

Ruijie Reyee RG-RAP Series Access Points

ReyeeOS 1.218

Web-based Configuration Guide



Copyright

Copyright © 2023 Ruijie Networks

All rights are reserved in this document and this statement.

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

Trademarks including  are owned by Ruijie Networks.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

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 Reye: <https://www.ruijienetworks.com/products/reeye>
- 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 features of the RG-RAP series access points and instructs users to configure the device.

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.....	41
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 Wireless Rate Limiting	48
3.12.1 Overview	48
3.12.2 Configuration Steps	49
3.13 Configuring Wi-Fi Blacklist or Whitelist.....	51
3.13.1 Overview	51
3.13.2 Configuration Steps	52
3.14 Optimizing Wi-Fi Network	53
3.14.1 Overview	53
3.14.2 Getting Started.....	53
3.14.3 Optimizing the Radio Channel.....	54
3.14.4 Optimizing the Channel Width	55
3.14.5 Optimizing the Transmit Power.....	56
3.14.6 Configuring the Multicast Rate.....	57
3.14.7 Configuring the Client Limit.....	58
3.14.8 Configuring the Kick-off Threshold	59
3.14.9 Configuring the Roaming Sensitivity.....	59
3.14.10 Configuring Access Threshold.....	60
3.14.11 Configuring Response RSSI Threshold.....	61

3.14.12 Configuring WIO	62
3.14.13 Configuring Wi-Fi Roaming Optimization (802.11k/v)	63
3.15 Configuring Healthy Mode	64
3.16 Configuring XPress	65
3.17 Configuring Wireless Schedule	66
3.18 Enabling Reye Mesh.....	66
3.19 Configuring AP Load Balancing.....	67
3.19.1 Overview	67
3.19.2 Configuring Client Load Balancing	67
3.19.3 Configuring Traffic Load Balancing.....	69
4 Network Settings	71
4.1 Switching Work Mode	71
4.1.1 Work Mode.....	71
4.1.2 Self-Organizing Network Discovery	71
4.1.3 Configuration Steps	71
4.1.4 Viewing Device Role	73
4.2 Configuring Internet Connection Type (IPv4)	73
4.3 Configuring Internet Connection Type (IPv6)	74
4.4 Configuring LAN Port.....	75
4.5 Configuring Repeater Mode.....	76
4.5.1 Wired Repeater	76
4.5.2 Wireless Repeater	77
4.6 Creating a VLAN.....	79
4.7 Configuring Port VLAN	81

4.8 Changing MAC Address	83
4.9 Changing MTU.....	83
4.10 Configuring DHCP Server.....	84
4.10.1 DHCP Server	84
4.10.2 Configuring the DHCP Server Function.....	84
4.10.3 Displaying Online DHCP Clients.....	85
4.10.4 Displaying the DHCP Static IP Address List.....	86
4.11 Link Aggregation	86
4.12 Configuring DNS.....	87
4.13 Hardware Acceleration	87
4.14 Configuring Port Flow Control	88
4.15 Configuring ARP Binding	88
4.16 Configuring LAN Ports	89
4.17 IPv6 Settings.....	90
4.17.1 Overview	90
4.17.2 IPv6 Basic	90
4.17.3 IPv6 Address Assignment Methods	91
4.17.4 Enabling IPv6.....	92
4.17.5 Configuring the IPv6 Address for the WAN Port.....	92
4.17.6 Configuring the IPv6 Address for the LAN Port	94
4.17.7 Viewing DHCPv6 Clients	96
4.17.8 Configuring the Static DHCPv6 Address	96
4.17.9 Configuring the IPv6 Neighbor List.....	97
5 System Settings	99

5.1 PoE	99
5.2 PoE Settings	99
5.3 Setting the Login Password.....	100
5.4 Setting the Session Timeout Duration.....	101
5.5 Setting and Displaying System Time.....	101
5.6 Configuring Reboot.....	103
5.6.1 Rebooting the Current Device	103
5.6.2 Rebooting All Devices in the Network.....	103
5.6.3 Rebooting the Specified Device.....	104
5.7 Configuring Scheduled Reboot.....	105
5.7.1 Configuring Scheduled Reboot for the Current Device	105
5.8 Configuring Backup and Import.....	106
5.9 Restoring Factory Settings	107
5.9.1 Restoring the Current Device to Factory Settings.....	107
5.9.2 Restoring All Devices to Factory Settings.....	108
5.10 Performing Upgrade and Checking System Version.....	108
5.10.1 Online Upgrade.....	108
5.10.2 Local Upgrade.....	109
5.11 Switching System Language	109
5.12 Configuring LED Status Control	110
6 Network Diagnosis Tools.....	111
6.1 Network Check.....	111
6.2 Network Tools.....	112
6.3 Alarms	113

6.4 Fault Collection	114
7 FAQs.....	115
7.1 Login Failure	115
7.2 Factory Setting Restoration	115
7.3 Password Loss.....	115

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

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-SXXXX (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.
-

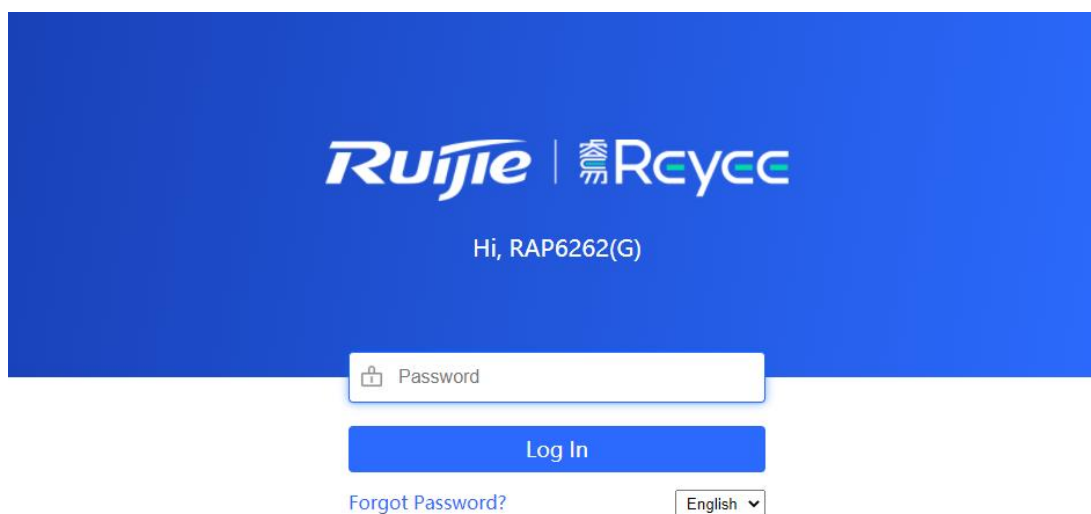
1.3.3 Logging in to the Web Page

- (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.



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

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

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

 **Caution**

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

1.4 Work Mode

The device can work in 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

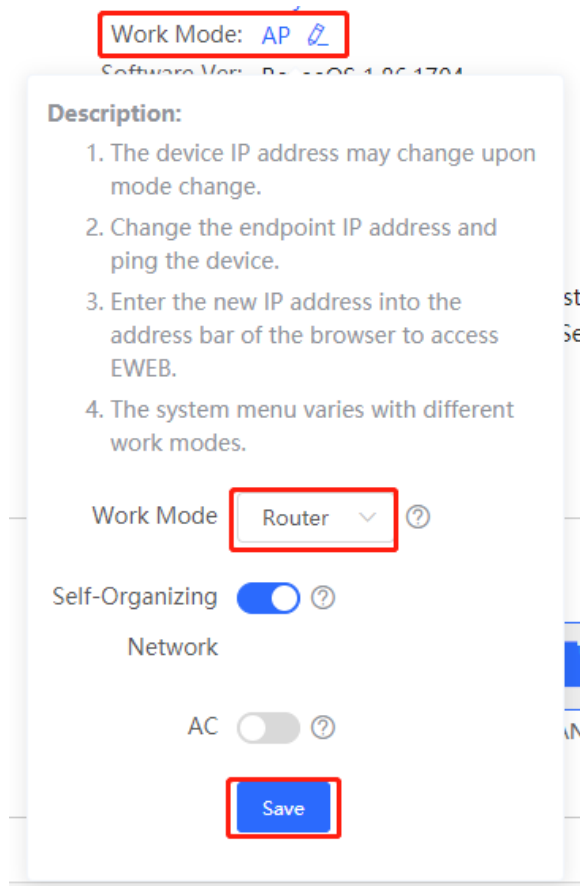
The device does not support the routing and DHCP server functions in the wireless repeater mode. IP addresses of the clients are assigned and managed by the primary router. On an available network, the device can be connected to the primary router through wireless connection to expand the Wi-Fi coverage 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.
- (1) 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:
 - o Figure out whether the Internet connection type is PPPoE, DHCP mode, or static IP address mode.
 - o In the PPPoE mode, a username, a password, and possibly a service name are needed.
 - o In the static IP address mode, an IP address, a subnet mask, a gateway, and a DNS server need to be configured.
- (2) 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

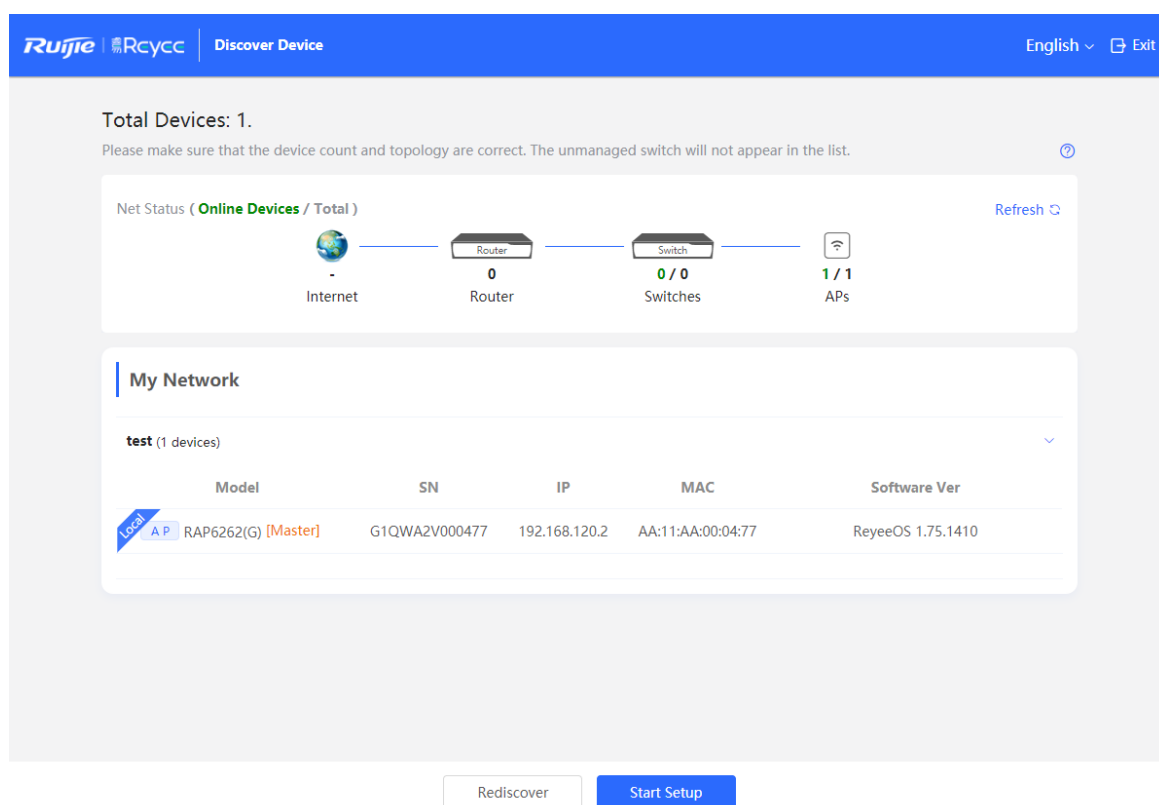
1. Add a Device to Network

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.



Total Devices: 1.
Please make sure that the device count and topology are correct. The unmanaged switch will not appear in the list.

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

Internet — Router (0) — Switches (0 / 0) — APs (1 / 1)

My Network

test (1 devices)

	Model	SN	IP	MAC	Software Ver
Local A P	RAP6262(G) [Master]	G1QWA2V000477	192.168.120.2	AA:11:AA:00:04:77	ReyeeOS 1.75.1410

Rediscover **Start Setup**

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.

(1) **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**.

- o **Static IP:** Enter the IP address, subnet mask, gateway, and DNS server, and click **Next**.
- (2) **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.
 - (3) **Management Password:** The password is used for logging in to the management page.
 - (4) **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.
 - (5) **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.

Ruijie | Rcycc | Create Network English ▾ Exit

* Network Name

Network Settings

Internet PPPoE DHCP Static IP
⚠ Checking IP assignment

* SSID

Wi-Fi Password Security Open

Management Password (Please remember the password.)

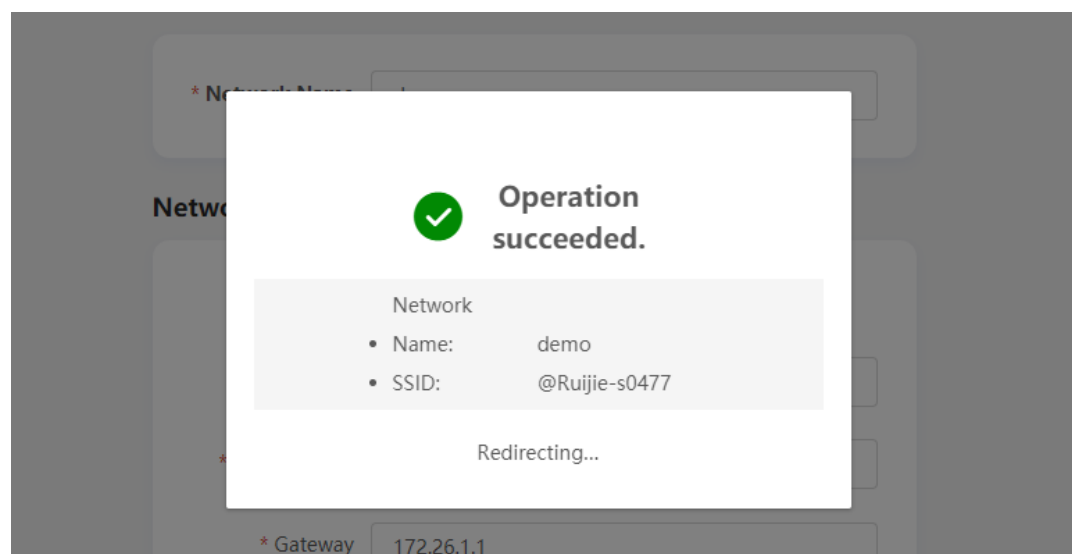
* Management Password

Country/Region/Time Zone ▾

* Country/Region ▾

* 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. See [Creating a New Project](#) for details.

The screenshot shows the 'Create Network' configuration wizard. At the top, there is a header with the Ruijie logo, 'Rcycc', and 'Create Network' text, along with a language dropdown set to 'English' and an 'Exit' button. The main configuration area is divided into several sections:

- Network Name:** A text input field with the placeholder 'Example: XX hotel.'
- Network Settings:**
 - Internet:** Radio buttons for 'DHCP' (selected) and 'Static IP'.
 - SSID:** A text input field containing '@Ruijie-s0477'.
 - Wi-Fi Password:** Radio buttons for 'Security' (selected) and 'Open', followed by a password input field with masked characters and a 'Show/Hide' icon.
- Management Password (Please remember the password.):** A text input field with the placeholder 'Please remember the management pas:' and a 'Show/Hide' icon.
- Country/Region/Time Zone:** A section with a dropdown arrow on the right, containing:
 - Country/Region:** A dropdown menu showing 'China (CN)'.
 - Time Zone:** A dropdown menu showing '(GMT+8:00)Asia/Shanghai'.

At the bottom of the form is a blue button labeled 'Create Network & Connect'.

1.7 Configuration Wizard (Wireless Repeater Mode)

1.7.1 Getting Started

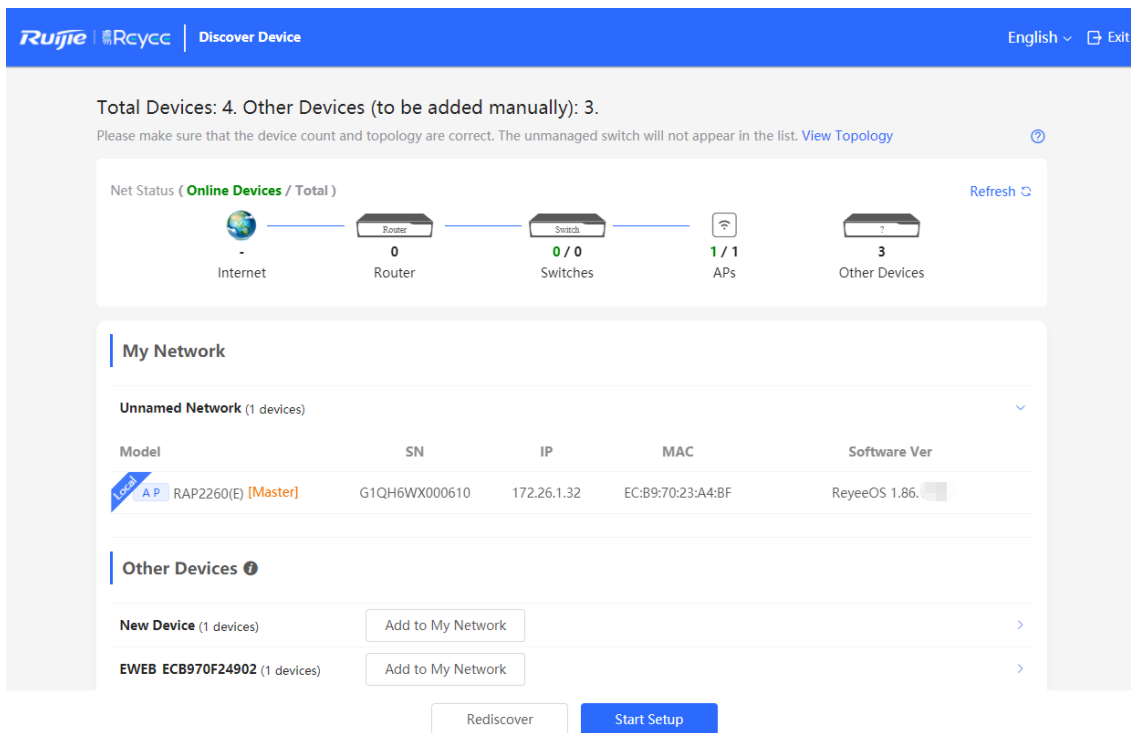
- Before configuring the wireless repeater mode, configure the primary router and test that the primary router can access the Internet.
- Place the device where it can discover at least two-bar Wi-Fi signal of the primary router.

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**.



The screenshot shows the Ruijie Rcycc web interface. At the top, there is a blue header with the Ruijie logo and 'Rcycc Discover Device'. The main content area displays network status and device discovery options.

Total Devices: 4. Other Devices (to be added manually): 3.
Please make sure that the device count and topology are correct. The unmanaged switch will not appear in the list. [View Topology](#)

Net Status (Online Devices / Total)

- Internet: -
- Router: 0
- Switches: 0 / 0
- APs: 1 / 1
- Other Devices: 3

My Network

Unnamed Network (1 devices)

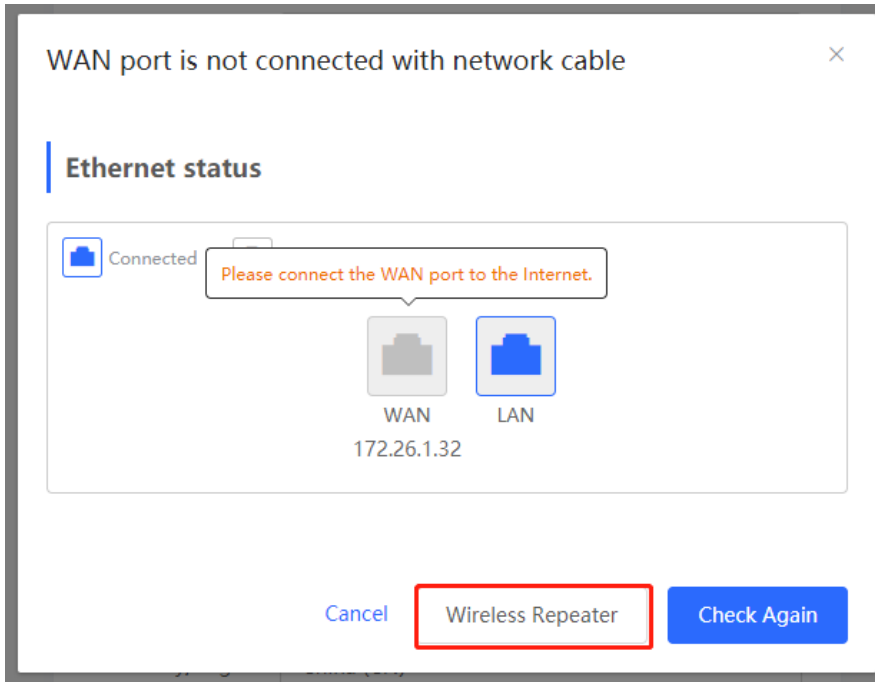
Model	SN	IP	MAC	Software Ver
Local A P RAP2260(E) [Master]	G1QH6WX000610	172.26.1.32	EC:B9:70:23:A4:BF	ReyeeOS 1.86.

Other Devices

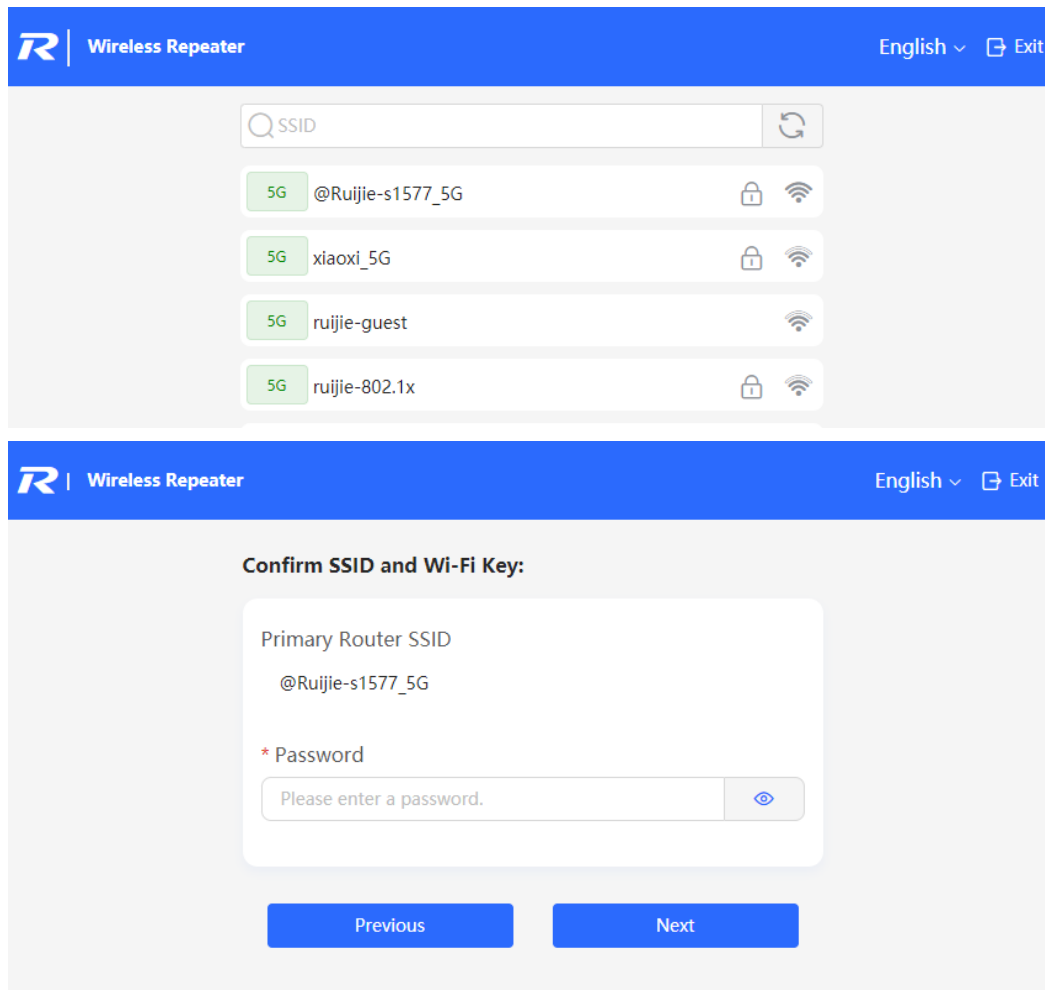
- New Device (1 devices)** Add to My Network
- EWEB ECB970F24902 (1 devices)** Add to My Network

Buttons: Rediscover, 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-RAP2260 and RG-RAP6262 models, please refer to Dual Management Webpages.

