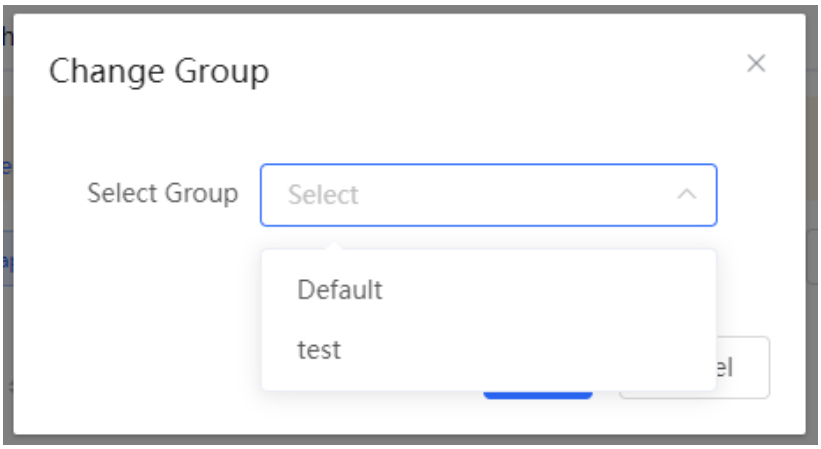
(2) Click **Expand** to view all groups on the left part of the **Device List** page. Click + to create a new group. Up to 8 groups can be added. You can click ✎ to edit the group name and click 🗑 to delete the group. The default group cannot be deleted and its name cannot be edited.





(3) Click the group name on the left part to view all devices in this group. A device can only belong to a group. By default, all devices belong to the default group. Select an entry in the list and click **Change Group** to move the target device to a specified group, and then the device will apply the configurations of this group. Click **Delete Offline Devices** to remove the offline device from the list.





3.2 Configuring SSID and Wi-Fi Password

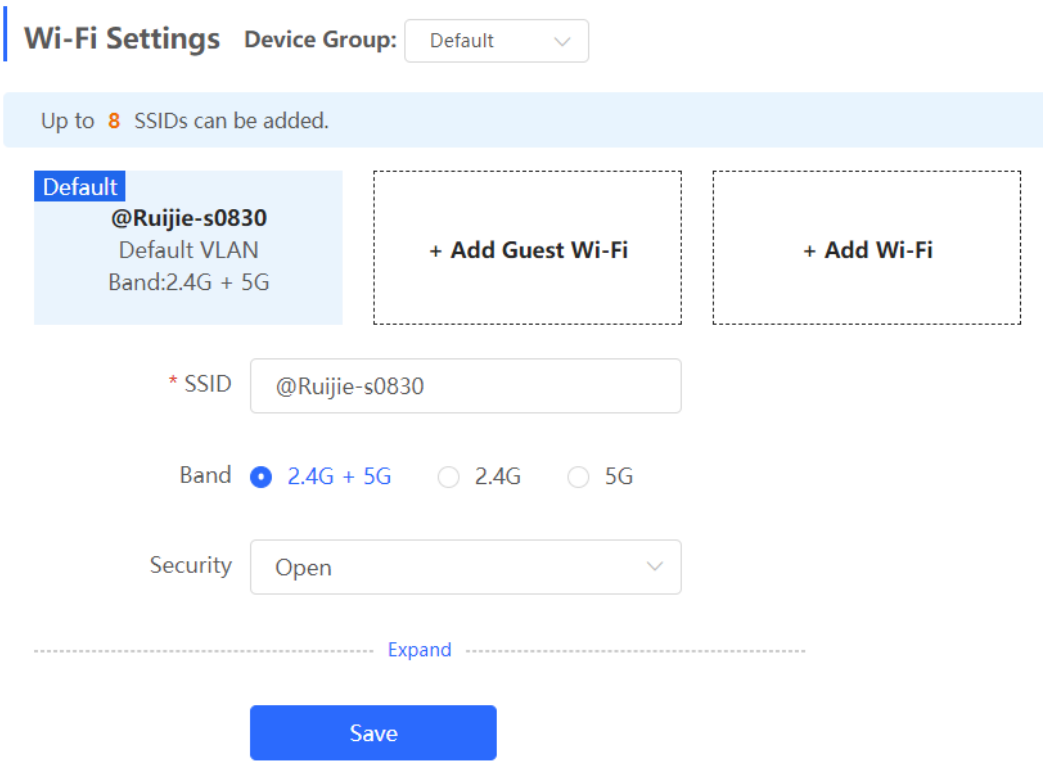
(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Click the target Wi-Fi network, change the SSID and Wi-Fi password of the Wi-Fi network, and click **Save**.

Caution

After the configuration is saved, all online clients will be disconnected from the Wi-Fi network. You have to enter the new password to connect to the Wi-Fi network.



3.3 Hiding the SSID

3.3.1 Overview

Hiding the SSID can prevent unauthorized clients from accessing the Wi-Fi network and enhance network security. After this function is enabled, the mobile phone or PC cannot search out the SSID. Instead, you have to manually enter the correct SSID and Wi-Fi password. Remember the SSID so that you can enter the correct SSID after the function is enabled.

3.3.2 Configuration Steps

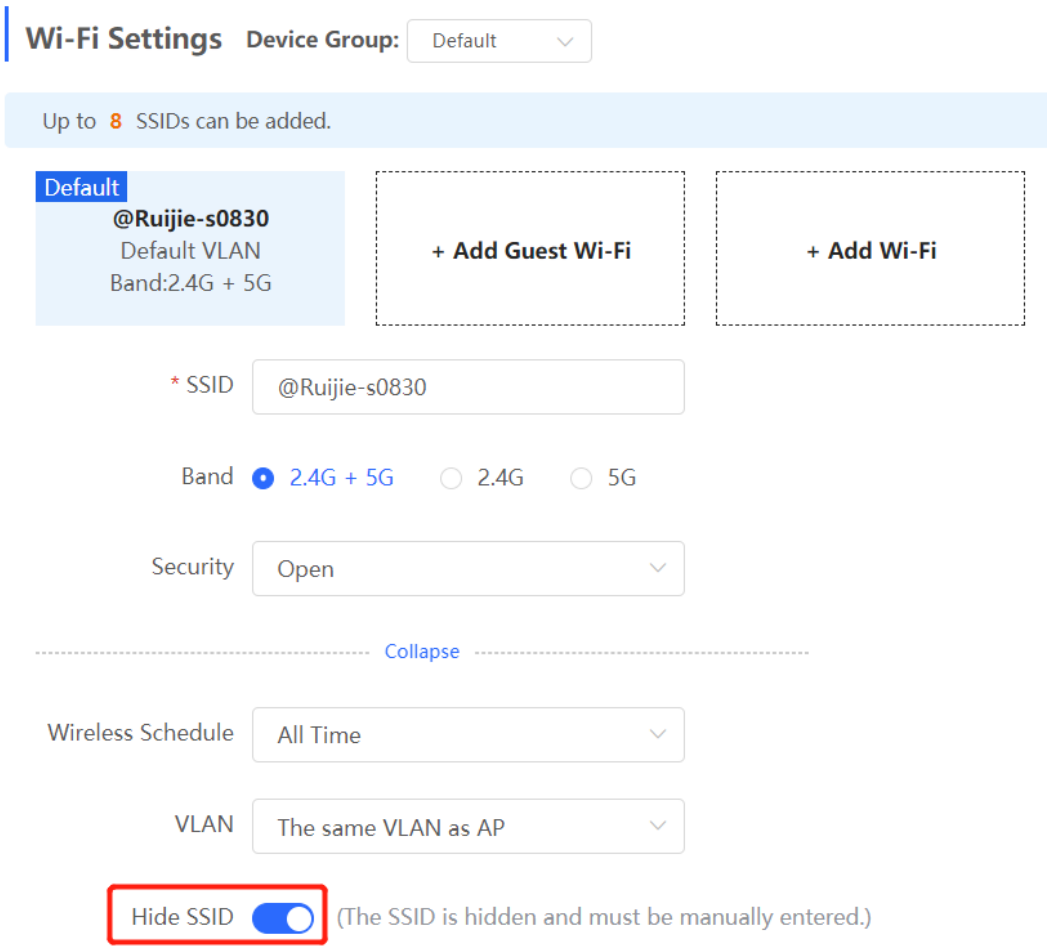
(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Click **Expand**, turn on **Hide SSID** in the expanded settings and click **Save**.

Caution

After the configuration is saved, you have to manually enter the SSID and Wi-Fi password before connecting any device to the Wi-Fi network. Therefore, exercise caution when performing this operation.



3.4 Checking Wireless Clients

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models:

If the self-organizing network is disabled, choose **WLAN** > **Clients**

If the self-organizing network is enabled, in **Network** mode, choose **Clients** > **Online Clients** > **Wireless**

For other RAP models:

Choose **WLAN** > **Clients**

Check information about all wireless clients connected to the Wi-Fi network. Click **Add to Blacklist** to disconnect a client and ban the client from accessing the Wi-Fi network.

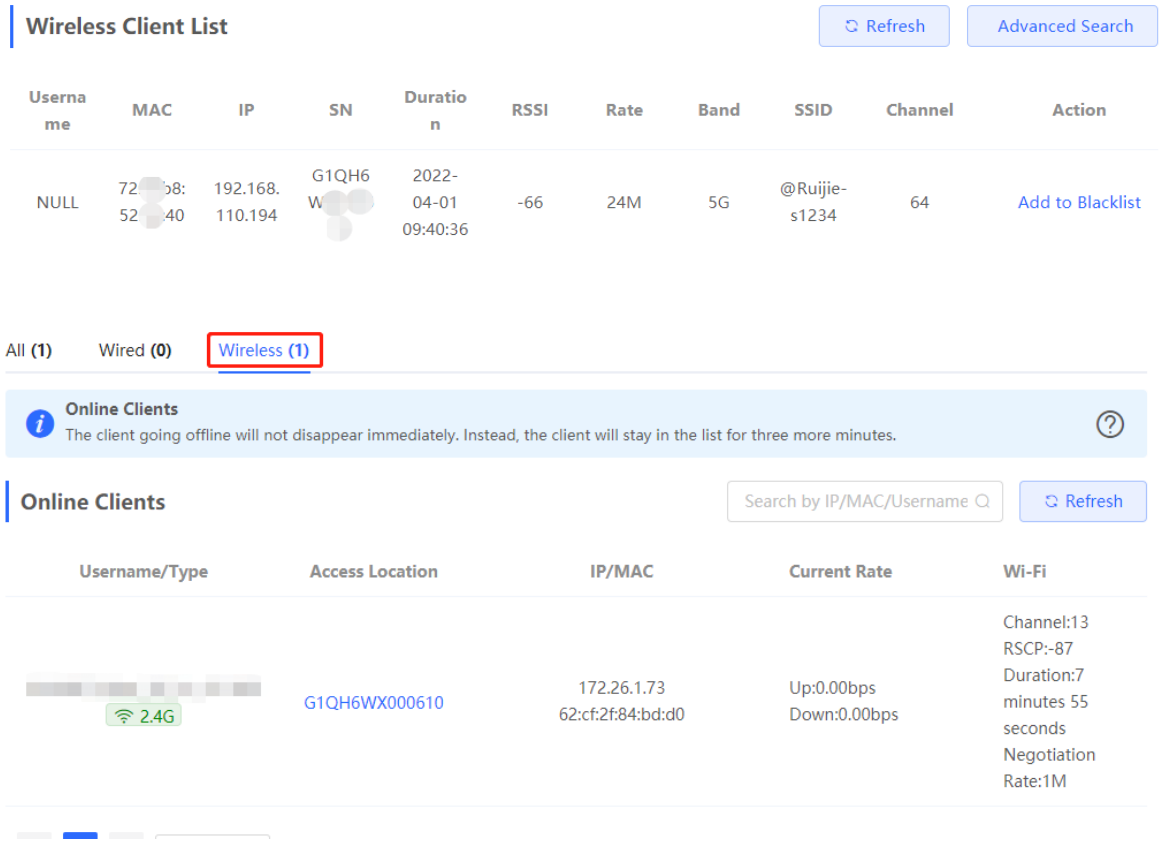


Table 3-1 Description of Wireless Client Information

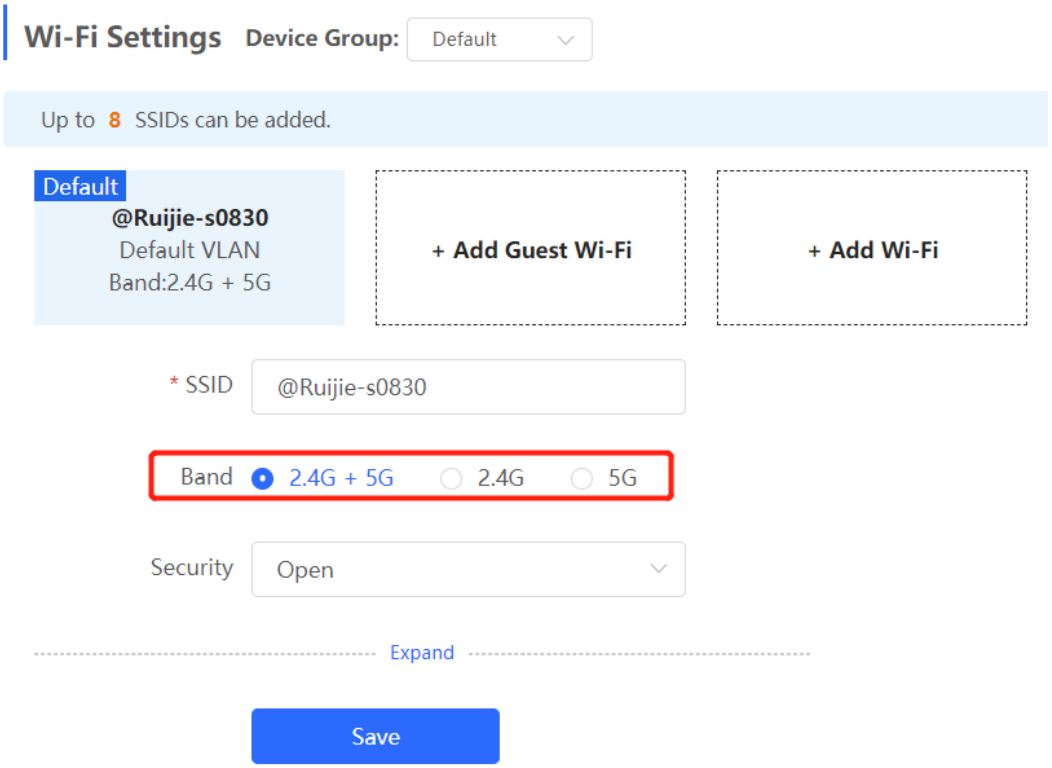
Item	Description
Username	Name of a client
MAC	MAC address of the client
IP	IPv4 address of the client
SN	SN of the device associated with the client
Duration	Time when the client connects to the Wi-Fi network
RSSI	RSSI of the Wi-Fi network associated with the client
Rate/Negotiation Rate	Association rate of the client and AP
Band	Band type of the Wi-Fi network, to which the client connects
SSID	Name of the Wi-Fi network associated with the client
Channel	Channel of the Wi-Fi network associated with the client
Current Rate	Uplink and downlink data rate.

3.5 Configuring Wi-Fi Band

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Set the band of Wi-Fi signals. The device supports the 2.4 GHz and 5 GHz bands. Compared with the 2.4 GHz band, the 5 GHz band supports a higher network transmission rate and is less susceptible to interference, but is inferior in signal coverage and through-wall penetration. You can select an appropriate signal band based on actual requirements. The default Wi-Fi band is **2.4G+5G**, indicating that Wi-Fi signals are emitted in both 2.4 GHz and 5 GHz bands.



3.6 Configuring Band Steering

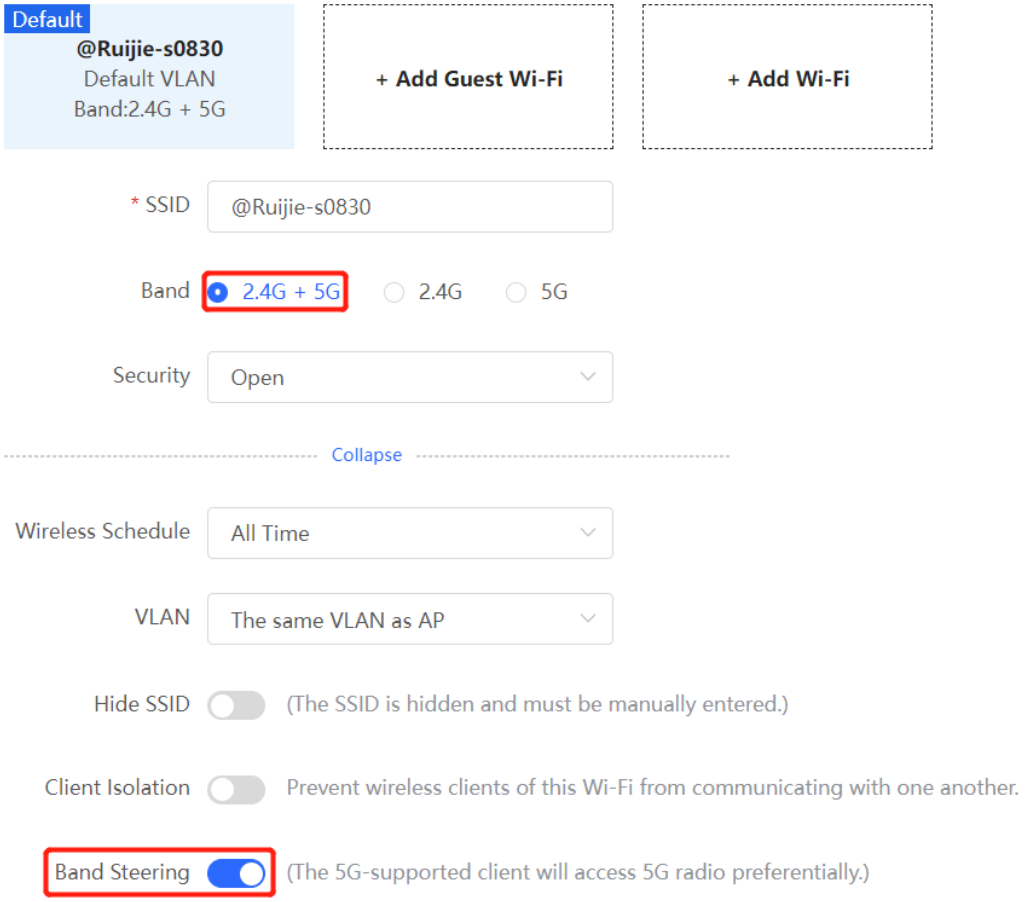
Caution

This function can be enabled only after the dual-band integration (**Band** is set to **2.4G+5G**) is enabled on the Wi-Fi network. A client automatically selects a band only when the SSIDs of the 2.4 GHz and 5 GHz bands are the same.

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Click **Expand**, turn on **Band Steering** in the expanded settings, and click **Save**. After the function is enabled, the client supporting 5 GHz selects the 5G Wi-Fi network preferentially.



3.7 Configuring Wi-Fi 6

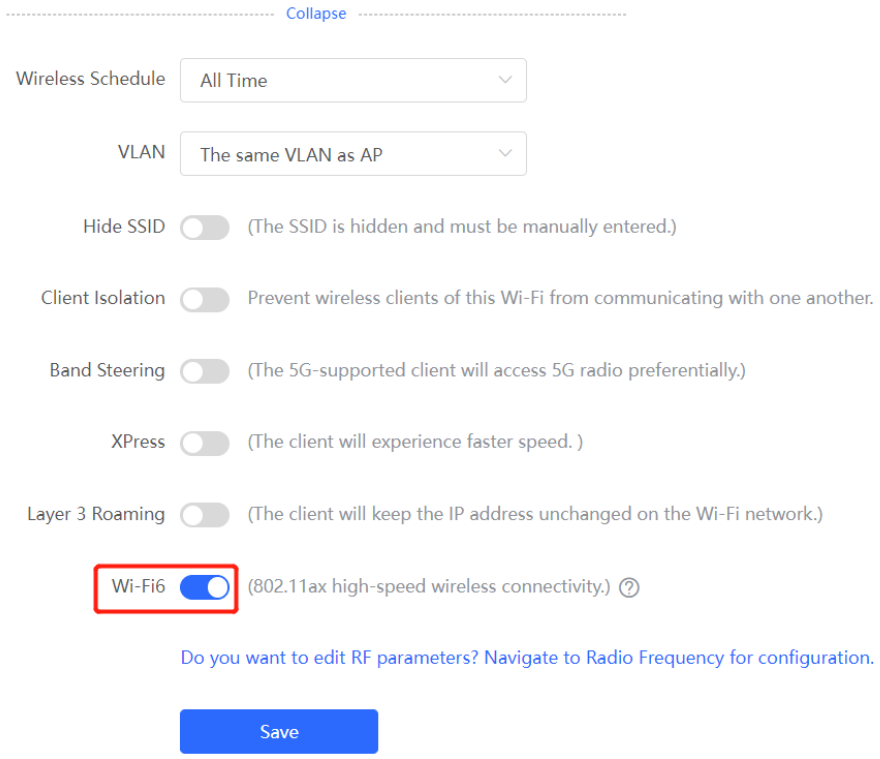
Caution

The function takes effect only on APs supporting the IEEE 802.11ax protocol. In addition, access clients must support IEEE 802.11ax so that clients can enjoy high-speed Internet access experience brought by Wi-Fi 6. If clients do not support Wi-Fi 6, you can disable this function.

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Click **Expand**, turn on **Wi-Fi6** in the expanded settings, and click **Save**. After this function is enabled, wireless clients can enjoy faster Internet access service.

