

# Ruijie Reyee RG-RAP and RG-EAP Series Access Points

Web-based Configuration Guide ReyeeOS 1.95



## 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](mailto:service_rj@ruijienetworks.com)

## Conventions

### 1. GUI Symbols

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

### 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-EAP and 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 Login to Eweb .....	1
1.2.1 Connecting to the Access Point .....	1
1.2.2 Configuring the IP Address of the Management Client .....	1
1.2.3 Logging in to the Web Page .....	2
1.3 Work Mode.....	3
1.3.1 AP Mode.....	3
1.3.2 Router Mode .....	3
1.3.3 Wireless Repeater Mode .....	3
1.4 Configuration Wizard (Router Mode).....	3
1.4.1 Getting Started.....	4
1.4.2 Configuration Steps .....	4
1.5 Configuration Wizard (AP Mode).....	7
1.5.1 Getting Started.....	7
1.5.2 Configuration Steps .....	7
1.6 Configuration Wizard (Wireless Repeater Mode).....	7
1.6.1 Getting Started.....	7
1.6.2 Configuration Steps .....	8
1.7 Introduction to the Eweb GUI.....	10
1.7.1 Dual Management Webpages .....	10

2 Network Monitoring .....	12
2.1 Viewing the Network Information .....	12
2.2 Adding Network Devices .....	14
2.2.1 Wired Connection .....	14
2.2.2 AP Mesh .....	16
2.3 Managing Network Devices .....	17
2.4 Configuring Network Planning .....	19
2.4.1 Configuring Wired VLAN .....	19
2.4.2 Configuring Wi-Fi VLAN .....	21
2.5 Troubleshooting Fault Alerts .....	23
3 Wi-Fi Network Settings .....	25
3.1 Configuring AP Groups .....	25
3.1.1 Overview .....	25
3.1.2 Procedures .....	25
3.2 Configuring SSID and Wi-Fi Password .....	27
3.3 Hiding the SSID .....	27
3.3.1 Overview .....	27
3.3.2 Configuration Steps .....	28
3.4 Checking Wireless Clients .....	28
3.5 Configuring Wi-Fi Band .....	29
3.6 Configuring Band Steering .....	30
3.7 Configuring Wi-Fi 6 .....	31
3.8 Configuring Layer-3 Roaming .....	32
3.9 Configuring AP Isolation .....	33

3.10 Adding a Wi-Fi Network .....	34
3.11 Configuring a Guest Wi-Fi .....	35
3.11.1 Overview .....	35
3.11.2 Configuration Steps.....	35
3.12 Configuring Wi-Fi Blacklist or Whitelist.....	36
3.12.1 Overview .....	36
3.12.2 Configuration Steps .....	36
3.13 Optimizing Wi-Fi Network .....	38
3.13.1 Overview .....	38
3.13.2 Getting Started.....	38
3.13.3 Optimizing the Radio Channel .....	39
3.13.4 Optimizing the Channel Width .....	40
3.13.5 Optimizing the Transmit Power.....	41
3.13.6 Configuring the Kick-off Threshold .....	42
3.13.7 Configuring the Client Limit.....	42
3.13.8 Configuring the Roaming Sensitivity.....	43
3.13.9 Configuring WIO .....	44
3.14 Configuring Healthy Mode .....	45
3.15 Configuring Xpress .....	46
3.16 Configuring Wireless Schedule .....	47
3.17 Enabling Reyee Mesh.....	48
4 Network Settings .....	49
4.1 Switching Work Mode .....	49
4.1.1 Work Mode.....	49

4.1.2 Self-Organizing Network Discovery .....	49
4.1.3 Configuration Steps .....	49
4.1.4 Viewing Device Role .....	51
4.2 Configuring Internet Type .....	51
4.3 Configuring LAN Port .....	52
4.4 Configuring Repeater Mode.....	53
4.4.1 Wired Repeater .....	53
4.4.2 Wireless Repeater .....	54
4.5 Creating a VLAN .....	56
4.6 Configuring Port VLAN .....	58
4.7 Changing MAC Address .....	59
4.8 Changing MTU.....	60
4.9 Configuring DHCP Server.....	61
4.9.1 DHCP Server .....	61
4.9.2 Configuring the DHCP Server Function.....	61
4.9.3 Displaying Online DHCP Clients.....	62
4.9.4 Displaying the DHCP Static IP Address List.....	63
4.10 Link Aggregation .....	63
4.11 Configuring DNS .....	64
4.12 Hardware Acceleration .....	64
4.13 Configuring Port Flow Control .....	64
4.14 Configuring ARP Binding .....	65
4.15 Configuring LAN Ports .....	66
5 System Settings .....	68