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

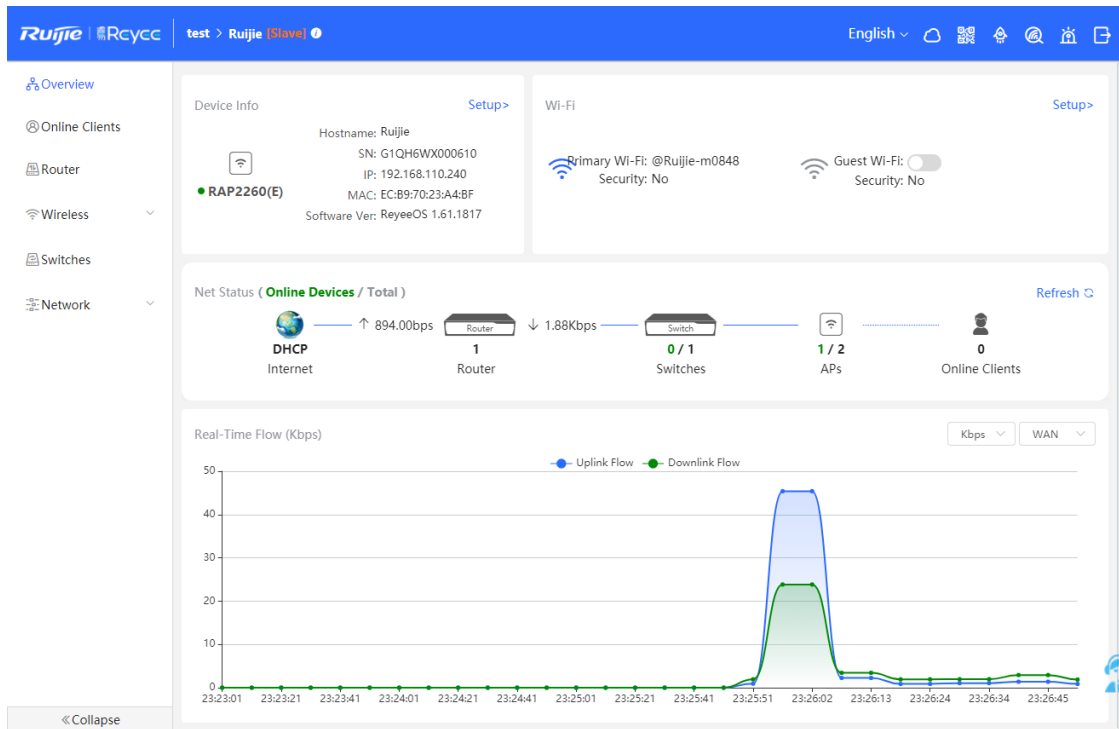
Note

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).

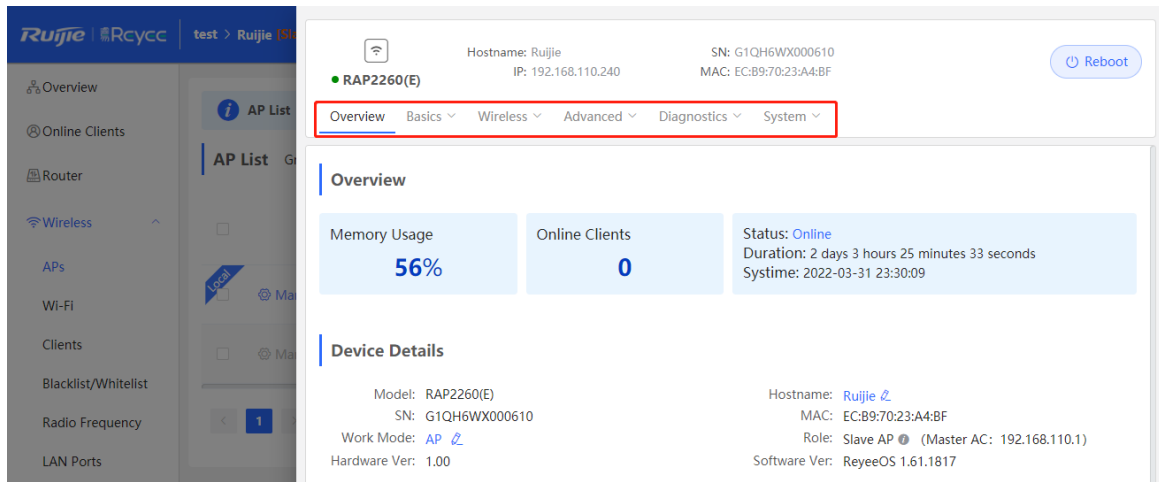


2. Standalone Management

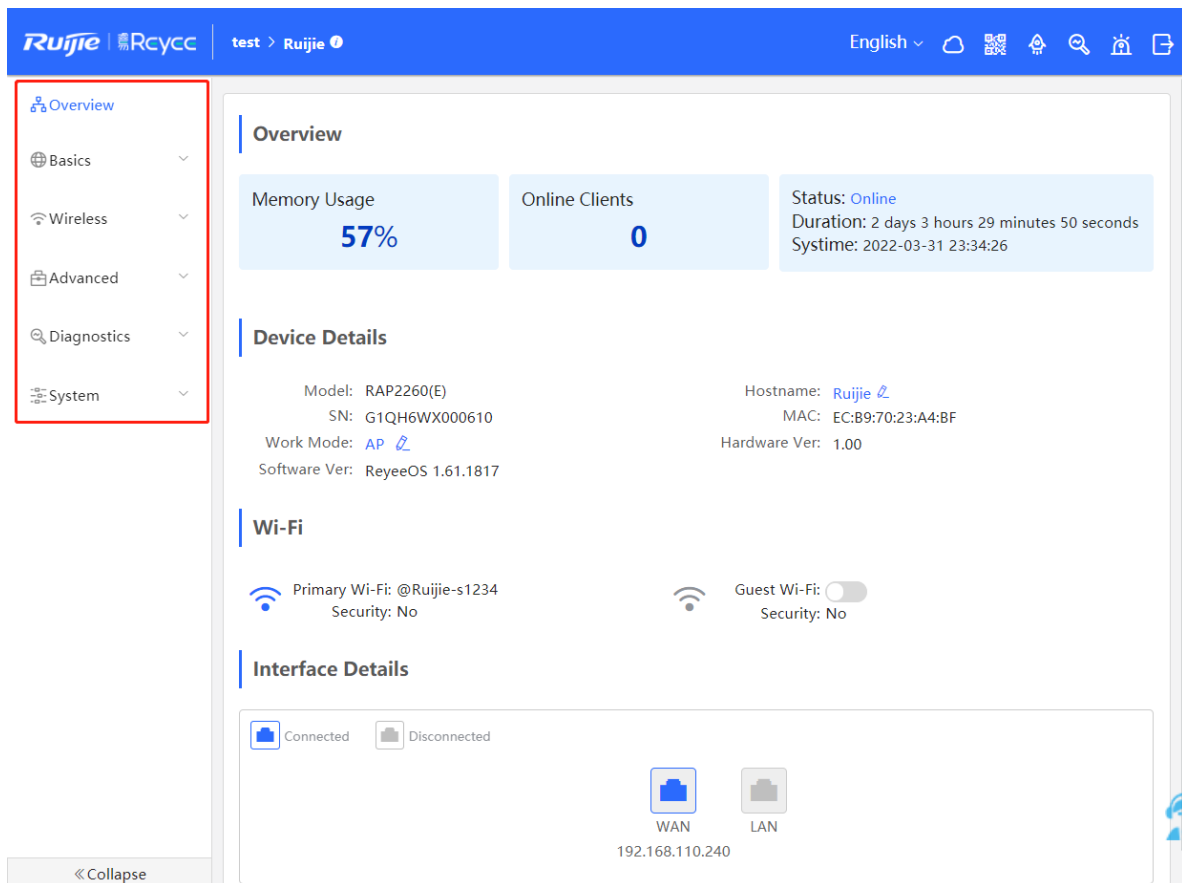
- If a device is in self-organizing network mode, click the name of the currently logged in device or click **Manage** of a specified device in the device list to configure and manage the device.

The screenshot shows the 'AP List' section of the Ruijie Rcycc web interface. The table lists the following devices:

	Action	Hostname	IP	MAC	Status	Model	Clients	
<input type="checkbox"/>	Manage Reboot	Ruijie	192.168.110.240	EC:B9:70:23:A4:BF	Online	RAP2260(E)	0	R
<input type="checkbox"/>	Manage Reboot	Ruijie	192.168.110.29	AA:11:AA:00:04:77	Offline	RAP6262(G)	1	R



- 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

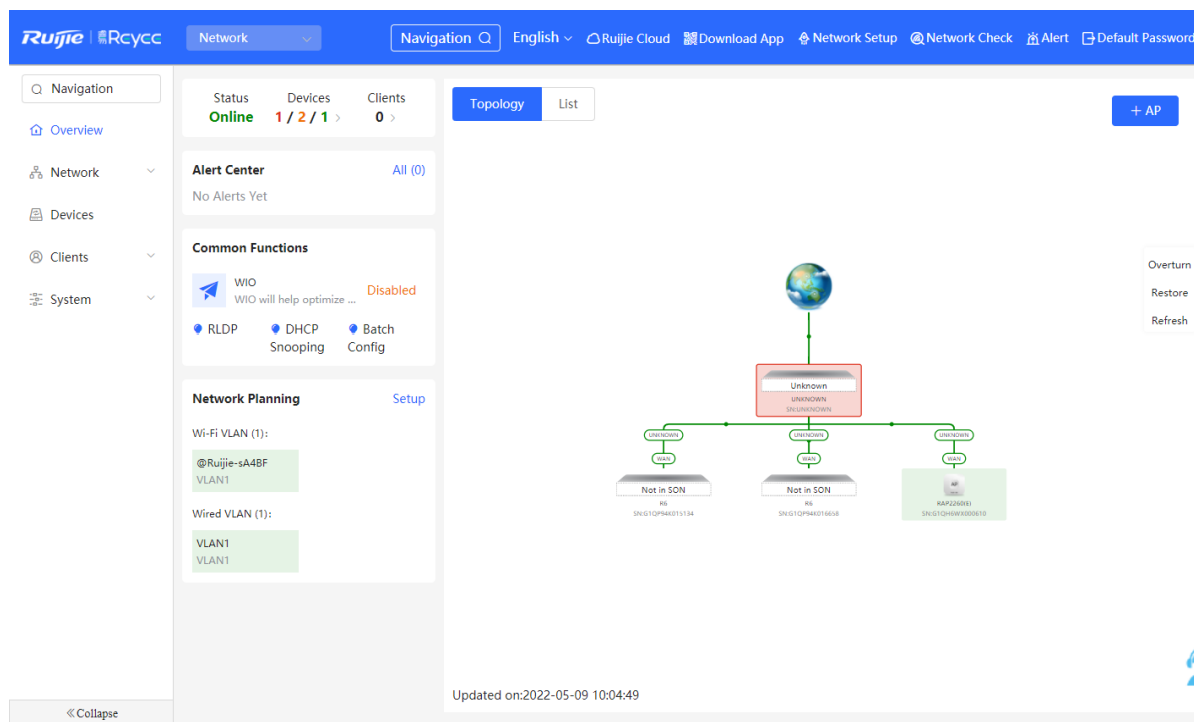
1. Introducing the Management Mode

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.

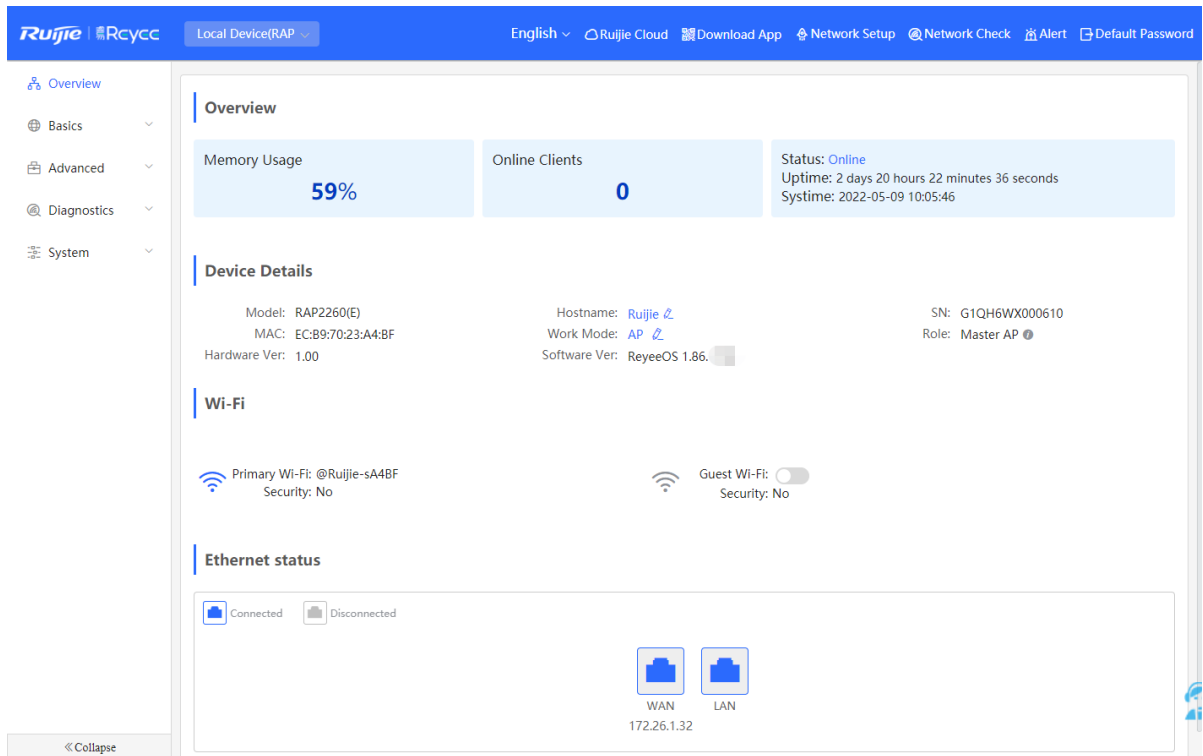
If the self-organizing network is enabled, the device can work in the network mode and the local device mode. The two modes can be switched on the Web page.

- 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

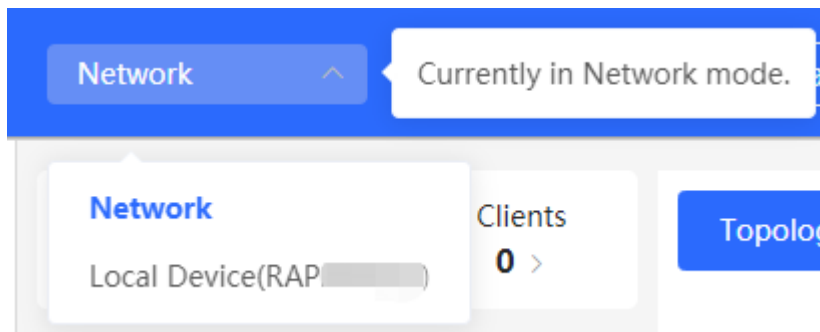


Local Device mode webpage



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.



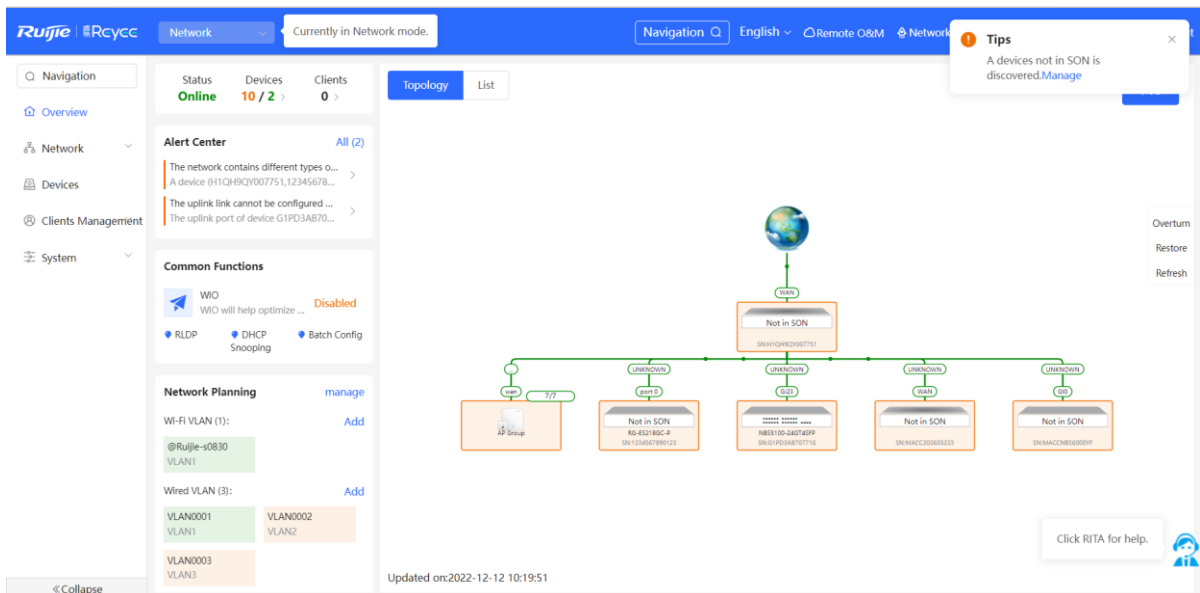
2 Network Monitoring

⚠ Caution

The functions mentioned in this chapter are supported by only RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP2260, and RG-RAP6262.

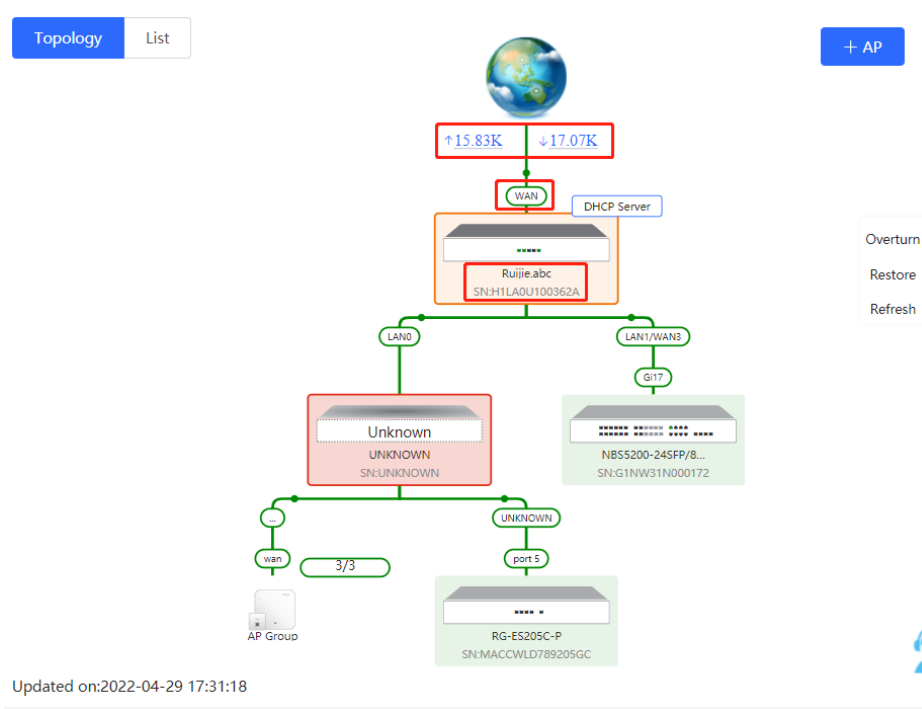
In **Network** mode, select  **Overview**.

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.

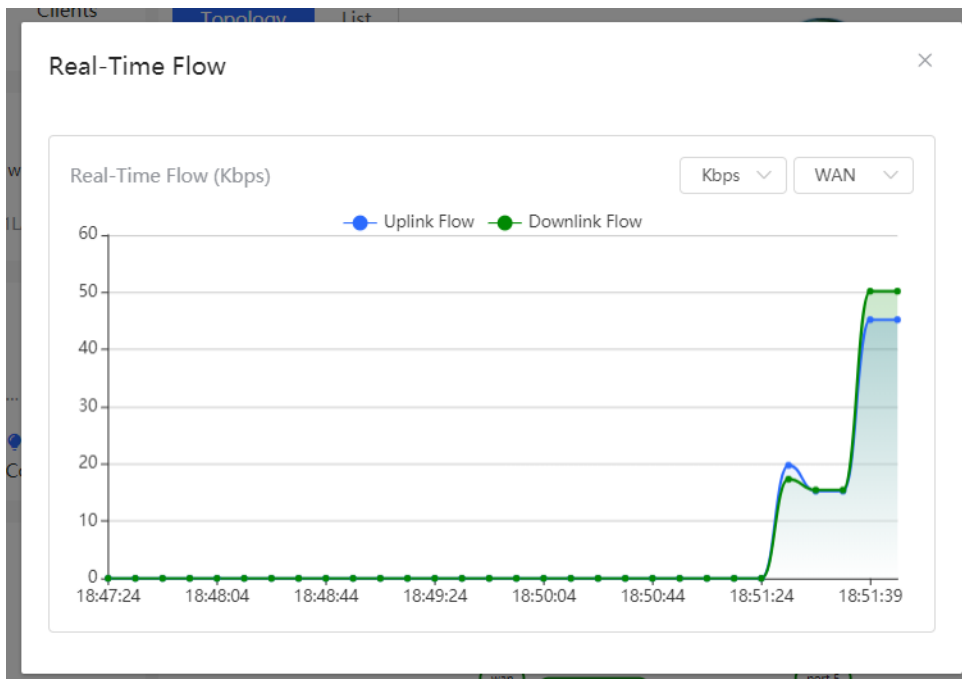



2.1 Viewing the Network Information

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 screenshot displays the Ruijie network management interface. On the left, a network topology diagram shows a central switch connected to various devices. The main panel shows the configuration for a specific device, 'Ruijie.abc'. The 'Port Status' section shows the status of LAN0, LAN1, LAN2, WAN1, and WAN ports. The 'VLAN' section shows the default VLAN configuration for the LAN0,1 interface.

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

Port Status

LAN0 LAN1 LAN2 WAN1 WAN

VLAN

Default VLAN

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

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

- 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.

The screenshot shows a simplified network topology diagram. A central switch, 'Ruijie.abc', is connected to a WAN port and two LAN ports (LAN0 and LAN1/WAN3). The WAN port is connected to a DHCP Server. The switch is labeled with its model 'EG205G' and serial number 'SN: H1LA0U100362A'. The 'Refresh' button in the bottom right corner is highlighted with a red box.