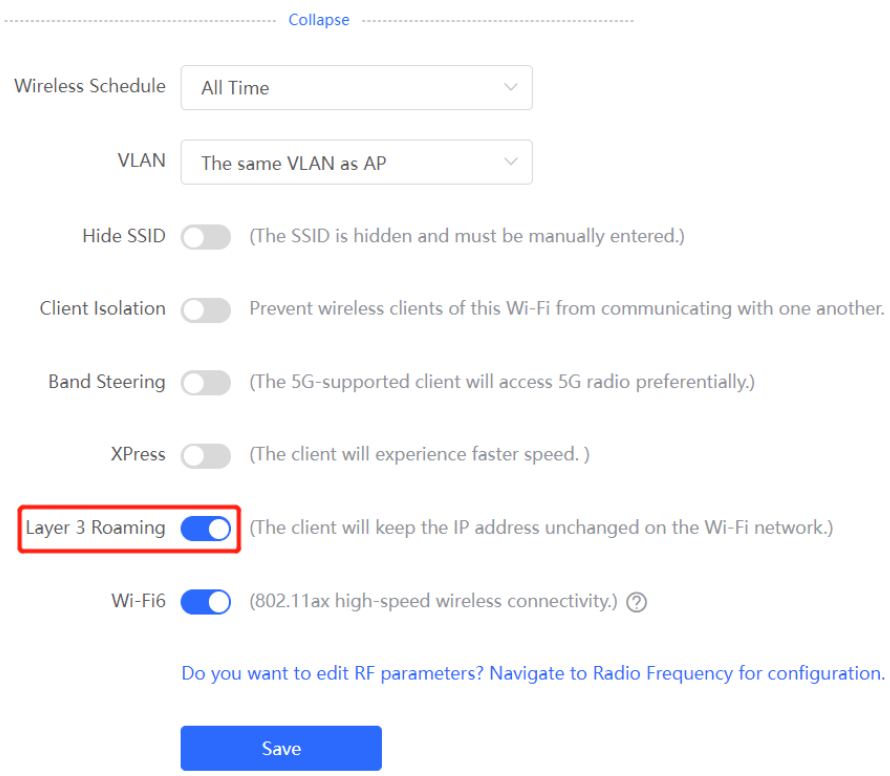


3.8 Configuring Layer-3 Roaming

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Click **Expand**, turn on **Layer 3 Roaming** in the expanded settings and click **Save**. The client will keep the IP address unchanged in this Wi-Fi network, improving roaming experience across VLANs.

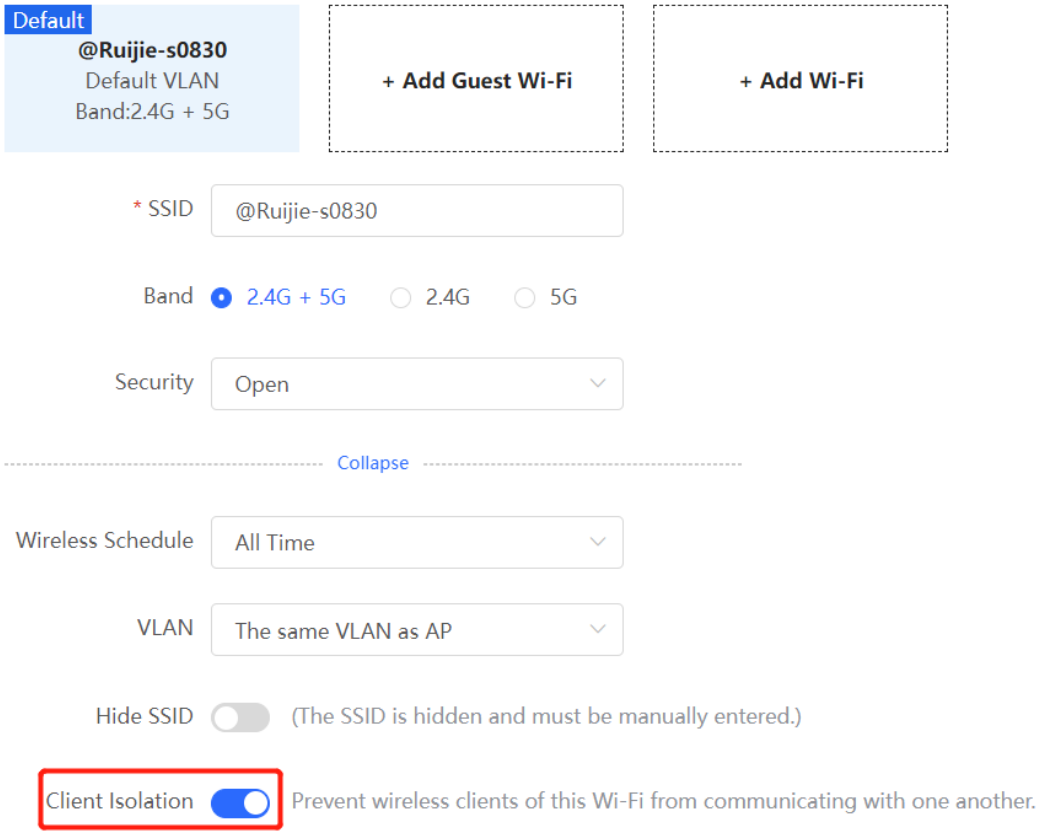


3.9 Configuring AP Isolation

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Click **Expand**, turn on **AP Isolation** in the expanded settings and click **Save**. The clients joining in this Wi-Fi network will be isolated. The clients associated with the same access point cannot access each other.

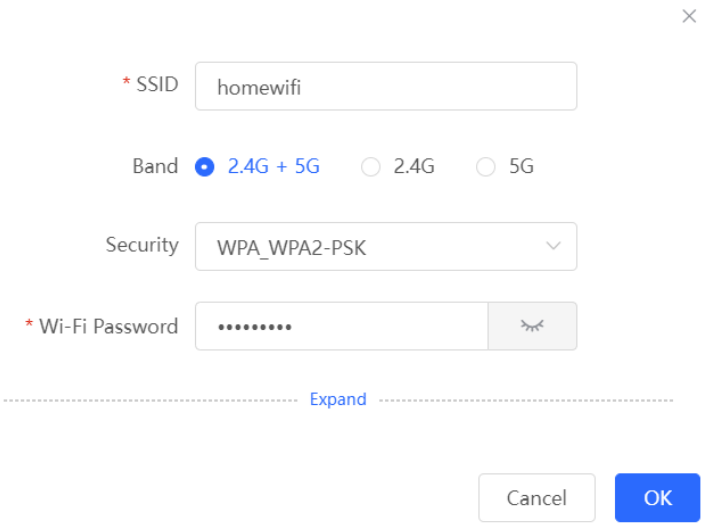


3.10 Adding a Wi-Fi Network

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi Settings**.
- Method 2: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi List**.

(2) Click **Add**, enter the SSID and Wi-Fi password and click **OK** to add a Wi-Fi network. Click **Expand** to configure more Wi-Fi features in the expanded settings. After the Wi-Fi network is added successfully, it will be displayed in the list. The client will be able to scan the new Wi-Fi network.



3.11 Configuring a Guest Wi-Fi

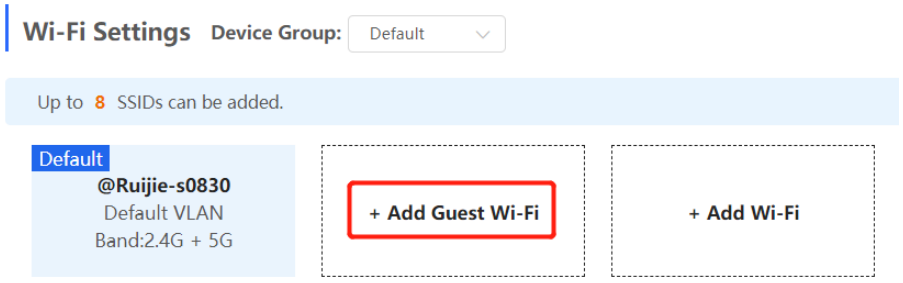
3.11.1 Overview

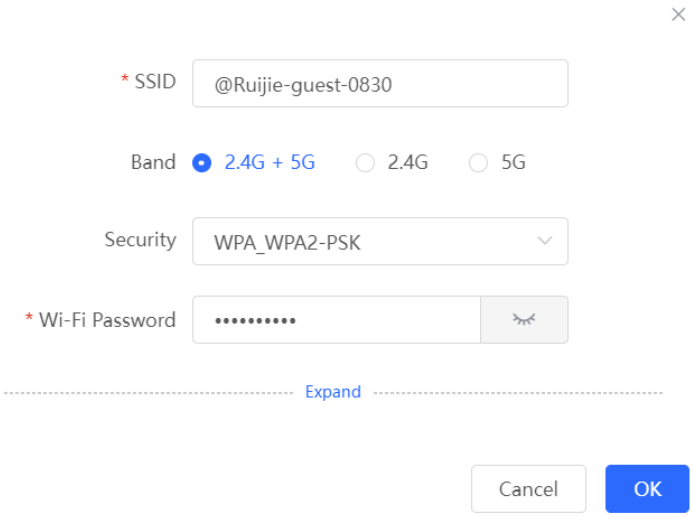
This Wi-Fi network is provided for guests and is disabled by default. It supports client isolation, that is, access clients are isolated from each other. They can only access the Internet via Wi-Fi, but cannot access each other, improving security. The guest Wi-Fi network can be turned off as scheduled. When the time expires, the guest network is off.

3.11.2 Configuration Steps

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

Click **Add Guest Wi-Fi** to configure the SSID and password of the Guest Wi-Fi. Click **Expand** to configure the effective time period and other Wi-Fi features in the expanded settings. Click **Save**, and the guest Wi-Fi network will be created. Guests can access the guest Wi-Fi network by entering the SSID and Wi-Fi password.





3.12 Configuring Wi-Fi Blacklist or Whitelist

3.12.1 Overview

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

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

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

Caution

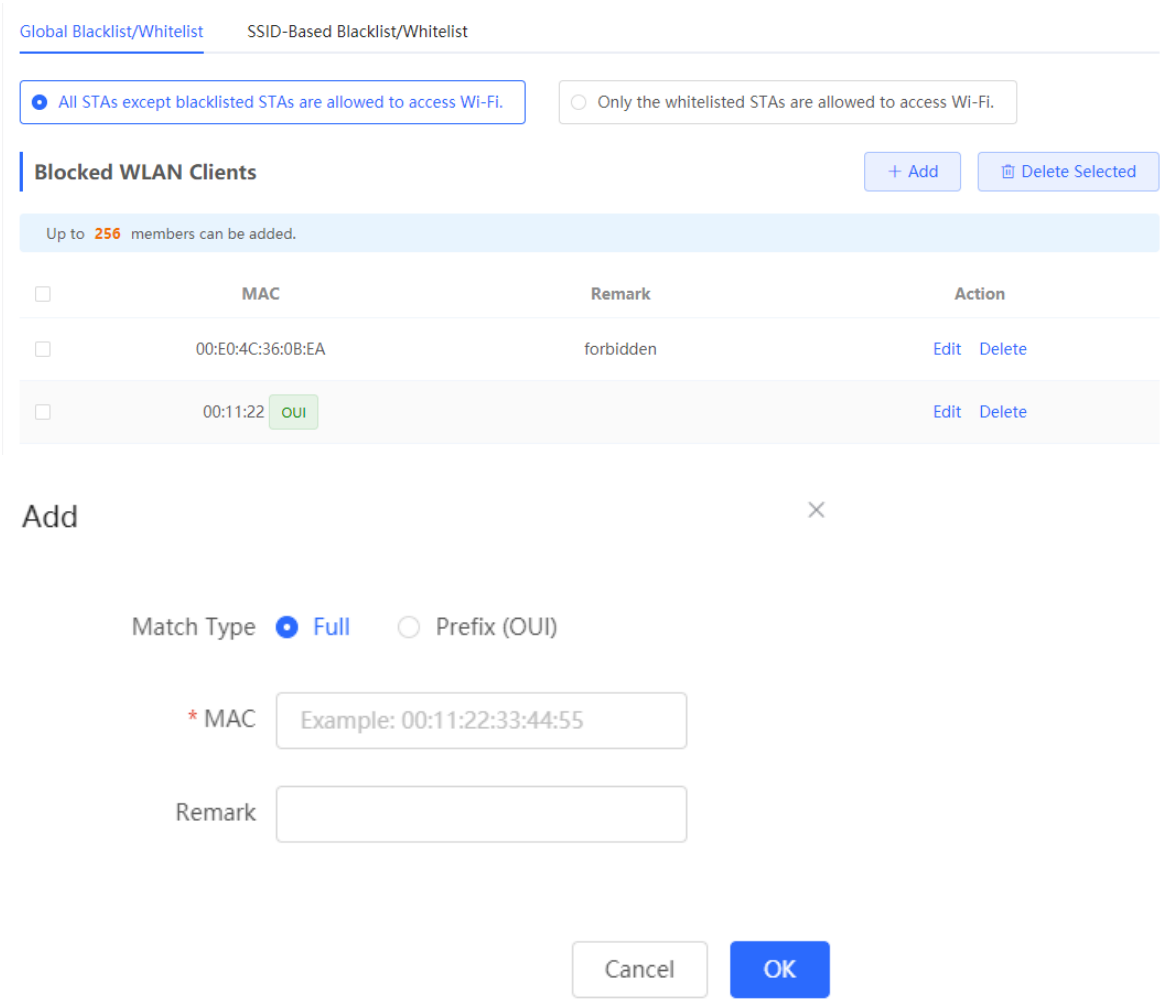
If the whitelist is empty, the whitelist does not take effect. In this case, all clients are allowed to access the Internet.

3.12.2 Configuration Steps

1. Configuring a Global Blacklist/Whitelist

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

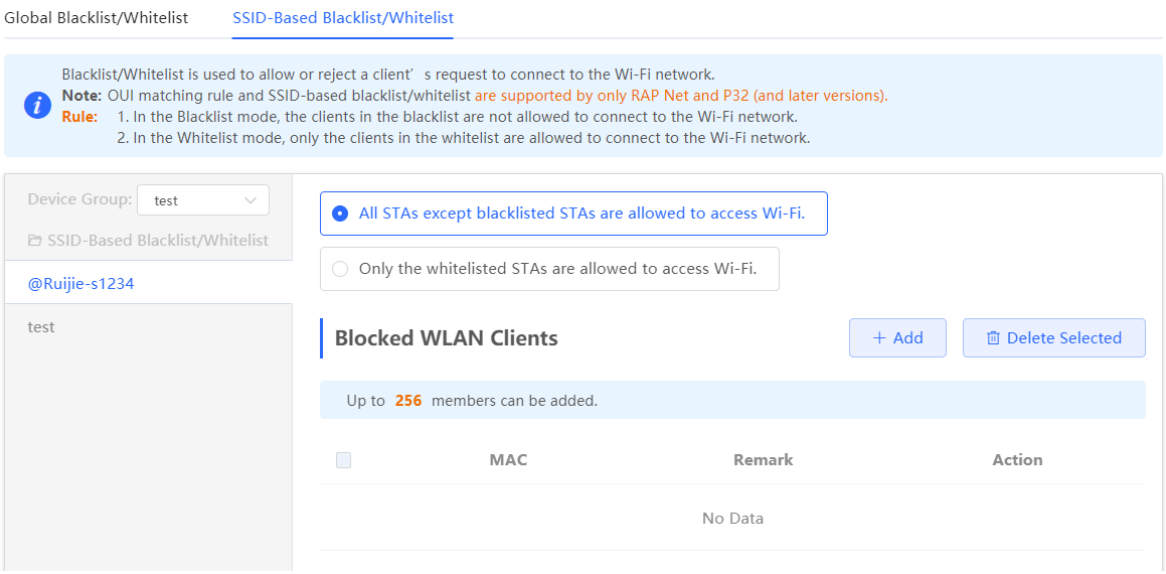
Select the blacklist or whitelist mode and click **Add** to configure a blacklist or whitelist client. In the **Add** window, enter the MAC address and remark of the target client and click **OK**. If a client is already associated with the access point, its MAC address will pop up automatically. Click the MAC address directly for automatic input. All clients in the blacklist will be forced offline and not allowed to access the Wi-Fi network. The global blacklist and whitelist settings take effect on all Wi-Fi networks of the access point.



2. Configuring an SSID-based Blacklist/Whitelist

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

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



3.13 Optimizing Wi-Fi Network

3.13.1 Overview

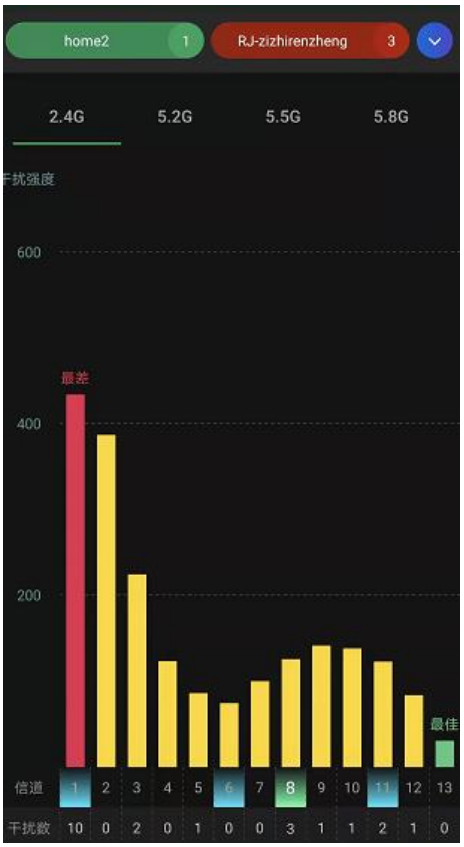
The device detects the surrounding wireless environment and selects the appropriate configuration upon power-on. However, network stalling caused by wireless environment changes cannot be avoided. You can optimize the network with one single click, analyze the wireless environment around the access point and select appropriate parameters.

Caution

After being optimized, the Wi-Fi network will restart, and clients need to reconnect to the W-Fi network. Therefore, exercise caution when performing this operation.

3.13.2 Getting Started

Install Wi-Fi Moho or other Wi-Fi scanning app on the mobile phone and check interference analysis results to find out the best channel.



3.13.3 Optimizing the Radio Channel

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models:

- Configure the master device. Choose **Network** (**WLAN**) > **Radio Frequency**
- Configure the slave device. Choose **Devices** > Select the target device in the device list and click **SN** > **Radio Frequency**

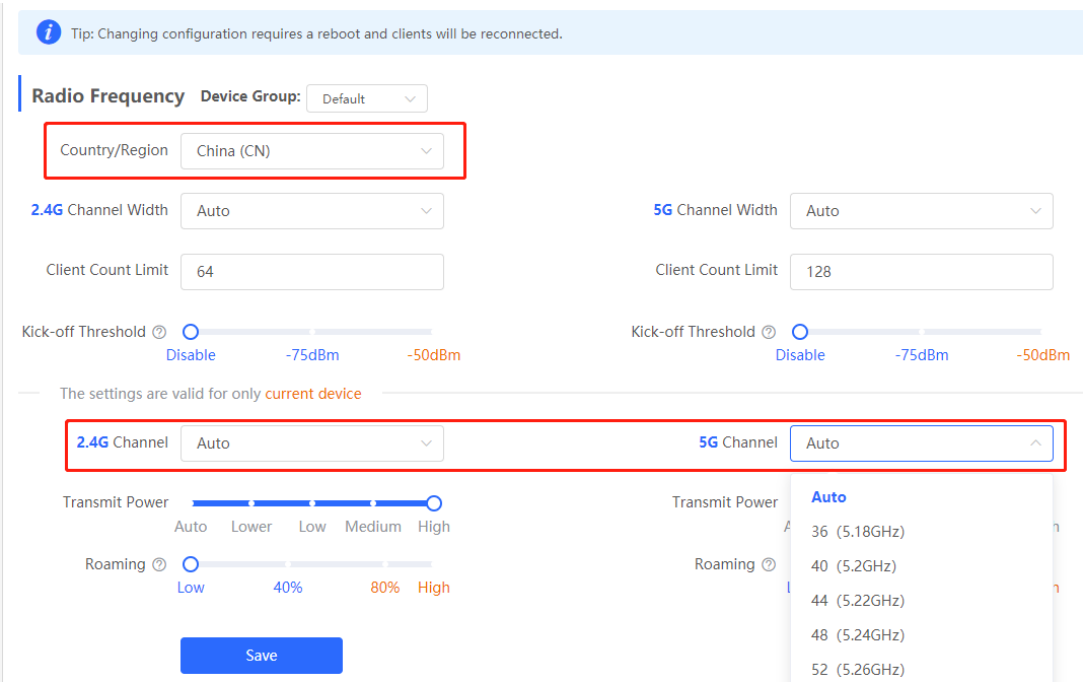
For other RAP models:

- Configure the master device. Choose **WLAN** > **Radio Frequency**
- Configure the slave device. Choose **WLAN** > **APs** > Select the target device in the device list and click **Manage** > **WLAN** > **Radio Frequency**

Choose the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. The more devices in a channel, the greater the interference.

Note

The available channel is related to the country or region code. Select the local country or region.



3.13.4 Optimizing the Channel Width

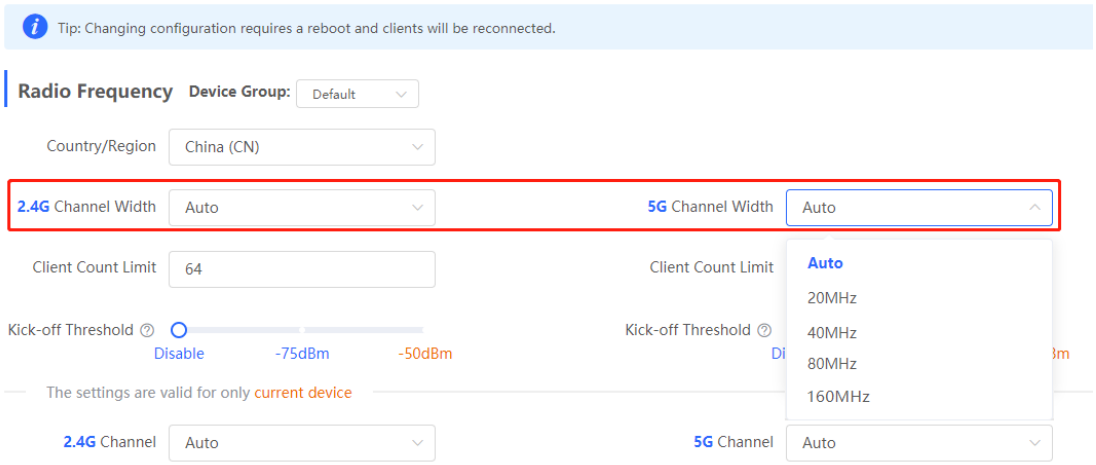
Choose **Network** (**WLAN**) > **Radio Frequency**.

A network with a lower channel width is more stable, while a network with a higher channel width is susceptible to interference. If the interference is severe, choose a lower channel width to avoid network stalling to a certain extent. The access point supports the channel width of 20 MHz and 40 MHz in the 2.4 GHz channel, and the channel width of 20 MHz and 40 MHz and 80 MHz and 160 MHz in the 5 GHz channel.