5.1 PoE Settings .....	68
5.2 Setting the Login Password.....	68
5.3 Setting the Session Timeout Duration.....	69
5.4 Setting and Displaying System Time.....	69
5.5 Configuring Reboot.....	70
5.5.1 Rebooting the Current Device .....	71
5.5.2 Rebooting All Devices in the Network.....	71
5.5.3 Rebooting the Specified Device.....	71
5.6 Configuring Scheduled Reboot.....	72
5.6.1 Configuring Scheduled Reboot for the Current Device .....	72
5.7 Configuring Backup and Import.....	73
5.8 Restoring Factory Settings .....	74
5.8.1 Restoring the Current Device to Factory Settings .....	74
5.8.2 Restoring All Devices to Factory Settings.....	74
5.9 Performing Upgrade and Checking System Version.....	75
5.9.1 Online Upgrade.....	75
5.9.2 Local Upgrade.....	76
5.10 Switching System Language .....	76
5.11 Configuring LED Status Control .....	77
6 Network Diagnosis Tools.....	78
6.1 Network Check.....	78
6.2 Network Tools.....	79
6.3 Alarms .....	80
6.4 Fault Collection .....	81

7 FAQs..... 82

7.1 What can I do when I failed to log in to the Eweb management system? .....82

7.2 How can I restore the device to factory settings? .....82

7.3 What can I do when I forget the password? .....82

# 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 Login to Eweb

### 1.2.1 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 [1.2.2 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 [1.2.2 Configuring the IP Address of the Management Client](#).

### 1.2.2 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.

**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.
--	--

**⚠ 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.

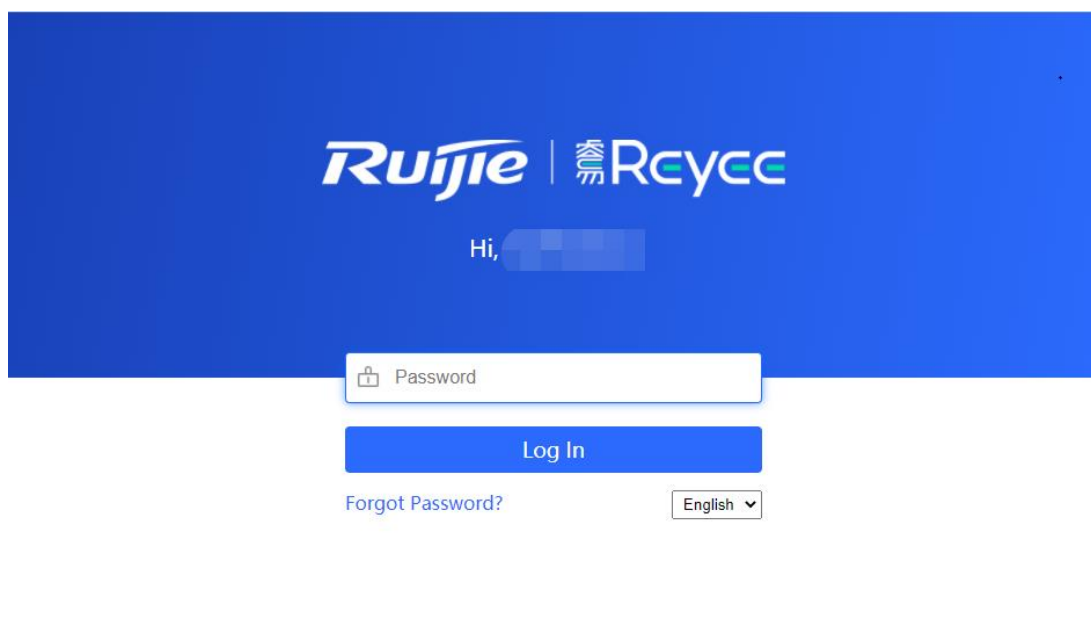
### 1.2.3 Logging in to the Web Page

- (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.

**i 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.

---

## 1.3 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/EAP works in the AP mode by default. If you want to switch the work mode, see [4.1 Switching Work Mode](#).

### 1.3.1 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.

### 1.3.2 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.

---

### 1.3.3 Wireless Repeater Mode

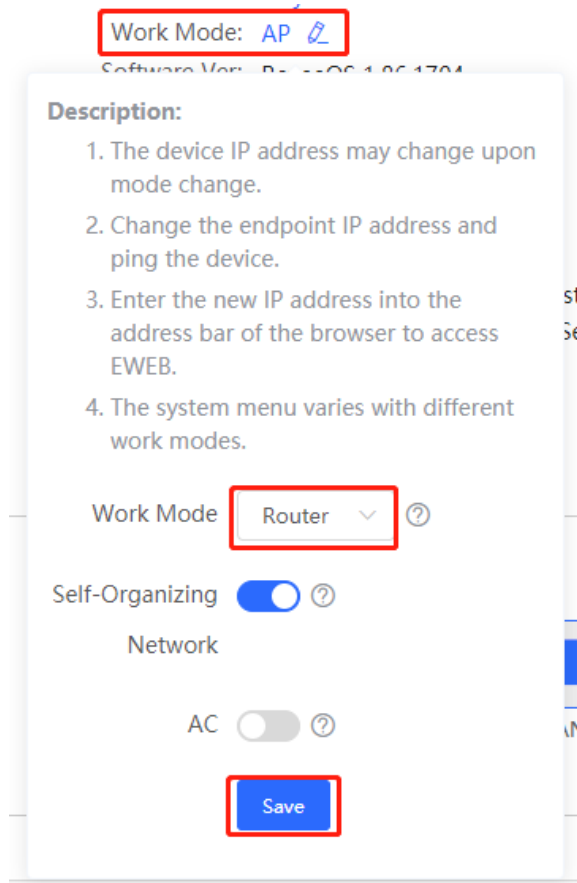
The device does not support the routing and DHCP server functions in the wireless repeater mode. IP addresses of the clients are assigned and managed by the primary router. On an available network, the device can be connected to the primary router through wireless connection to expand the Wi-Fi coverage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