↑ 14.05K ↓ 22.45K

WAN DHCP Server

Ruijie.abc
 SN: H1LA0U100362A

LAN0 LAN1/WAN3

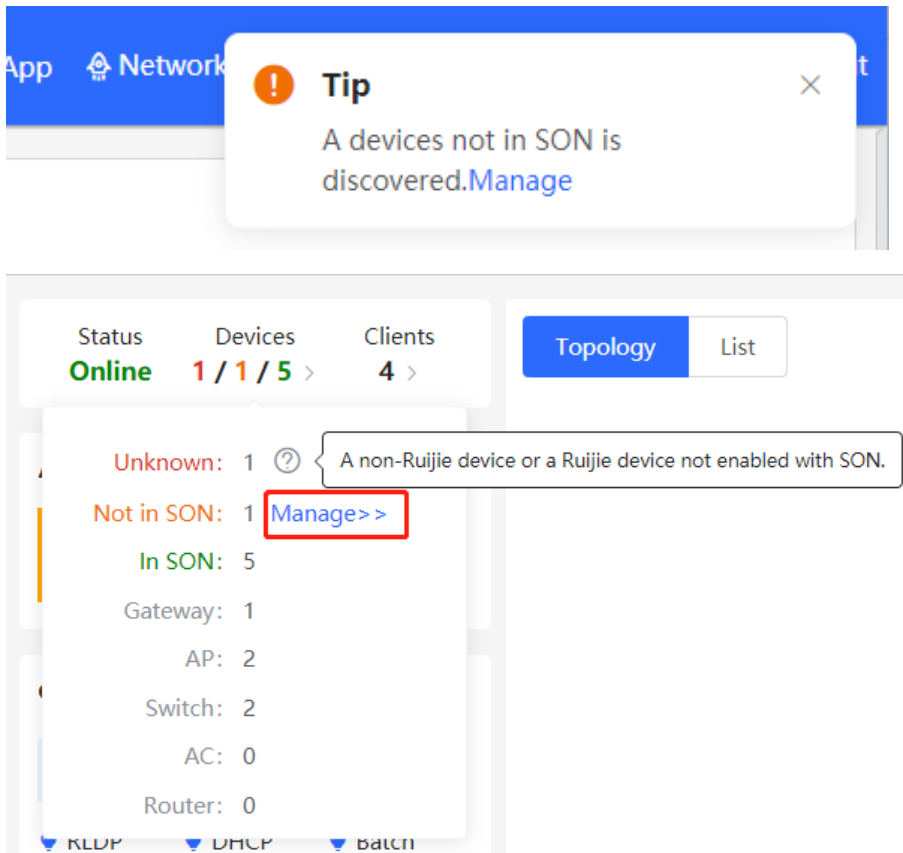
Overturn
 Restore
Refresh

2.2 Adding Network Devices

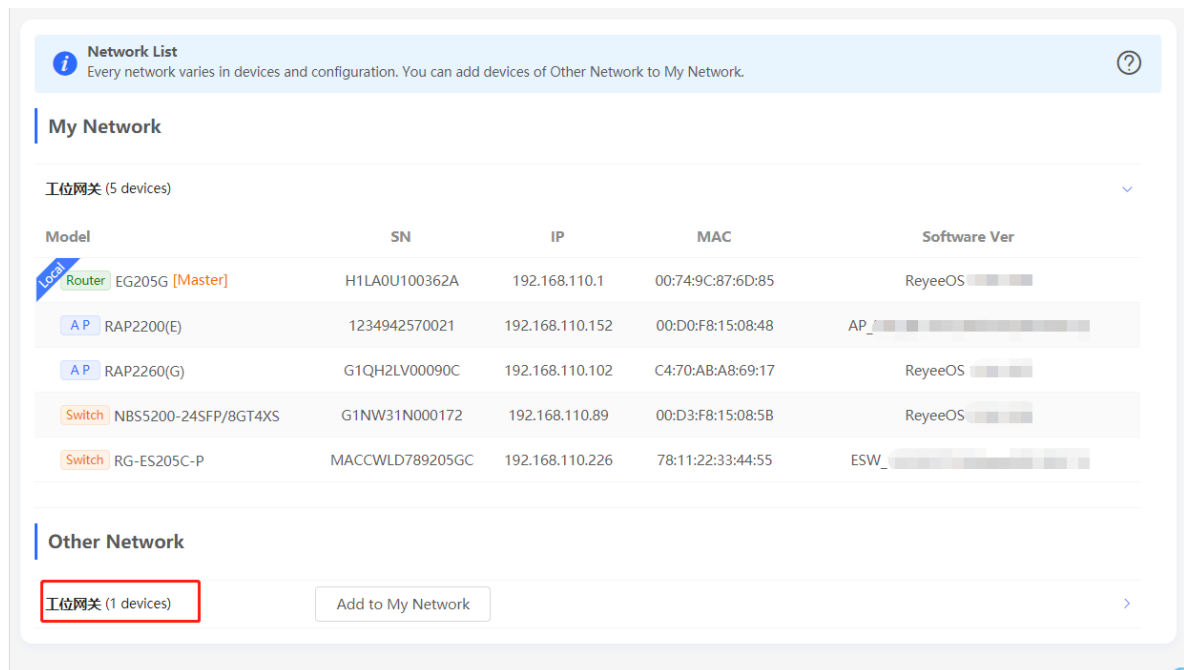
2.2.1 Wired Connection

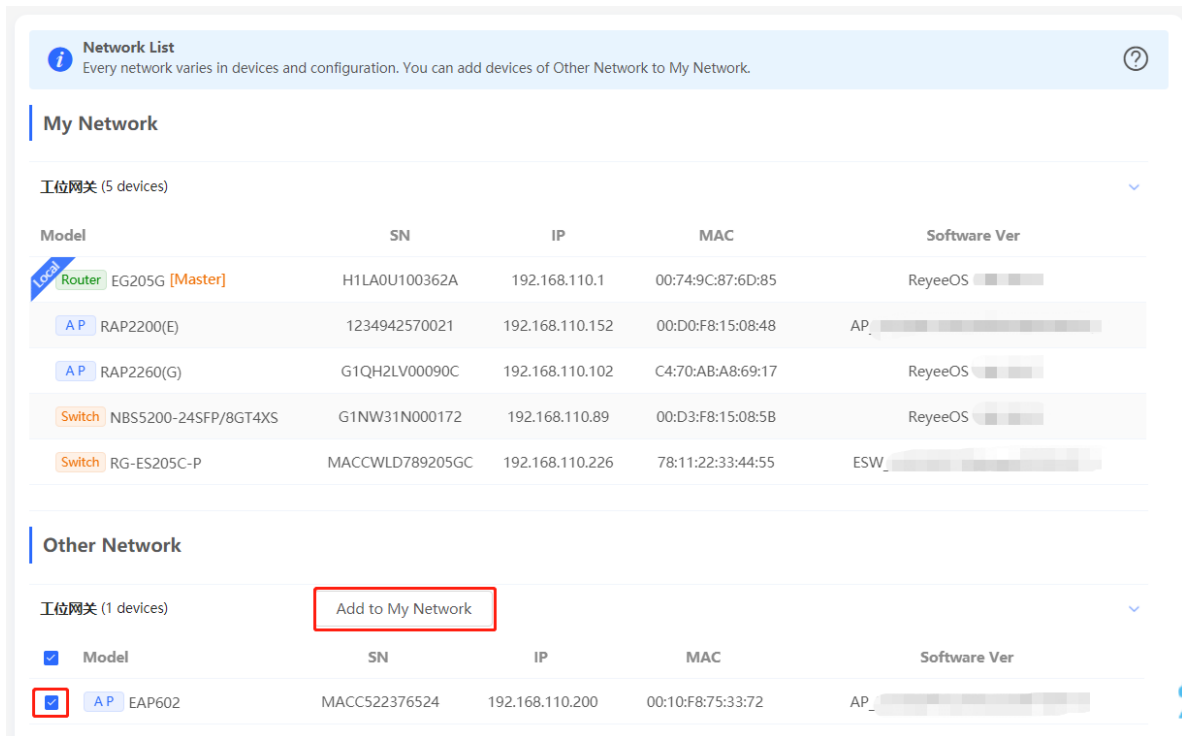
- If a new device is connected to the device in the network through wired connection, a prompt message will pop up, indicating that a device not in SON (Self-Organizing Network) is discovered. The number (in orange)

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.

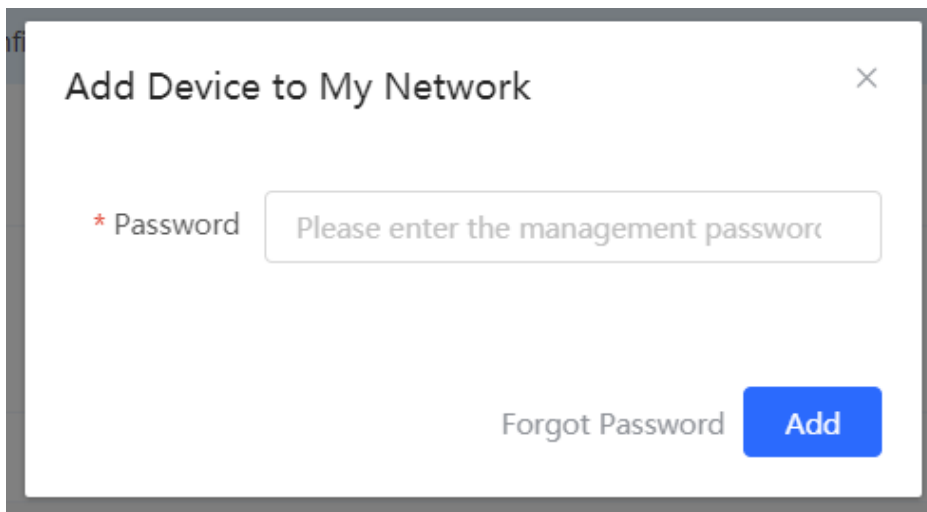


(2) Go to the **Network List** page, click **Other Network** to select the target device and click **Add to My Network**.





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).

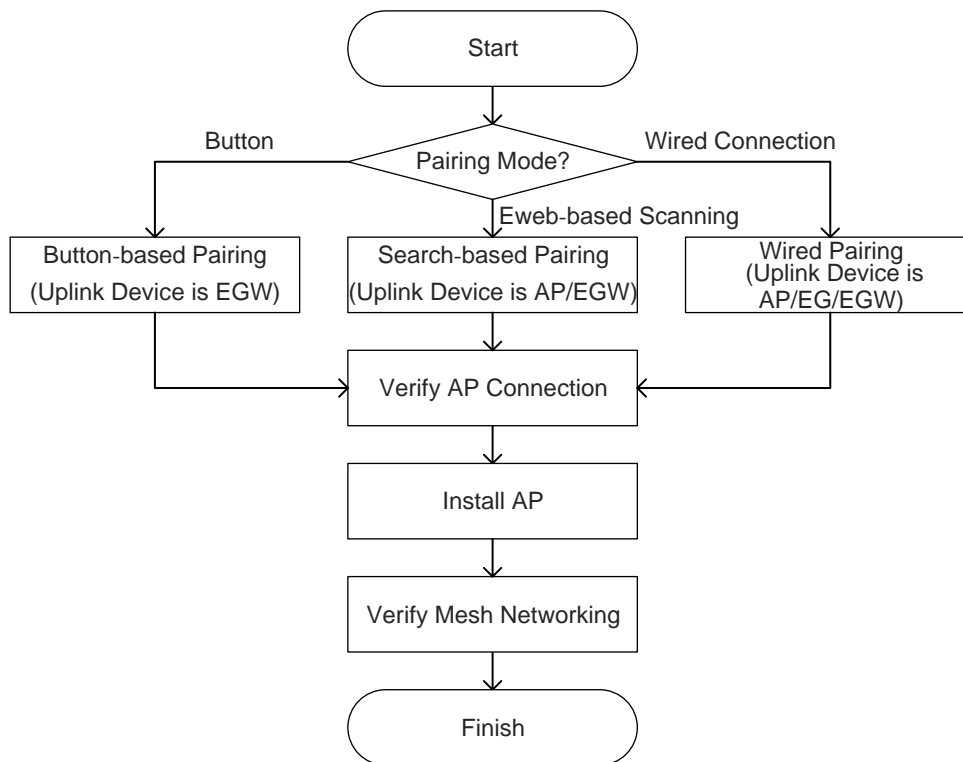
1. Overview

After being powered on and enabled with Mesh (see 3.18 ___ 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

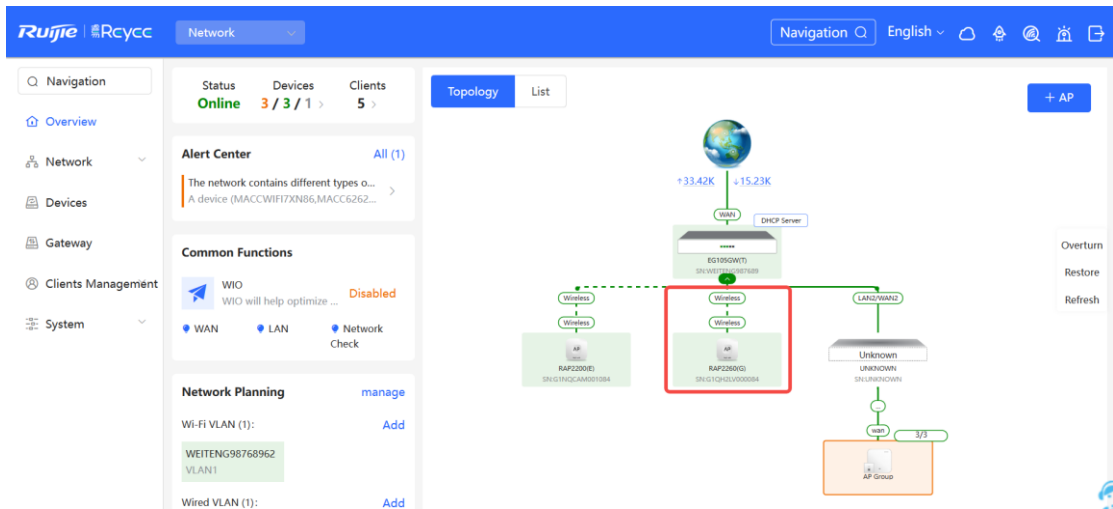
- Only EG105GW-X and EG105GW(T) support button-based pairing and each router can be paired with up to 15 new APs.
- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh (see 3.18 ___ for details).

- 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.

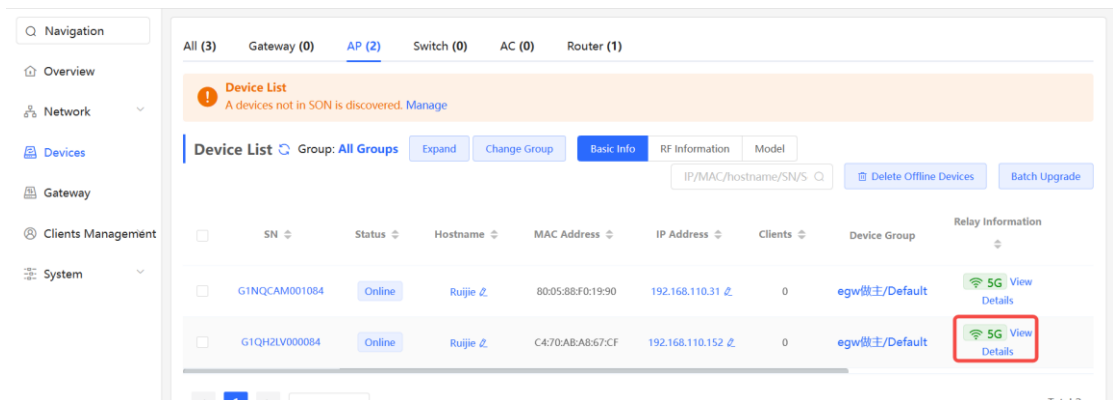
(3) Check the topology on the **Overview** page to make sure that the new AP has connected to the uplink device in wireless mode.




(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.

All (3) Gateway (0) **AP (2)** Switch (0) AC (0) Router (1)

Device List
A devices not in SON is discovered. [Manage](#)

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

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

SN	Status	Hostname	MAC Address
G1NQCAM001084	Online	Ruijie	80:05:88:F0:19:90
G1QH2LV000084	Online	Ruijie	C4:70:AB:A8:67:CF

Noise Floor: -86 dBm
Channel Utilization: 13 %
RSSI: -37 dBm **Good**
Negotiation Rate: 866 Mbps
Uptime: 4 minutes 4 seconds

Uplink Local

Model: EG105GW(T) Model: RAP2260(G)
SN: WEITENG987689 SN: G1QH2LV000084
IP: 192.168.110.1 IP: 192.168.110.152

Relay Information

5G View Details

5G View Details

Total 2

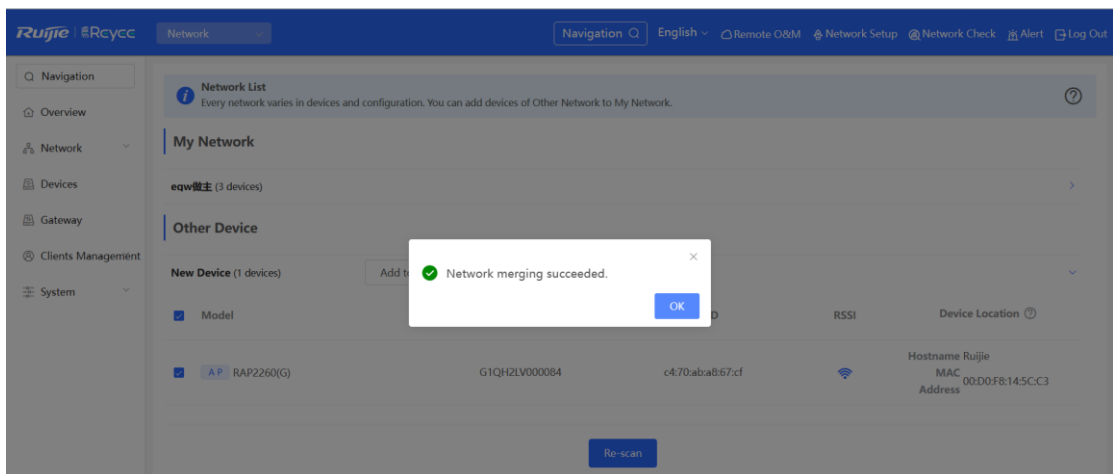
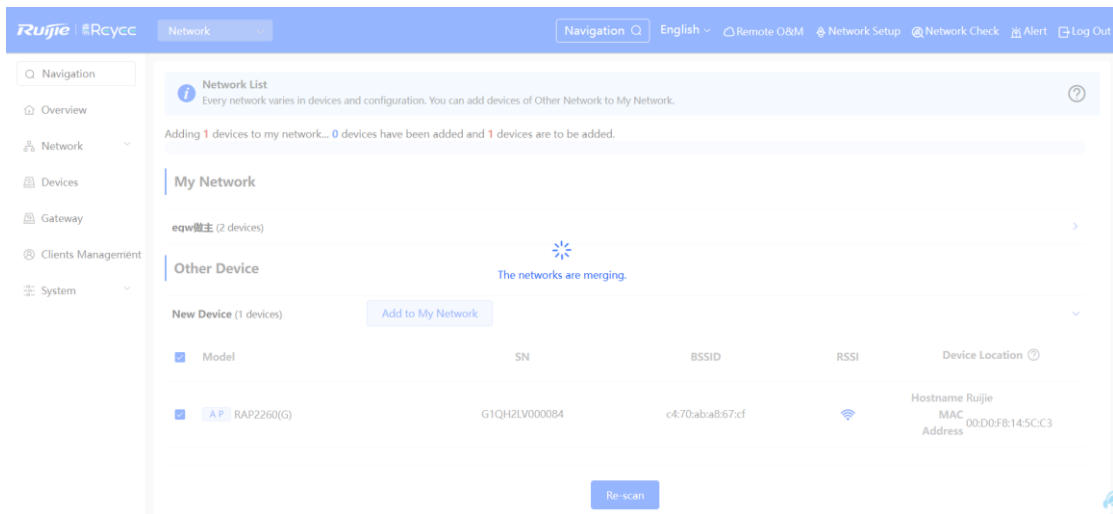
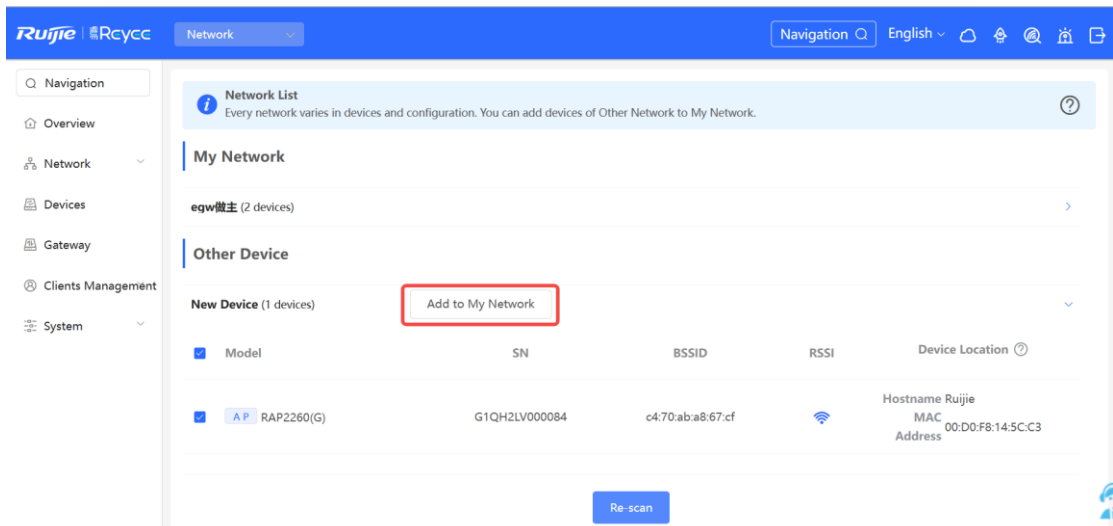
4. Configuration Steps for Search-based Pairing (Uplink Device is an AP or EGW Router)

Caution

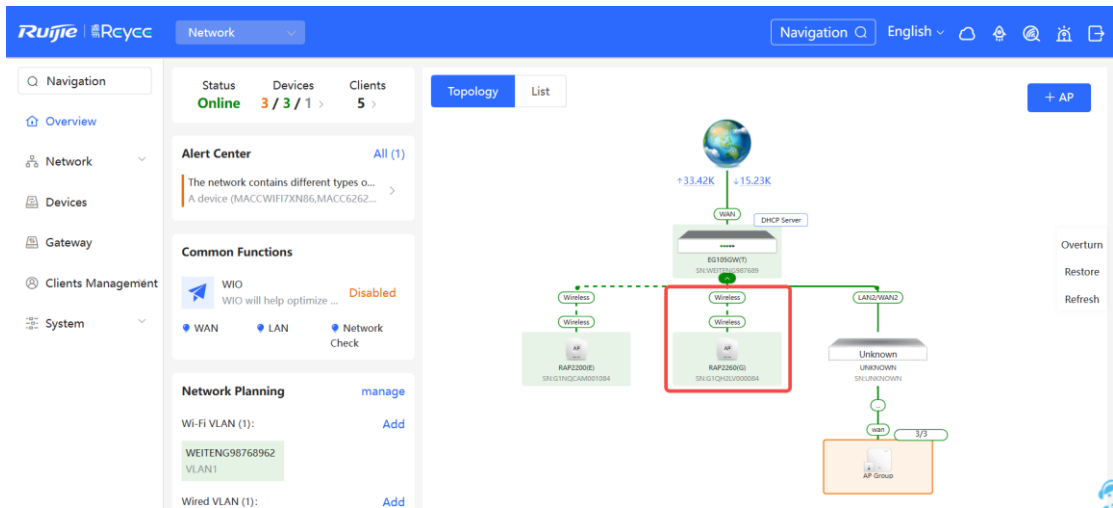
- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh (see 3.18___ for details).
- Place the new AP no more than 2 meters away from the uplink device to ensure that the new AP can receive the Wi-Fi signal from the uplink device. The new AP may fail 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.

SN	Status	Hostname	MAC Address	IP Address	Clients	Device Group	Relay Information
G1NQCAM001084	Online	Ruijie	80:05:88:F0:19:90	192.168.110.31	0	egw/默认/Default	 View Details
G1QH2LV000084	Online	Ruijie	C4:70:AB:AB:67:CF	192.168.110.152	0	egw/默认/Default	 View Details

Click **View Details** following the  icon to obtain information about the uplink device and RSSI.