The default value is **Auto**, indicating that the channel width is automatically selected based on the environment. After changing the channel width, click **Save** to make the configuration take effect immediately.

Caution

In the self-organizing network mode, the channel width settings will be synchronized to all devices in the network.



3.13.5 Optimizing the Transmit Power

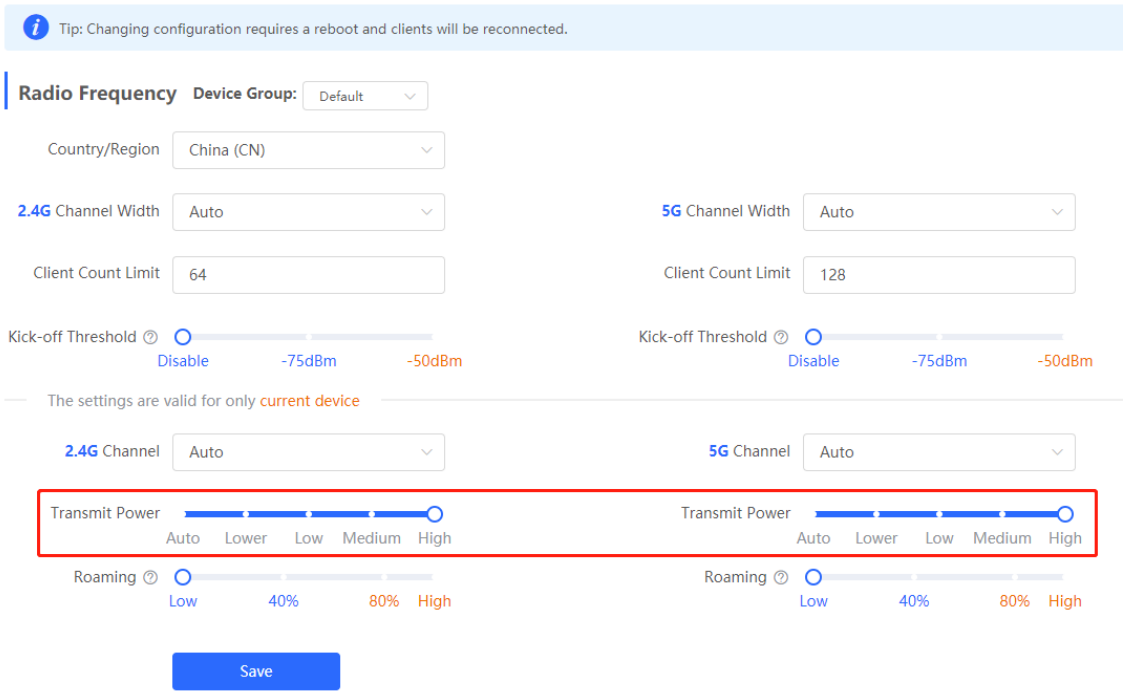
For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models:

- Configure the master device. Choose **Network** (**WLAN**) > **Radio Frequency**
- Configure the slave device. Choose **Devices** > Select the target device in the device list and click **SN** > **Radio Frequency**

For other RAP models:

- Configure the master device. Choose **WLAN** > **Radio Frequency**
- Configure the slave device. Choose **WLAN** > **APs** > Select the target device in the device list and click **Manage** > **WLAN** > **Radio Frequency**

A greater transmit power indicates a larger coverage and brings stronger interference to surrounding wireless routers. In a high-density scenario, you are advised to set the transmit power to a small value. The **Auto** mode is recommended, indicating automatic adjustment of the transmit power.

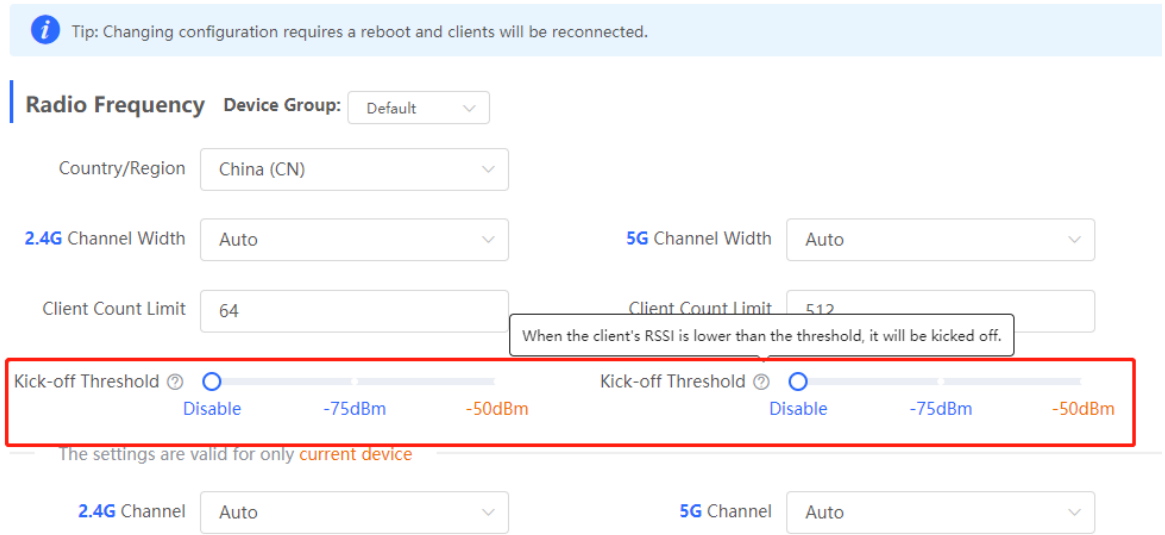


3.13.6 Configuring the Kick-off Threshold

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

In the case of multiple Wi-Fi signals, setting the kick-off threshold can improve the wireless signal quality to a certain extent. The farther the client is away from the access point, the lower the signal strength is. If the signal is lower than the kick-off threshold, the Wi-Fi will be disconnected, and the client will be forced offline and select a nearer Wi-Fi signal.

However, the higher the kick-off threshold is, the easier it is for the client to be kicked offline. To ensure normal Internet access, you are advised to disable the kick-off threshold or set the value to less than -75dBm.



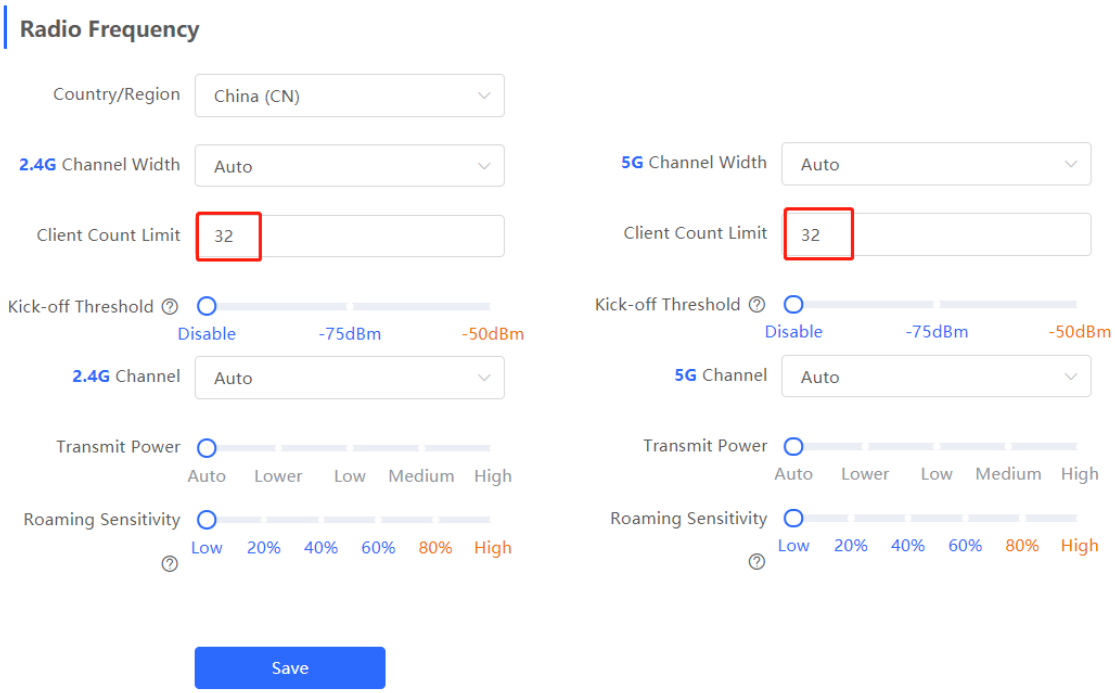
Caution

In the self-organizing network mode, the kick-off threshold settings will be synchronized to all devices in the network.

3.13.7 Configuring the Client Limit

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

If the access point is associated with too many clients, it will have a lower performance, affecting user experience. After you configure the threshold, new clients over the threshold will not be allowed to access the Wi-Fi network. You can lower the threshold if there is requirement for bandwidth per client. You are advised to keep the default settings unless there are special cases.



Note

In the self-organizing network mode, the client limit refers to the maximum number of clients accessing all Wi-Fi networks in the current AP group.

3.13.8 Configuring the Roaming Sensitivity

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models:

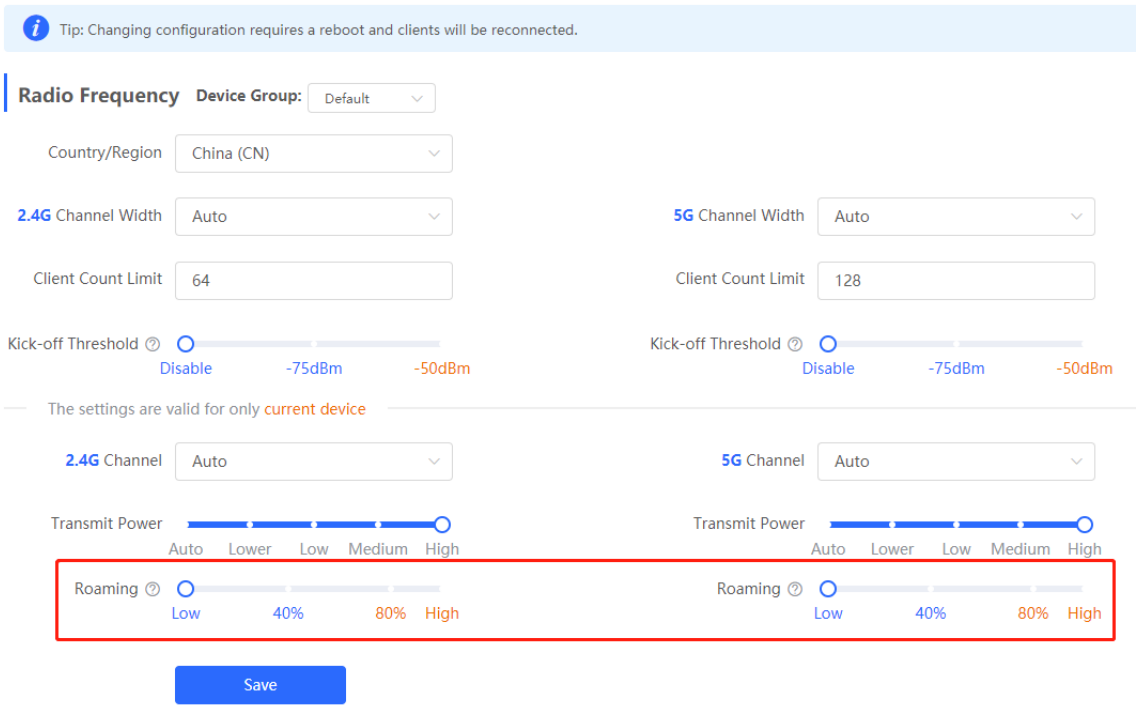
- Configure the master device. Choose **Network** (**WLAN**) > **Radio Frequency**

- Configure the slave device. Choose **Devices** > Select the target device in the device list and click **SN** > **Radio Frequency**

For other RAP models:

- Configure the master device. Choose **WLAN** > **Radio Frequency**
- Configure the slave device. Choose **WLAN** > **APs** > Select the target device in the device list and click **Manage** > **WLAN** > **Radio Frequency**

The roaming sensitivity enables the device to actively disconnect a client from the Wi-Fi network when the client is far away, forcing the client to re-select the nearest signal and thus improving the sensitivity of wireless roaming. Higher the roaming sensitivity level, smaller the wireless signal coverage. To improve the signal quality for a client moving within more than one Wi-Fi coverage, improve the roaming sensitivity level. You are advised to keep the default settings.



3.13.9 Configuring WIO

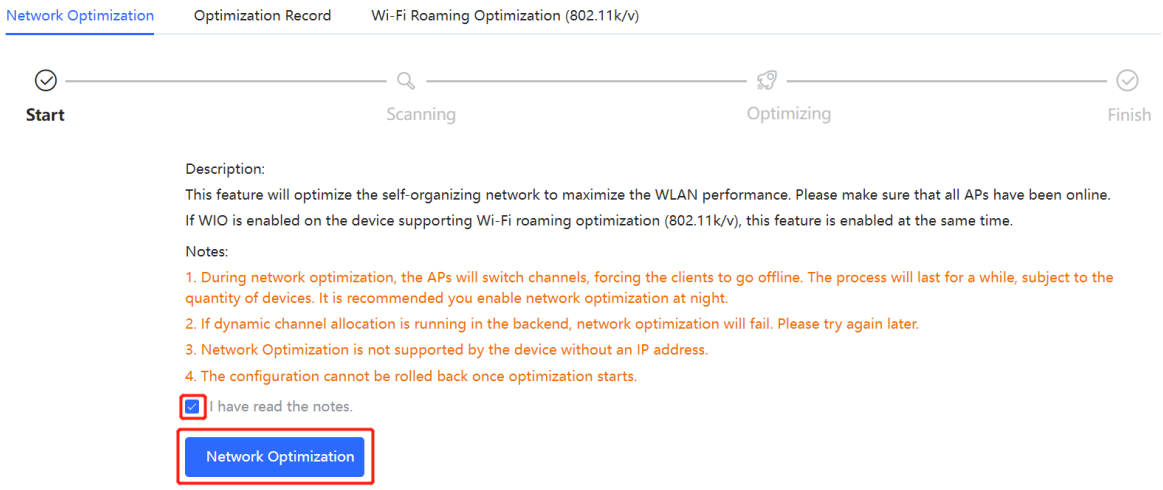
For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Network** mode, choose **Network** >**WIO**

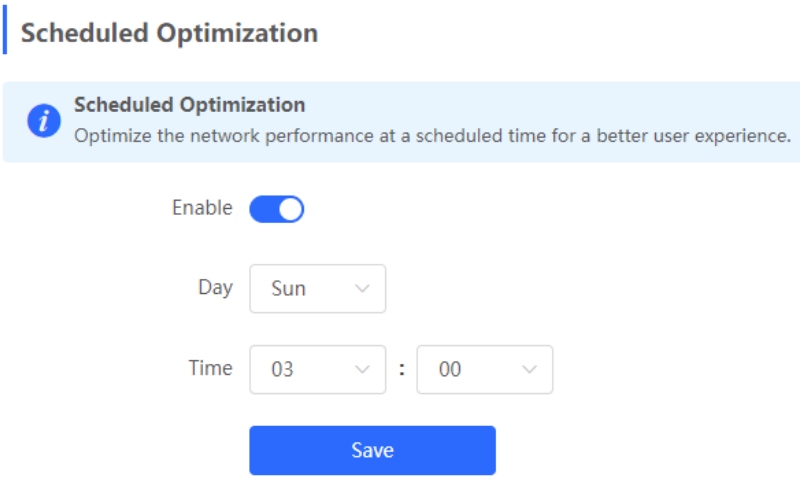
For other RAP models: Choose **WLAN** > **WIO**

Check **I have read the notes.** And click **Network Optimization** to optimize the wireless network. You are advised to set a scheduled task to optimize the wireless network in the early hours of the morning or when the network is idle.

Caution

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





3.13.10 Configuring Wi-Fi Roaming Optimization (802.11k/v)

Note

The functions mentioned in this chapter are not applicable to such models as RG-RAP1200(F), and RG-RAP2200(F).

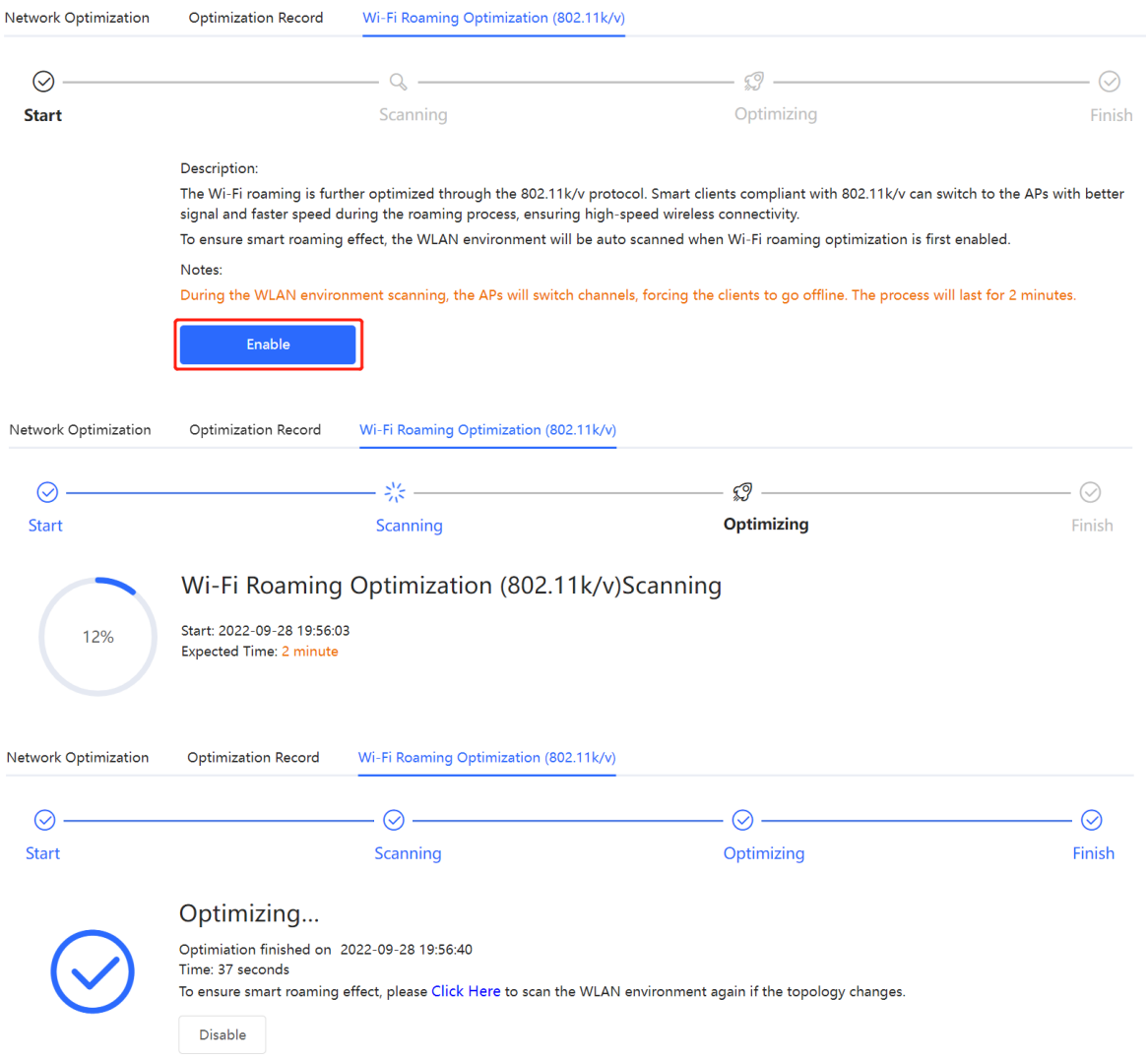
For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Network** mode, choose **Network** > **WIO** > **Wi-Fi Roaming Optimization (802.11k/v)**.

For other RAP models: Choose **WLAN** > **WIO** > **Wi-Fi Roaming Optimization (802.11k/v)**.

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

Caution

- WIO is supported only in the self-organizing network mode.
- During the WLAN environment scanning, the APs will switch channels, forcing the clients to go offline. The process will last for 2 minutes.

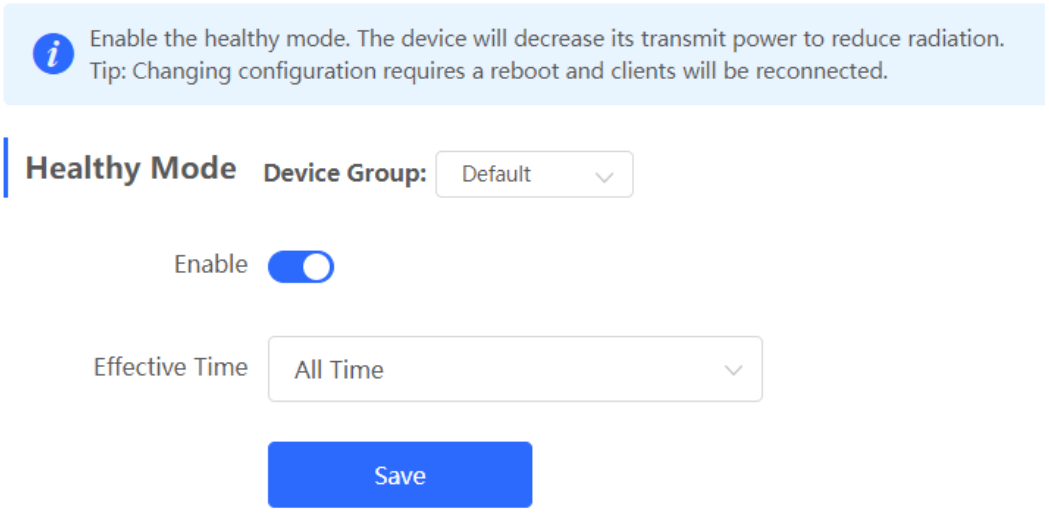


3.14 Configuring Healthy Mode

Choose **Network** (**WLAN**) > **Wi-Fi** > **Healthy Mode**.

Select **Device Group** from the drop-down list box. Click **Enable** to enable the healthy mode. You are allowed to set the effective time period for the healthy mode.

After the healthy mode is enabled, the transmit power and the Wi-Fi coverage area will decrease. The healthy mode may reduce signal strength and cause network stalling. You are advised to disable it or enable it when the network is idle.