## 1.4 Configuration Wizard (Router Mode)

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

### 1.4.1 Getting Started

- (1) Connect the device to a power supply and connect the port of the device to an upstream device with an Ethernet cable. Or you can connect an Ethernet cable to the device.
- (2) Configure the Internet connection type according to requirements of the local Internet Service Provider (ISP). Otherwise, the Internet access may fail due to improper configuration. You are advised to contact your local ISP to confirm the Internet connection type:
  - 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.
- (3) The device works in the AP mode by default. If you want to switch the work mode to the router mode, perform the configuration on the work mode setting page. See [4.1 Switching Work Mode](#) for more details.



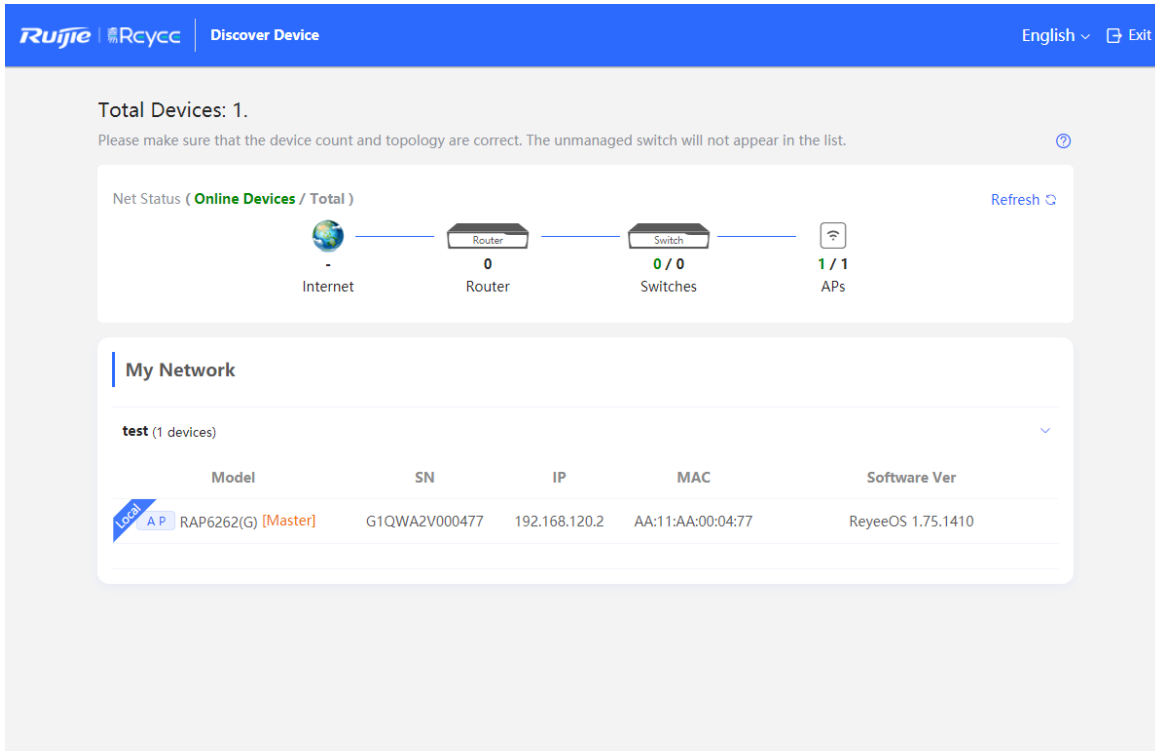
### 1.4.2 Configuration Steps

#### 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.



The screenshot displays the 'Discover Device' page in the Ruijie Rcycc web interface. At the top, it shows 'Total Devices: 1' and a message: 'Please make sure that the device count and topology are correct. The unmanaged switch will not appear in the list.' Below this is a 'Net Status' section showing a topology diagram with 'Internet', 'Router' (0), 'Switches' (0/0), and 'APs' (1/1). A 'Refresh' button is present. The 'My Network' section shows a table with one device:

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

At the bottom, there are 'Rediscover' and 'Start Setup' buttons.

## 2. Creating a Network Project

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

- (1) **Network Name:** Identify the network where the device is located.
- (2) **Internet:** Configure the Internet connection type according to requirements of the local Internet Service Provider (ISP).
  - o **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.
  - o **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**.
- (3) **SSID and Wi-Fi Password:** The device has no Wi-Fi password by default, indicating that the Wi-Fi network is an open network. You are advised to configure a complex password to enhance the network security.
- (4) **Management Password:** The password is used for logging in to the management page.
- (5) **Country/Region:** The Wi-Fi channel may vary from country to country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.
- (6) **Time Zone:** Set the system time. The network time server is enabled by default to provide the time service. You are advised to select the actual time zone.