The screenshot shows the 'Device List' page with a popup window displaying RF information for a Ruijie device. The popup includes the following data:

- Noise Floor: -86 dBm
- Channel Utilization: 13 %
- RSSI: -37 dBm **Good**
- Negotiation Rate: 866 Mbps
- Uptime: 4 minutes 4 seconds

Below the text, there is a diagram showing an 'EWR' (E-Wireless Router) and an 'AP' (Access Point) connected via a '5G' link. The EWR is labeled 'Ruijie' and the AP is labeled 'Ruijie'. The popup also lists the model and IP addresses for both devices:

- EWR Model: EG105GW(T), SN: WEITENG987689, IP: 192.168.110.1
- AP Model: RAP2260(G), SN: G1QH2LV000084, IP: 192.168.110.152

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 [3.18](#) for details).

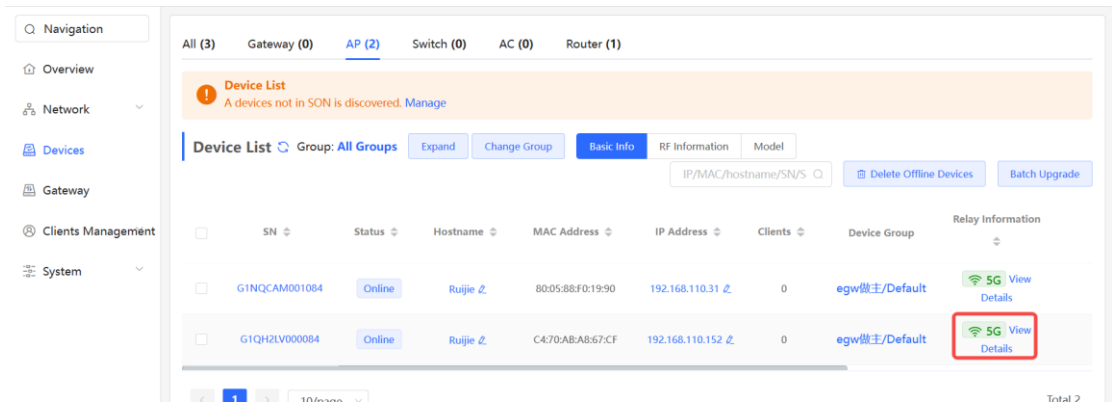
- (1) Plug one end of the Ethernet cable to the uplink port of the new AP, and the other end to the downlink port of an AP, EG router, or EGW router on the target network. Mesh networking takes one to three minutes. When the system status LED is steady on, it indicates that Mesh networking finishes.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


The screenshot shows the 'Device List' page with a table of devices. The new AP is highlighted with a red box. The table columns are SN, Status, Hostname, MAC Address, IP Address, Software Ver, and Model.

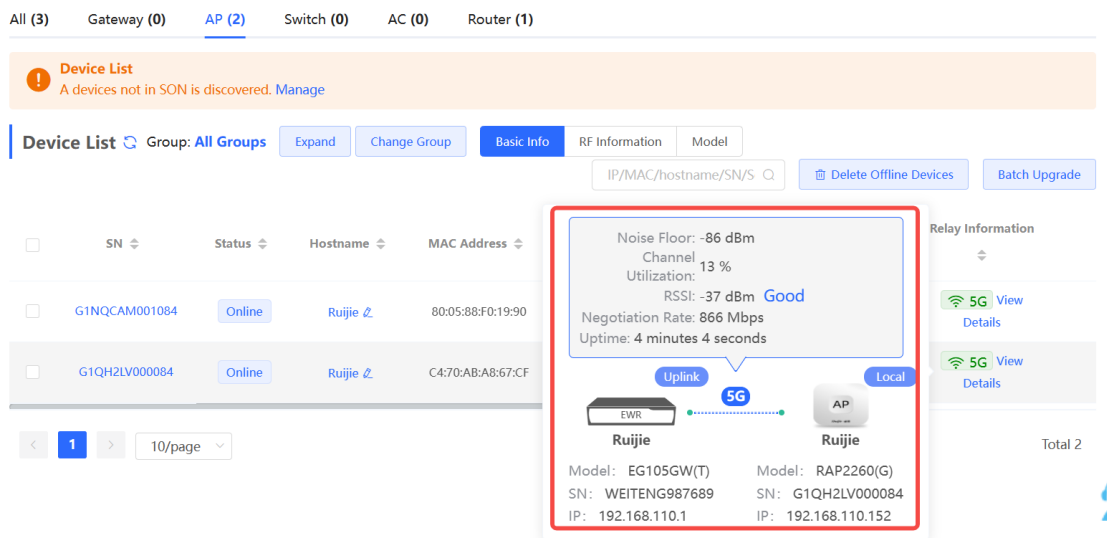
SN	Status	Hostname	MAC Address	IP Address	Software Ver	Model
WEITENG987689	Online	Ruijie [Master]	00:D0:F8:14:5C:C3	10.18.108.1	ReyeeOS 1.218.1308	EG105GW(T)
G1NQCAM001084	Online	Ruijie	80:05:88:F0:19:90	192.168.110.31	ReyeeOS 1.218.2427	RAP2200(E)

- (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.



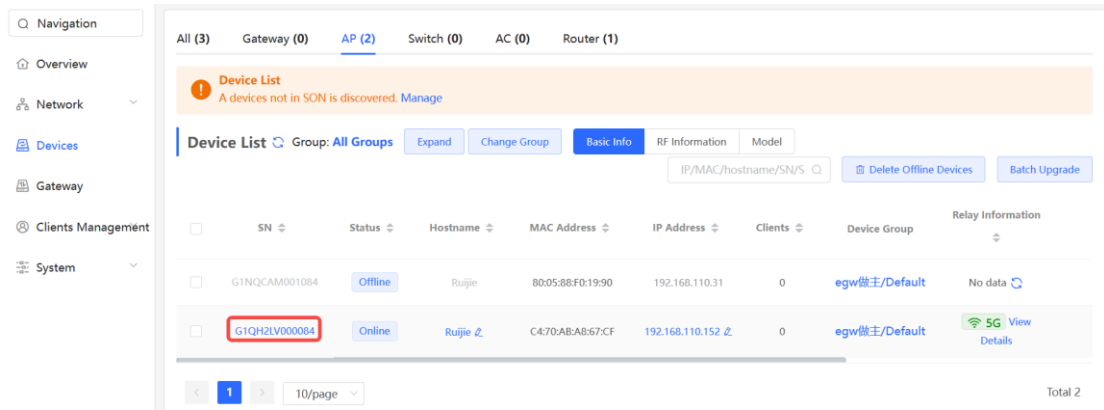
Click **View Details** following the  icon to obtain information about the uplink device and RSSI.



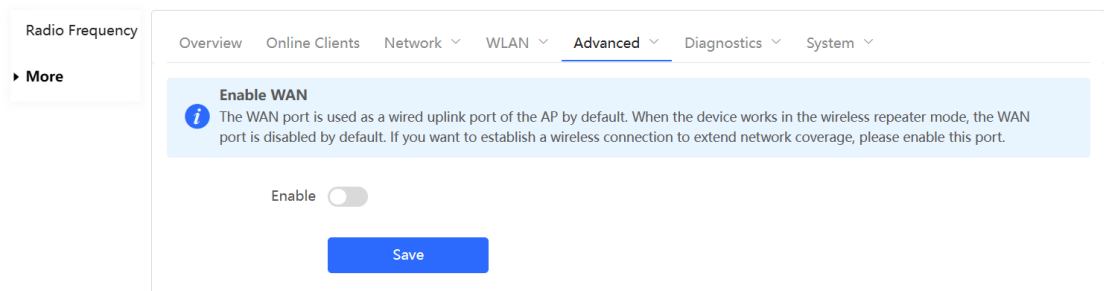
6. Enabling WAN Port

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**.

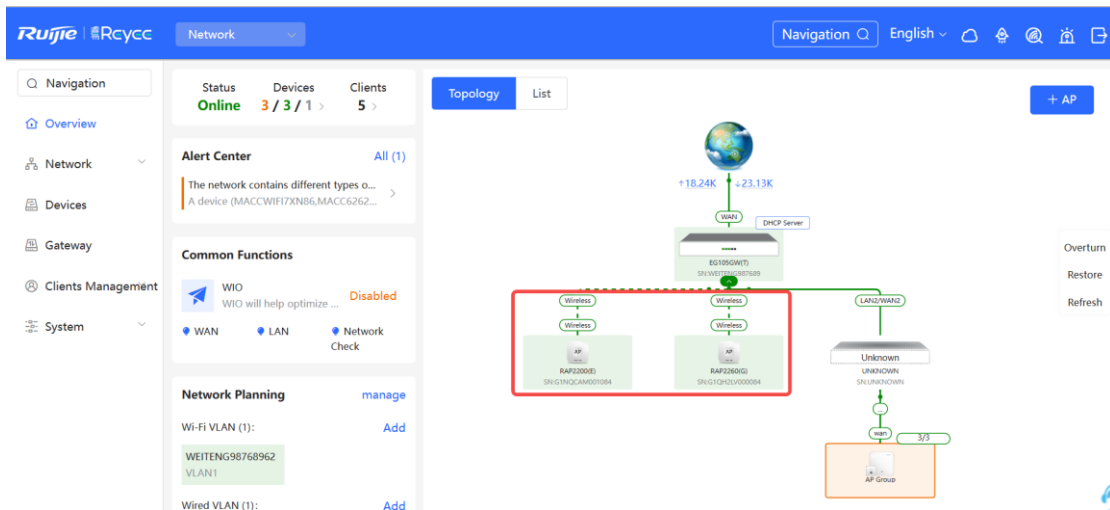



7. Querying Mesh APs and Mesh Details

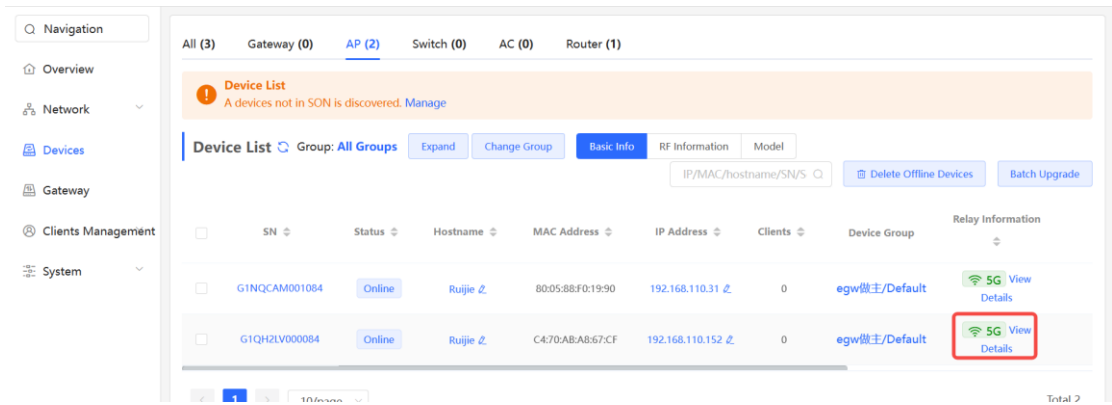
(1) Log in to the Eweb of a device on the target network.

(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.

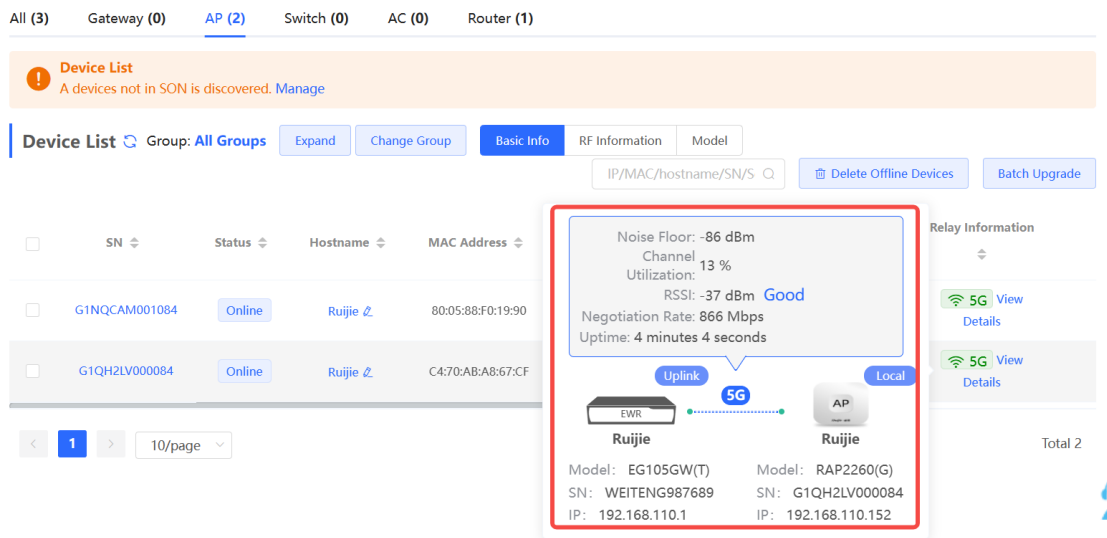


- Method 2: In **Network** mode, choose **Devices > AP**. If an entry contains icon  in the **Relay Information** column, the corresponding AP is a Mesh AP.



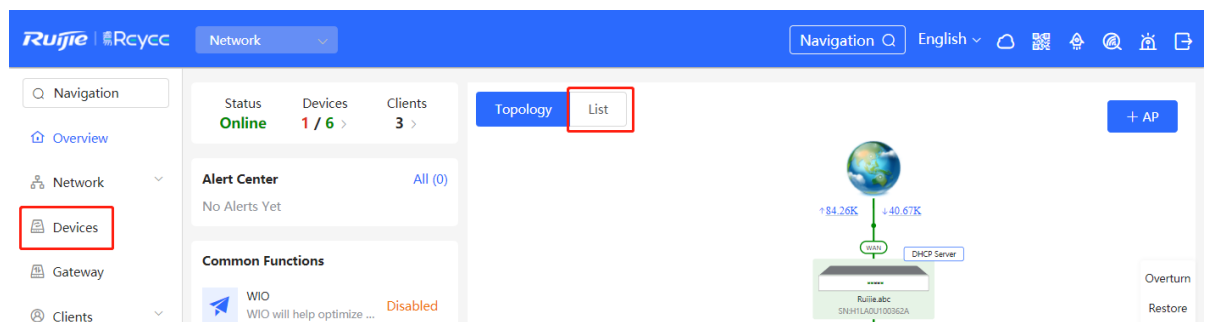
(3) Query Mesh networking details.

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.



Topology	List	IP/MAC/hostname/SN/S	Delete Offline Devices	Batch Upgrade			
<input type="checkbox"/>	SN	Status	Hostname	MAC	IP	Software Ver	Model
<input type="checkbox"/>	MACCWLD789205GC	Online	ruijie	78:11:22:33:44:55	192.168.110.226	ESW_	RG-ES205C-P
<input checked="" type="checkbox"/>	H1LA0U100362A	Online	Ruijie.abc [Master]	00:74:9C:87:6D:85	192.168.110.1	ReyeeOS	EG205G
<input type="checkbox"/>	G1NW31N000172	Online	Ruijie	00:D3:F8:15:08:5B	192.168.110.89	ReyeeOS	NBS5200-24SFP/8GT4XS
<input type="checkbox"/>	1234942570021	Online	RAP2200e	00:D0:F8:15:08:48	192.168.110.152	AP_ new	RAP2200(E)
<input type="checkbox"/>	G1QH2LV00090C	Online	Ruijie	C4:70:AB:A8:69:17	192.168.110.102	ReyeeOS	RAP2260(G)

< 1 > 10/page Total 5

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

Hostname: Ruijie
Model: NBS5200-24SFP/8GT4XS
Software Ver: ReyeeOS 1.86.1704
MGMT IP: 11.1.1.89
MAC: 00:D3:F8:15:08:5B

Port Status

VLAN Info

Port

Route Info

RLDP

More

VLAN

VLAN1 | VLAN33 | VLAN88

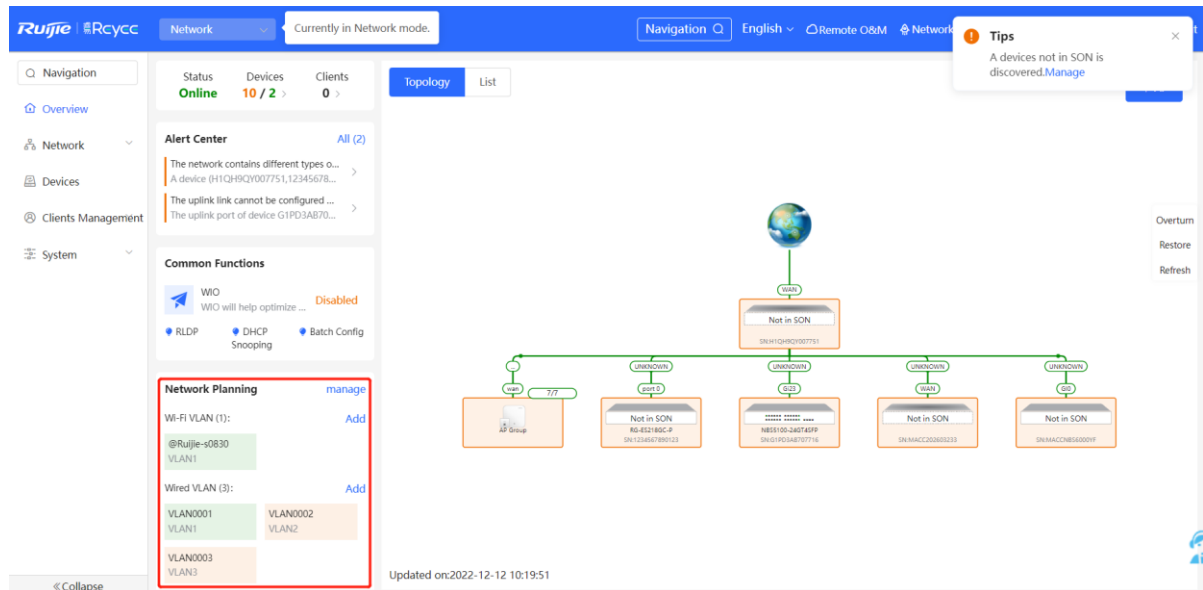
Interface	IP	IP Range	Remark
Gi2,Gi4,Gi6,Gi17-24,Te25-28,Ag1-4,Ag8	11.1.1.89		

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

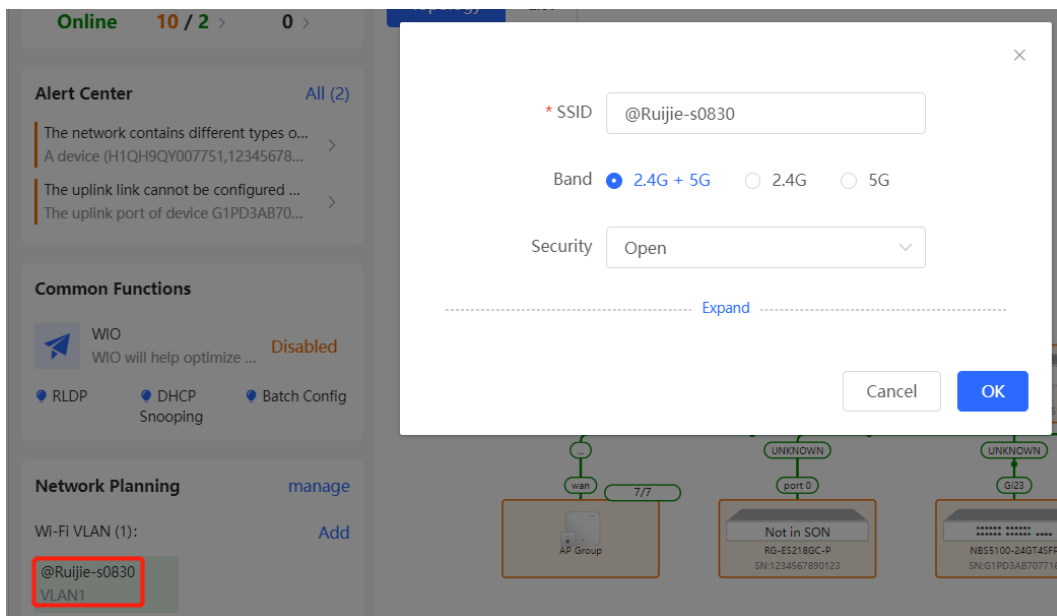
Topology	List	IP/MAC/hostname/SN/S	Delete Offline Devices	Batch Upgrade			
<input checked="" type="checkbox"/>	SN	Status	Hostname	MAC	IP	Software Ver	Model
<input type="checkbox"/>	MACCWLD789205GC	Online	ruijie	78:11:22:33:44:55	192.168.110.226		RG-ES205C-P
<input checked="" type="checkbox"/>	H1LA0U100362A	Online	Ruijie.abc [Master]	00:74:9C:87:6D:85	192.168.110.1		EG205G
<input type="checkbox"/>	G1NW31N000172	Online	Ruijie	00:D3:F8:15:08:5B	11.1.1.89		NBS5200-24SFP/8GT4XS
<input checked="" type="checkbox"/>	G1QH2LV00090C	Offline	Ruijie	C4:70:AB:A8:69:17	192.168.110.102		RAP2260(G)
<input type="checkbox"/>	1234942570021	Online	RAP2200e	00:D0:F8:15:08:48	192.168.110.152		RAP2200(E)
<input type="checkbox"/>	MACCS22376524	Online	Ruijie	00:10:F8:75:33:72	192.168.110.200		EAP602

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](#).



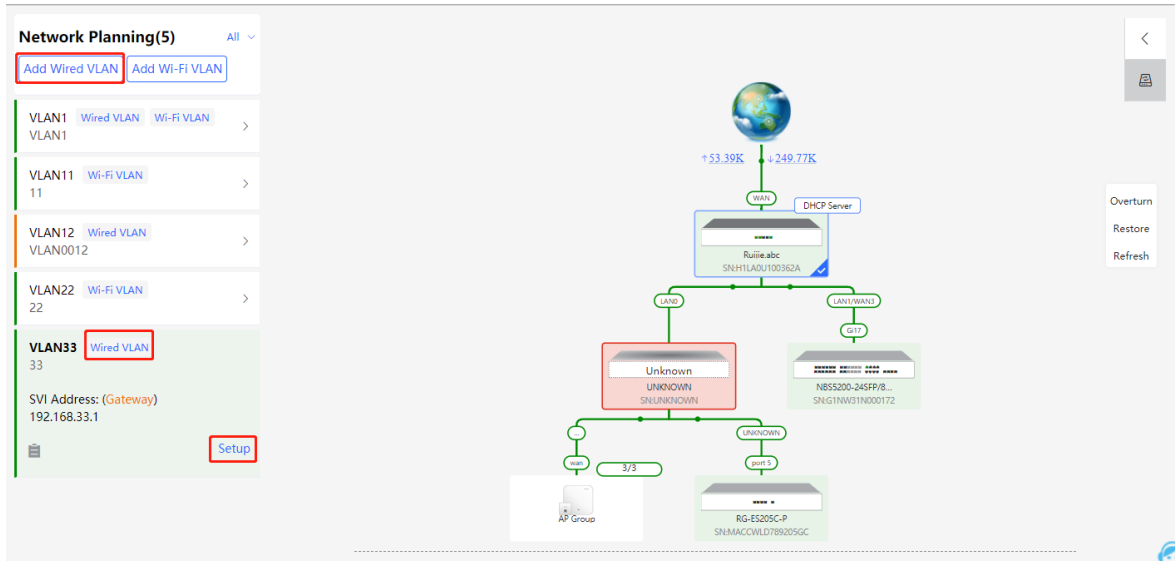
2.4.1 Configuring Wired VLAN

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

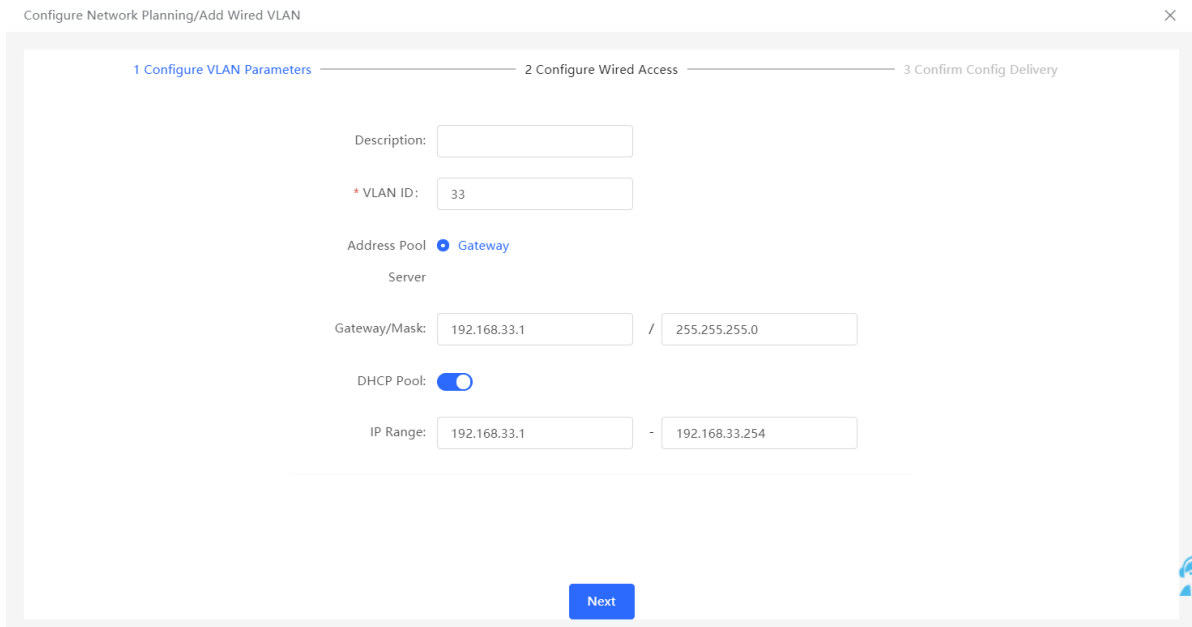
- Method 1: Click **Add** beside **Wired VLAN** in the **Network Planning** area on the **Overview** page to add the

wired VLANs.