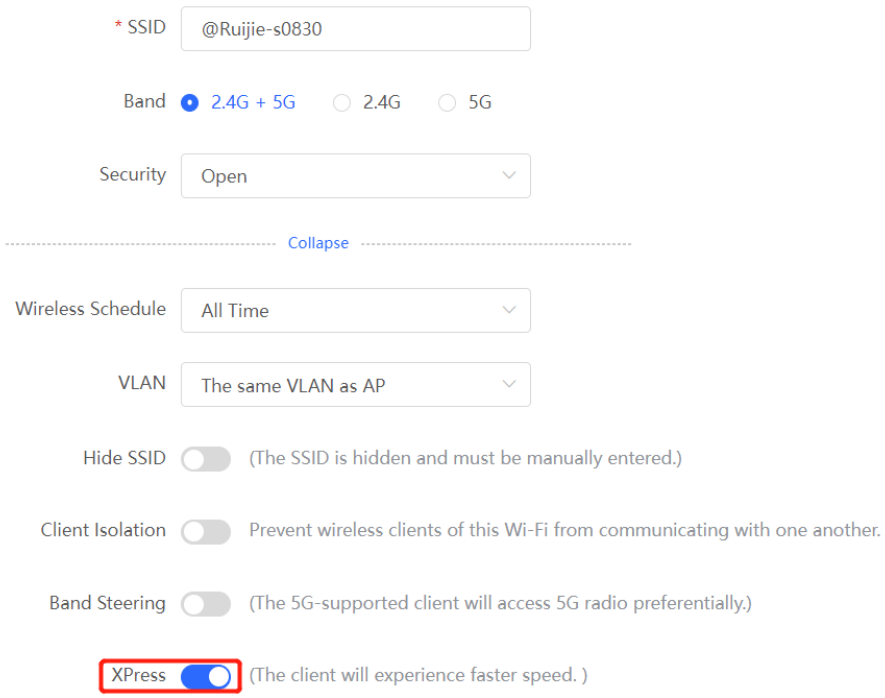


3.15 Configuring XPress

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Click **Expand**, turn on **XPress** in the expanded settings and click **Save**. After XPress is enabled, the gaming traffic will be prioritized, ensuring a more stable gaming experience.

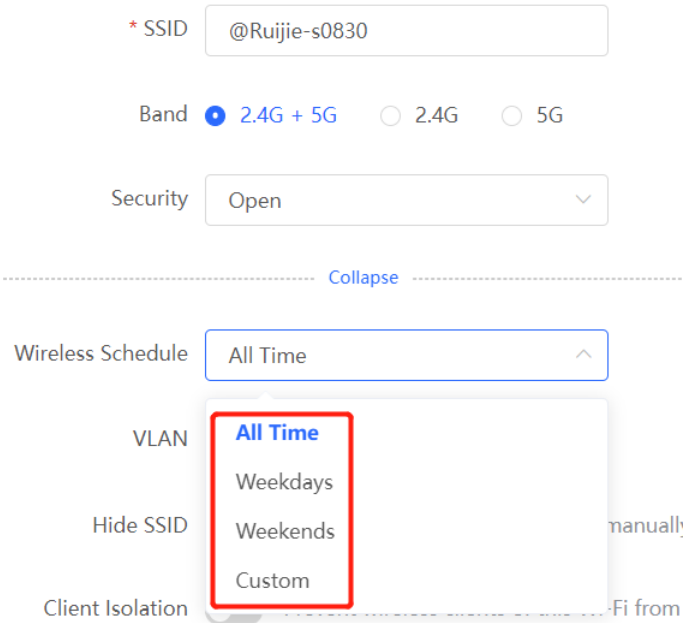


3.16 Configuring Wireless Schedule

(1) Go to the page for configuration.

- Method 1: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi Settings**. Select the target Wi-Fi.
- Method 2: Choose **Network** (**WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action column.

(2) Click **Expand**, select a scheduled time span to turn on Wi-Fi and click **Save**. Clients will be allowed to access the Internet only in the specified time span.

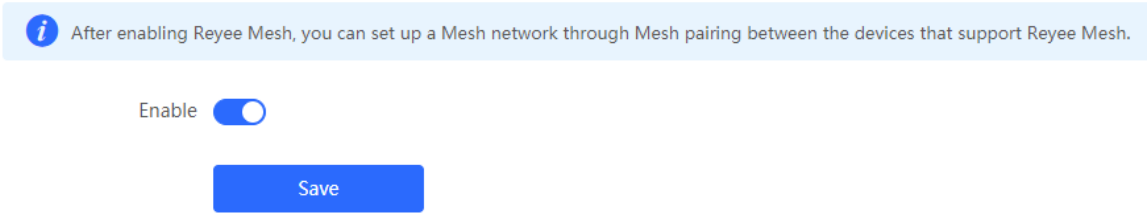


3.17 Enabling Reyee Mesh

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Network** mode, choose **Network** > **Reyee Mesh**

For other RAP models: Choose **WLAN** > **APs** > **Manage** > **Advanced** > **Reyee Mesh**

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



3.18 Configuring AP Load Balancing

Note

This function is supported by only RG-RAP series access points.

3.18.1 Overview

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

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

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

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

3.18.2 Configuring Client Load Balancing

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

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

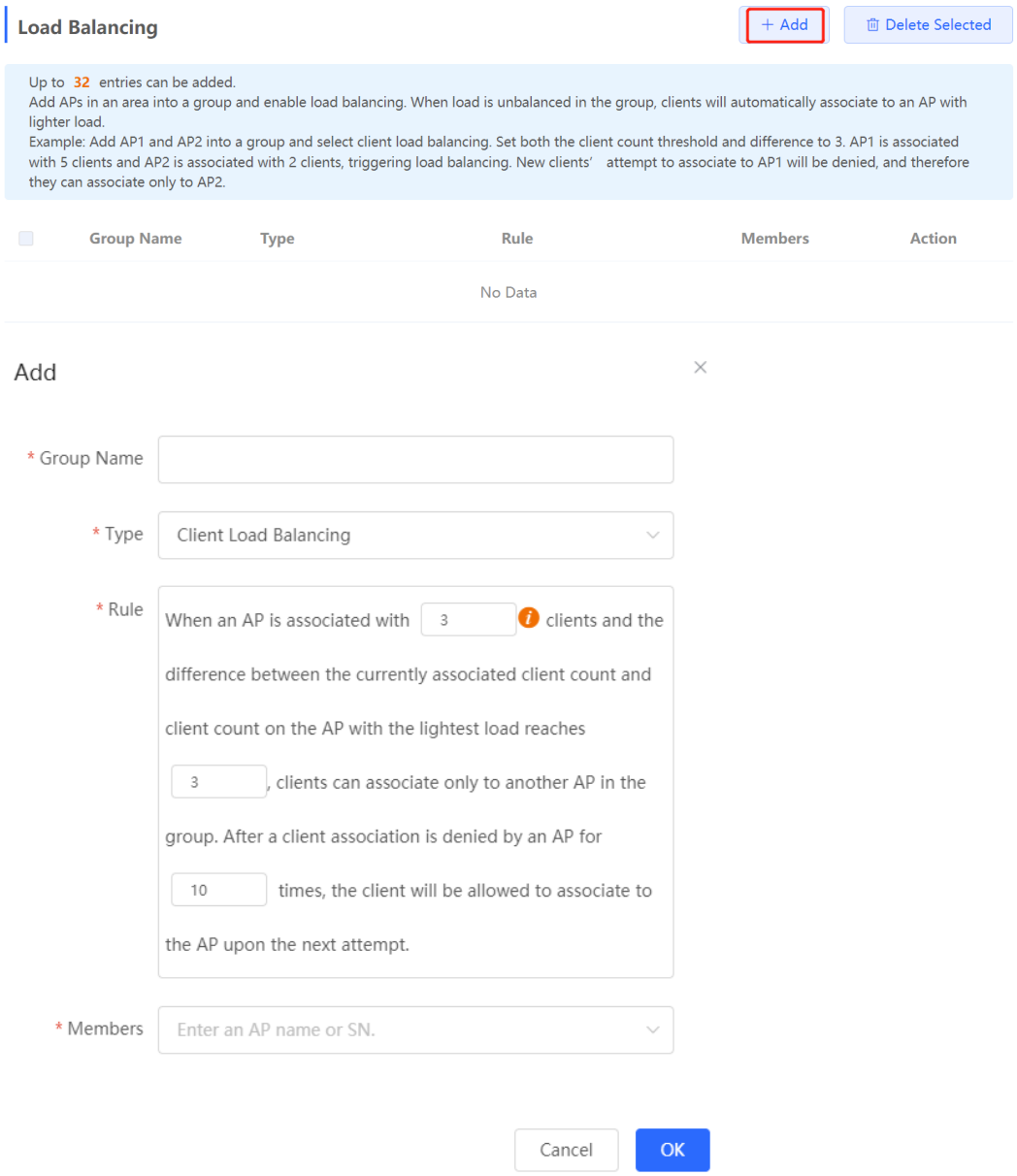


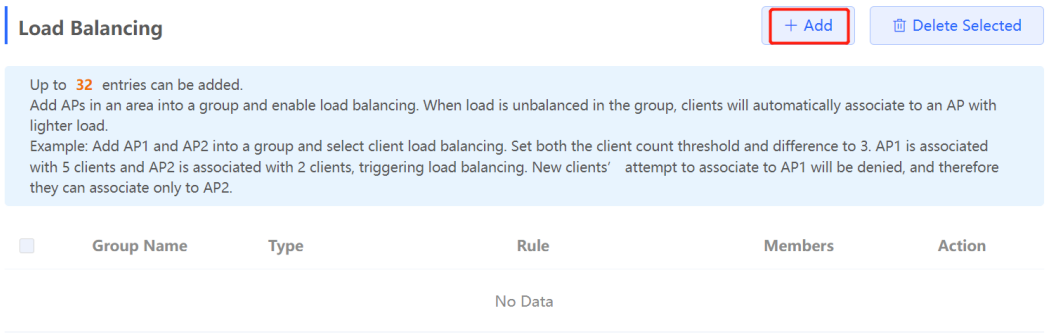
Table 3-1 Client load balancing configuration

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

3.18.3 Configuring Traffic Load Balancing

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

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



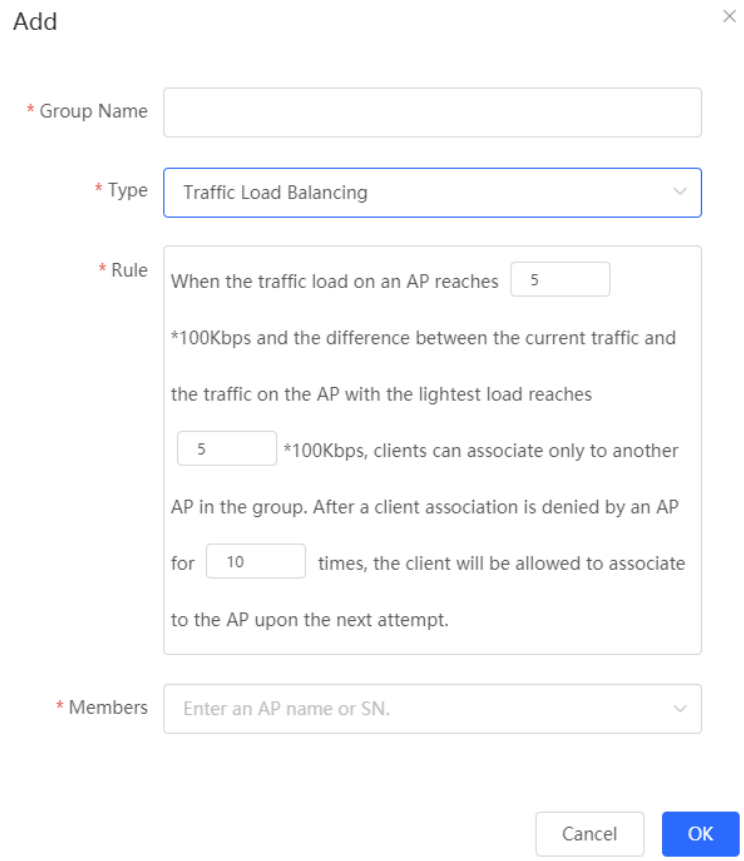


Table 3-2 Traffic load balancing configuration

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

4 Network Settings

Note

This chapter takes the currently logged in device as an example to describe the entry of each function setting page. If you need to configure other devices in the network, please refer to the following path to enter the configuration page of the corresponding device, and then configure the function:

- For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: Click **Manage Network Device**:
- For other RAP models, Choose WLAN > APs > Select the target device in the device list and click **Manage**.

4.1 Switching Work Mode

4.1.1 Work Mode

See Work Mode for details.

4.1.2 Self-Organizing Network Discovery

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

After the self-organizing network discovery function is enabled, the device can be discovered in the network and discover other devices in the network. Devices network with each other based on the device status and synchronize global configuration. You can log in to the Web management page of any device in the network to check information about all devices in the network. After this function is enabled, clients can maintain and manage the current network more efficiently. You are advised to keep this function enabled.

If the self-organizing network discovery function is disabled, the device will not be discovered in the network and it runs in standalone mode. After logging in to the Web page, you can configure and manage only the currently logged in device. If only one device is configured or global configuration does not need to be synchronized to the device, you can disable the self-organizing network discovery function.

4.1.3 Configuration Steps

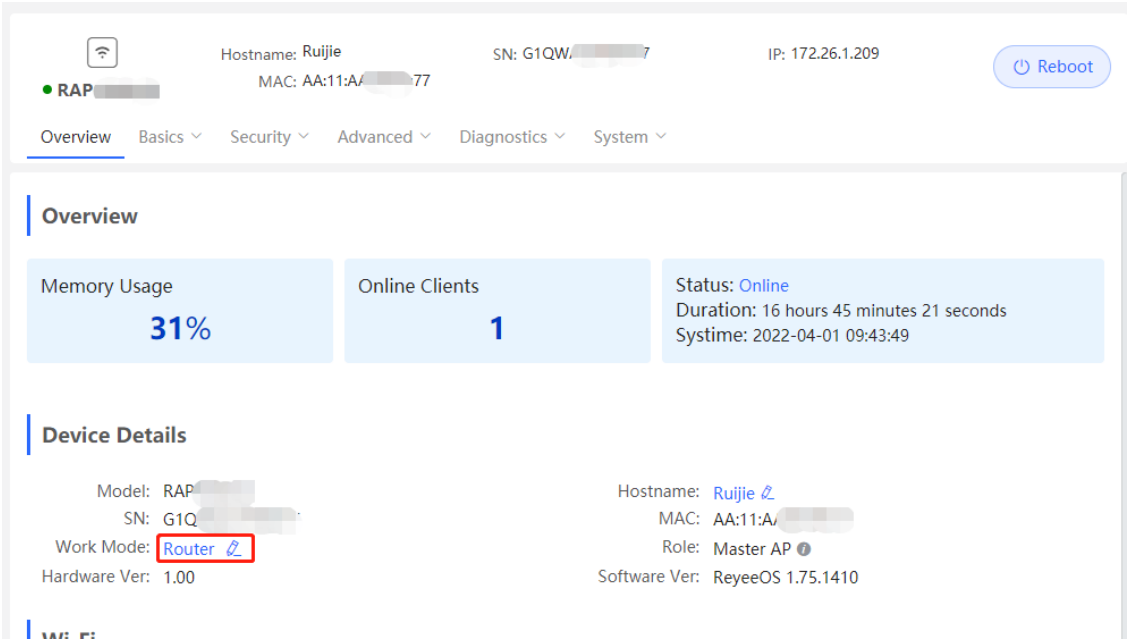
Note

If you need to switch the work mode to wireless bridging mode, please see Wireless Repeater Mode for details.

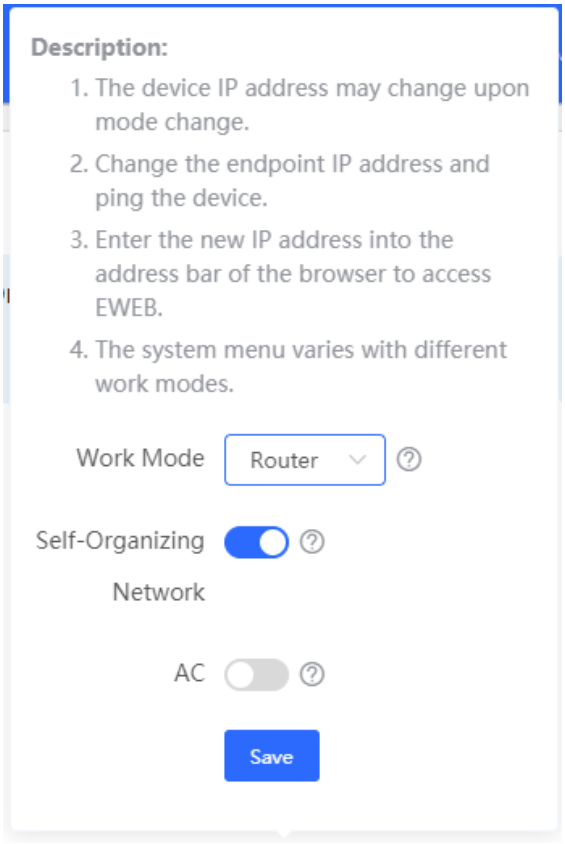
For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Overview** > **Device Details**

For other RAP models: Choose (**WLAN** > **APs** > **Manage**) **Overview** > **Device Details**

Click the current work mode to change the work mode.



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



Caution

After the self-organizing network discovery is enabled, you can check the role of the device in self-organizing network mode.

4.1.4 Viewing Device Role

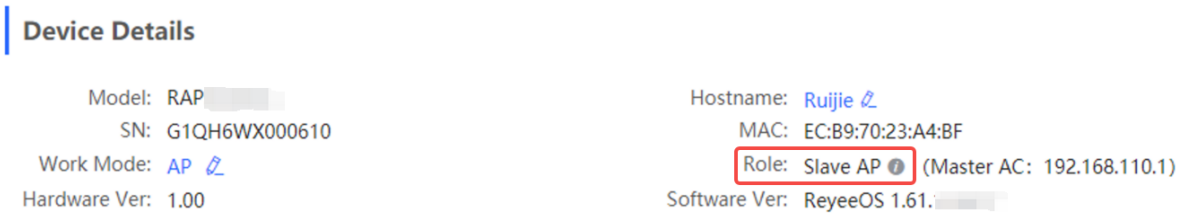
For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Overview** > **Device Details**

For other RAP models: Choose (**WLAN** > **APs** > **Manage**) **Overview** > **Device Details**

If the self-organizing network is enabled, you can view the device role on the **Device Details** page.

Master AP/AC: The device can manage downlink devices.

Slave AP/Device: The device has been managed by an AC. The slave Aps are managed by the master AP/AC in a unified manner. Some wireless network settings cannot be edited alone, and thus the master AP/AC delivers configurations to edit the network settings in a unified manner.

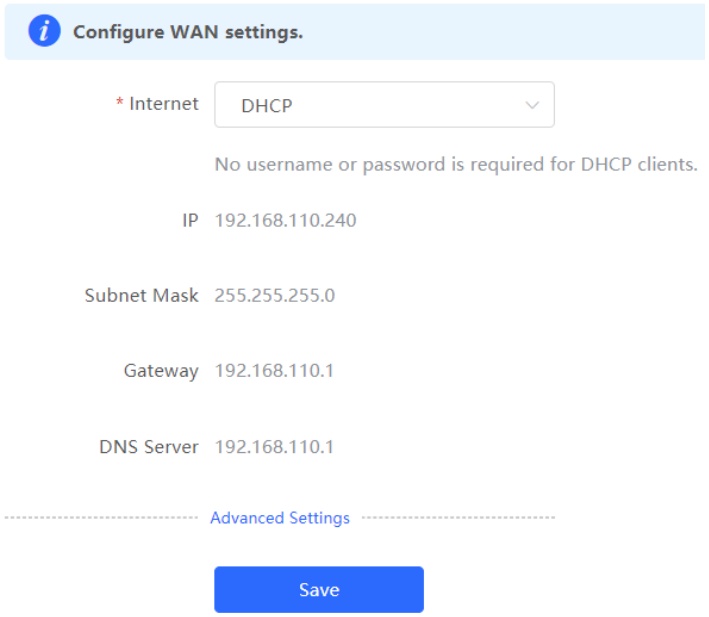


4.2 Configuring Internet Type

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Network** > **WAN**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Network** > **WAN**

Select the Internet connection type after confirming with the ISP. For detailed configuration, see Work Mode.



4.3 Configuring LAN Port

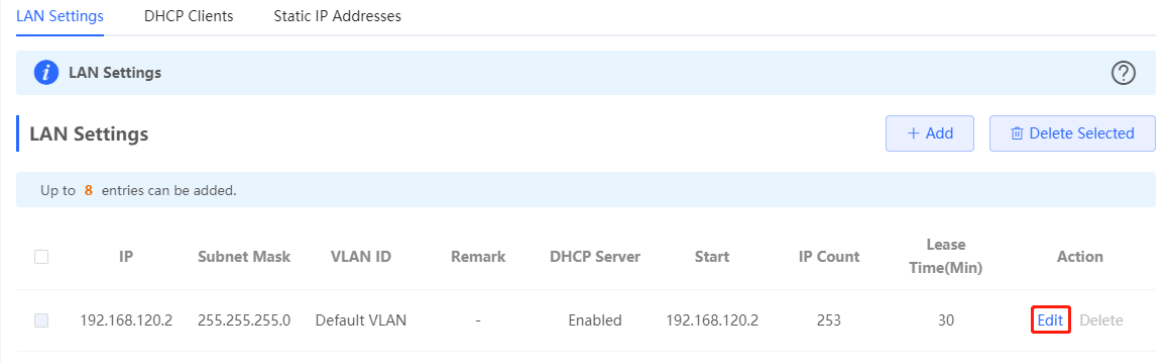
Caution

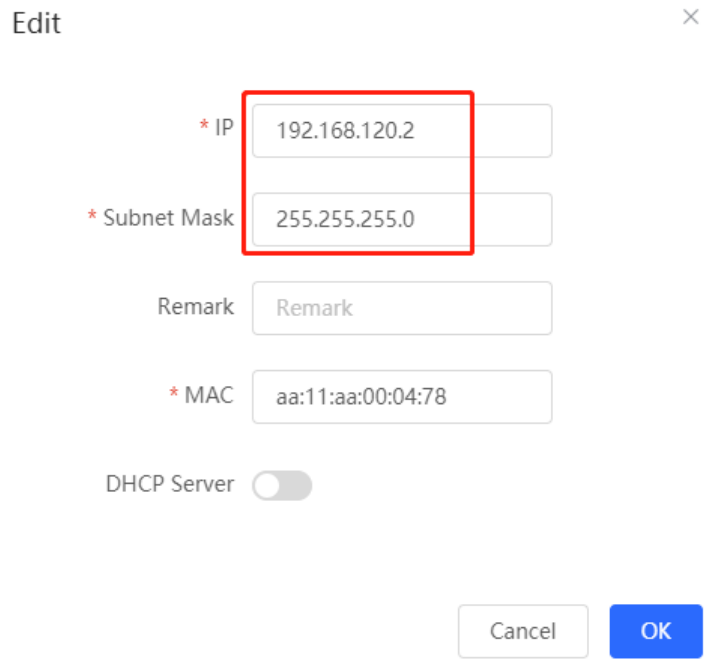
This function is not supported when the device works in AP mode.