**\* Network Name** Example: XX hotel.

**Network Settings**

Internet  PPPoE  DHCP  Static IP  
⚠ Checking IP assignment

**\* SSID**

Wi-Fi Password  Security  Open

**Management Password (Please remember the password.)**

**\* Management Password** Please remember the management password

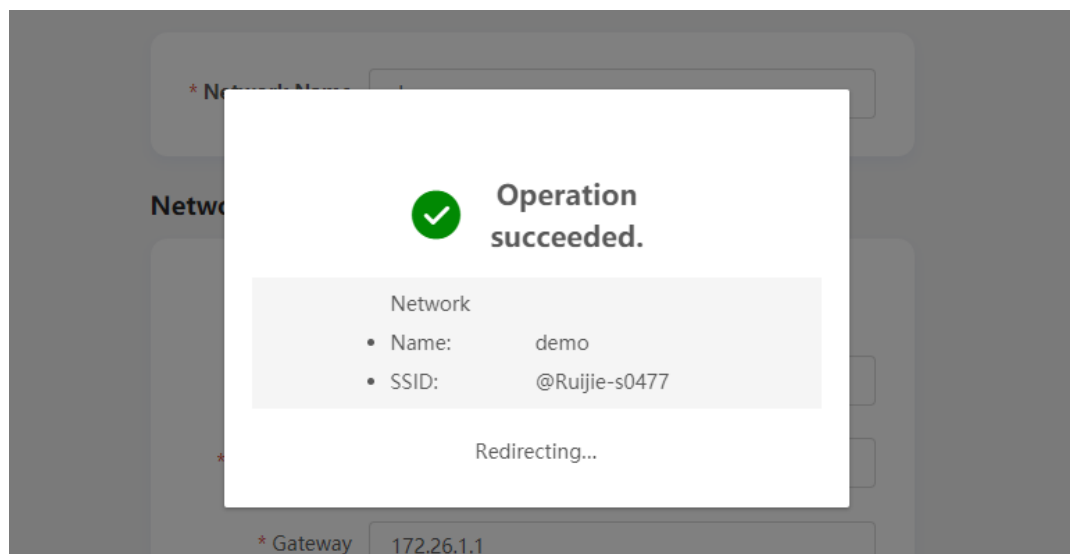
**Country/Region/Time Zone**

**\* Country/Region** China (CN)

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

Previous Create Network & Connect

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.

**i 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.



## 1.5 Configuration Wizard (AP Mode)

### 1.5.1 Getting Started

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

### 1.5.2 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 [1.4.2 Configuration Steps](#) for details.

The screenshot shows the 'Create Network' configuration wizard in the Ruijie Rcycc web interface. The interface is in English and includes the following sections:

- Network Name:** A text input field with the placeholder text 'Example: XX hotel.'
- Network Settings:**
  - Internet connection type: 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 text 'Please remember the management pas:' and a show/hide icon.
- Country/Region/Time Zone:**
  - Country/Region: A dropdown menu showing 'China (CN)'.
  - Time Zone: A dropdown menu showing '(GMT+8:00)Asia/Shanghai'.

A blue button labeled 'Create Network & Connect' is located at the bottom of the form.