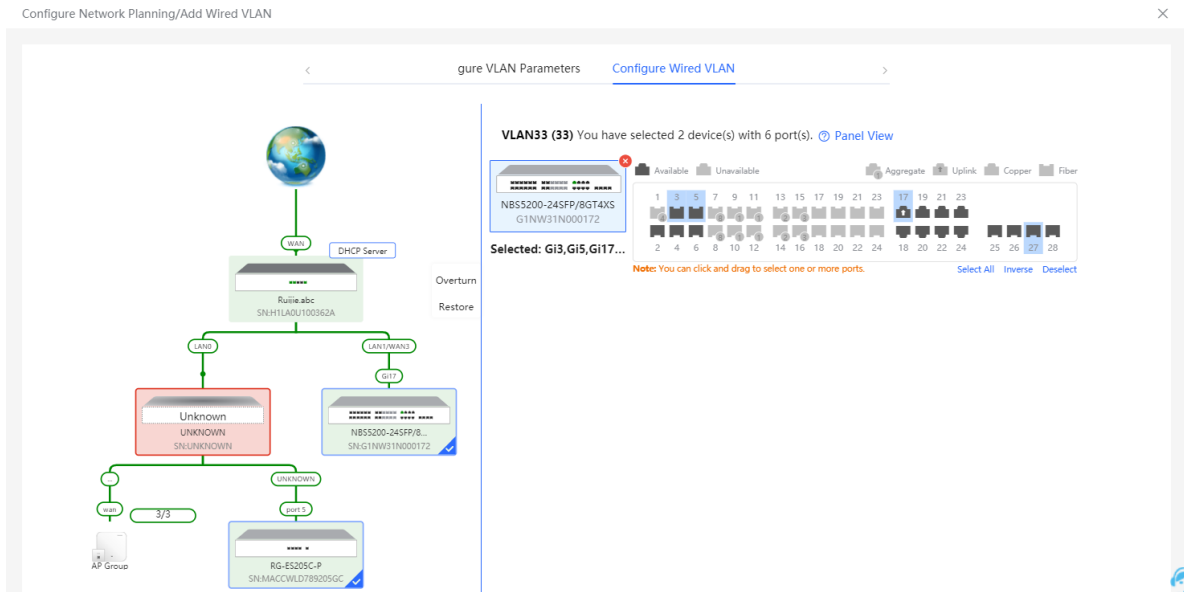
- Method 2: Click **manage** in the **Network Planning** area on the **Overview** page to go to the **Network Planning** page for configuration (**Network > Network Planning**). Click **Add Wired VLAN** to add the wired VLANs to the live network or select the available wired VLANs. Click **Setup** to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



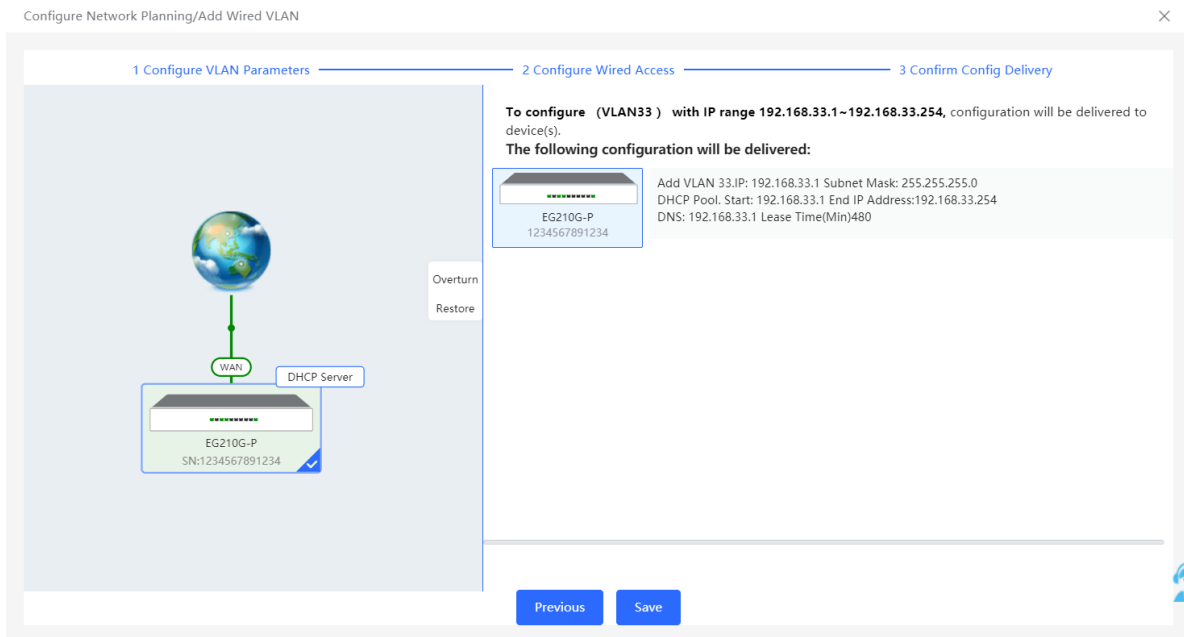
- (1) Configure the VLAN ID, address pool server, and DHCP pool. The gateway is configured as the address pool server by default to assign IP addresses to clients. If an access switch exists in the network, you can select the access switch as the address pool server. Click **Next** after VLAN parameters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



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



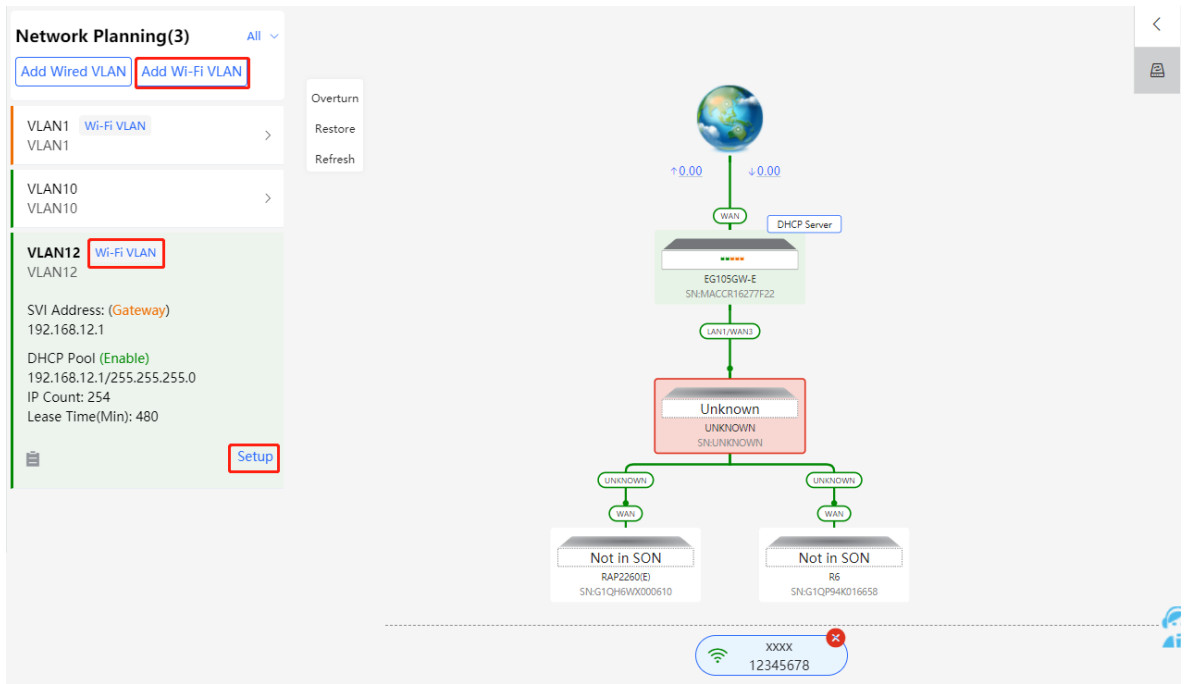
(3) Please confirm the delivered configurations and click **Save**. The configurations will take effect after a few minutes.



2.4.2 Configuring Wi-Fi VLAN

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

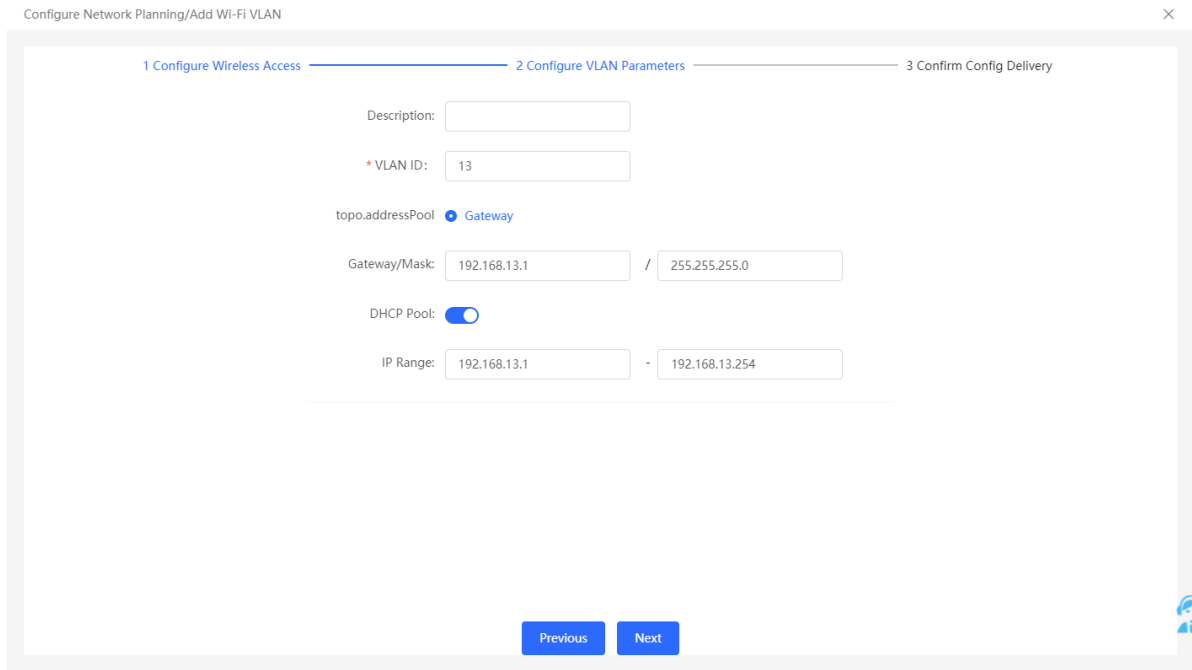
- Method 1: Click **Add** beside **Wi-Fi VLAN** in the **Network Planning** area on the **Overview** page to add the Wi-Fi VLANs.
- Method 2: Click **manage** in the **Network Planning** area on the **Overview** page to go to the **Network Planning** page for configuration (**Network > Network Planning**).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



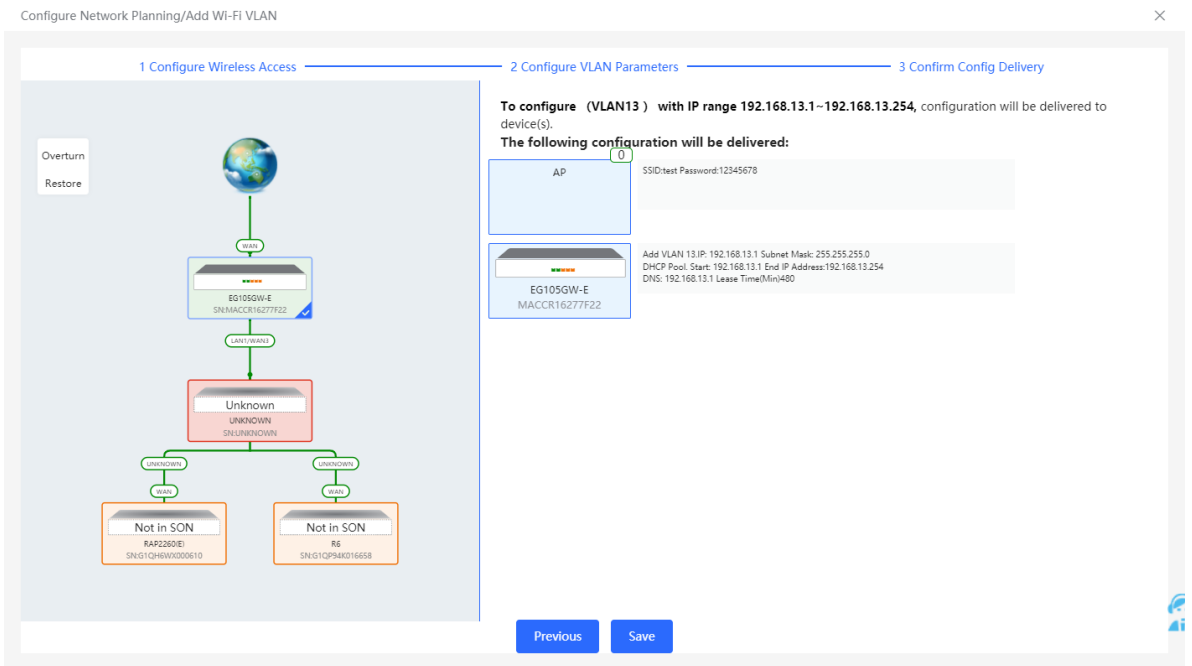
- (1) Configure the SSID, Wi-Fi password and band. Click **Expand** to expand the advanced settings and set the parameters. Then, click **Next**.

The screenshot shows the 'Configure Network Planning/Add Wi-Fi VLAN' configuration page. It has three steps: 1. Configure Wireless Access, 2. Configure VLAN Parameters, and 3. Confirm Config Delivery. A blue information box states: 'The configuration will take effect after being delivered to AP.' The configuration fields are: SSID (text input), Band (radio buttons for 2.4G + 5G, 2.4G, and 5G), Security (dropdown menu set to Open), Wireless Schedule (dropdown menu set to All Time), Hide SSID (toggle switch), Client Isolation (toggle switch with description: 'Prevent wireless clients of this Wi-Fi from communicating with one another.'), Band Steering (toggle switch with description: 'The 5G-supported client will access 5G radio preferentially.'), and XPress (toggle switch with description: 'The client will faster speed.'). A blue 'Next' button is located at the bottom right.

- (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) 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.

The screenshot shows a network management dashboard. At the top, there's a navigation bar with 'Network' and 'English'. Below it, a status bar shows 'Status Online', 'Devices 1/1/5', and 'Clients 4'. The main area is divided into a left sidebar with navigation icons and a main content area. The main content area has a 'Topology' tab selected, showing a network diagram. The diagram includes a central 'Gateway' device (Ruijie abc, SN:H1LA0U100362A) connected to a 'WAN' interface. Below it, there are 'LAN0' and 'LAN1/WAN3' interfaces. The 'LAN1/WAN3' interface is connected to a 'Switch' (NB55200-24SFP/8..., SN:G1NW31N000172). The 'LAN0' interface is connected to an 'Unknown' device (UNKNOWN, SN:UNKNOWN). The 'Unknown' device is connected to a 'wan' interface (3/3) and a 'port 5' interface. The 'port 5' interface is connected to another 'Switch' (RG-ES205C-P, SN:MACCWLD789205GC). There are also 'AP Group' and 'AP' icons. On the right side, there are buttons for 'Overturn', 'Restore', and 'Refresh'. At the bottom, it says 'Updated on:2022-04-29 17:31:18'. In the left sidebar, the 'Alert Center' is highlighted with a red box, showing a message: 'The gateway is not configured with a VLAN. The downlink port of device H1LA0U1...'. Below the alert center are sections for 'Common Functions' (WIO, RLDP, DHCP Snooping, Batch Config) and 'Network Planning' (Setup).

The screenshot shows the 'Alerts' section of the network management dashboard. The 'Alert Center' is highlighted with a red box, showing a message: 'The gateway is not configured with a VLAN. The downlink port of device H1LA0U1...'. Below the alert center are sections for 'Common Functions' (WIO, RLDP, DHCP Snooping, Batch Config) and 'Network Planning' (Setup). The main content area shows an 'Alerts' section with a 'Current Alert' section. The alert message is: '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.' Below the alert message is a network diagram showing the topology. The diagram includes a central 'Gateway' device (Ruijie abc, SN:H1LA0U100362A) connected to a 'WAN' interface. Below it, there are 'LAN0' and 'LAN1/WAN3' interfaces. The 'LAN1/WAN3' interface is connected to a 'Switch' (NB55200-24SFP/8..., SN:G1NW31N000172). The 'LAN0' interface is connected to an 'Unknown' device (UNKNOWN, SN:UNKNOWN). The 'Unknown' device is connected to a 'wan' interface (3/3) and a 'port 5' interface. The 'port 5' interface is connected to another 'Switch' (RG-ES205C-P, SN:MACCWLD789205GC). There are also 'AP Group' and 'AP' icons. On the right side, there are buttons for 'Overturn' and 'Restore'. At the bottom, it says 'Updated on:2022-04-29 17:31:18'. In the left sidebar, the 'Alert Center' is highlighted with a red box, showing a message: 'The gateway is not configured with a VLAN. The downlink port of device H1LA0U1...'. Below the alert center are sections for 'Common Functions' (WIO, RLDP, DHCP Snooping, Batch Config) and 'Network Planning' (Setup).

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

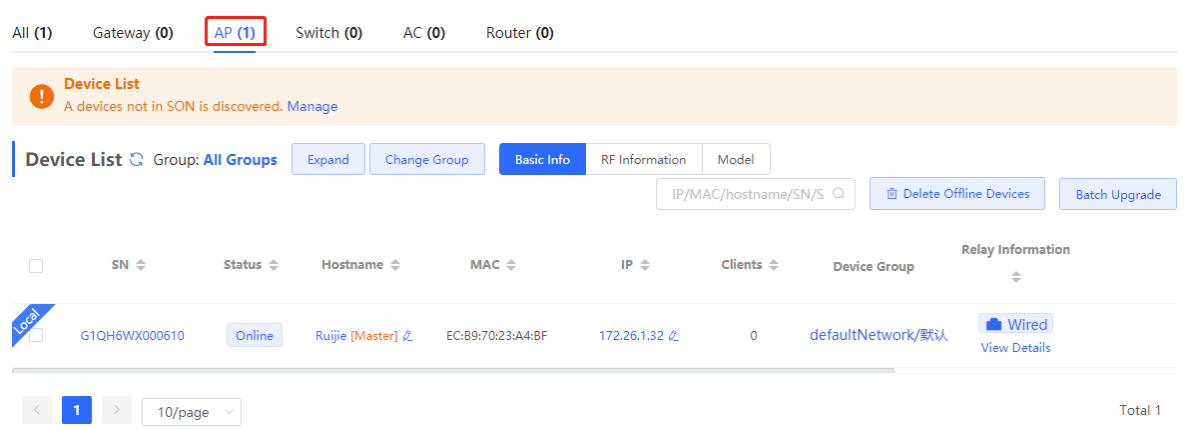
If you specify a group when setting up a wireless network, the corresponding configuration will take effect on the wireless devices in the specified group.

3.1.2 Procedures


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

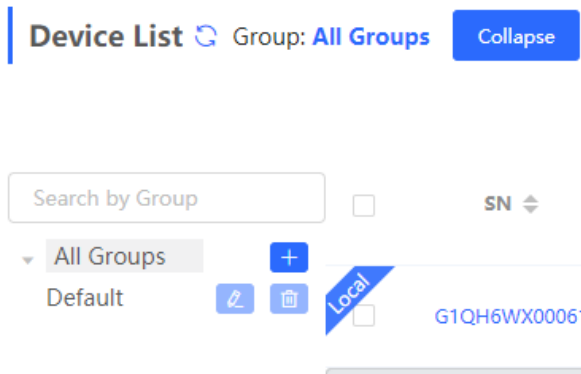
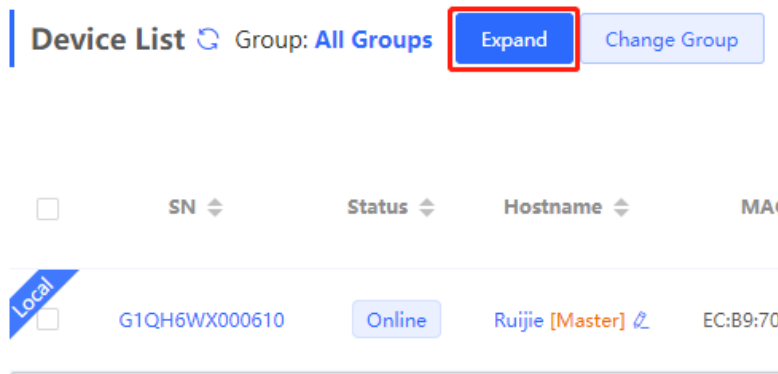
For other RAP models, choose  **WLAN** > **APs**

- 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.