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Network** > **LAN** > **LAN Settings**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Network** > **LAN** > **LAN Settings**

Click **Edit**. In the displayed dialog box, enter the IP address and subnet mask, and click **OK**. Change the IP address of the LAN port. Enter the new IP address in the browser and log in to the device again to configure and manage the device.





4.4 Configuring Repeater Mode

Caution

RG-RAP1200(F) access point does not support this function.

4.4.1 Wired Repeater

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Network** > **Repeater Mode**

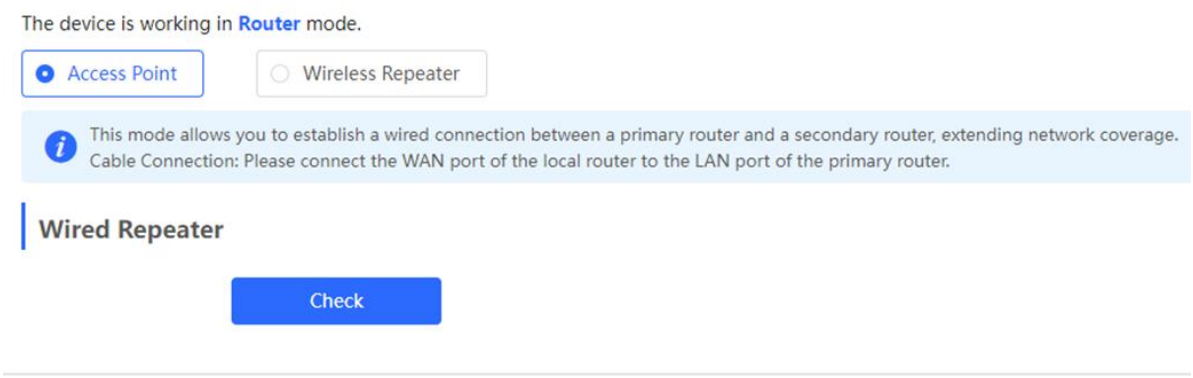
For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Network** > **Repeater Mode**

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

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

Caution

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



4.4.2 Wireless Repeater

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

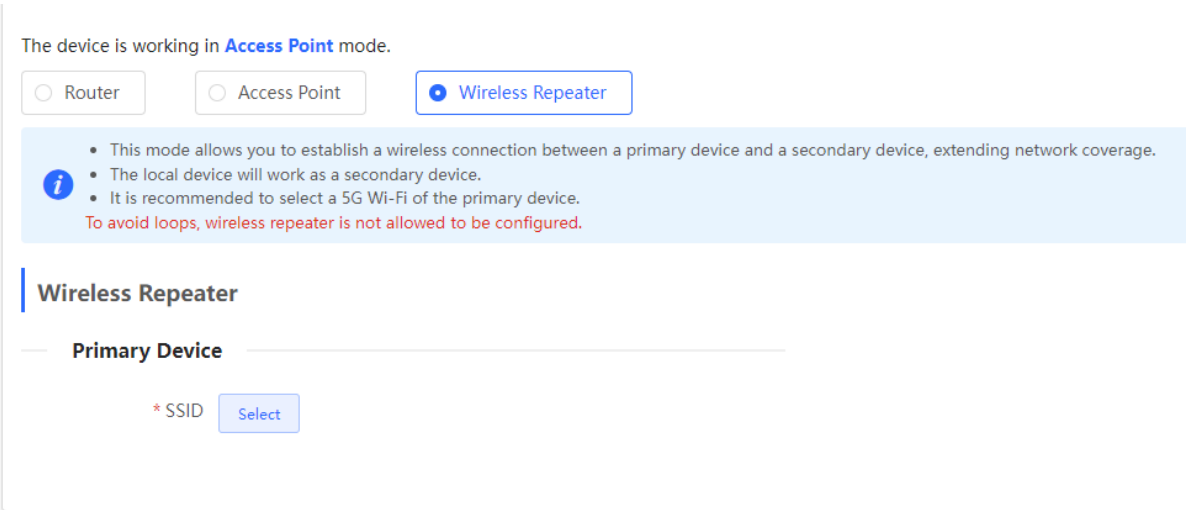
Note

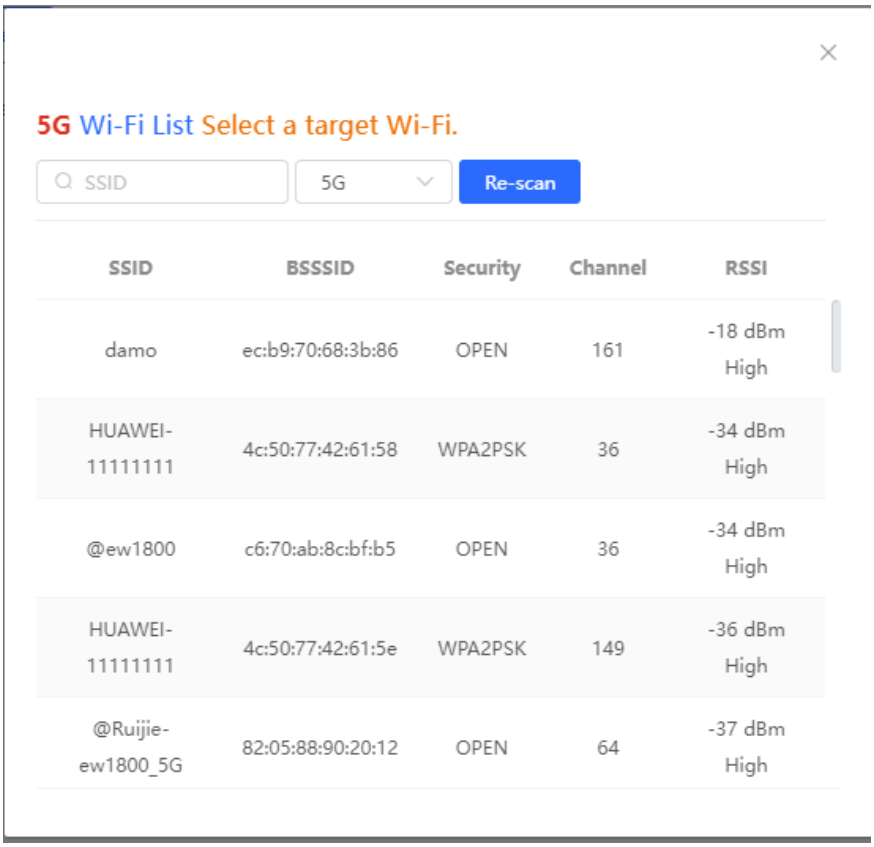
- To avoid loops in wireless repeater mode, remove the network cable from the WAN port.
- Obtain the Wi-Fi name and Wi-Fi password of the upper-layer router.

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Network** > **Repeater Mode**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Network** > **Repeater Mode**

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

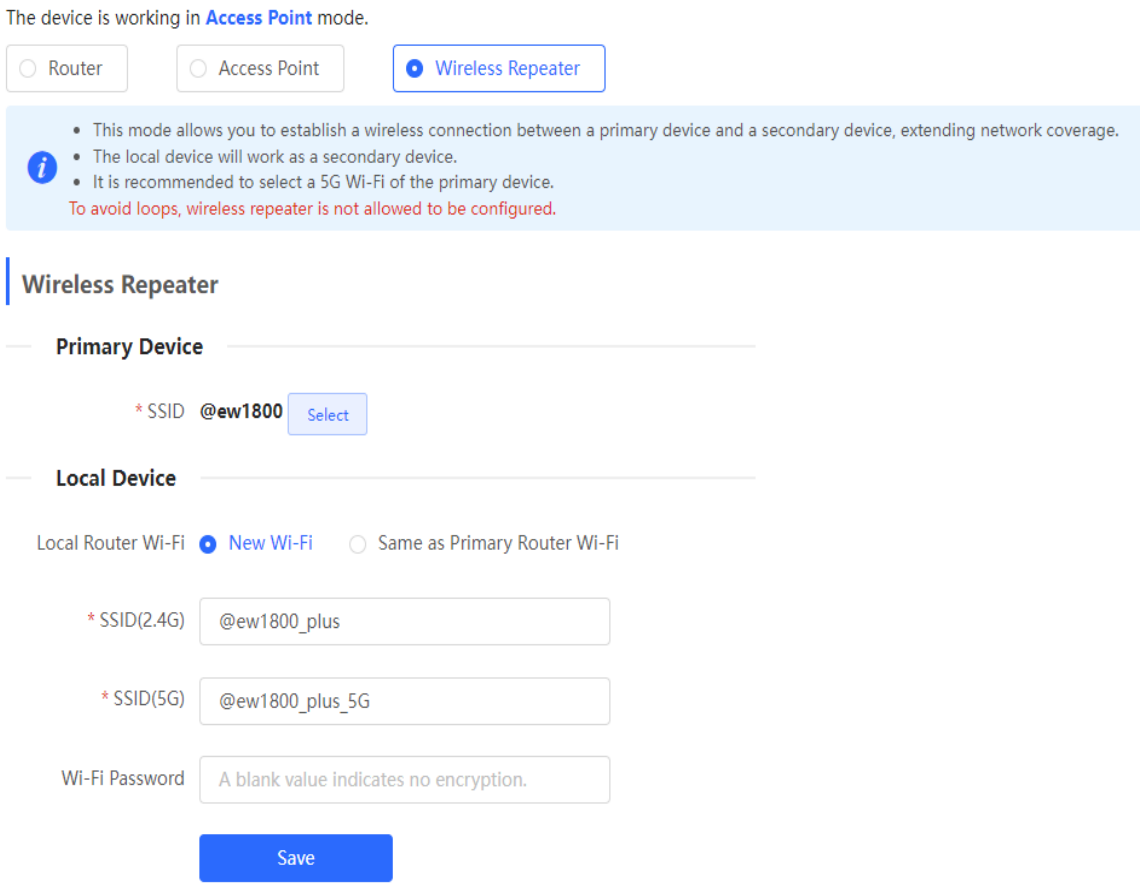




(2) Select the Wi-Fi signal of the upper-layer device that you want to extend. The configuration items of the local device are displayed. If the signal of the upper-layer device is encrypted, enter the Wi-Fi password of the upper-layer device.

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

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



Caution

- After the configuration is saved, the AP will be disconnected from the Wi-Fi network and needs to connect to the new Wi-Fi network. Exercise caution when performing this operation. Record the new Wi-Fi name and password.
- You are advised to install the AP in a position where the RSSI is greater than two bars of signal to prevent signal loss. If the signal at the installation position is too weak, the Wi-Fi extension may fail or the quality of extended signal may be poor.

4.5 Creating a VLAN

Caution

This function is not supported when the device works in AP mode.

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Network** > **LAN** > **LAN Settings**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Network** > **LAN** > **LAN Settings**

A LAN can be classified into multiple VLANs. Click **Add** to create a VLAN.

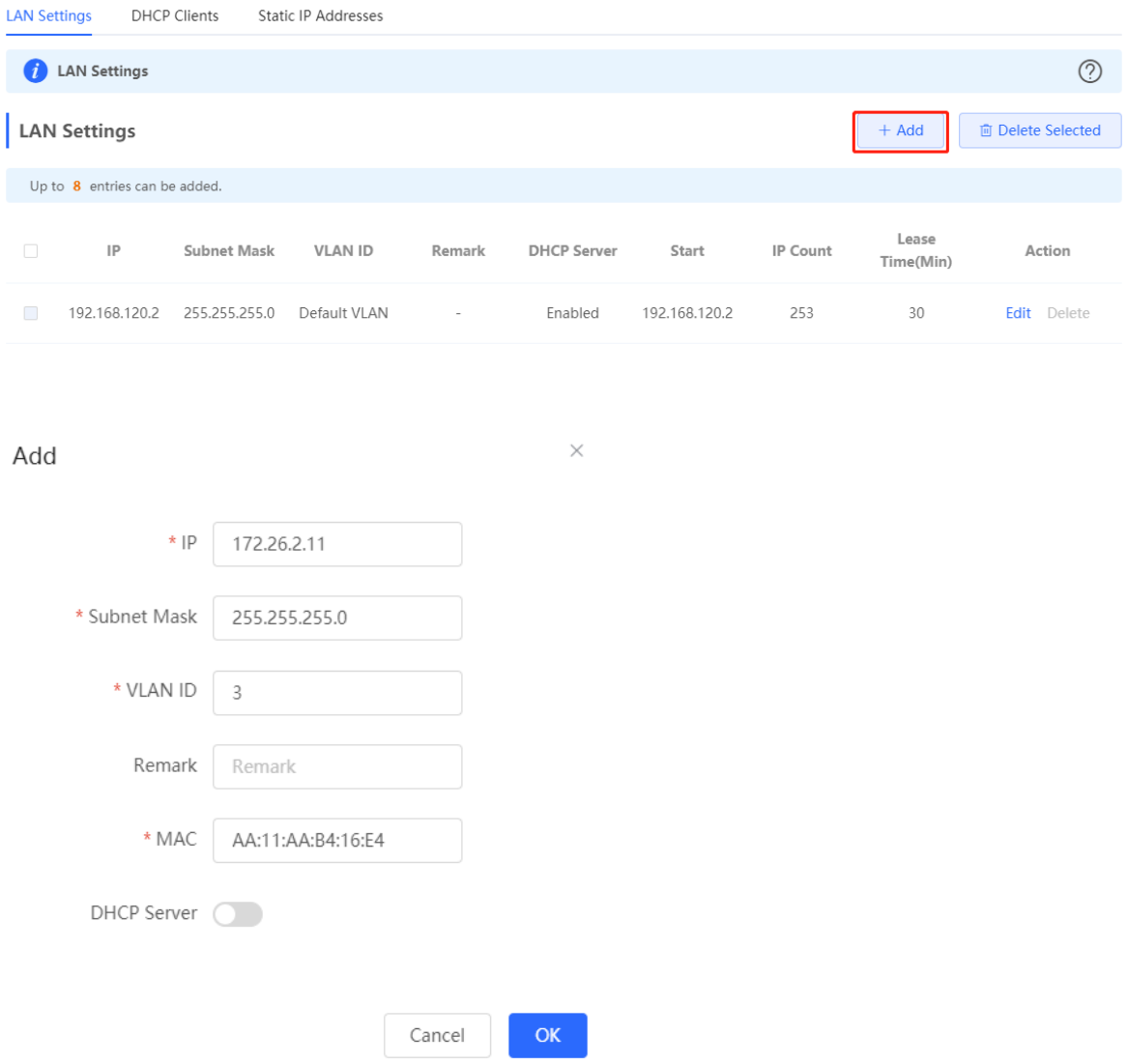


Table 4-1 VLAN Configuration

Parameter	Description
IP	IP address of the VLAN interface. The default gateway of devices that access the Internet through the current LAN should be set to this IP address.
Subnet Mask	Subnet mask of the IP address of the VLAN interface.
VLAN ID	VLAN ID.
Remark	VLAN description.
MAC	MAC address of the VLAN interface.

Parameter	Description
DHCP Server	Enable the DHCP server function. After it is enabled, devices on the LAN can automatically obtain IP addresses. After the DHCP service is enabled, you need to configure the start IP address to be assigned, number of IP addresses to be assigned, and address lease term for the DHCP server, and other DHCP server options. For details, see Configuring DHCP Server.

Caution

VLAN configuration is associated with the configuration of the uplink device. Therefore, refer to the configuration of the uplink device when configuring a VLAN.

4.6 Configuring Port VLAN

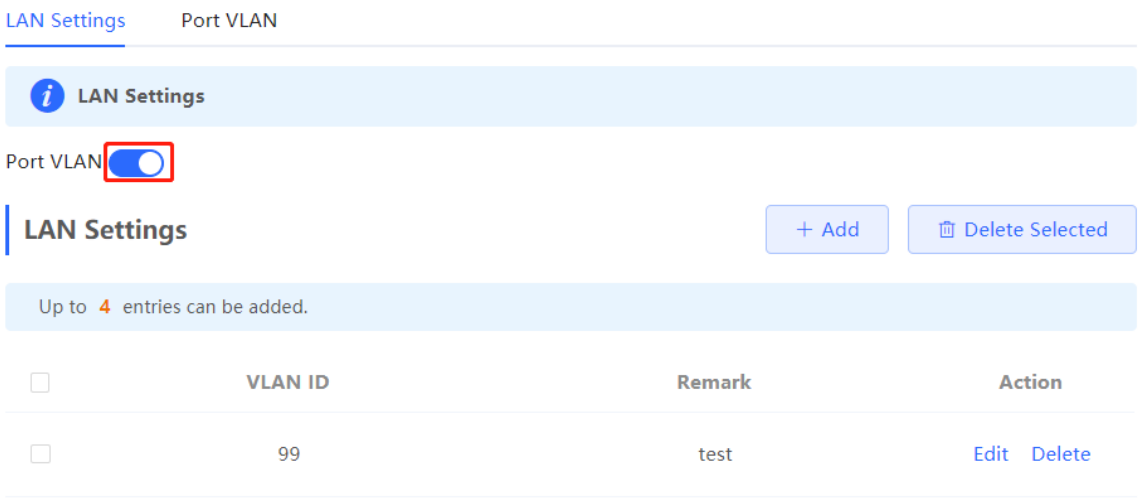
Caution

The port VLAN can be configured only when the device works in AP mode.

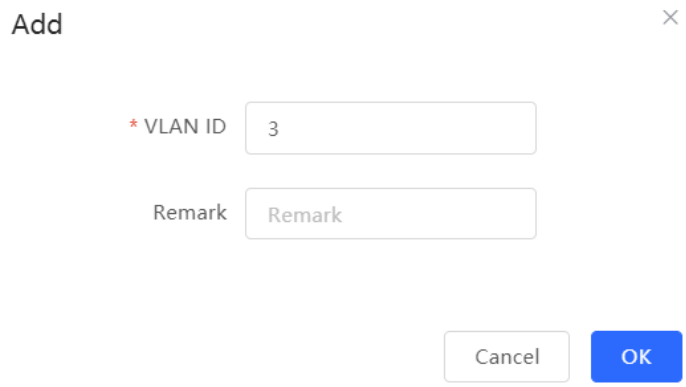
For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Network** > **LAN**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Network** > **LAN**

(1) On the **LAN Settings** tab page, turn on **Port VLAN**, and click **OK** in the confirmation dialog box.

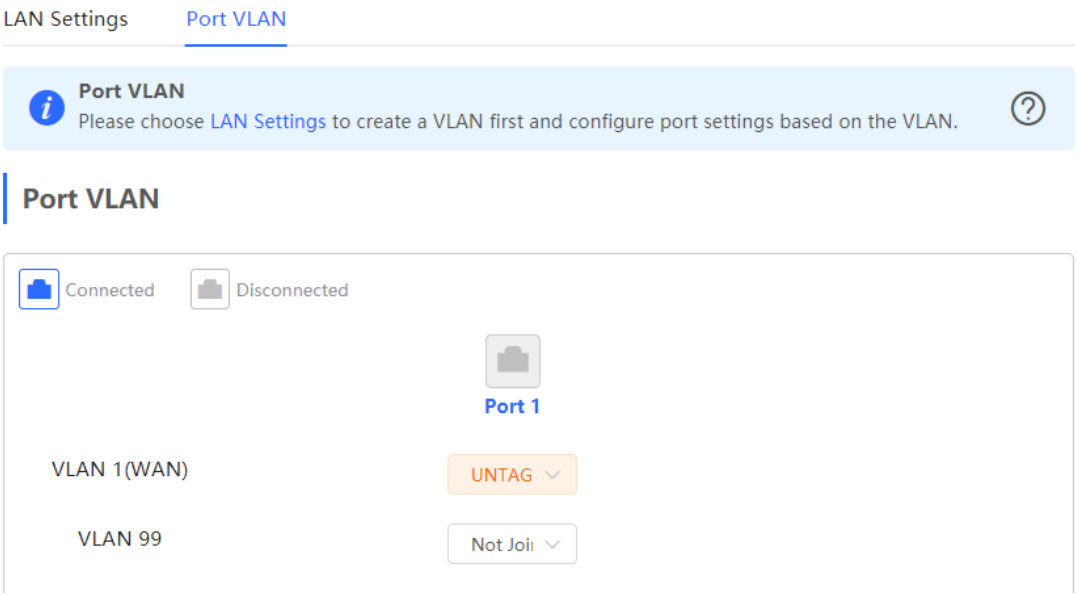


(2) Click **Add**. Enter the VLAN ID and description, and click **OK** to create a VLAN. The added VLAN is used to set the VLAN, to which a port belongs.



(3) Switch to the **Port VLAN** tab page and configure VLANs for the port. Click the option box below the port, select the mapping between a VLAN and the port from the drop-down list box, and click **Save**.

- **UNTAG**: Configure the VLAN as the native VLAN of the port. That is, when receiving a packet from this VLAN, the port removes the VLAN tag from the packet and forwards the packet. When receiving an untagged packet, the port adds the VLAN tag to the packet and forwards the packet through the VLAN. Only one VLAN can be configured as an untagged VLAN on each port.
- **TAG**: Configure the VLAN as an allowed VLAN of the port, but the VLAN cannot be the native VLAN. That is, VLAN packets carry the original VLAN tag when they are forwarded by the port.
- **Not Join**: Configure the port not to allow packets from this VLAN to pass through. For example, if VLAN 10 and VLAN 20 are not added to port 2, port 2 will neither receive nor send packets from or to VLAN 10 and VLAN 20.