## 1.6 Configuration Wizard (Wireless Repeater Mode)

### 1.6.1 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.

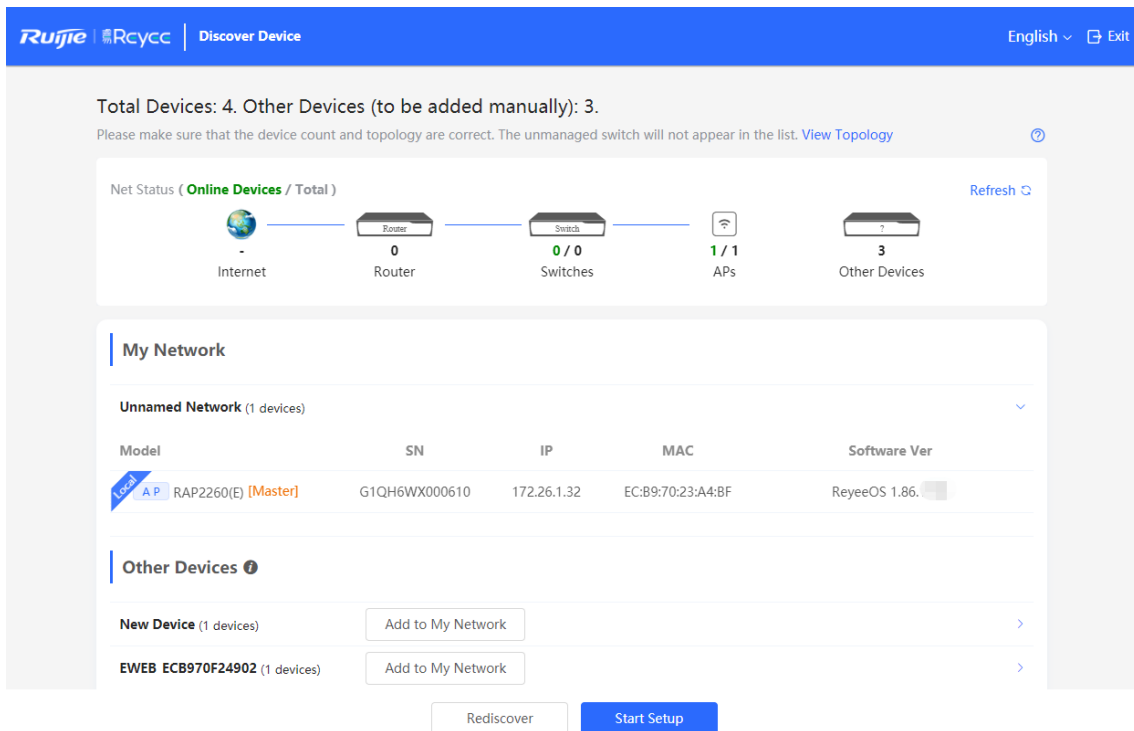
---

**⚠ Caution**

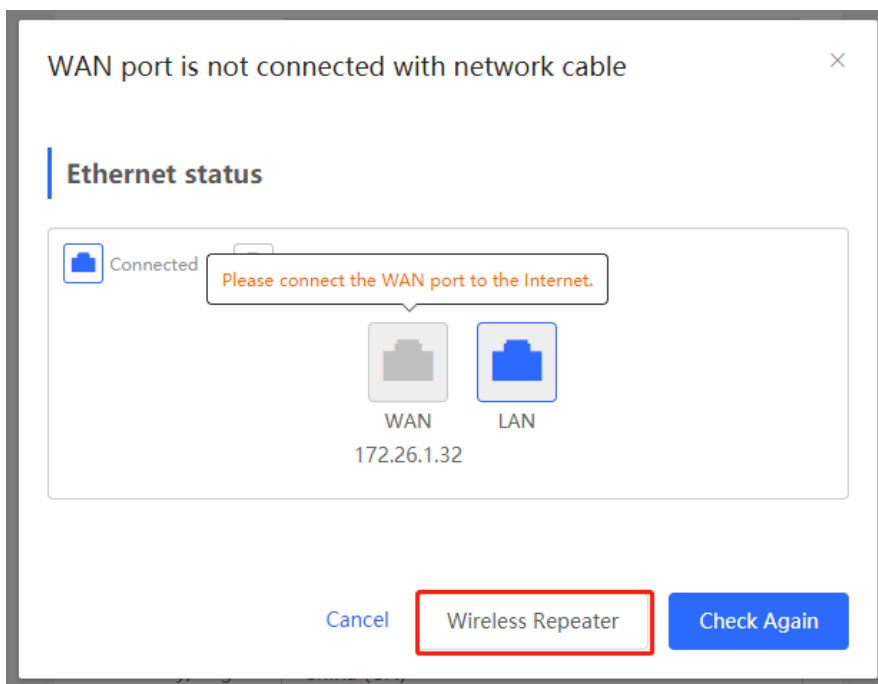
- No Ethernet cable is required in the wireless repeater mode. The wireless network stability can be affected by many factors. Therefore, the wired connection is recommended.
-

### 1.6.2 Configuration Steps

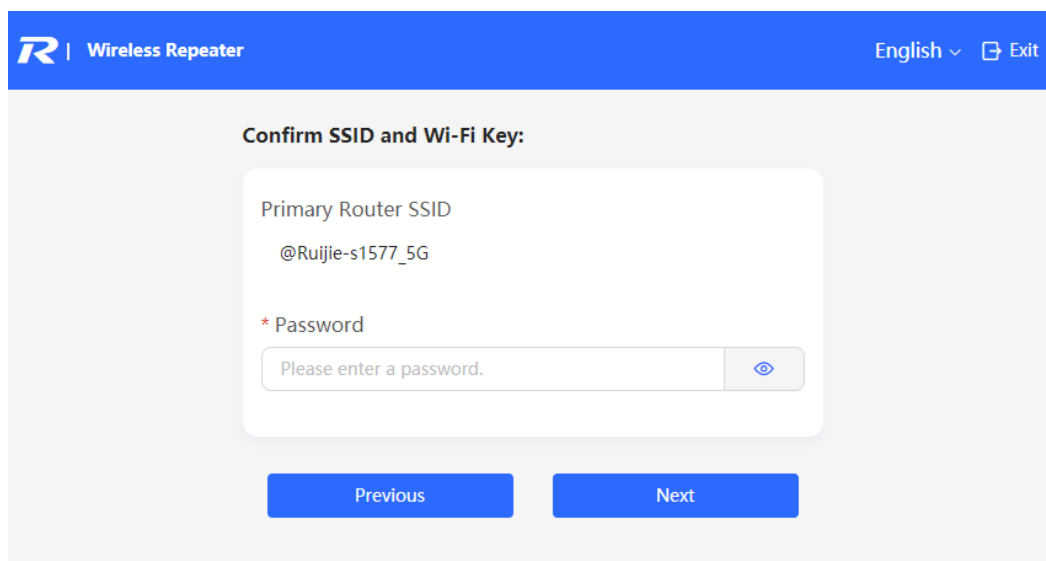
- (1) Connect the device to a power supply without connecting an Ethernet cable to the uplink port, and click **Start Setup**.