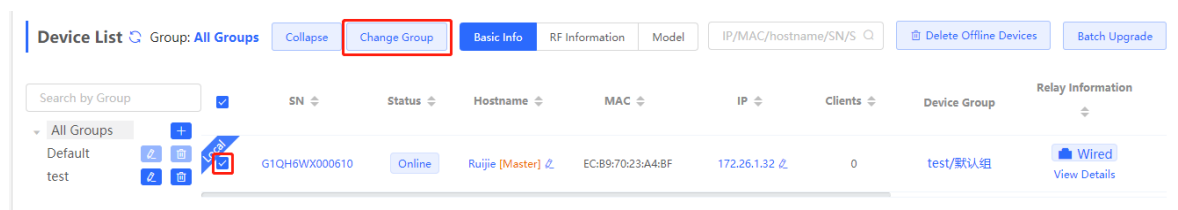


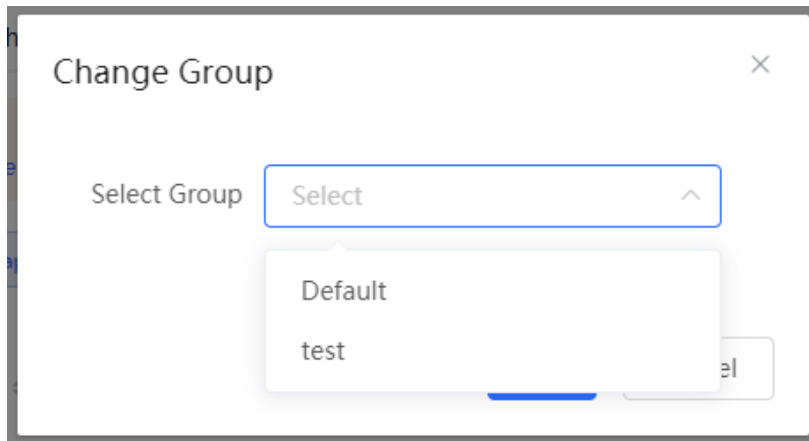
The screenshot shows the 'Device List' page in a web interface. At the top, there are tabs for 'All (1)', 'Gateway (0)', 'AP (1)', 'Switch (0)', 'AC (0)', and 'Router (0)'. The 'AP (1)' tab is selected and highlighted with a red box. Below the tabs is a 'Device List' section with a warning icon and the text 'A devices not in SON is discovered. Manage'. There are buttons for 'Expand', 'Change Group', 'Basic Info', 'RF Information', and 'Model'. A search bar contains 'IP/MAC/hostname/SN/S'. There are also buttons for 'Delete Offline Devices' and 'Batch Upgrade'. Below this is a table with the following columns: SN, Status, Hostname, MAC, IP, Clients, Device Group, and Relay Information. The table contains one row with the following data: SN: G1QH6WX000610, Status: Online, Hostname: Ruijie [Master], MAC: EC:B9:70:23:A4:BF, IP: 172.26.1.32, Clients: 0, Device Group: defaultNetwork/默认, Relay Information: Wired (with a 'View Details' link). At the bottom, there is a pagination control showing '1' of 10 per page and a 'Total 1' count.

- (1) 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.







- (2) 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.

(1) 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.

Wi-Fi Settings Device Group:

Up to 8 SSIDs can be added.

<p>Default</p> <p>@Ruijie-s0830</p> <p>Default VLAN</p> <p>Band:2.4G + 5G</p>	<p>+ Add Guest Wi-Fi</p>	<p>+ Add Wi-Fi</p>
---	--------------------------	--------------------

* SSID

Band 2.4G + 5G 2.4G 5G

Security

----- Expand -----





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.

(1) 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.

Wi-Fi Settings Device Group: Default

Up to 8 SSIDs can be added.

Default

@Ruijie-s0830

Default VLAN

Band:2.4G + 5G

+ Add Guest Wi-Fi

+ Add Wi-Fi

* SSID

Band 2.4G + 5G 2.4G 5G

Security Open

----- Collapse -----

Wireless Schedule All Time

VLAN The same VLAN as AP

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

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-RAP2260 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.

Wireless Client List [Refresh](#) [Advanced Search](#)

Username	MAC	IP	SN	Duration	RSSI	Rate	Band	SSID	Channel	Action
NULL	72:58:52:40	192.168.110.194	G1QH6W	2022-04-01 09:40:36	-66	24M	5G	@Ruijie-s1234	64	Add to Blacklist

All (1) Wired (0) **Wireless (1)**

Online Clients ?

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

Online Clients Search by IP/MAC/Username Q Refresh

Username/Type	Access Location	IP/MAC	Current Rate	Wi-Fi
 2.4G	G1QH6WX000610	172.26.1.73 62:cf:2f:84:bd:d0	Up:0.00bps Down:0.00bps	Channel:13 RSCP:-87 Duration:7 minutes 55 seconds Negotiation Rate:1M

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.

- (1) 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.

Wi-Fi Settings Device Group:

Up to 8 SSIDs can be added.

<p>Default</p> <p>@Ruijie-s0830</p> <p>Default VLAN</p> <p>Band:2.4G + 5G</p>	+ Add Guest Wi-Fi	+ Add Wi-Fi
--	-------------------	-------------

* SSID

Band 2.4G + 5G 2.4G 5G

Security





----- Expand -----

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.

- (1) 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.

Default

@Ruijie-s0830
Default VLAN
Band:2.4G + 5G

+ Add Guest Wi-Fi

+ Add Wi-Fi

* SSID

Band 2.4G + 5G 2.4G 5G

Security

Collapse

Wireless Schedule

VLAN

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

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

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

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.

(1) 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.

..... Collapse

Wireless Schedule

VLAN

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

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

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

XPress (The client will experience faster speed.)





Layer 3 Roaming (The client will keep the IP address unchanged on the Wi-Fi network.)

Wi-Fi6 (802.11ax high-speed wireless connectivity.) ⓘ

[Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.](#)

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.
- (1) 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.

----- Collapse -----

Wireless Schedule

VLAN

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

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

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

XPress (The client will experience faster speed.)





Layer 3 Roaming (The client will keep the IP address unchanged on the Wi-Fi network.)

Wi-Fi6 (802.11ax high-speed wireless connectivity.) [?](#)

[Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.](#)

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.

(1) 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.

Default
@Ruijie-s0830
 Default VLAN
 Band:2.4G + 5G

+ Add Guest Wi-Fi

+ Add Wi-Fi

* SSID

Band 2.4G + 5G 2.4G 5G

Security

Collapse

Wireless Schedule

VLAN

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

Client Isolation

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

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**.

(1) 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.

×

* SSID

Band 2.4G + 5G 2.4G 5G

Security

* Wi-Fi Password

..... Expand

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.

Wi-Fi Settings Device Group:

Up to 8 SSIDs can be added.

Default @Ruijie-s0830 Default VLAN Band:2.4G + 5G	+ Add Guest Wi-Fi	+ Add Wi-Fi
---	--------------------------	--------------------

×

* SSID

Band 2.4G + 5G 2.4G 5G

Security

* Wi-Fi Password

[Expand](#)

3.12 Configuring Wireless Rate Limiting

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-RAP2260, and RG-RAP6262.

3.12.1 Overview

The device supports four rate limiting modes: client-based rate limiting, SSID-based rate limiting, AP-based rate limiting, and packet-based rate limiting. For the same client, if multiple rate limiting modes are configured, the priority order is as follows: client-based rate limiting > SSID-based rate limiting > AP-based rate limiting.

- Client-based rate limiting: This function allows you to limit the rate based on the MAC address of the client, so as to limit or guarantee the bandwidth required by specific clients.
- SSID-based rate limiting: This function provides two rate limiting modes for a specified SSID: **Rate Limit Per User** and **Rate Limit All Users**. **Rate Limit Per User** means that all clients connected to the SSID use the same rate limit. **Rate Limit All Users** means that the configured rate limit value is evenly allocated to all clients connected to the SSID. The rate limit value of each client dynamically changes with the number of clients connected to the SSID.
- AP-based rate limiting: This function limits the client rates based on the whole network. All clients connected to the network will work according to the configured rate limit value.
- Packet-based rate limiting: This function limits the client rates based on the downlink broadcast and multicast packets. The device supports rate limiting for specific broadcast packets (such as ARP and DHCP), multicast packets (such as MDNS and SSDP), or all types of broadcast and multicast packets. If network stalling remains during network access and there is no client with large traffic, you are advised to adjust the rate between 1 kbps and 512 kbps.

3.12.2 Configuration Steps

1. Configuring Client-based Rate Limiting

Choose  **Network** ( **WLAN**) > **LimitSpeed** > **Client-based Rate Limiting**.

- (1) Enable Wireless Rate Limiting.
- (2) Click **Add**. In the dialog box that appears, set the MAC address and uplink and downlink rate limit values of the client, and click **OK**.

Wireless Rate Limiting

[Client-based Rate Limiting](#)
[Wi-Fi-based Rate Limiting](#)
[AP-based Rate Limiting](#)
[Packet-based Rate Limiting](#)

Client-based Rate Limiting
The rate limiting mode based on wireless clients can limit or provide the bandwidth for specific clients.

Up to **512** entries can be added.

<input type="checkbox"/>	Client MAC	Uplink Rate Limit	Downlink Rate Limit	Remarks	Action
No Data					

Total 0

Add ×

* Client MAC

Uplink Rate

Limit Current: Kbps. Range: 1-1700000 Kbps

Downlink Rate

Limit Current: Kbps. Range: 1-1700000 Kbps

Remarks

2. Configuring SSID-based Rate Limiting

Choose  **Network** ( **WLAN**) > **LimitSpeed** > **SSID-based Rate Limiting**.

- (1) Enable Wireless Rate Limiting.
- (2) Click **Edit** in the **Action** column of the target SSID. In the dialog box that appears, set the uplink and downlink rate limit modes and values, and click **OK**.

Wireless Rate Limiting

Client-based Rate Limiting [SSID-based Rate Limiting](#) AP-based Rate Limiting Packet-based Rate Limiting

SSID-based Rate Limiting
This function provides rate limit per user and dynamic rate limiting for a specified SSID. Rate Limit per User indicates that all clients connected to the SSID use the same rate limit. Rate Limit All Users indicates that all clients connected to the SSID share the rate limit in average. The priority of this function is lower than that of client-based rate limiting.

SSID-based Rate Limiting Device Group: [Are you sure you want to add a Wi-Fi? Click to go.](#)

SSID	Uplink Rate Limit	Downlink Rate Limit	Action
333	Rate Limit All Users 1111K bps	No Limit	Edit Disable
111	No Limit	No Limit	Edit Disable
wbctest	No Limit	No Limit	Edit Disable
@Ruijie-guest-6D85	Rate Limit All Users 111K bps	Rate Limit Per User 2M bps	Edit Disable

Edit ×

Uplink Rate Limit Rate Limit Per User Rate Limit All Users ?

Rate Limit ▼
Current: Kbps. Range: 1-1700000 Kbps

Downlink Rate Limit Rate Limit Per User Rate Limit All Users

Rate Limit ▼
Current: Kbps. Range: 1-1700000 Kbps

3. Configuring AP-based Rate Limiting

Choose  Network ( WLAN) > LimitSpeed > AP-based Rate Limiting.

- (1) Enable Wireless Rate Limiting.
- (2) Set the uplink and downlink rate limit modes to **Rate Limit Per User**, configure the rate limit values, and click **OK**.

Wireless Rate Limiting

Client-based Rate Limiting Wi-Fi-based Rate Limiting AP-based Rate Limiting Packet-based Rate Limiting

AP-based Rate Limiting
This function provides client rate limiting based on the whole network. All devices connected to the network use the preset rate limiting value. The priority of this function is lower than that of client-based rate limiting and SSID-based rate limit per user.

AP-based Rate Limiting

Uplink Rate Limit No Limit Rate Limit Per User

 Kbps

Current: Kbps. Range: 1-1700000 Kbps

- Wechat texts, voice messages and webpage services: 1 Mbps to 2 Mbps,
- Real-time video calls and HD videos: 2 Mbps to 4 Mbps,
- Ultra HD/4K/Blue-ray videos and live videos: 5 Mbps to 10 Mbps,
- Other: You are not advised to set the value to 20 Mbps. It may affect the Internet experience of other users in the internal network.

Downlink Rate Limit No Limit Rate Limit Per User

 Kbps

Current: Kbps. Range: 1-1700000 Kbps

OK

4. Configuring Packet-based Rate Limiting

Choose Network (WLAN) > LimitSpeed > Packet-based Rate Limiting.

- (1) Enable Wireless Rate Limiting.
- (2) Select the specific type of packets for rate limiting, configure the rate limit value, and click **Save**.

Wireless Rate Limiting

Client-based Rate Limiting Wi-Fi-based Rate Limiting AP-based Rate Limiting Packet-based Rate Limiting

Packet-based Rate Limiting
This function allows users to limit the downlink rate for broadcast and multicast packets. If the internet access is still slow and unstable when no client needs large amounts of traffic, you are advised to set the rate ranging from 1 Kbps to 512 Kbps. Smaller rate brings better network improvement.
[wqos.mcDescTip](#)

Packet-based Rate Limiting

Broadcast Rate Limiting Disable Limit All Limit Part

ARP Packet DHCP Packet

Multicast Rate Limiting Disable Limit All Limit Part

MDNS Packet SSDP Packet

* Rate Limit Kbps

Current: 0 Kbps. Range: 1-1700000 Kbps

Save

3.13 Configuring Wi-Fi Blacklist or Whitelist

3.13.1 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.

3.13.2 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.

Global Blacklist/Whitelist
SSID-Based Blacklist/Whitelist

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

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

Blocked WLAN Clients

+ Add
Delete Selected

Up to 256 members can be added.

	MAC	Remark	Action
<input type="checkbox"/>	00:E0:4C:36:0B:EA	forbidden	Edit Delete
<input type="checkbox"/>	00:11:22 OUI		Edit Delete

Add

×

Match Type Full Prefix (OUI)

* MAC

Remark

Cancel
OK

52

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.

Global Blacklist/Whitelist SSID-Based Blacklist/Whitelist

Blacklist/Whitelist is used to allow or reject a client's request to connect to the Wi-Fi network.
Note: OUI matching rule and SSID-based blacklist/whitelist are supported by only RAP Net and P32 (and later versions).
Rule: 1. In the Blacklist mode, the clients in the blacklist are not allowed to connect to the Wi-Fi network.
 2. In the Whitelist mode, only the clients in the whitelist are allowed to connect to the Wi-Fi network.

Device Group: test

SSID-Based Blacklist/Whitelist

@Ruijie-s1234

test

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

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

Blocked WLAN Clients + Add Delete Selected

Up to **256** members can be added.

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

3.14 Optimizing Wi-Fi Network

3.14.1 Overview

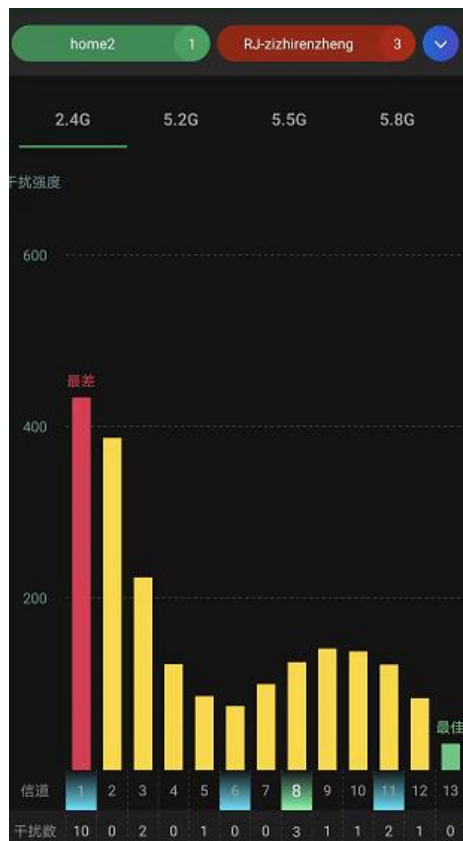
The device detects the surrounding wireless environment and selects the appropriate configuration upon power-on. However, network stalling caused by wireless environment changes cannot be avoided. You can optimize the network with one single click, analyze the wireless environment around the access point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

3.14.2 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.



3.14.3 Optimizing the Radio Channel

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP2260 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.

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

Radio Frequency Device Group: Default

Country/Region: China (CN)

2.4G Channel Width: Auto Multicast Rate (Mbps): Auto

Client Count Limit: 64

Disconnection Threshold: Disable -85dBm -65dBm

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

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

Transmit Power: Auto Lower Low Medium High

Roaming: Low 40% 80% High

5G Channel Width: Auto Multicast Rate (Mbps): Auto

Client Count Limit: Auto 36 (5.18GHz) 40 (5.2GHz) 44 (5.22GHz) 48 (5.24GHz) 52 (5.26GHz) 56 (5.28GHz) 60 (5.3GHz)

Disconnection Threshold: Disable -85dBm -65dBm

Transmit Power: Auto Lower Low Medium High

Roaming: Low 40% 80% High

3.14.4 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.

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

Radio Frequency Device Group:

Country/Region:

2.4G Channel Width **5G Channel Width**

Multicast Rate (Mbps): Multicast Rate (Mbps):

Client Count Limit: Client Count Limit:

Disconnection Threshold: -85dBm -65dBm Disconnection Threshold: -85dBm -65dBm




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

2.4G Channel **5G Channel**



Transmit Power: Lower Low Medium High Transmit Power: Lower Low Medium High

3.14.5 Optimizing the Transmit Power

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP2260 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. After adjusting the configuration, click **Save**.

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

Radio Frequency Device Group: Default

Country/Region: China (CN)

2.4G Channel Width: Auto

Multicast Rate (Mbps): Auto

Client Count Limit: 64

Disconnection Threshold: Disable -85dBm -65dBm

5G Channel Width: Auto

Multicast Rate (Mbps): Auto
 20MHz
 40MHz
 80MHz
 160MHz

Client Count Limit: 64

Disconnection Threshold: Disable -85dBm -65dBm

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

2.4G Channel: Auto

5G Channel: Auto

Transmit Power: Auto Lower Low Medium High

Roaming: Low 40% 80% High

Access Threshold: Disable -85dBm -65dBm

Transmit Power: Auto Lower Low Medium High

Roaming: Low 40% 80% High

Access Threshold: Disable -85dBm -65dBm

3.14.6 Configuring the Multicast Rate

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-RAP2260, and RG-RAP6262.

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

If the multicast rate is too high, the packet loss rate of multicast packets may increase. If the multicast rate is too low, the radio interface may become busy. When network stalling is serious, you are advised to configure a high multicast rate. When network stalling is minor, configure a medium multicast rate. After adjusting the configuration, click **Save**.

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

Radio Frequency Device Group: Default

Country/Region: China (CN)

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

Multicast Rate (Mbps): Auto Multicast Rate (Mbps): Auto

Client Count Limit: 64 Client Count Limit: 64

Disconnection Threshold: Disable -85dBm -65dBm Disconnection Threshold: Disable -85dBm -65dBm

The settings are valid for only current device

2.4G Channel: Auto 5G Channel: Auto

Transmit Power: Auto Lower Low Medium High Transmit Power: Auto Lower Low Medium High

3.14.7 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. After adjusting the configuration, click **Save**.

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

Radio Frequency Device Group: Default

Country/Region: China (CN)

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

Multicast Rate (Mbps): Auto Multicast Rate (Mbps): Auto

Client Count Limit: 64 Client Count Limit: 512

Disconnection Threshold: Disable -85dBm -65dBm Disconnection Threshold: Disable -85dBm -65dBm

The settings are valid for only current device

2.4G Channel: Auto 5G Channel: Auto

Transmit Power: Auto Lower Low Medium High Transmit Power: Auto Lower Low Medium High

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.

3.14.8 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. After adjusting the configuration, click **Save**.

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

Radio Frequency Device Group: Default

Country/Region: China (CN)

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

Multicast Rate (Mbps): Auto Multicast Rate (Mbps): Auto

Client Count Limit: 64 Client Count Limit: 512

Disconnection Threshold: Disable -85dBm -65dBm Disconnection Threshold: Disable -85dBm -65dBm

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

2.4G Channel: Auto 5G Channel: Auto

Transmit Power: Auto Lower Low Medium High Transmit Power: Auto Lower Low Medium High


Caution

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



3.14.9 Configuring the Roaming Sensitivity

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP2260 and RG-RAP6262 models:

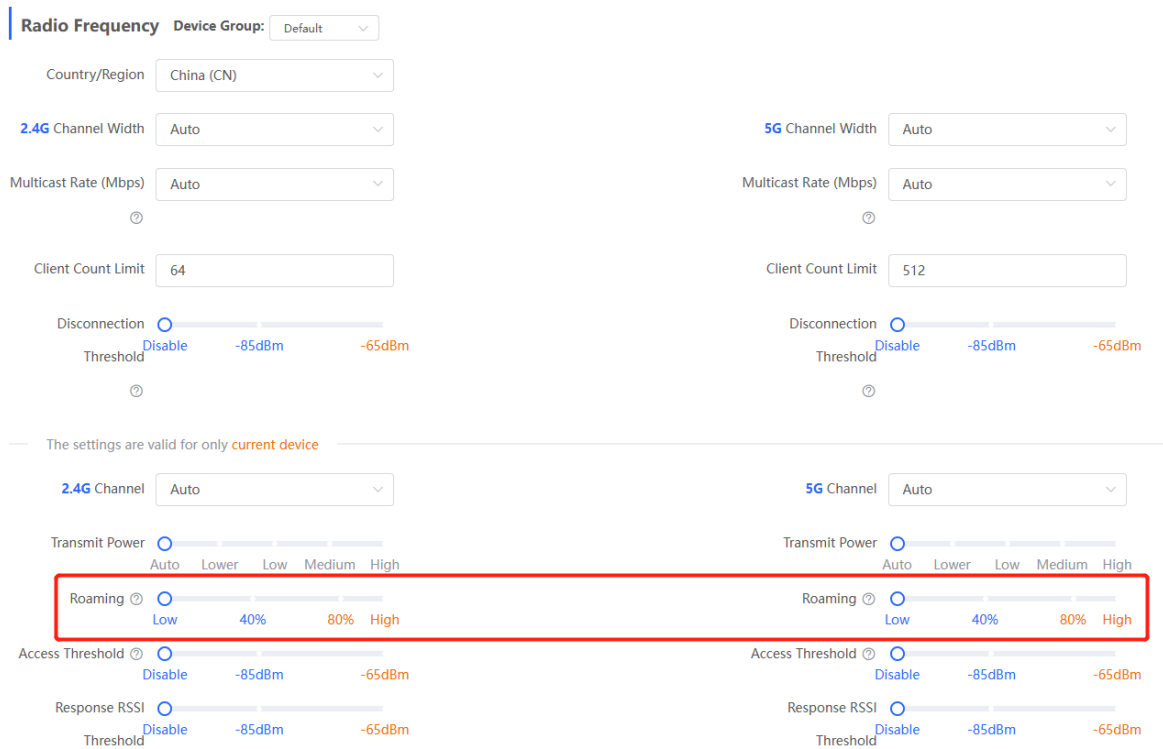
- Configure the master device. Choose  **Network** ( **WLAN**) > **Radio Frequency**

- 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. After adjusting the configuration, click **Save**.




The screenshot displays the 'Radio Frequency' configuration interface. It is divided into two columns for 2.4G and 5G settings. The 2.4G side shows 'Country/Region' set to 'China (CN)', 'Channel Width' set to 'Auto', 'Multicast Rate (Mbps)' set to 'Auto', 'Client Count Limit' set to '64', and 'Disconnection Threshold' set to 'Disable'. The 5G side shows 'Channel Width' set to 'Auto', 'Multicast Rate (Mbps)' set to 'Auto', 'Client Count Limit' set to '512', and 'Disconnection Threshold' set to 'Disable'. Below these, a note states 'The settings are valid for only current device'. Further down, '2.4G Channel' and '5G Channel' are both set to 'Auto'. 'Transmit Power' is set to 'Auto' for both. The 'Roaming' slider is highlighted with a red box and is set to 'Low'. 'Access Threshold' and 'Response RSSI Threshold' are both set to 'Disable' for both bands.