4.7 Changing MAC Address

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Network** > **WAN**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Network** > **WAN**

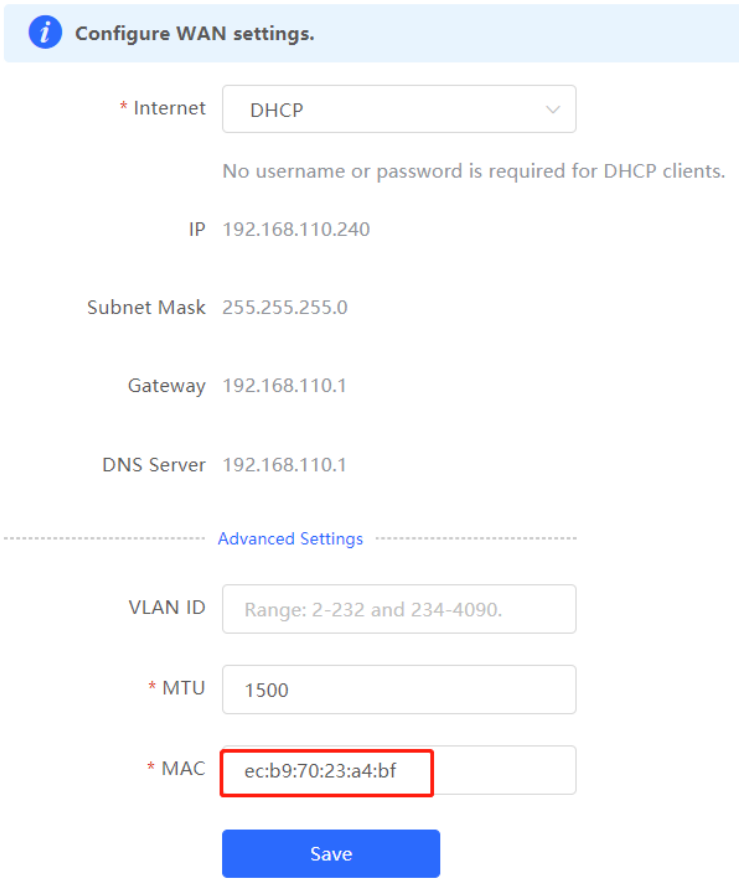
ISPs may restrict the access of devices with unknown MAC addresses to the Internet for the sake of security. In this case, you can change the MAC address of the WAN port.

Click to expand **Advanced Settings**, enter the MAC address, and click **Save**. You do not need to change the default MAC address unless in special cases.

In the router mode, change the MAC address of the LAN port on **Network** > **LAN**.

Caution

Changing the MAC address will disconnect the device from the network. You need to reconnect the device to the network or restart the device. Therefore, exercise caution when performing this operation.

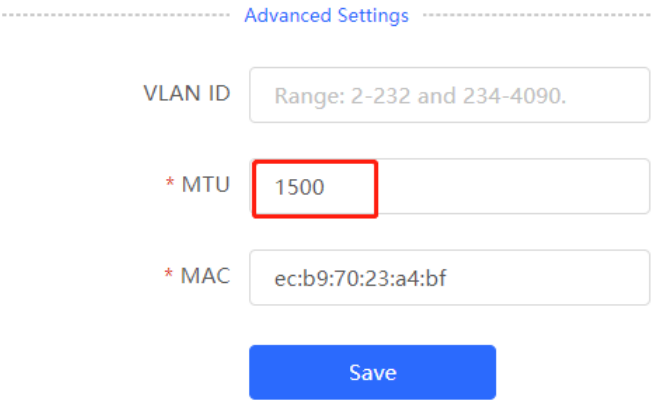


4.8 Changing MTU

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Network** > **WAN**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Network** > **WAN**

WAN interface MTU indicates the maximum transmission unit (MTU) allowed by the WAN interface. The default value is 1500 bytes, indicating the maximum data forwarding efficiency. Sometimes, ISP networks restrict the speed of large data packets or forbid large data packets from passing through. As a result, the network speed is unsatisfactory or even the network is disconnected. In this case, you can set the MTU value to a smaller value.



4.9 Configuring DHCP Server

Caution

This function is not supported when the device works in AP mode.

4.9.1 DHCP Server

In the router mode, the DHCP server function can be enabled on the device to automatically assign IP addresses to clients so that clients connected to the LAN ports or Wi-Fi network of the device obtain IP addresses for Internet access.

4.9.2 Configuring the DHCP Server Function

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Network** > **LAN** > **LAN Settings**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Network** > **LAN** > **LAN Settings**

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

Caution

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

Start: Enter the start IP address of the DHCP address pool. A client obtains an IP address from the address pool. If all the addresses in the address pool are used up, no IP address can be obtained from the address pool.

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

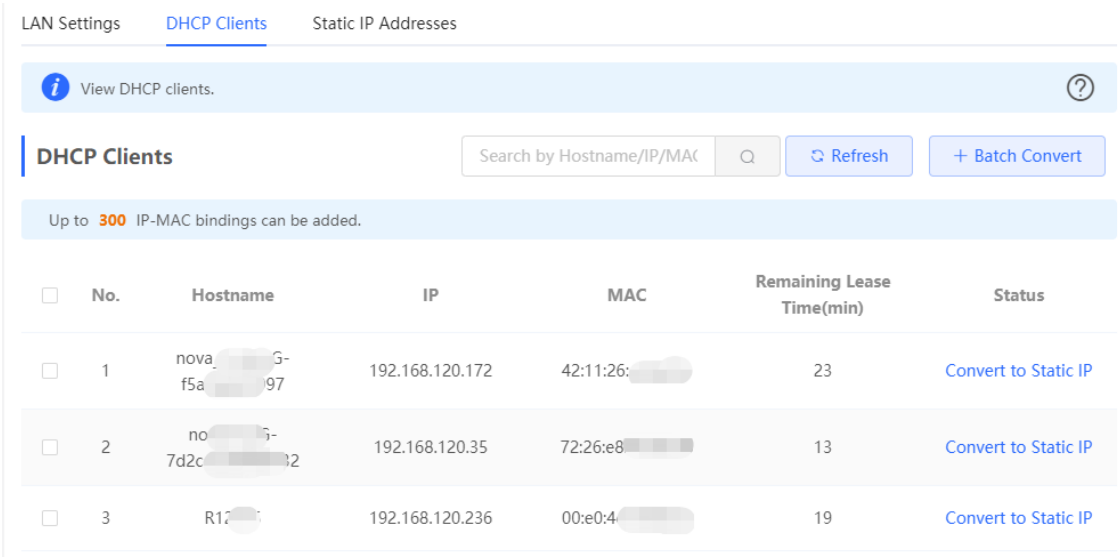
Lease Time(Min): Enter the address lease term. When a client is connected, the leased IP address is automatically renewed. If a leased IP address is not renewed due to client disconnection or network instability, the IP address will be reclaimed after the lease term expires. After the client connection is restored, the client can request an IP address again. The default lease term is 30 minutes.

4.9.3 Displaying Online DHCP Clients

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Network** > **LAN** >**DHCP Clients**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Network** > **LAN** > **DHCP Clients**

Check information about an online client. Click **Convert to Static IP**. Then, the static IP address will be obtained each time the client connects to the network.

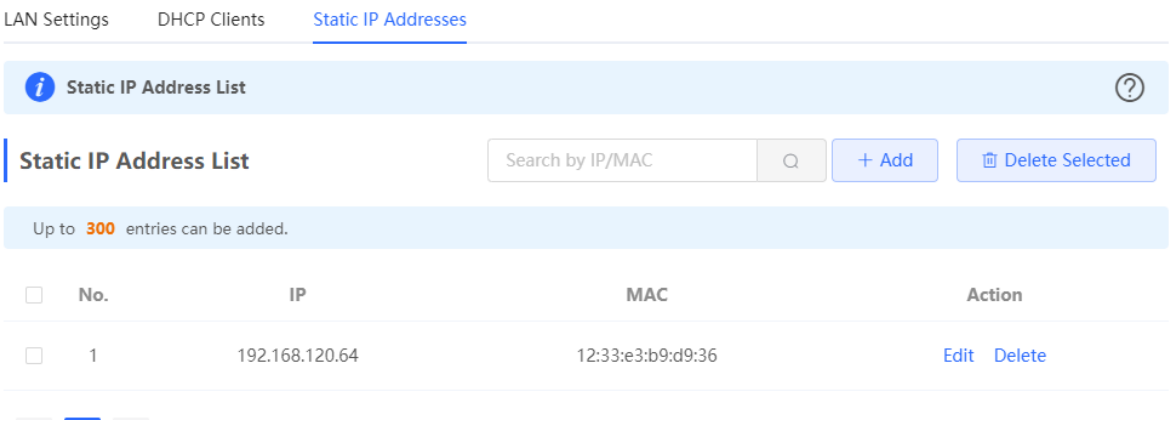


4.9.4 Displaying the DHCP Static IP Address List

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Network** > **LAN** > **Static IP Addresses**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Network** > **LAN** > **Static IP Addresses**

Click **Add**. In the displayed static IP address binding dialog box, enter the MAC address and IP address of the client to be bound, and click **OK**. After a static IP address is bound, the bound IP address will be obtained each time the client connects to the network.



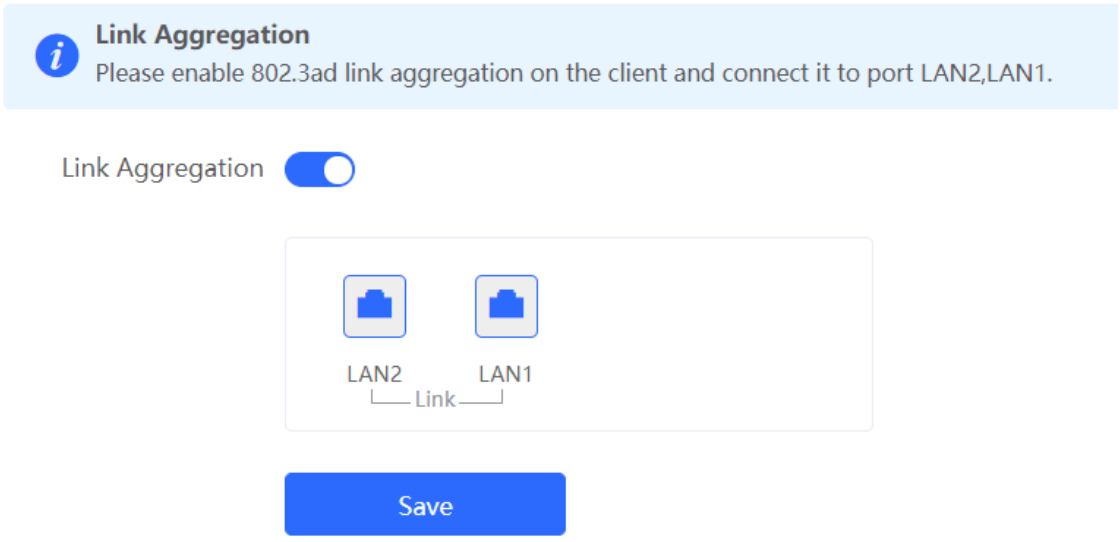
4.10 Link Aggregation

Caution

The function is supported by only RG-RAP2260(H).

In **Local Device** mode, choose **Advanced** > **Link Aggregation**.

Link Aggregation can improve the throughput in the network and deal with link congestion.

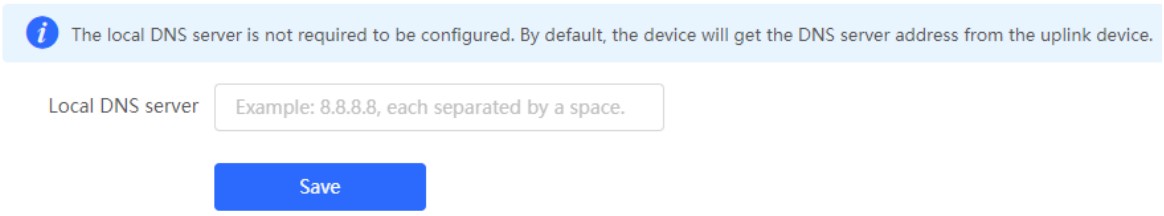


4.11 Configuring DNS

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Advanced** > **Local DNS**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Advanced** > **Local DNS**

Enter the IP address of the DNS server and click **Save**. The local DNS server is optional. The device obtains the DNS server address from the connected uplink device by default. The default configuration is recommended. The available DNS service varies from region to region. You can consult the local ISP.



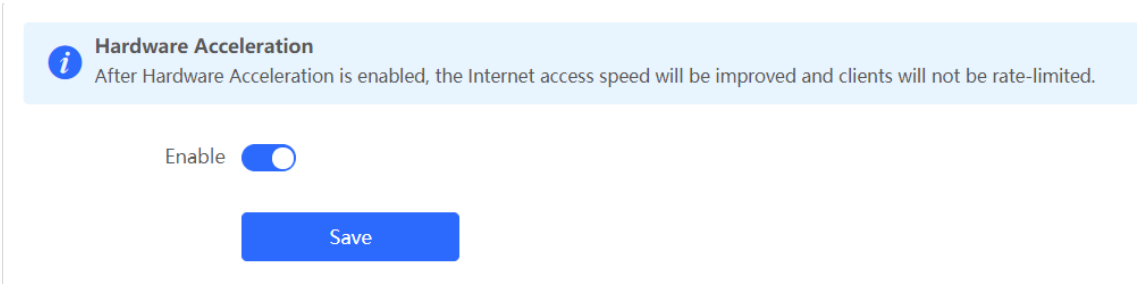
4.12 Hardware Acceleration

Note

The functions mentioned in this chapter are only applicable to such models as RAP2260(H), RAP6260(H), RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RAP2260, RG-RAP1260 and RAP6262.

In Local Device mode, choose Advanced > Hardware Acceleration.

After Hardware acceleration is enabled, the Internet access speed will be improved.

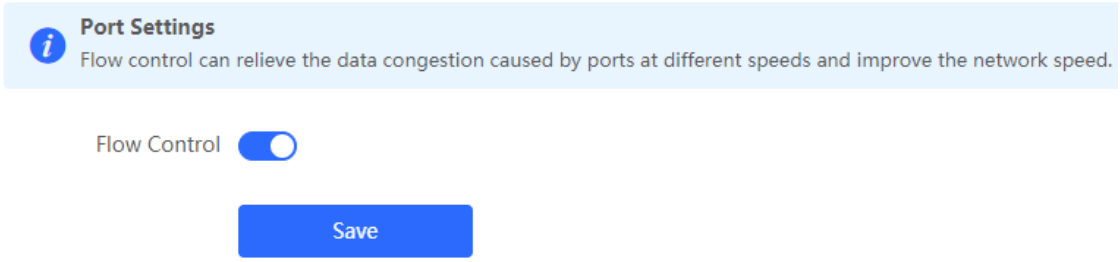


4.13 Configuring Port Flow Control

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Advanced** > **Port Settings**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Advanced** > **Port Settings**

When the LAN ports work at different rates, data congestion may occur, which can slow down the network speed and affect the Internet access experience. Enabling port flow control can help mitigate this problem.



4.14 Configuring ARP Binding

Caution

This function is not supported when the device works in AP mode.

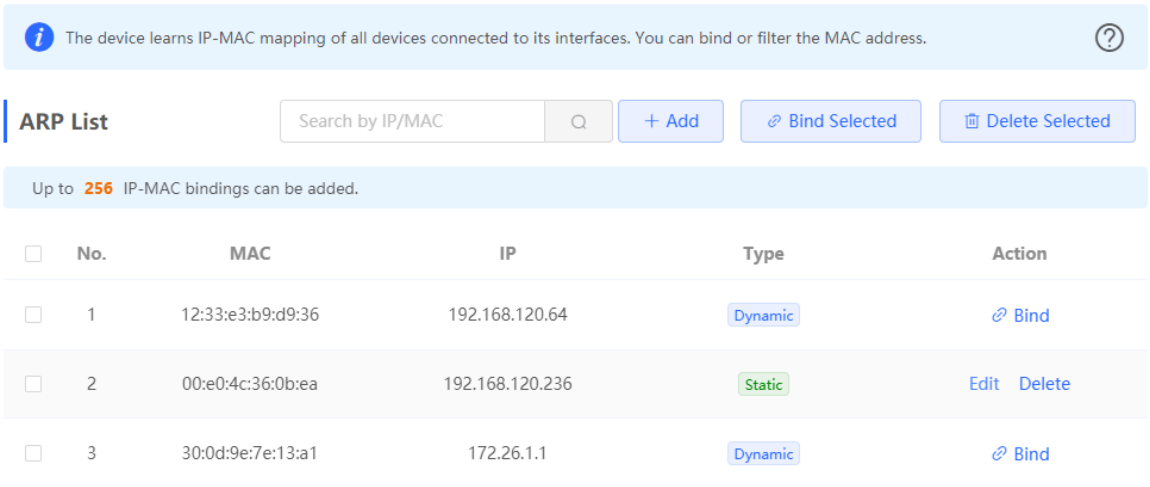
The device learns the IP and MAC addresses of network devices connected to ports of the device and generates ARP entries. You can bind ARP mappings to improve network security.

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Security** > **ARP List**

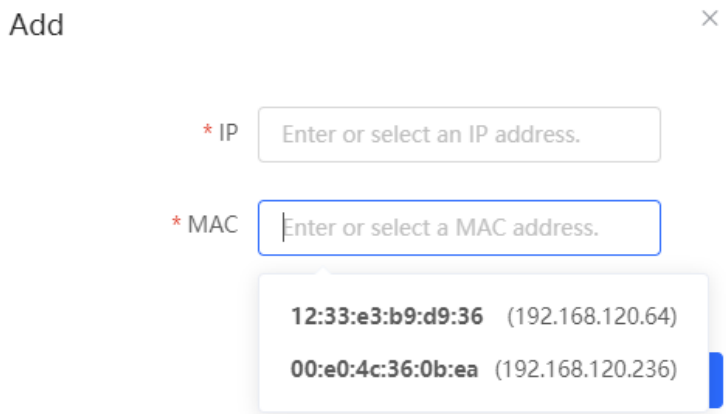
For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Security** > **ARP List**

ARP mappings can be bound in two ways:

(1) Select a dynamic ARP entry in the ARP list and click **Bind**. You can select multiple entries to be bound at one time and click **Bind Selected** to bind them. To remove the binding between a static IP address and a MAC address, click **Delete** in the **Action** column.



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



4.15 Configuring LAN Ports

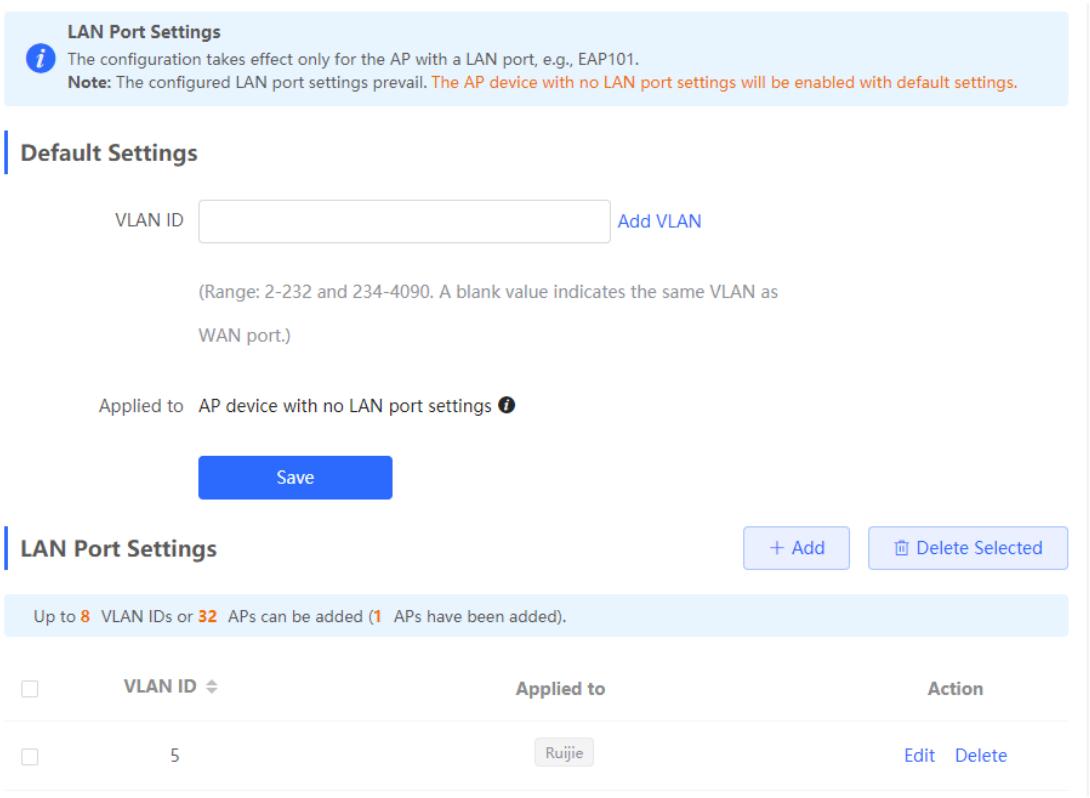
Caution

The configuration takes effect only on APs having wired LAN ports.