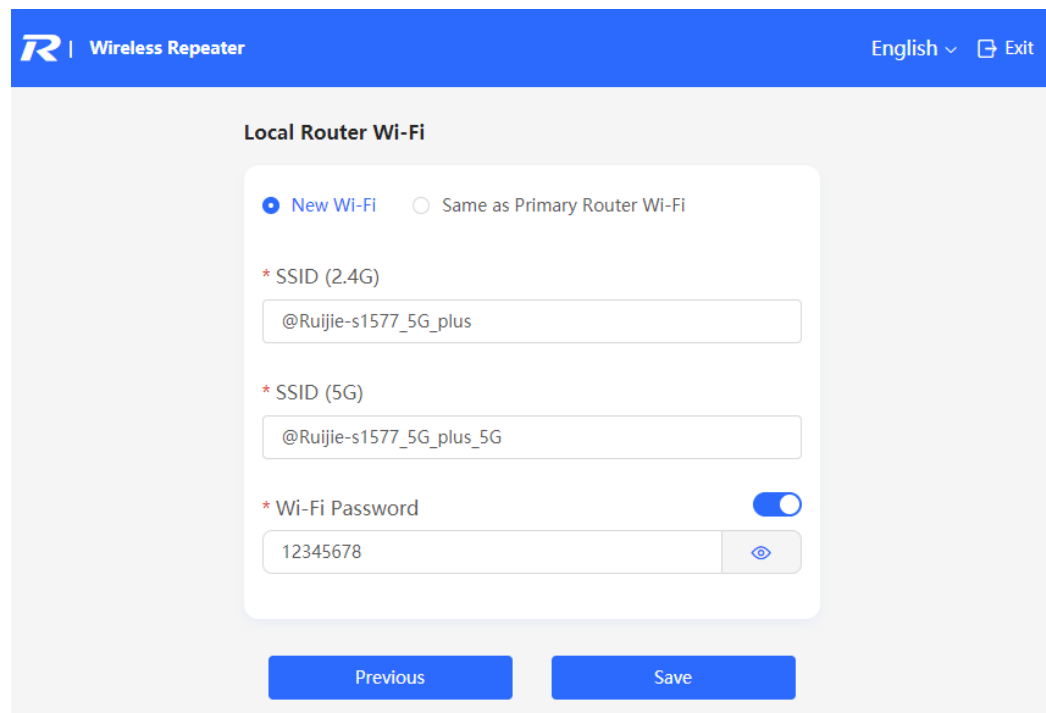
- (2) If you see a dialogue box indicating that the Ethernet cable is not connected to the WAN port, click **Wireless Repeater**.