3.14.10 Configuring Access Threshold

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP2260 and RG-RAP6262 models:

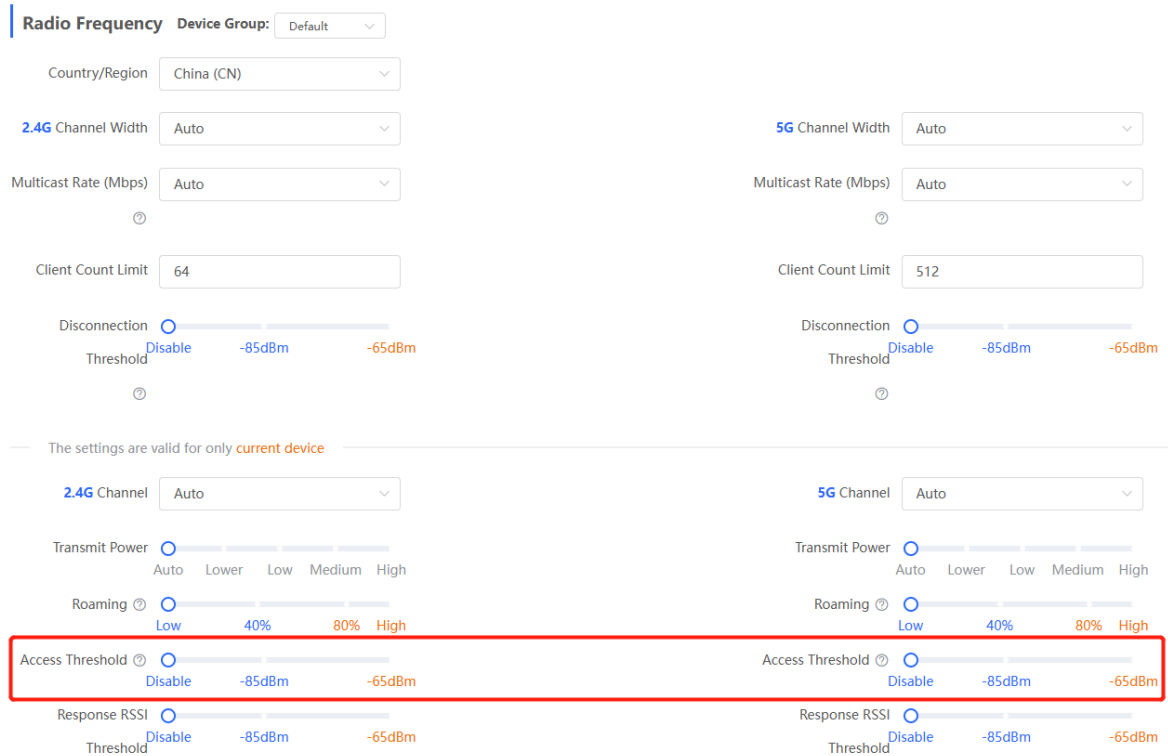
- Configure the master device. Choose  **Network** ( **WLAN**) > **Radio Frequency**
- Configure the slave device. Choose  **Devices** > Select the target device in the device list and click **SN** > **Radio Frequency**

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**




When the wireless signal of the end user is lower than the access threshold set on the device, the client cannot detect the wireless signal of the device. After adjusting the configuration, click **Save**.




The screenshot displays the configuration interface for a slave device. It is divided into two columns for 2.4G and 5G settings. The 2.4G side includes Country/Region (China (CN)), Channel Width (Auto), Multicast Rate (Mbps) (Auto), Client Count Limit (64), Disconnection Threshold (Disable, -85dBm, -65dBm), 2.4G Channel (Auto), Transmit Power (Auto, Lower, Low, Medium, High), Roaming (Low, 40%, 80%, High), Access Threshold (Disable, -85dBm, -65dBm), and Response RSSI Threshold (Disable, -85dBm, -65dBm). The 5G side includes Channel Width (Auto), Multicast Rate (Mbps) (Auto), Client Count Limit (512), Disconnection Threshold (Disable, -85dBm, -65dBm), 5G Channel (Auto), Transmit Power (Auto, Lower, Low, Medium, High), Roaming (Low, 40%, 80%, High), Access Threshold (Disable, -85dBm, -65dBm), and Response RSSI Threshold (Disable, -85dBm, -65dBm). A red box highlights the Access Threshold and Response RSSI Threshold settings on both sides.


3.14.11 Configuring Response RSSI Threshold

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP2260 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 the 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**

When the wireless signal of the end user is lower than the response RSSI threshold configured on the device, the client cannot detect the wireless signal of the device. The smaller the response RSSI threshold is configured,

the less the environmental factors interfere with the AP. However, the connection of the client may be affected. After adjusting the configuration, click **Save**.

Radio Frequency Device Group:

Country/Region:

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

Multicast Rate (Mbps): Multicast Rate (Mbps):

Client Count Limit: Client Count Limit:

Disconnection Threshold: -85dBm -65dBm Disconnection Threshold: -85dBm -65dBm

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

2.4G Channel: **5G** Channel:

Transmit Power: Lower Low Medium High Transmit Power: Lower Low Medium High


Roaming: 40% 80% High Roaming: 40% 80% High


Access Threshold: -85dBm -65dBm Access Threshold: -85dBm -65dBm

Response RSSI Threshold: -85dBm -65dBm Response RSSI Threshold: -85dBm -65dBm

3.14.12 Configuring WIO

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H),

RG-RAP6260(H), RG-RAP2260 and RG-RAP6262 models: In **Network** mode, choose  **Network >WIO**

For the 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.

Network Optimization Optimization Record Wi-Fi Roaming Optimization (802.11k/v)

Start Scanning Optimizing Finish

Description:
 This feature will optimize the self-organizing network to maximize the WLAN performance. Please make sure that all APs have been online. If WIO is enabled on the device supporting Wi-Fi roaming optimization (802.11k/v), this feature is enabled at the same time.

Notes:
 1. During network optimization, the APs will switch channels, forcing the clients to go offline. The process will last for a while, subject to the quantity of devices. It is recommended you enable network optimization at night.
 2. If dynamic channel allocation is running in the backend, network optimization will fail. Please try again later.
 3. Network Optimization is not supported by the device without an IP address.
 4. The configuration cannot be rolled back once optimization starts.

I have read the notes.

Network Optimization

Scheduled Optimization

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

Enable

Day

Time :

Save

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

Caution

This function is not supported by 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-RAP2260 and RG-RAP6262 models: In **Network** mode, choose **Network > WIO > Wi-Fi Roaming Optimization (802.11k/v)**.

For the 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.

Network Optimization Optimization Record **Wi-Fi Roaming Optimization (802.11k/v)**

Start Scanning Optimizing Finish

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

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

Enable

Network Optimization Optimization Record **Wi-Fi Roaming Optimization (802.11k/v)**

Start Scanning Optimizing Finish

12%

Wi-Fi Roaming Optimization (802.11k/v) Scanning

Start: 2022-09-28 19:56:03
 Expected Time: 2 minute

Network Optimization Optimization Record **Wi-Fi Roaming Optimization (802.11k/v)**

Start Scanning Optimizing Finish

Optimizing...

Optimization finished on 2022-09-28 19:56:40
 Time: 37 seconds
 To ensure smart roaming effect, please [Click Here](#) to scan the WLAN environment again if the topology changes.


Disable

3.15 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.

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

Healthy Mode Device Group:





Enable

Effective Time

Save

3.16 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.
- (1) 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.

* SSID

Band 2.4G + 5G 2.4G 5G

Security

[Collapse](#)

Wireless Schedule

VLAN

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





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

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

XPress (The client will experience faster speed.)

3.17 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.
- (1) 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.

* SSID

Band 2.4G + 5G 2.4G 5G

Security

[Collapse](#)


Wireless Schedule

VLAN

Hide SSID


Client Isolation

3.18 Enabling Reye Mesh

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP2260 and RG-RAP6262 models: In **Network** mode, choose  **Network** > **Reye Mesh**

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

After Reye Mesh is enabled, you can set up a Mesh network through Mesh pairing between the devices that support Reye 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. Reye Mesh is enabled on the device by default.

 After enabling Reyee Mesh, you can set up a Mesh network through Mesh pairing between the devices that support Reyee Mesh.

Enable

Save

3.19 Configuring AP Load Balancing

Caution

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

3.19.1 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.

3.19.2 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**.

Load Balancing

+ Add

Delete Selected

Up to **32** entries can be added.
 Add APs in an area into a group and enable load balancing. When load is unbalanced in the group, clients will automatically associate to an AP with lighter load.
 Example: Add AP1 and AP2 into a group and select client load balancing. Set both the client count threshold and difference to 3. AP1 is associated with 5 clients and AP2 is associated with 2 clients, triggering load balancing. New clients' attempt to associate to AP1 will be denied, and therefore they can associate only to AP2.

<input type="checkbox"/>	Group Name	Type	Rule	Members	Action
No Data					

Add ×

* Group Name

* Type Client Load Balancing ▼

* Rule
 When an AP is associated with i clients and the difference between the currently associated client count and client count on the AP with the lightest load reaches , clients can associate only to another AP in the group. After a client association is denied by an AP for times, the client will be allowed to associate to the AP upon the next attempt.

* Members Enter an AP name or SN. ▼

Cancel
OK

Table 3-2 Client load balancing configuration

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

Parameter	Description
Rule	<p>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.</p> <p>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.</p>
Members	Specify the APs to be added to the AP load balancing group.

3.19.3 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**.

Load Balancing

+ Add
Delete Selected

Up to **32** entries can be added.
 Add APs in an area into a group and enable load balancing. When load is unbalanced in the group, clients will automatically associate to an AP with lighter load.
 Example: Add AP1 and AP2 into a group and select client load balancing. Set both the client count threshold and difference to 3. AP1 is associated with 5 clients and AP2 is associated with 2 clients, triggering load balancing. New clients' attempt to associate to AP1 will be denied, and therefore they can associate only to AP2.

<input type="checkbox"/>	Group Name	Type	Rule	Members	Action
No Data					

Add
×

* Group Name

* Type Traffic Load Balancing ▼

* Rule

When the traffic load on an AP reaches *100Kbps and the difference between the current traffic and the traffic on the AP with the lightest load reaches *100Kbps, clients can associate only to another AP in the group. After a client association is denied by an AP for times, the client will be allowed to associate to the AP upon the next attempt.

* Members Enter an AP name or SN. ▼

Cancel
OK


Table 3-3 Traffic load balancing configuration

Parameter	Description
Group Name	Enter the name of the AP load balancing group.
Type	Select Traffic Load Balancing .
Rule	<p>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.</p> <p>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.</p>
Members	Specify the APs to be added to the AP load balancing group.

4 Network Settings

i 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-RAP2260, and RG-RAP6262: Click **Manage Network Device**.
 - For the 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

i Note

If you need to switch the work mode to wireless bridging mode, please see [Wireless Repeater](#) for details.

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP2260 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.

The screenshot shows the Ruijie web-based configuration interface. At the top, there is a header with a Wi-Fi icon, a green dot labeled 'RAP', and device information: Hostname: Ruijie, SN: G1QW/..., IP: 172.26.1.209, MAC: AA:11:A/..., and a 'Reboot' button. Below the header is a navigation menu with 'Overview' selected, and other options: Basics, Security, Advanced, Diagnostics, and System. The main content area is divided into two sections: 'Overview' and 'Device Details'. The 'Overview' section contains three cards: 'Memory Usage' at 31%, 'Online Clients' at 1, and 'Status: Online' with a duration of 16 hours 45 minutes 21 seconds and a system time of 2022-04-01 09:43:49. The 'Device Details' section lists: Model: RAP..., SN: G1Q..., Work Mode: Router (highlighted with a red box), Hardware Ver: 1.00, Hostname: Ruijie, MAC: AA:11:A..., Role: Master AP, and Software Ver: ReyeeOS 1.75.1410.


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.

The screenshot shows a configuration page with a 'Description:' section containing four numbered steps: 1. The device IP address may change upon mode change. 2. Change the endpoint IP address and ping the device. 3. Enter the new IP address into the address bar of the browser to access EWEB. 4. The system menu varies with different work modes. Below the description are three configuration items: 'Work Mode' set to 'Router' with a dropdown arrow and a help icon; 'Self-Organizing Network' with a blue toggle switch turned on and a help icon; and 'AC' with a grey toggle switch turned off and a help icon. A blue 'Save' button is located at the bottom.

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-RAP2260 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.


Device Details

Model: RAP2261(E)
MAC Address: 58:69:6C:22:08:30
Hardware Ver: 1.00

Hostname: Ruijie 
Work Mode: Router 
Software Ver: ReyeeOS 1.218.2415


SN: MACCR10825107
Role: **Master AP** 

4.2 Configuring Internet Connection Type (IPv4)

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

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

Select the Internet connection type after confirming with the ISP. For detailed configuration, see [Work Mode](#). After completing the configuration, click **Save**.

 **WAN**

* Internet

No username or password is required for DHCP clients.

IP Address 192.168.111.210

Subnet Mask 255.255.255.0

Gateway 192.168.111.1

DNS Server 192.168.111.1

..... [Advanced Settings](#)

The device supports the following Internet connection types:

- **PPPoE:** This Internet connection type is supported only when the device works in routing mode. You need to manually configure the PPPoE username and password.
- **DHCP:** The current device will act as a DHCP client and apply for the IPv4 address/prefix from the upstream network device.
- **Static IP:** If this Internet connection type is selected, you need to manually configure a static IPv4 address, subnet mask, gateway address, and DNS server.

4.3 Configuring Internet Connection Type (IPv6)

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-RAP2260, and RG-RAP6262 in the AP mode.

In **Local Device** mode, choose  **Network > WAN > WAN_V6 Settings**.

Select the Internet connection type after confirming with the ISP. For detailed configuration, see [Work Mode](#). After completing the configuration, click **Save**.

WAN **WAN_V6 Settings**

* Internet

IPv6 Address

IPv6 Prefix

Gateway

DNS Server


The device supports the following Internet connection types:

- **DHCP:** The current device will act as a DHCPv6 client and apply for the IPv6 address/prefix from the upstream network device.
- **Static IP:** If this Internet connection type is selected, you need to manually configure a static IPv6 address, gateway address, and DNS server.
- **Null:** The IPv6 function is disabled on the current WAN port.

4.4 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-RAP2260 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.

LAN Settings DHCP Clients Static IP Addresses

LAN Settings ⓘ

Up to 8 entries can be added.

<input type="checkbox"/>	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
<input checked="" type="checkbox"/>	192.168.120.2	255.255.255.0	Default VLAN	-	Enabled	192.168.120.2	253	30	<input type="button" value="Edit"/> Delete

Edit
×

* IP

* Subnet Mask

Remark

* MAC


DHCP Server

4.5 Configuring Repeater Mode

Caution

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

4.5.1 Wired Repeater

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP2260 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.

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

Access Point
 Wireless Repeater

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

Wired Repeater


Check

4.5.2 Wireless Repeater

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

i 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-RAP2260 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.

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

Router
 Access Point
 Wireless Repeater

i

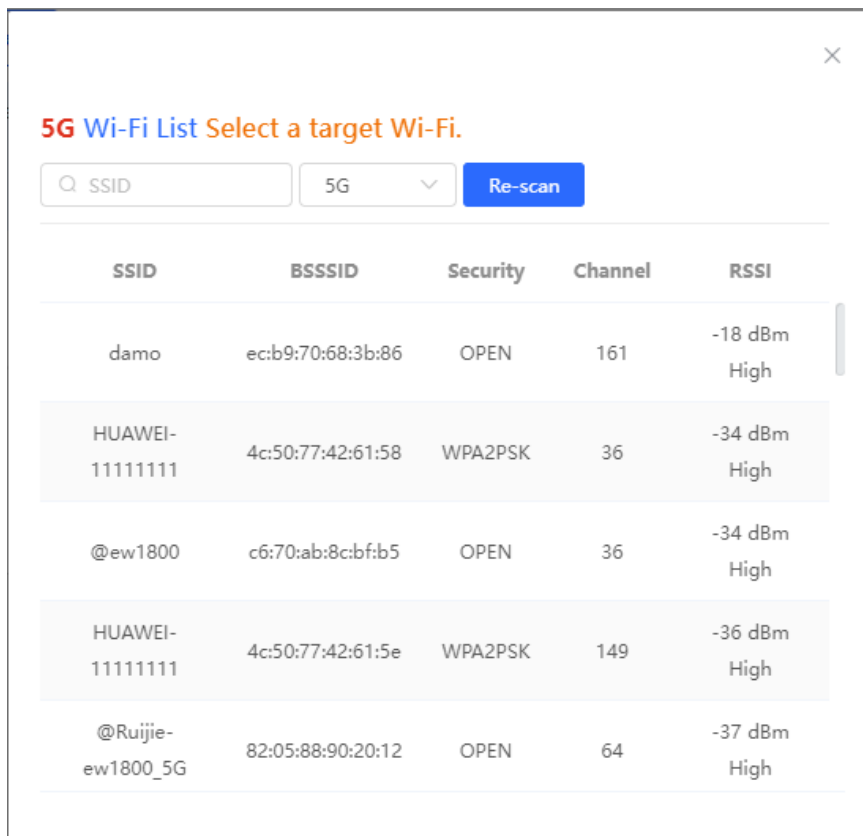
- This mode allows you to establish a wireless connection between a primary device and a secondary device, extending network coverage.
- The local device will work as a secondary device.
- It is recommended to select a 5G Wi-Fi of the primary device.

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

Wireless Repeater

Primary Device

* SSID



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

Q SSID 5G Re-scan

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

- (1) 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.
- (2) Configure Local Router Wi-Fi. You can select New Wi-Fi or Same as Primary Router Wi-Fi.
 - o 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.
 - o If **New Wi-Fi** is selected, you can set a local Wi-Fi name and password. Clients will search out different Wi-Fi signals.

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

Router
 Access Point
 Wireless Repeater

i

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

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

Wireless Repeater

Primary Device

* SSID @ew1800

Local Device

Local Router Wi-Fi **New Wi-Fi** Same as Primary Router Wi-Fi

* SSID(2.4G)

* SSID(5G)

Wi-Fi Password


⚠ 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.

4.6 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-RAP2260 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.

LAN Settings DHCP Clients Static IP Addresses

LAN Settings + Add Delete Selected

Up to 8 entries can be added.

<input type="checkbox"/>	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
<input type="checkbox"/>	192.168.120.2	255.255.255.0	Default VLAN	-	Enabled	192.168.120.2	253	30	Edit Delete

Add ×

* IP

* Subnet Mask

* VLAN ID

Remark

* MAC

DHCP Server

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 the 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.

4.7 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-RAP2260 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.

LAN Settings Port VLAN

 LAN Settings

Port VLAN

LAN Settings + Add Delete Selected

Up to 4 entries can be added.

<input type="checkbox"/>	VLAN ID	Remark	Action
<input type="checkbox"/>	99	test	Edit Delete

(1) 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.

Add ×

* VLAN ID

Remark

- (2) 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.

LAN Settings [Port VLAN](#)

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


Port VLAN

Connected Disconnected

Port 1

VLAN 1(WAN)	UNTAG ▾
VLAN 99	Not Joi ▾

4.8 Changing MAC Address

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

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

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

VLAN ID	<input type="text" value="Range: 2-232 and 234-4090."/>
* MTU	<input type="text" value="1500"/>
* MAC	<input type="text" value="ec:b9:70:23:a4:bf"/>
<input type="button" value="Save"/>	

4.9 Changing MTU

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

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

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

VLAN ID

* MTU

* MAC

4.10 Configuring DHCP Server


Caution

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

4.10.1 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.

4.10.2 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-RAP2260 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.

Edit ×

* IP

* Subnet Mask

Remark

* MAC


DHCP Server

* Start

* IP Count

* Lease Time(Min)

4.10.3 Displaying Online DHCP Clients

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP2260 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.

LAN Settings **DHCP Clients** Static IP Addresses

i View DHCP clients. ?

DHCP Clients Search by Hostname/IP/MAC

Up to **300** IP-MAC bindings can be added.

<input type="checkbox"/>	No.	Hostname	IP	MAC	Remaining Lease Time(min)	Status
<input type="checkbox"/>	1	nova-f5a...G-97	192.168.120.172	42:11:26:...	23	Convert to Static IP
<input type="checkbox"/>	2	no-7d2c...G-12	192.168.120.35	72:26:e8:...	13	Convert to Static IP
<input type="checkbox"/>	3	R1...	192.168.120.236	00:e0:4:...	19	Convert to Static IP

4.10.4 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-RAP2260 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.

LAN Settings DHCP Clients **Static IP Addresses**

i Static IP Address List ?

Static IP Address List Search by IP/MAC

Up to **300** entries can be added.

<input type="checkbox"/>	No.	IP	MAC	Action
<input type="checkbox"/>	1	192.168.120.64	12:33:e3:b9:d9:36	Edit Delete


4.11 Link Aggregation

Caution

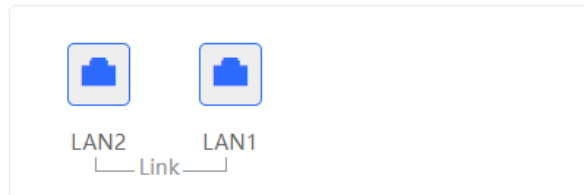
The function is supported by only RG-RAP2260(H).

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

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


 **Link Aggregation**
Please enable 802.3ad link aggregation on the client and connect it to port LAN2,LAN1.

Link Aggregation




Save

4.12 Configuring DNS

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP2260 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.

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

Local DNS server

Save


4.13 Hardware Acceleration

Caution

This function is supported by only RAP2260(H), RAP6260(H), RAP2260, and RAP6262.

In Local Device mode, choose  **Advanced > Hardware Acceleration**.


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

 **Hardware Acceleration**
 After Hardware Acceleration is enabled, the Internet access speed will be improved and clients will not be rate-limited.

Enable


[Save](#)

4.14 Configuring Port Flow Control

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP2260 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.

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

Flow Control


[Save](#)

4.15 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-RAP2260 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.

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

ARP List

Q
+ Add
Bind Selected
Delete Selected

Up to 256 IP-MAC bindings can be added.

<input type="checkbox"/>	No.	MAC	IP	Type	Action
<input type="checkbox"/>	1	12:33:e3:b9:d9:36	192.168.120.64	Dynamic	Bind
<input type="checkbox"/>	2	00:e0:4c:36:0b:ea	192.168.120.236	Static	Edit Delete
<input type="checkbox"/>	3	30:0d:9e:7e:13:a1	172.26.1.1	Dynamic	Bind

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

Add
×

* IP

* MAC

12:33:e3:b9:d9:36
(192.168.120.64)

00:e0:4c:36:0b:ea
(192.168.120.236)

4.16 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
<input type="checkbox"/>	5	Ruijie	Edit Delete

4.17 IPv6 Settings

Caution

This function is supported only by RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP2260, and RG-RAP6262 in the router mode.

4.17.1 Overview

Internet Protocol Version 6 (IPv6) is the next generation IP protocol designed by the Internet Engineering Task Force (IETF) to replace IPv4 and solve the IPv4 problems such as address depletion.

4.17.2 IPv6 Basic

1. IPv6 Address Format

IPv6 increases the length of the address from 32 bits in IPv4 to 128 bits, and therefore has a larger address space than IPv4.

The basic format of an IPv6 address is **X:X:X:X:X:X:X**. The 128-bit IPv6 address is divided into eight 16-bit sections that are separated by colons (:), and 16 bits in each section are represented by four hexadecimal characters (0–9 and A–F). Each **X** represents a 4-character hexadecimal number.

For example: 2001:ABCD:1234:5678:AAAA:BBBB:1200:2100, 800:0:0:0:0:0:1, 1080:0:0:0:8:800:200C:417A

The number **0** in the IPv6 address can be abbreviated as follows:

- The starting 0s can be omitted. For example, 2001:00CD:0034:0078:000A:000B:1200:2100 can be written as 2001:CD:34:78:A:B:1200:2100.
- Consecutive 0s can be replaced by two colons (::). For example, **800:0:0:0:0:0:1** can be written as **800::1**. Consecutive 0s can be replaced by two colons only when the 16-bit section contains all 0s, and the two colons can only appear once in the address.

2. IPv6 Prefix

An IPv6 address consists of two parts:

- Network prefix: It contains n bits, and is equivalent to the network ID in an IPv4 address.
- Interface identifier: It contains (128 - n) bits, and is equivalent to the host ID in an IPv4 address.

The length of the network prefix is separated from the IPv6 address by a slash (/). For example, **12AB::CD30:0:0:0/60** indicates that the length of the prefix used for routing in the address is 60 bits.

3. Special IPv6 Address

There are also some special IPv6 addresses, for example:

fe80::/8 is a link local address, and equivalent to 169.254.0.0/16 in IPv4.

fc00::/7 is a local address, and similar to 10.0.0.0/8, 172.16.0.0/16, or 192.168.0.0/16 in IPv4.

ff00::/12 is a multicast address, and similar to 224.0.0.0/8 in IPv4.

4. NAT66

IPv6-to-IPv6 Network Address Translation (NAT66) is the process of converting the IPv6 address in an IPv6 packet header to another IPv6 address. NAT66 prefix translation is an implementation of NAT66. It replaces the IPv6 address prefix in the packet header with another IPv6 address prefix to achieve IPv6 address translation. NAT66 can realize mutual access between an intranet and Internet.