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

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

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


LAN Port Settings
The configuration takes effect only for the AP with a LAN port, e.g., EAP101.
Note: The configured LAN port settings prevail. The AP device with no LAN port settings will be enabled with default settings.
Default Settings
VLAN ID
Add VLAN
(Range: 2-232 and 234-4090. A blank value indicates the same VLAN as WAN port.)
Applied to
AP device with no LAN port settings
Save
LAN Port Settings
+ Add
Delete Selected
Up to 8 VLAN IDs or 32 APs can be added (1 APs have been added).
VLAN ID
Applied to
Action
5
Ruijie
Edit
Delete

5 System Settings

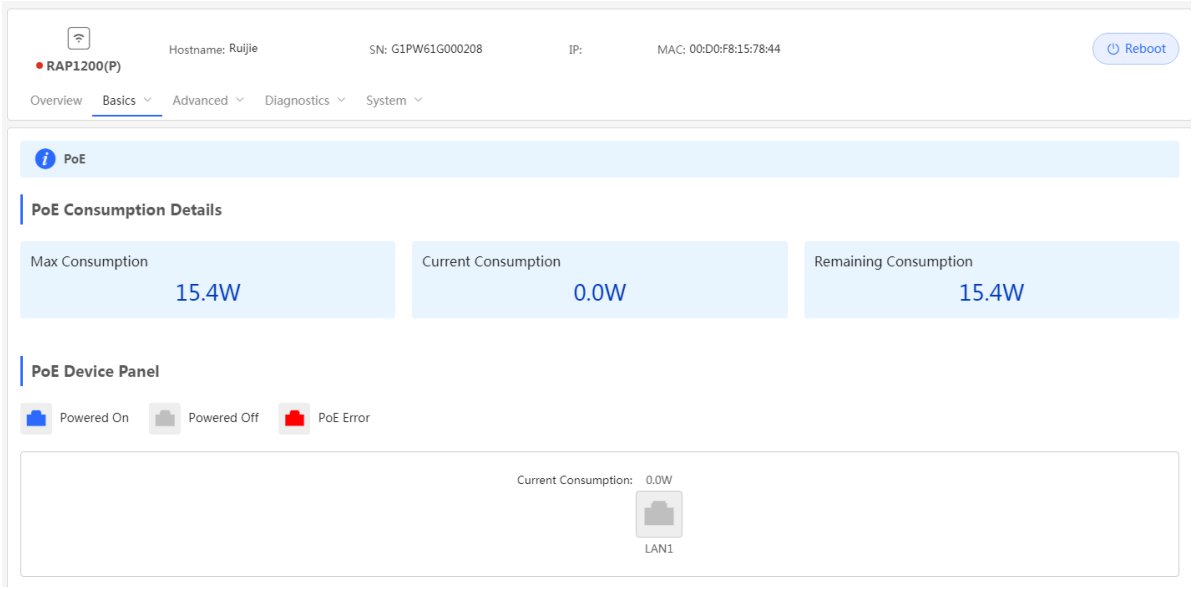
5.1 PoE

Caution

Only RG-RAP1200(P) supports this function.

Choose **Wireless** > **APs** > **Manage** > **Basics** > **PoE**.

The device supplies power to PoE powered devices through ports. You can check the total power, current consumption, remaining consumption, and whether PoE power supply status is normal. Move the cursor over a port. The power switch icon appears. You can click it to control whether to enable PoE on the port.



5.2 PoE Settings

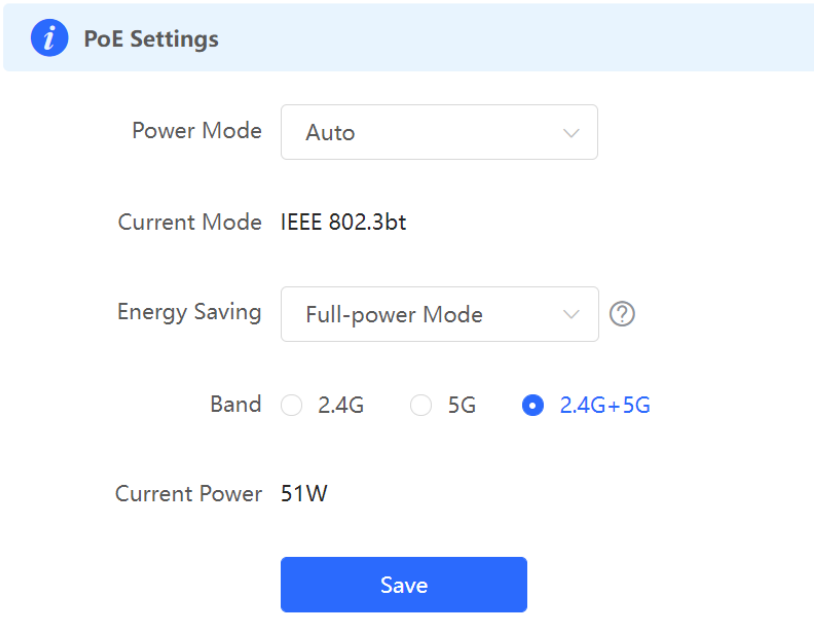
Caution

This function is supported by only RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262.

In **Local Device** mode, choose **Advanced** > **PoE Settings**.

Set the power mode for the AP to accept power over PoE. In AF mode, the maximum power supported by the device is 15.4 W. In AT mode, the maximum power is 30 W according to the IEEE 802.3at standard. In BT mode, the maximum power is 51 W according to the IEEE 802.3bt standard. By default, the device automatically

negotiates with the power sourcing equipment (PSE) about the power mode. The default configuration is recommended.



5.3 Setting the Login Password

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models:

If the device works in self-organizing network mode, and **Network** mode webpage is displayed, choose **System** > **Login Password**

In standalone mode: Choose **System** > **Login** > **Login Password**

For other RAP models:

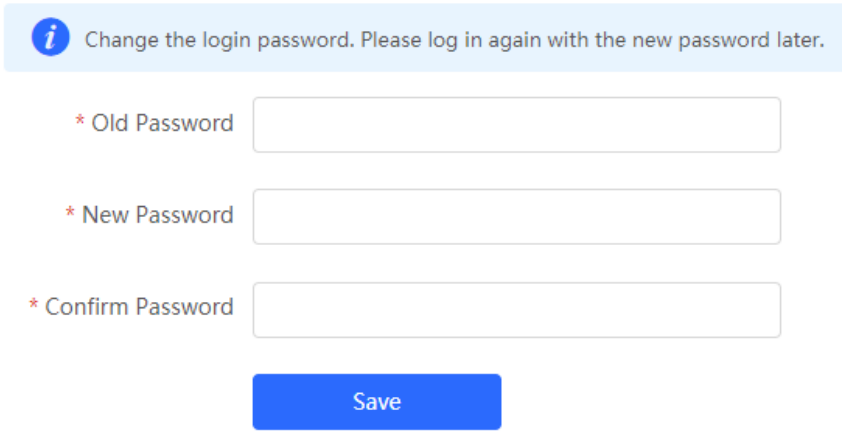
In self-organizing network mode: Choose **Network** > **Password**

In standalone mode: Choose **System** > **Login** > **Login Password**

Enter the old password and new password. After saving the configuration, use the new password to log in.

Caution

In self-organizing network mode, the login password of all devices in the network will be changed synchronously.



5.4 Setting the Session Timeout Duration

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models:

If the device works in self-organizing network mode, and **Local Device** mode webpage is displayed, choose **System** > **Login**

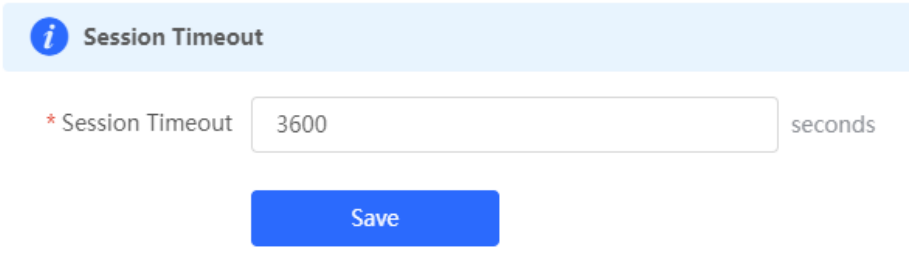
In standalone mode: Choose **System** > **Login** > **Session Timeout**

For other RAP models:

In self-organizing network mode: Choose **WLAN** > **APs** > **Manage** > **System** > **Login** > **Session Timeout**

In standalone mode: Choose **System** > **Login** > **Session Timeout**

If no operation is performed on the Web page within a period of time, the session is automatically disconnected. When you need to perform operations again, enter the password to log in again. The default timeout duration is 3600 seconds, that is, 1 hour.



5.5 Setting and Displaying System Time

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models:

If the device works in self-organizing network mode, and **Network** mode webpage is displayed, choose **System** > **System Time**

In standalone mode: Choose **System** > **System Time**

For other RAP models:

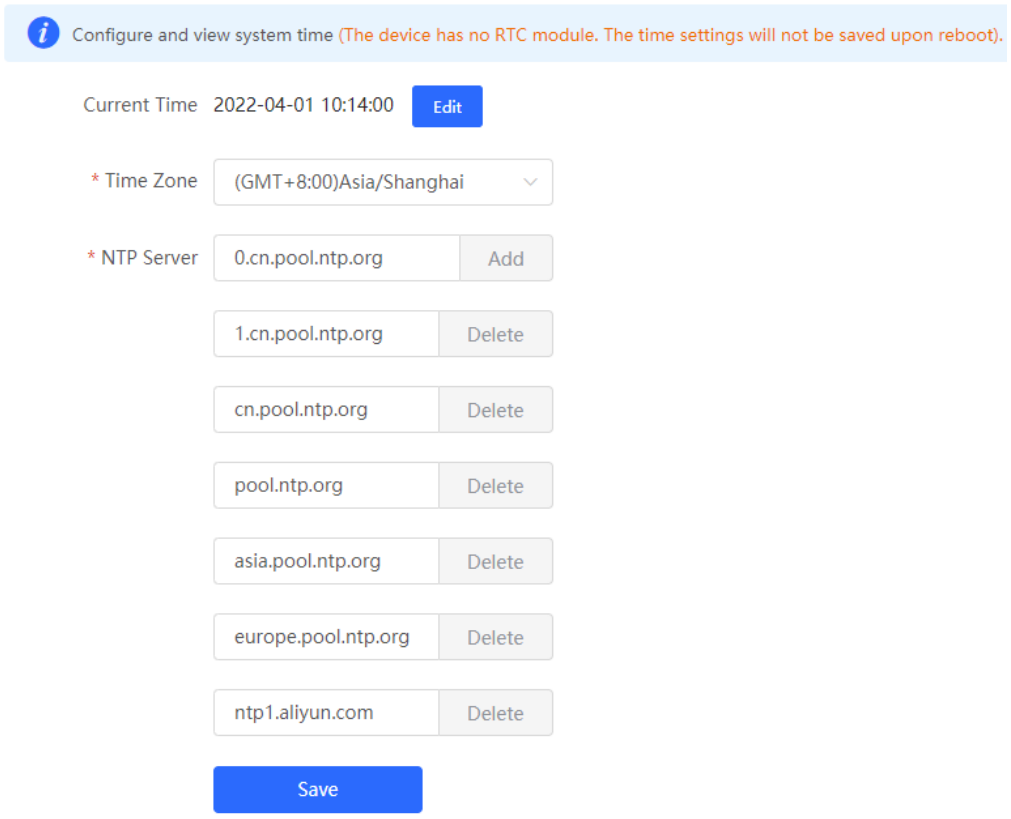
In self-organizing network mode: Choose **Network** > **Time**

In standalone mode: Choose **System** > **System Time**

You can view the current system time. If the time is incorrect, check and select the local time zone. If the time zone is correct but time is still incorrect, click **Edit** to manually set the time. In addition, the device supports Network Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete the local server.

Caution

In self-organizing network mode, the system time of all devices in the network will be changed synchronously.



5.6 Configuring Reboot

Caution

- Do not cut off power during system reboot to avoid device damage.
- Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the Web service becomes available, the device automatically jumps to the login page.
- Rebooting the device affects the network. Therefore, exercise caution when performing this operation.

5.6.1 Rebooting the Current Device

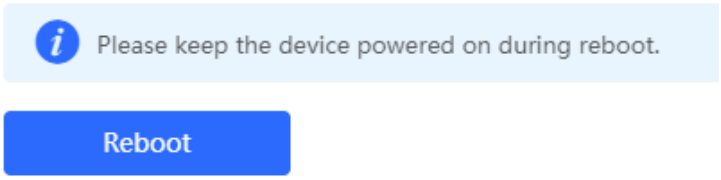
For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **System** > **Reboot** > **Reboot**

For other RAP models:

In self-organizing network mode: Choose **WLAN** > **APs** > **Reboot**

In standalone mode: Choose **System** > **Reboot** > **Reboot**

Click **Reboot**. The device will restart.



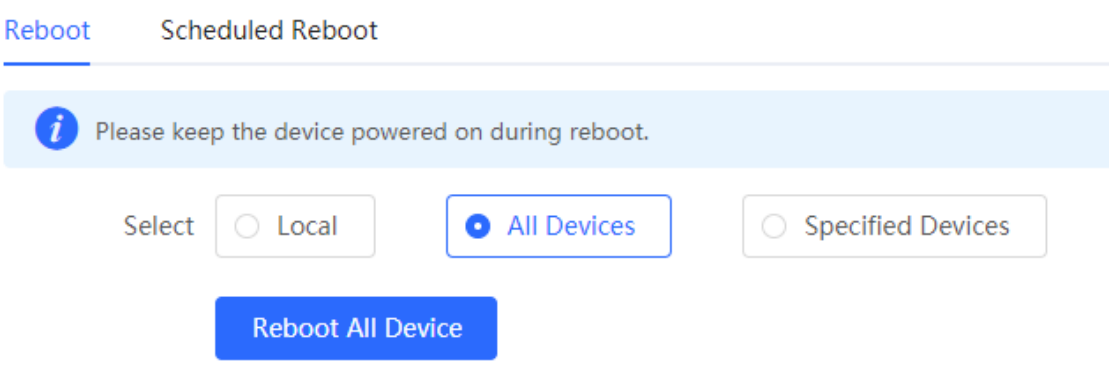
5.6.2 Rebooting All Devices in the Network

In self-organizing network mode, you can reboot all devices in the network in batches.

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Network** mode, choose **System** > **Reboot** > **Reboot**

For other RAP models: Choose **Network** > **Reboot & Reset** > **Reboot**

Click **Reboot**, select **All Devices**, and click **Reboot All Device** to reboot all devices in the current network.



Caution

It takes time to reboot all devices in the current network. The action may affect the whole network. Please be cautious.

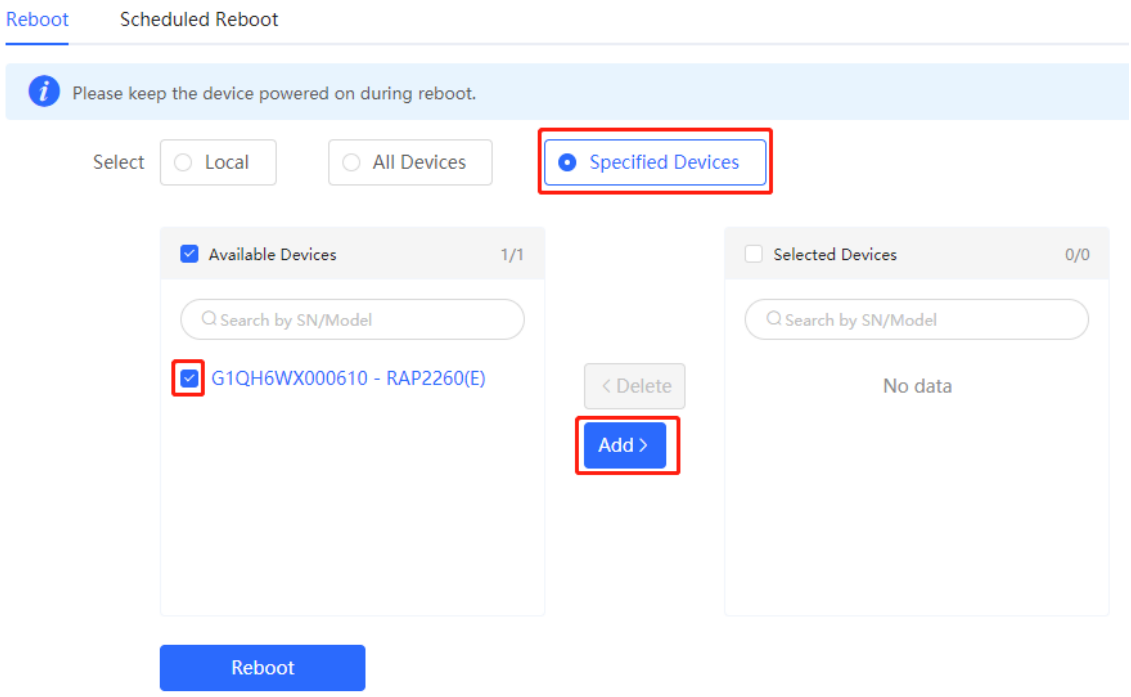
5.6.3 Rebooting the Specified Device

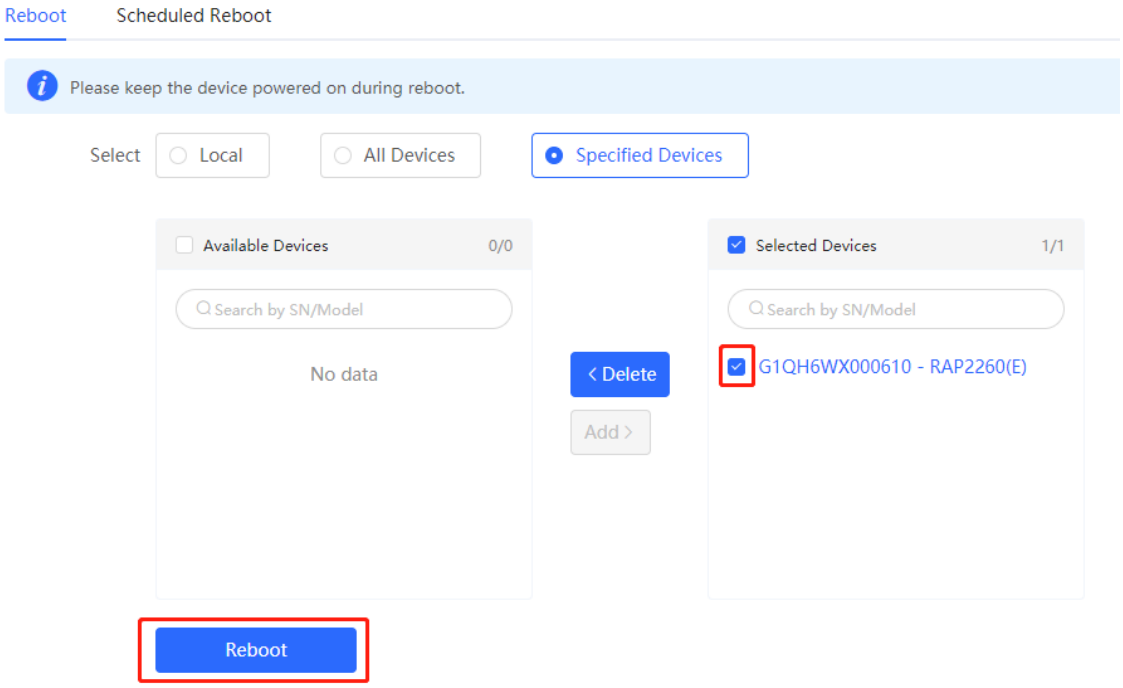
In self-organizing network mode, you can reboot specified devices in the network in batches.

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Network** mode, choose **System** > **Reboot** > **Reboot**

For other RAP models: **Network** > **Reboot & Reset** > **Reboot**

Click **Reboot**, click **Specified Devices**, select required devices from the **Available Devices** list, and click **Add** to add devices to the **Selected Devices** on the right. Click **Reboot**. Specified devices in the **Selected Devices** list will be rebooted.





5.7 Configuring Scheduled Reboot

5.7.1 Configuring Scheduled Reboot for the Current Device

Confirm that the system time is accurate to avoid network interruption caused by device reboot at wrong time. For details about how to configure the system time, see Setting the Session Timeout Duration.

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: Choose **System** > **Reboot** > **Scheduled Reboot**

For other RAP models:

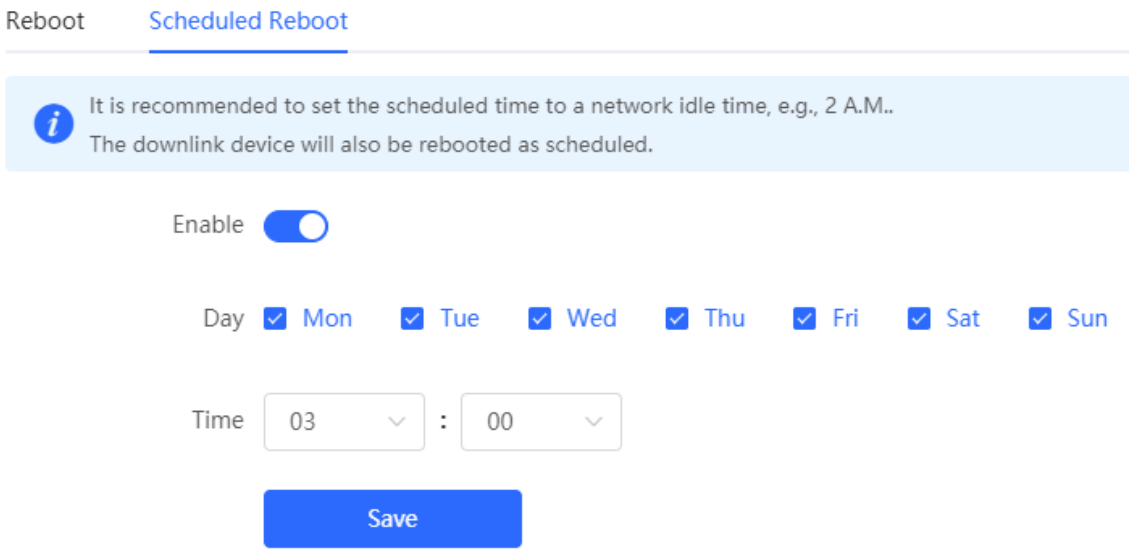
To configure scheduled reboot for the current device, choose (**WLAN** > **APs** > **Manage** >) **System** > **Reboot** > **Scheduled Reboot**

To configure scheduled reboot for all devices in the network, choose **Network**>> **Scheduled Reboot**

Caution

If you configure scheduled reboot on the management webpage, all devices will restart when the system time matches with the scheduled reboot time. Please be cautious.

Click **Enable**, and select the date and time of scheduled reboot every week. Click **Save**. When the system time matches with the scheduled reboot time, the device will restart. You are recommended to set scheduled reboot time to off-peak hours.