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



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



## 1.7 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 [4.1 Switching Work Mode](#).

**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.

### 1.7.1 Dual Management Webpages

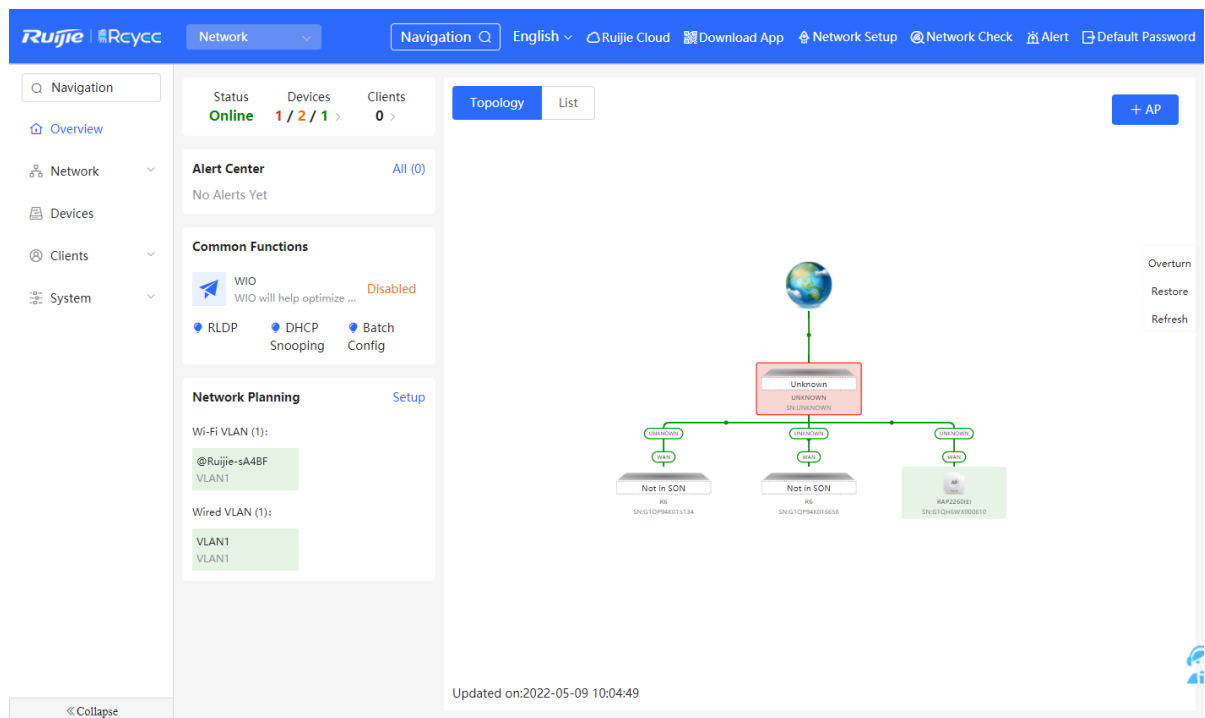
#### 1. Introducing the Management Mode

If the self-organizing network is disabled (The function is enabled by default. See [4.1 Switching Work Mode](#) for details.), the device works in the local device mode displayed on the Web page.

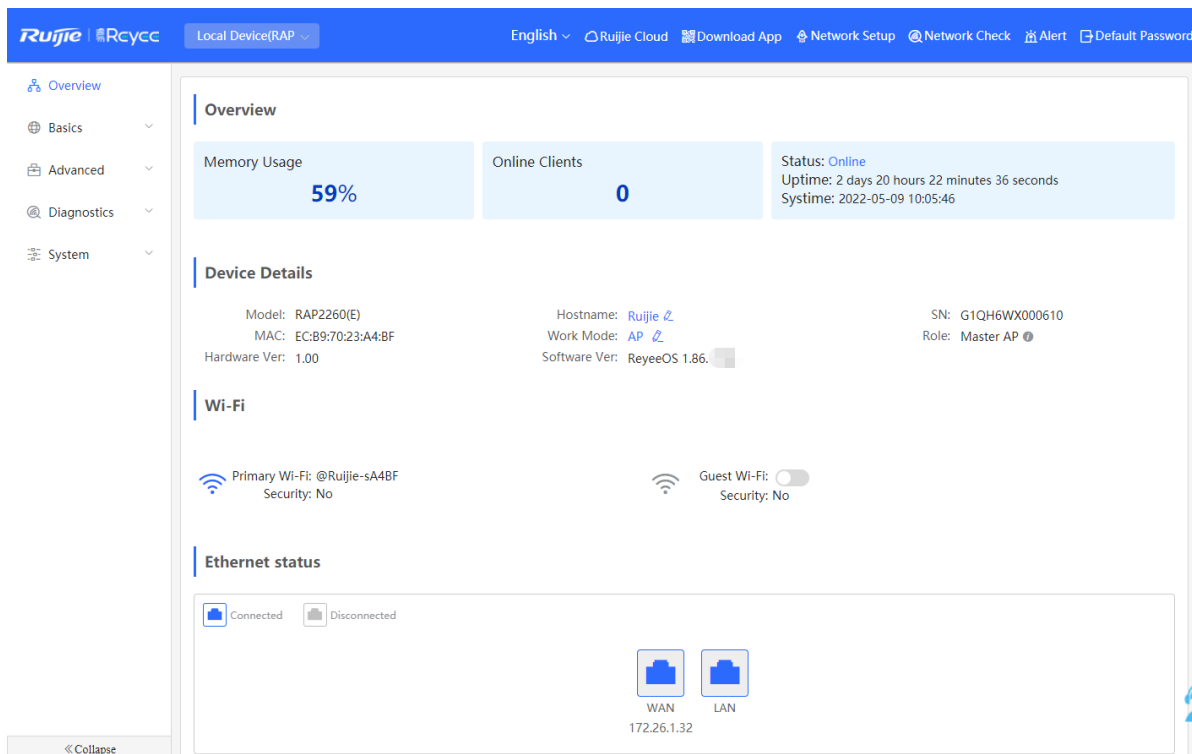
If the self-organizing network is enabled, the device can work in the network mode and the local device mode. The two modes can be switched on the Web page.