4.17.3 IPv6 Address Assignment Methods


- Manual configuration: The IPv6 address/prefix and other network configuration parameters are manually configured.
- Stateless Address Autoconfiguration (SLAAC): The link local address is generated based on the interface ID, and then the local address is automatically configured based on the prefix information contained in the route advertisement packet.
- Stateful address autoconfiguration, that is, DHCPv6: DHCPv6 is divided into the following two types:
 - DHCPv6 autoconfiguration: The DHCPv6 server automatically configures the IPv6 address/prefix and other network configuration parameters.
 - DHCPv6 Prefix Delegation (PD): The lower-layer network device sends a prefix allocation application to the upper-layer network device. The upper-layer network device assigns an appropriate address prefix to the lower-layer device. The lower-layer device automatically subdivides the obtained prefix (generally less than 64 bits in length) into subnet segments with 64-bit prefix length, and then advertises the subdivided address prefixes to the user link directly connected to the IPv6 host through the route to realize automatic address configuration of the host.

4.17.4 Enabling IPv6

In **Local Device** mode, choose  **Network > IPv6 Address**.


Click **Enable**, and then click **OK** in the dialog box that appears to enable IPv6.

IPv6 Address

 1. When IPv6 is enabled, The MTU of IPV4 WAN port need higher than 1280.
 2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.


Enable

Tips ×

 Are you sure you want to enable IPv6 address?

After IPv6 is enabled, you can configure the IPv6 addresses of WAN and LAN ports, view the DHCPv6 client, and configure a static DHCPv6 address for the client.

IPv6 Address

 1. When IPv6 is enabled, The MTU of IPV4 WAN port need higher than 1280.
 2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.

Enable

WAN Settings
LAN Settings
DHCPv6 Clients
Static DHCPv6

* Internet

IPv6 Address

IPv6 Prefix

Gateway

DNS Server

NAT66

4.17.5 Configuring the IPv6 Address for the WAN Port

In **Local Device** mode, choose  **Network > IPv6 Address > WAN Settings**.

Configure the IPv6 address for the WAN port, and click **Save**.

IPv6 Address

i 1. When IPv6 is enabled, **The MTU of IPv4 WAN port need higher than 1280.**

2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.

Enable

[WAN Settings](#) [LAN Settings](#) [DHCPv6 Clients](#) [Static DHCPv6](#)

* Internet

IPv6 Address
DHCP
 Static IP
 Null

IPv6 Prefix

Gateway

DNS Server

NAT66

Save

Table 4-2 IPv6 Address Configuration Parameters of the WAN Port

Parameter	Description
Internet	Specify the method for obtaining an IPv6 address for the WAN port. <ul style="list-style-type: none"> ● DHCP: The current device will act as a DHCPv6 client and apply for the IPv6 address/prefix from the upstream network device. ● Static IP: If this Internet connection type is selected, you need to manually configure a static IPv6 address, gateway address, and DNS server. ● Null: The IPv6 function is disabled on the current WAN port.
IPv6 Address	If Internet is set to DHCP , the automatically obtained IPv6 address is displayed. If Internet is set to Static IP , you need to manually configure this parameter.
IPv6 Prefix	If Internet is set to DHCP and the current device obtains the IPv6 address prefix from the upstream device. The obtained IPv6 address prefix is displayed.
Gateway	If Internet is set to DHCP , the automatically obtained gateway address is displayed. If Internet is set to Static IP , you need to manually configure this parameter.
DNS Server	If Internet is set to DHCP , the automatically obtained DNS server address is displayed.

Parameter	Description
	If Internet is set to Static IP , you need to manually configure this parameter.
NAT66	If the current device cannot access the Internet in DHCP mode or cannot obtain the IPv6 address prefix, you must enable NAT66 to assign the IPv6 address to an intranet client.

4.17.6 Configuring the IPv6 Address for the LAN Port

In **Local Device** mode, choose  **Network > IPv6 Address > LAN Settings**.

When the device accesses the network in DHCP mode, the upstream device can assign an IPv6 address to the LAN port, and assign IPv6 addresses to the clients in the LAN based on the IPv6 address prefix. If the upstream device cannot assign an IPv6 address prefix to the current device, you need to manually configure an IPv6 address prefix for the LAN port, and assign IPv6 addresses to the clients in the LAN by enabling the NAT66 function (see [4.17.5 Configuring the IPv6 Address for the WAN Port](#)).

IPv6 Address

i 1. When IPv6 is enabled, The MTU of IPv4 WAN port need higher than 1280.
 2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.

Enable

WAN Settings | LAN Settings | DHCPv6 Clients | Static DHCPv6

LAN Settings + Add Delete Selected

Up to 8 entries can be added.

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

Click **Edit** corresponding to the default VLAN, and fill in a local address of no more than 64 bits in the **IPv6 Address/Prefix Length** column. This address will also be used as the IPv6 address prefix.

IPv6 Assignment specifies the method for assigning IPv6 addresses for clients. The following options are available:

- **Auto**: Both DHCPv6 and SLAAC are used to assign IPv6 addresses to clients.
- **DHCPv6**: DHCPv6 is used to assign IPv6 addresses to clients.
- **SLAAC**: SLAAC is used to assign IPv6 addresses to clients.
- **Null**: No IPv6 addresses are assigned to clients.

The setting of **IPv6 Assignment** is determined by the protocol supported by intranet clients. If you are not sure about the protocol supported by intranet clients, select **Auto**.

Edit ×

IPv6 Assignment ?

IPv6 Address/Prefix ?

Length

You can click **Advanced Settings** to configure more address attributes.

Edit ×

IPv6 Assignment ?

IPv6 Address/Prefix ?

Length

[Advanced Settings](#)

Subnet Prefix Name ?

Subnet Prefix Length ?

Subnet ID ?

* Lease Time (Min) ?

DNS Server

Table 4-3 IPv6 Address Configuration Parameters of the LAN Port


Parameter	Description
Subnet Prefix Name	Configure the interface from which the prefix is obtained, for example,

Parameter	Description
	WAN_V6. The default value is all interfaces.
Subnet Prefix Length	Configure the length of the subnet prefix. The value ranges from 48 to 64.
Subnet ID	Configure the subnet ID in hexadecimal notation. 0 indicates that the subnet ID automatically increments.
Lease Time (Min)	Configure the lease term of the IPv6 address. The unit is minutes.
DNS Server	Configure the address of the IPv6 DNS server.


4.17.7 Viewing DHCPv6 Clients

In **Local Device** mode, choose  **Network > IPv6 Address > DHCPv6 Clients.**

When the device acts as a DHCPv6 server to assign IPv6 addresses to clients, you can view information about the clients that obtain IPv6 addresses from the device on the current page. The information includes the host name, IPv6 address, remaining lease term, and DHCPv6 Unique Identifier (DUID) of each client.

Enter an IPv6 address or DUID in the search bar, and click  to quickly find the information of the specified DHCPv6 client.


IPv6 Address


 1. When IPv6 is enabled, The MTU of IPv4 WAN port need higher than 1280.
2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.

Enable

WAN Settings LAN Settings **DHCPv6 Clients** Static DHCPv6

DHCPv6 Clients

 You can view the DHCPv6 clients information on this page.

DHCPv6 Clients Search by IPv6 Address/DUID  [+ Batch Convert](#)

<input type="checkbox"/>	No.	Hostname	IPv6 Address	Remaining Lease Time(min)	DUID	Status
No Data						

Total 0

4.17.8 Configuring the Static DHCPv6 Address

Configure the IPv6 address statically bound to the DUID of a client so that the client can obtain the specified address each time.

In **Local Device** mode, choose  **Network > IPv6 Address > Static DHCPv6.**

IPv6 Address

i 1. When IPv6 is enabled, The MTU of IPv4 WAN port need higher than 1280.
 2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.

Enable

[WAN Settings](#) [LAN Settings](#) [DHCPv6 Clients](#) [Static DHCPv6](#)

Static IP Address List

Static IP Address List

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

<input type="checkbox"/>	No.	IPv6 Address	DUID	Action
No Data				

Total 0

(1) Click **Add**.

×

Add

* IPv6 Address

* DUID

(2) Enter the IPv6 address and DUID of the client.

(3) Click **OK**.

4.17.9 Configuring the IPv6 Neighbor List

In IPv6, Neighbor Discovery Protocol (NDP) is an important basic protocol. NDP replaces the ARP and ICMP route discovery protocols of IPv4, and supports the following functions: address resolution, neighbor status tracking, duplicate address detection, router discovery, and redirection.

In **Local Device** mode, choose **Security > IPv6 Neighbor List**.

IPv6 Neighbor List

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

<input type="checkbox"/>	No.	MAC Address	IP Address	Type	Ethernet status	Action
<input type="checkbox"/>	1	58:69:6c:22:08:30	fe80::5a69:6cff:fe22:830	Dynamic	WAN	Bind
<input type="checkbox"/>	2	42:93:d6:46:2e:ab	fe80::5e1a:a95:3ed7:9be4	Dynamic	LAN	Bind
<input type="checkbox"/>	3	f8:e4:3b:13:21:6f	fe80::9120:5120:d4df:562b	Dynamic	LAN	Bind

Total 3

(1) Click **Add** and add the interface, IPv6 address and MAC address of the neighbor.

Add ×

* Interface

* IPv6 Address

* MAC Address

(2) Select the IPv6 neighbor list to be bound, and click **Bind** in the **Action** column to bind the IPv6 address and MAC address.

IPv6 Neighbor List Search by IP Address/MAC A

Up to 256 IP-MAC bindings can be added.

<input type="checkbox"/>	No.	MAC Address	IP Address	Type	Ethernet status	Action
<input type="checkbox"/>	1	58:69:6c:22:08:30	fe80::5a69:6cff:fe22:830	Dynamic	WAN	Bind
<input type="checkbox"/>	2	42:93:d6:46:2e:ab	fe80::5e1a:a95:3ed7:9be4	Dynamic	LAN	Bind
<input type="checkbox"/>	3	f8:e4:3b:13:21:6f	fe80::9120:5120:d4df:562b	Dynamic	LAN	Bind

< **1** > 10/page

Total 3


5 System Settings

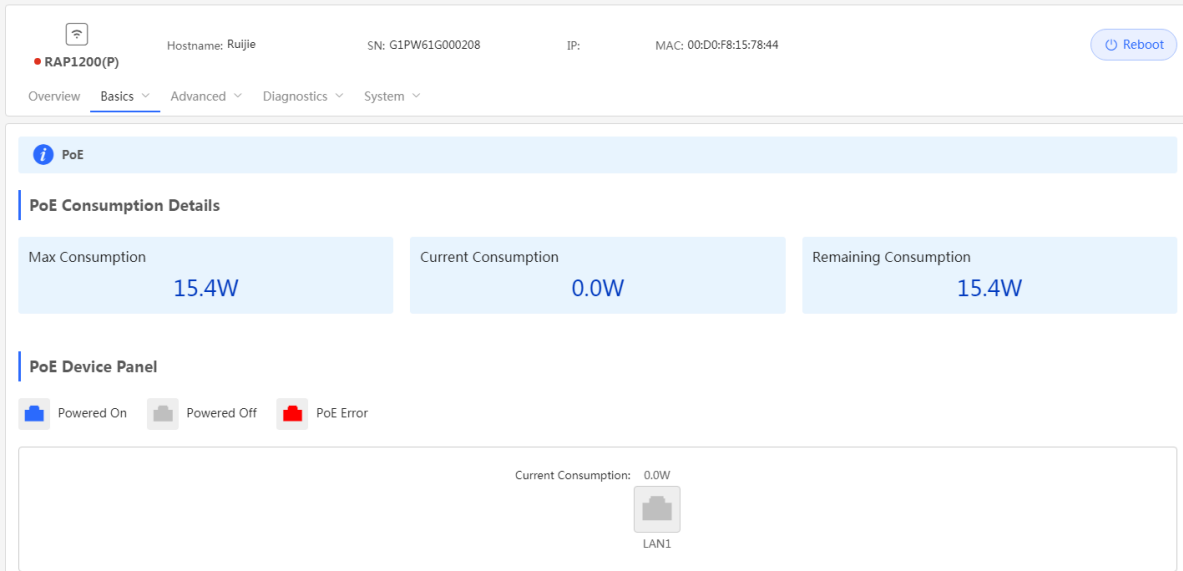
5.1 PoE

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.



Hostname: Ruijie SN: G1PW61G000208 IP: MAC: 00:D0:F8:15:78:44 [Reboot](#)




Overview **Basics** Advanced Diagnostics System

PoE


PoE Consumption Details

Max Consumption	Current Consumption	Remaining Consumption
15.4W	0.0W	15.4W

PoE Device Panel

 Powered On
  Powered Off
  PoE Error

Current Consumption: 0.0W

 LAN1

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-RAP2260, 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.

i **PoE Settings**

Power Mode

Current Mode IEEE 802.3bt

Energy Saving ?


Band 2.4G 5G 2.4G+5G


Current Power 51W

Save


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-RAP2260 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.

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

* Old Password

* New Password


* Confirm Password

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-RAP2260 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.


 **Session Timeout**

* Session Timeout seconds


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-RAP2260 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

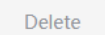
In self-organizing network mode, the system time of all devices in the network will be changed synchronously.

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

Current Time 2022-04-01 10:14:00 

* Time Zone 

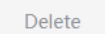
* NTP Server 
















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-RAP2260 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.




Please keep the device powered on during reboot.

Reboot

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-RAP2260 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.

Reboot

Scheduled Reboot



Please keep the device powered on during reboot.

Select


 Local All Devices Specified Devices**Reboot All Device****⚠ 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-RAP2260 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.

Reboot Scheduled Reboot

i Please keep the device powered on during reboot.

Select Local All Devices Specified Devices

Available Devices 1/1

Search by SN/Model

G1QH6WX000610 - RAP2260(E)

< Delete

Add >

Selected Devices 0/0

Search by SN/Model

No data

Reboot

Reboot Scheduled Reboot

i Please keep the device powered on during reboot.

Select Local All Devices Specified Devices

Available Devices 0/0

Search by SN/Model

No data

Selected Devices 1/1

Search by SN/Model

G1QH6WX000610 - RAP2260(E)

< Delete


Add >

Reboot



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-RAP2260 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.

Reboot [Scheduled Reboot](#)


 It is recommended to set the scheduled time to a network idle time, e.g., 2 A.M..
The downlink device will also be rebooted as scheduled.



Enable

Day Mon Tue Wed Thu Fri Sat Sun

Time :

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-RAP2260 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.

[Backup & Import](#) [Reset](#)

 If the target version is much later than the current version, some configuration may be missing. It is recommended to choose [Restore](#) before importing the profile. The device will be rebooted automatically later. 

Backup Profile


Backup Profile [Backup](#)

Import Profile

File Path [Browse](#) [Import](#)

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-RAP2260 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.

[Backup & Import](#) [Reset](#)

 Resetting the device will clear the current settings. If you want to keep the setup, please [Backup Profile](#) first.

[Reset](#)

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-RAP2260 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.

Backup & Import [Reset](#)

 Resetting the device will clear the current settings. If you want to keep the configuration, please [Backup Config](#) first.

Select Local All Devices

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

[Reset All Devices](#)

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-RAP2260 and RG-RAP6262 models: In **Local Device** mode, choose  **System > Upgrade > Online Upgrade**

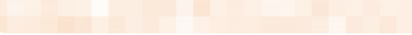
For other RAP models: Choose ( **WLAN > APs > Manage >**  **System > Upgrade > Online Upgrade**



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

[Online Upgrade](#) Local Upgrade

 Online upgrade will keep the current configuration. Please do not refresh the page or close th

Current Version ReyeeOS 1.86. 


New Version **ReyeeOS 1.** 

Description 1. 
2. 

Tip 1. If your device cannot access the Internet, please click [Download File](#).
2. Choose [Local Upgrade](#) to upload the file for local upgrade.

[Upgrade Now](#)


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-RAP2260 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.

[Online Upgrade](#) [Local Upgrade](#)

 Please do not refresh the page or close the browser.

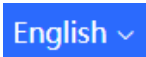
Model RAP 

Current Version ReyeeOS 1.86. 

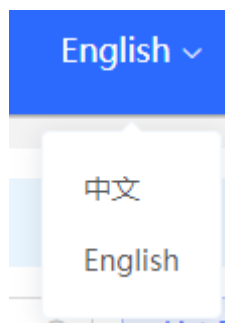
Keep Config (If the target version is much later than the current version, it is recommended not to keep the configuration.)

File Path [Browse](#) [Upload](#)

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-RAP2260 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.



LED Status Control

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


Enable

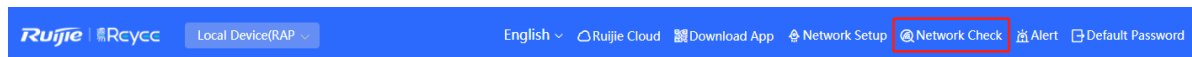
Save

6 Network Diagnosis Tools

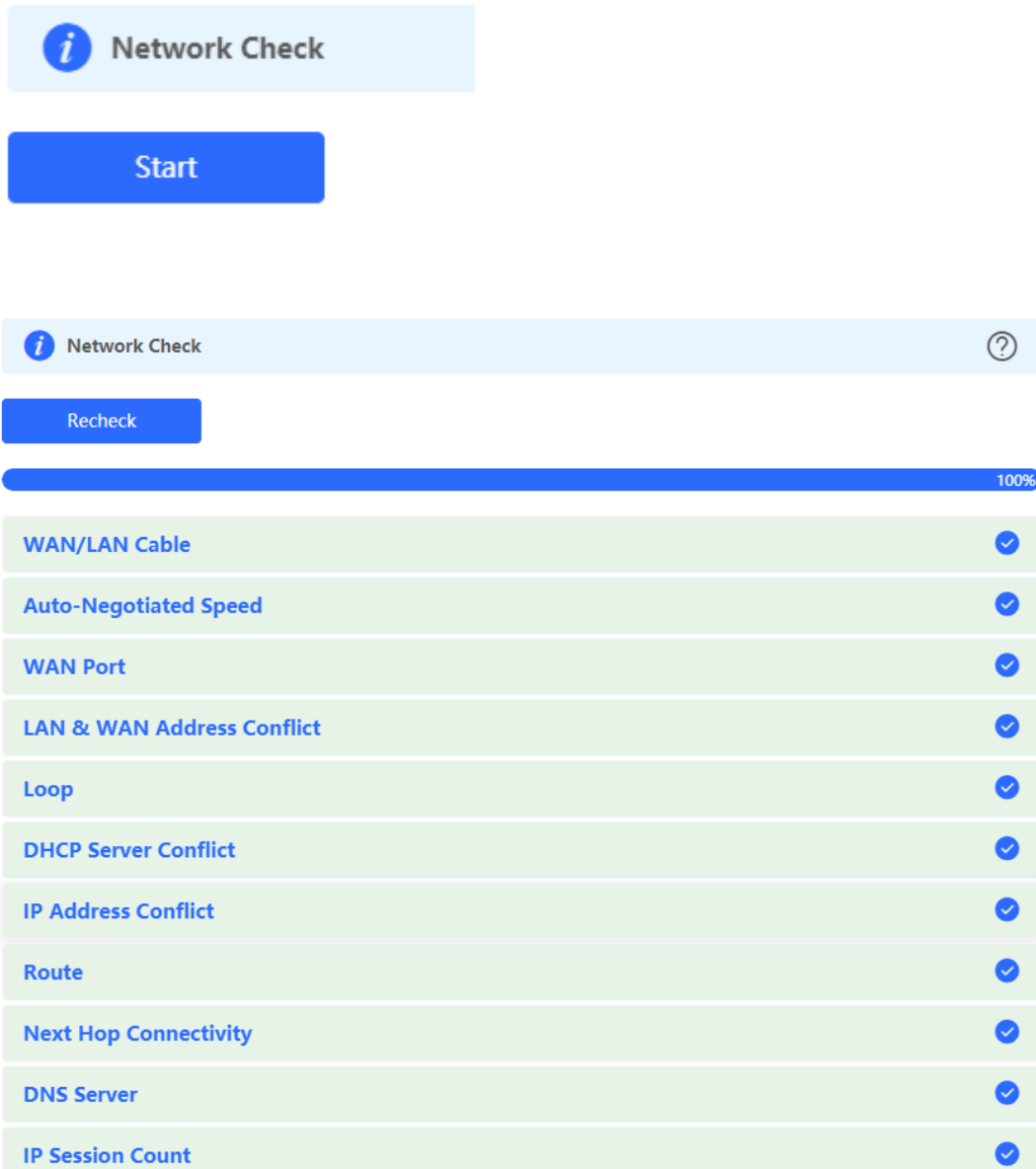
6.1 Network Check

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.



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

The image shows the 'Network Check' page. At the top, there is a light blue header with an information icon and the text 'Network Check'. Below this is a blue 'Start' button. Further down, there is another light blue header with an information icon, 'Network Check', and a help icon. Below that is a blue 'Recheck' button. A progress bar shows '100%' completion. Below the progress bar is a list of 12 items, each with a green background and a blue checkmark icon on the right:

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

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

IP Session Count
✔

DHCP Capacity
✔

Ruijie Cloud Server
!

Check Connection to Cloud Server

Result : The device is not connected with the cloud server. Cloud service may fail to start.

Suggestion : Please verify that the device SN is added to the cloud and check the network.

6.2 Network Tools

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

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

- The Ping tool tests 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.

Enter an IP address or a URL, and click **Start**. If you need to perform the ping or Traceroute operation, configure other parameters as required.

Network Tools

Tool Ping Traceroute DNS Lookup

Type IPv4 IPv6

* IP Address/Domain

* Ping Count

* Packet Size Bytes

PING www.baidu.com (163.177.151.109): 64 data bytes

72 bytes from 163.177.151.109: seq=0 ttl=51 time=18.896 ms

72 bytes from 163.177.151.109: seq=1 ttl=51 time=18.686 ms

72 bytes from 163.177.151.109: seq=2 ttl=51 time=18.284 ms

72 bytes from 163.177.151.109: seq=3 ttl=51 time=20.310 ms

Network Tools

Tool Ping Traceroute DNS Lookup

Type IPv4 IPv6

* IP Address/Domain

* Max TTL

traceroute to www.baidu.com (163.177.151.109), 20 hops max, 46 byte packets

1 192.168.111.1 (192.168.111.1) 0.621 ms 0.536 ms 0.548 ms

2 172.20.74.1 (172.20.74.1) 2.271 ms 9.091 ms 8.565 ms

3 172.20.255.109 (172.20.255.109) 2.974 ms 6.424 ms 10.932 ms

4 * * *

5 172.22.0.249 (172.22.0.249) 1.902 ms 1.453 ms 1.081 ms

6 112.111.60.97 (112.111.60.97) 3.215 ms 3.290 ms 2.794 ms

7 218.104.229.69 (218.104.229.69) 2.890 ms 2.639 ms

i **Network Tools**

Tool Ping Traceroute **DNS Lookup**

* IP Address/Domain

Start
Stop

```

Server:      127.0.0.1
Address:    127.0.0.1#53

Name:      www.baidu.com
www.baidu.com canonical name = www.a.shifen.com
Name:      www.a.shifen.com
Address 1: 163.177.151.109
Address 2: 163.177.151.110
www.baidu.com canonical name = www.a.shifen.com
                    
```

6.3 Alarms

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP2260 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.

Alert List
View Unfollowed Alert

Expand	Alerts	Suggestion	Action
▼	There is more than one DHCP server in the LAN network.	Please disable the extra DHCP server in the LAN network.	Delete Unfollow

Hostname	SN	Type	Time	Details	Action
Ruijie	1234567891234	EG210G-P	2022-04-24 09:39:08	A DHCP server conflict occurs in LAN network: MAC:58:69:6c:00:00:01,IP:192.168.11.1,VLAN ID:233; MAC:UNKNOWN,IP:192.168.112.1,VLAN ID:233	Delete

Are you sure you want to unfollow the alarm and delete it from the alarm list?

1. After being unfollowed, an alarm **will not appear again..**
2. You can click [View Unfollowed Alarm](#) to **re-follow** an unfollowed alarm.


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

View Unfollowed Alert ×

There is more than one DHCP server in the LAN network.


[Re-follow](#)

6.4 Fault Collection

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP2260 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.

 **Fault Collection**
Compress the configuration 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.
- (1) 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.)
- (2) Run the **Ping** command to check the connectivity between the PC and the device. If the ping fails, please check the network settings.
- (3) 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.