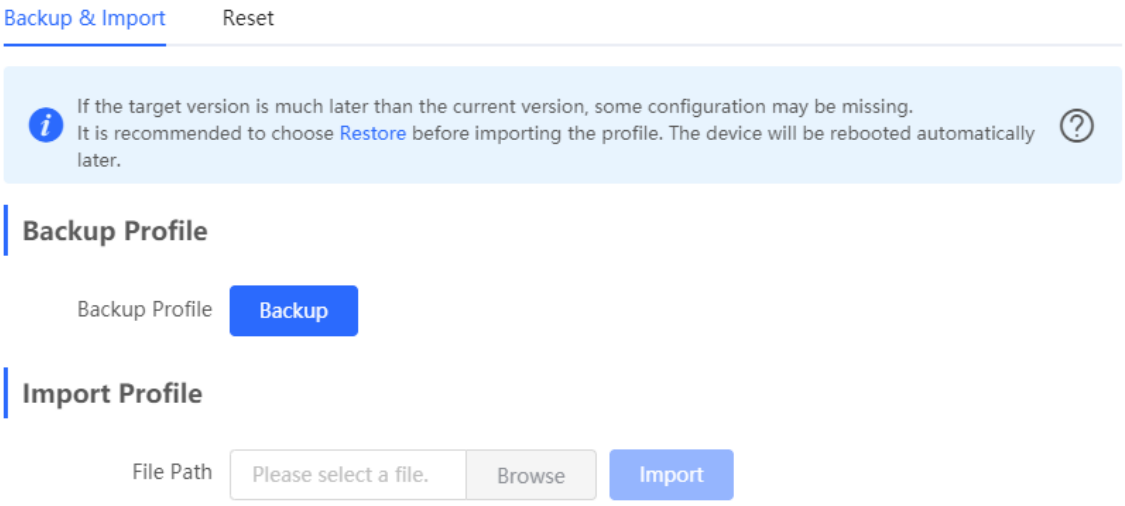
5.8 Configuring Backup and Import

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: Choose **System** > **Management** > **Backup & Import**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **System** > **Management** > **Backup & Import**

Configuration backup: Click **Backup** to download a configuration file locally.

Configuration import: Click **Browse**, select a backup file on the local PC, and click **Import** to import the configuration file. The device will restart.



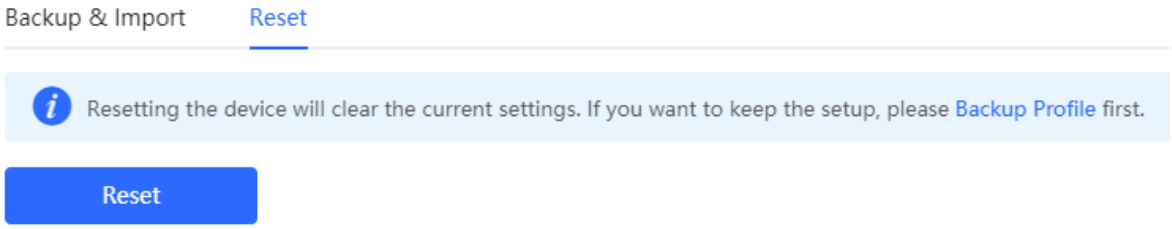
5.9 Restoring Factory Settings

5.9.1 Restoring the Current Device to Factory Settings

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **System** > **Management** > **Reset**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **System** > **Management** > **Reset**

Click **Reset** to restore the current device to the factory settings.



Caution

The operation will clear all configuration of the current device. If you want to retain the current configuration, back up the configuration first (See Configuring Backup and Import). Therefore, exercise caution when performing this operation.

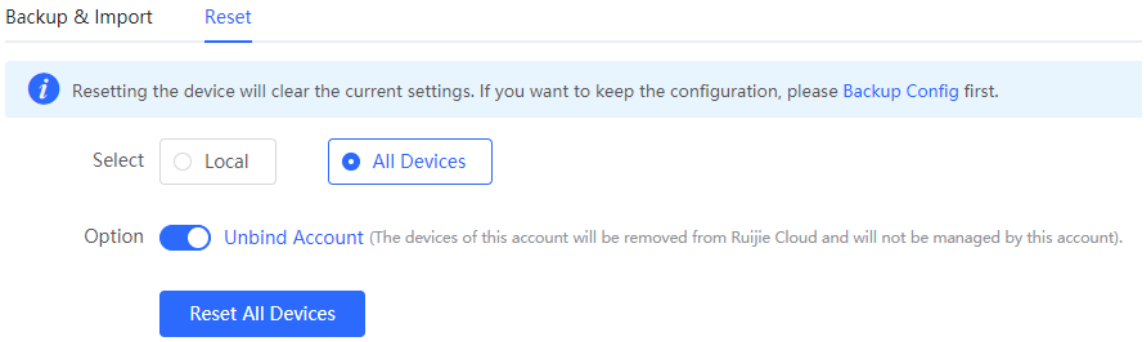
5.9.2 Restoring All Devices to Factory Settings

In the self-organizing network mode, all devices in the network will be restored to factory settings.

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Network** mode, choose **System** > **Management** > **Reset**

For other RAP models: Choose **Network** > **Reboot & Reset** > **Restore**

Click **All Devices**, select whether to enable **Unbind Account** and Click **Reset All Devices**. All devices in the network will be restored to factory settings.



Caution

The operation will clear all configuration of all devices in the network. Therefore, exercise caution when performing this operation.

5.10 Performing Upgrade and Checking System Version

Caution

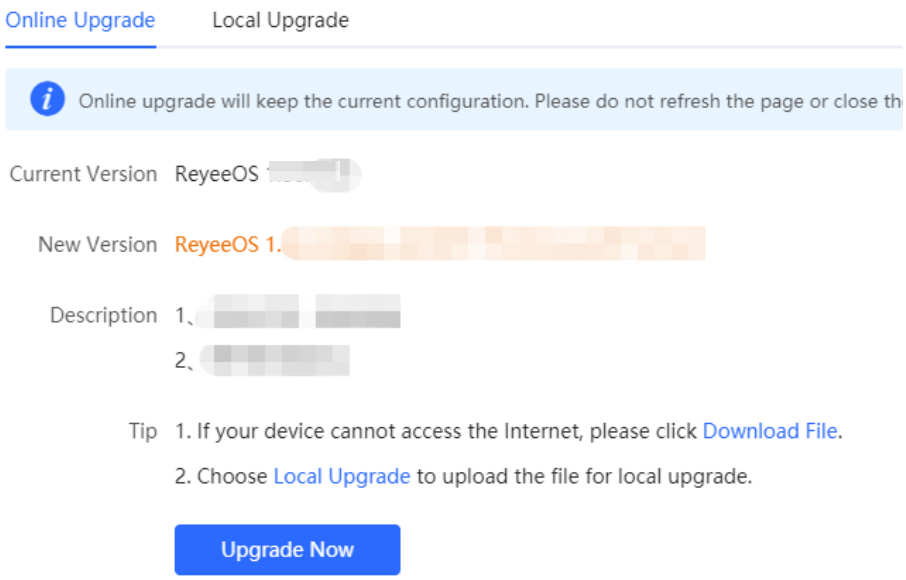
- You are advised to back up the configuration before upgrading the access point.
- After being upgraded, the access point will reboot. Therefore, exercise caution when performing this operation.

5.10.1 Online Upgrade

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **System** > **Upgrade** > **Online Upgrade**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **System** > **Upgrade** > **Online Upgrade**

You can view the current system version. If there is a new version available, you can click it for an update.

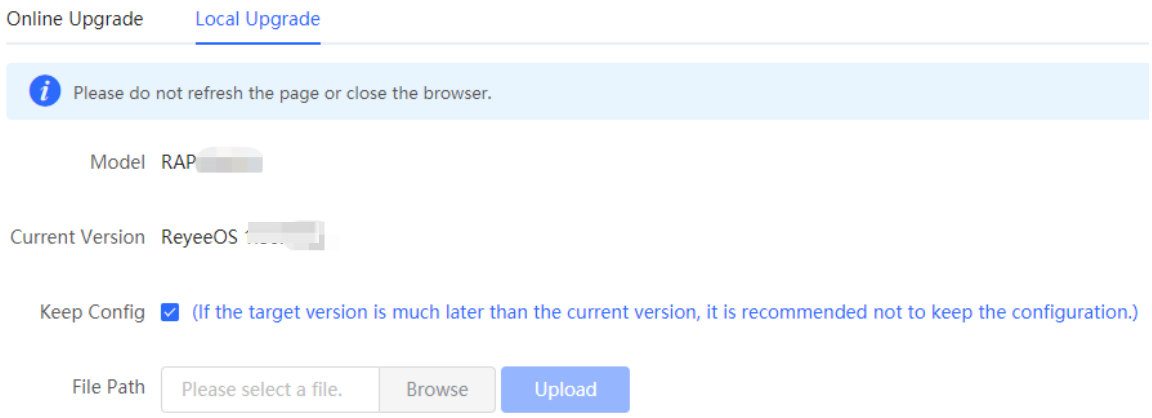


5.10.2 Local Upgrade

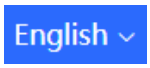
For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **System** > **Upgrade** > **Local Upgrade**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **System** > **Upgrade** > **Local Upgrade**

You can view the current software version, hardware version and device model. If you want to upgrade the device with the configuration retained, check **Keep** Setup. Click **Browse**, select an upgrade package on the local PC, and click **Upload** to upload the file. The device will be upgraded.

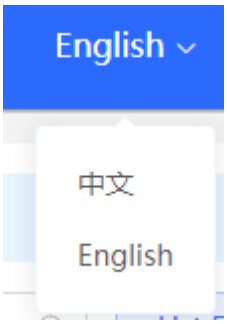


5.11 Switching System Language

Choose 

in the upper right corner of the Web page.

Click a required language to switch the system language.



5.12 Configuring LED Status Control

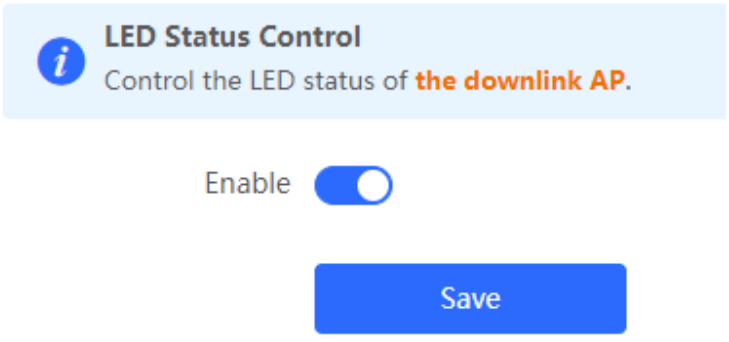
Caution

The LED Status Control function is not supported in the standalone mode (self-organizing network is not enabled).

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: Choose **Network** > **LED**

For other RAP models: Choose **WLAN** > **LED**

Turn on the LED of all downlink access points in the network.

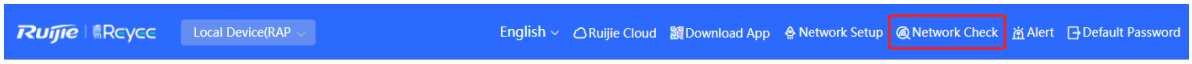


6 Network Diagnosis Tools

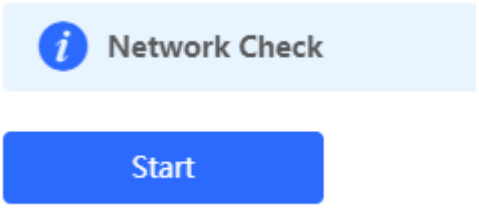
6.1 Network Check

When a network error occurs, perform **Network Check** to identify the fault and take the suggested action.

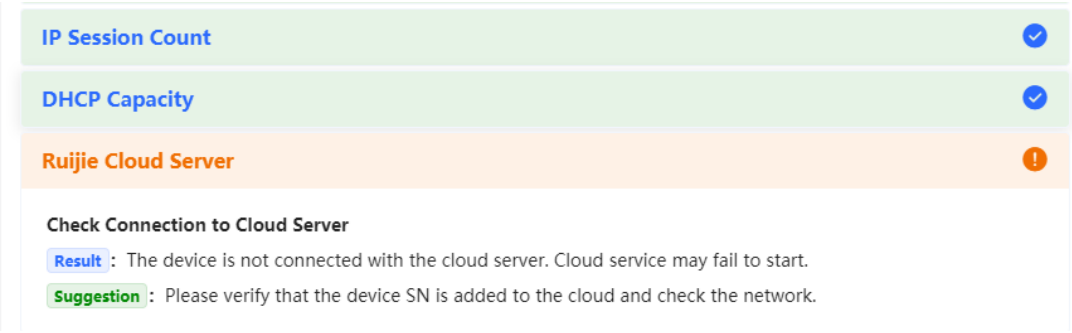
(1) Click  in the navigation bar, or choose **Diagnostics** > **Network Check** and go to the **Network Check** page.



(2) Click **Start** to perform the network check and show the result.



After performing the network check, you will find the check result and suggested action.



6.2 Network Tools

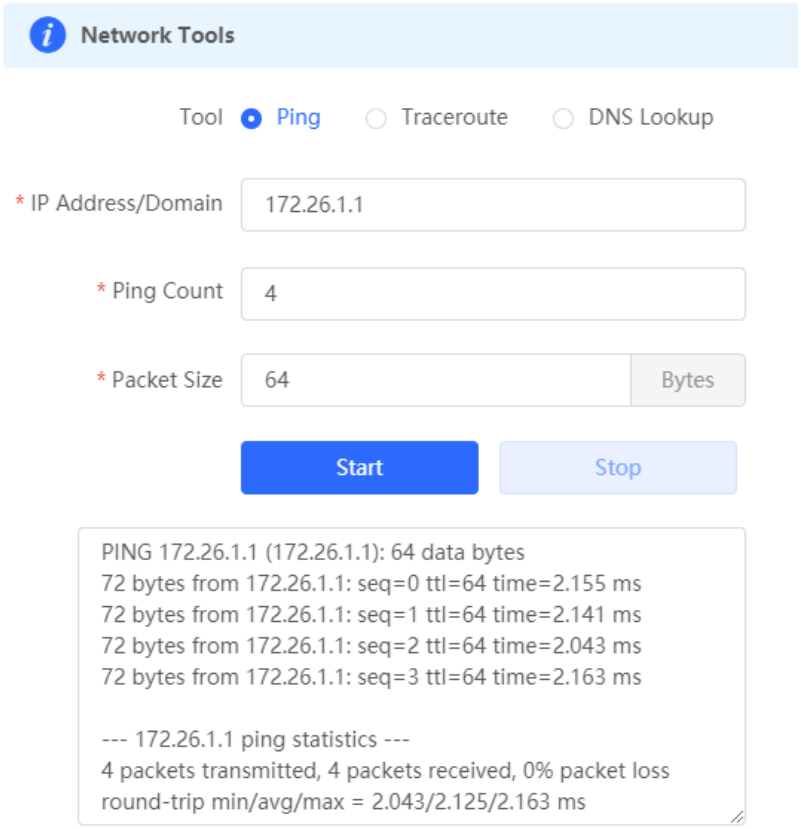
For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Diagnostics** > **Network Tools**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Diagnostics** > **Network Tools**

When you select the ping tool, you can enter the IP address or URL and click **Start** to test the connectivity between the access point and the IP address or URL. The message "Ping failed" indicates that the access point cannot reach the IP address or URL.

The Traceroute tool displays the network path to a specific IP address or URL.

The DNS Lookup tool displays the DNS server address used to resolve a URL.



6.3 Alarms

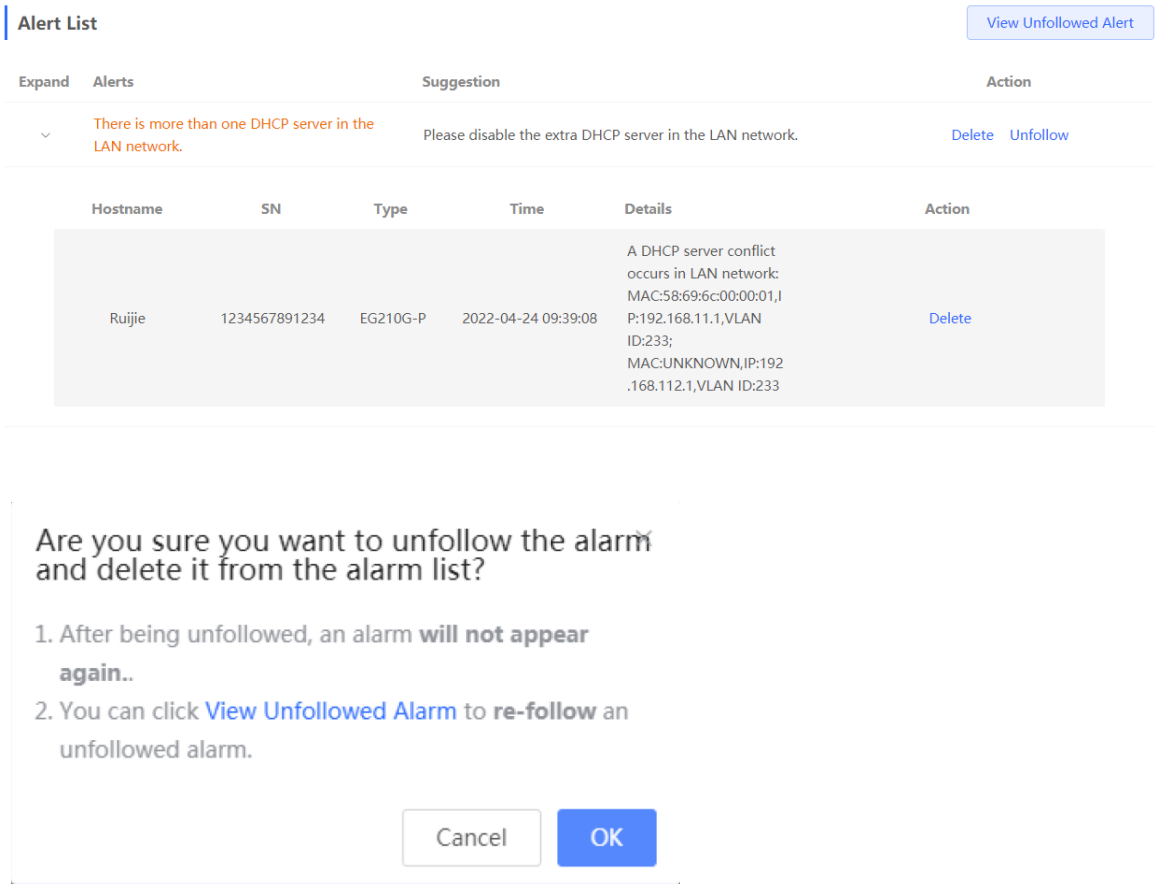
For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Network** mode, choose **Network** > **Alarms**

For other RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Diagnostics** > **Alarms**

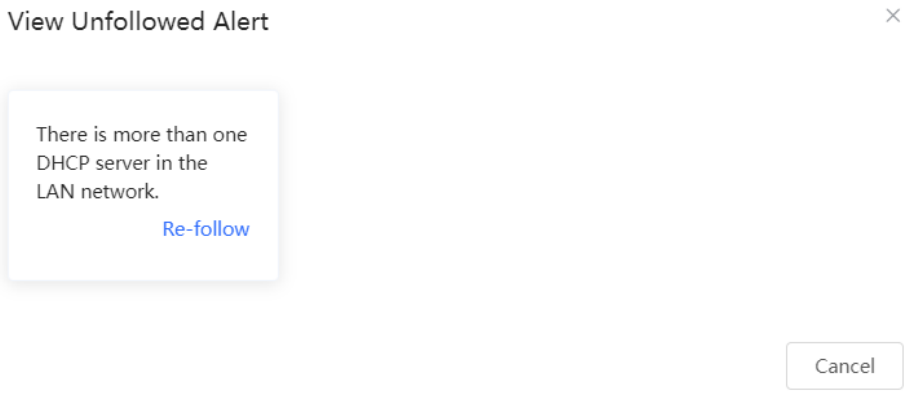
The Alarms page displays possible problems on the network environment and device. All types of alarms are followed by default. You can click **Unfollow** in the **Action** column to unfollow this type of alarm.

Caution

After unfollowing a type of alarm, you will not discover and process all alarms of this type promptly. Therefore, exercise caution when performing this operation.



Click **View Unfollowed Alarm** to view the unfollowed alarm. You can follow the alarm again in the pop-up window.

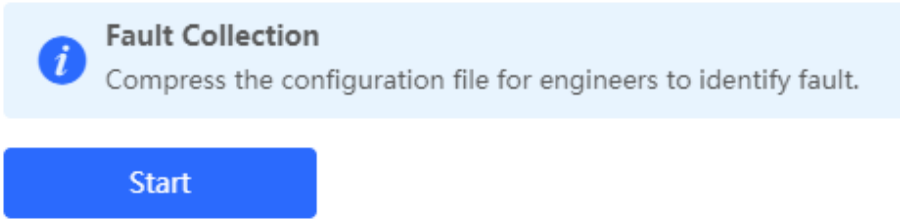


6.4 Fault Collection

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP1261, RG-RAP2266, RG-RAP2260, RG-RAP1260 and RG-RAP6262 models: In **Local Device** mode, choose **Diagnostics** > **Fault Collection**

For RAP models: Choose (**WLAN** > **APs** > **Manage** >) **Diagnostics** > **Fault Collection**

When an unknown fault occurs on the device, you can collect fault information on this page. Click **Start** to collect fault information and compress it into a file for engineers to identify fault.



7 FAQs

7.1 Login Failure

➢ **What can I do when I failed to log in to the eWeb management system?**

Perform the following steps:

(1) Check that the Ethernet cable is properly connected to the LAN port of the device.

(2) Before accessing the setup page, you are advised to choose **Auto** for the device enabled with DHCP service to assign an IP address to the PC. If you want to configure a static IP address for the PC, please make sure the IP address of the PC and the LAN port are in the same IP range. The default IP address of the LAN port is 10.44.77.254, and the subnet mask is 255.255.255.0. The IP address of the PC should be set to 10.44.77.X (X is an integer between 2 and 254), and the subnet mask is 255.255.255.0.

(3) Run the **Ping** command to check the connectivity between the PC and the device. If the ping fails, please check the network settings.

(4) If the login failure persists, restore the device to factory settings.

7.2 Factory Setting Restoration

➢ **How can I restore the device to factory settings?**

Power on the device and press the **Reset** button for more than 5 seconds. The device is restored to factory settings after it is restarted. Then, you can log in to the Eweb management system using the default IP address (10.44.77.254).

7.3 Password Loss

➢ **What can I do when I forget the password?**

- Webpage management password loss: Please enter the Wi-Fi password. If it is still incorrect, please restore the device to factory settings.
- Wi-Fi password loss: When the access point expands the Wi-Fi coverage, its Wi-Fi password is consistent with that of the master router. Please check the configuration of the master router and enter its Wi-Fi password. If the password is still incorrect, please restore the device to factory settings and reconfigure the Wi-Fi password.