- 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

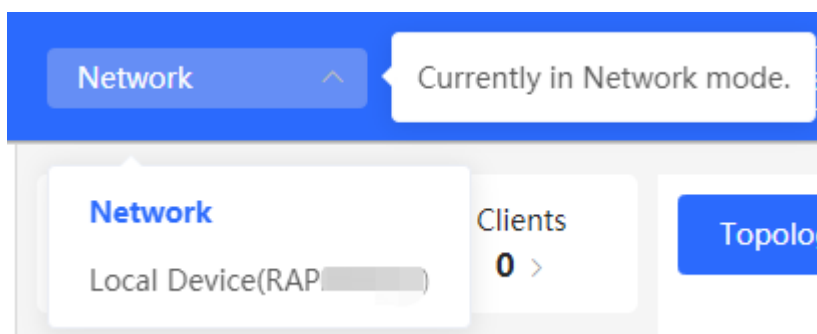


### Local Device mode webpage




## 2. Switching the Management Mode

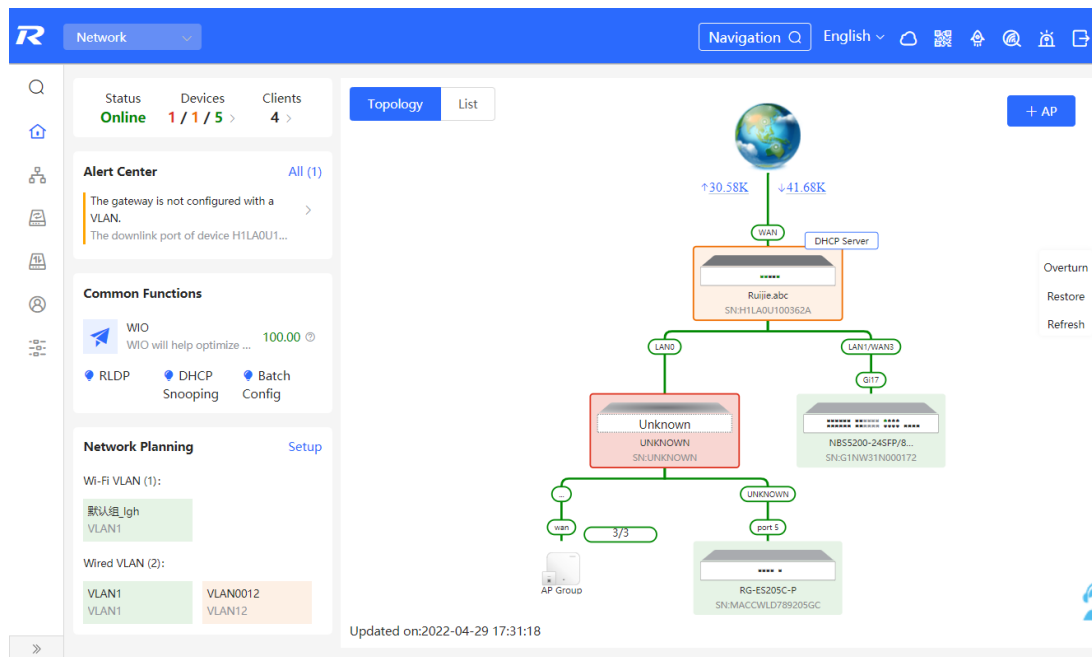
Click the current management mode in the navigation bar, and select the mode in the drop-down box to switch the work mode of the device.



# 2 Network Monitoring

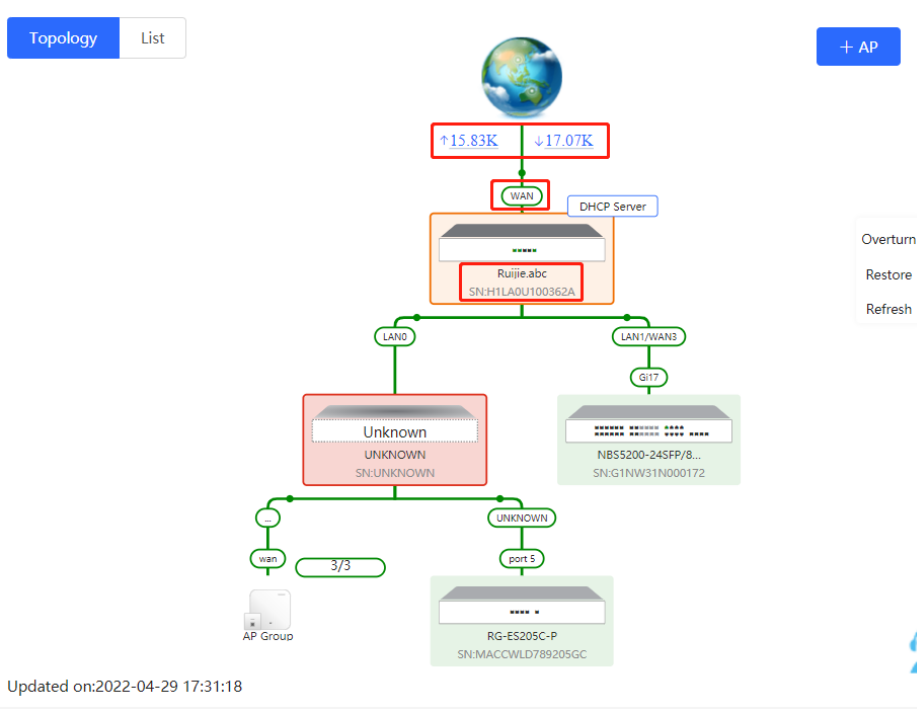
In **Network** mode, select  **Overview**.

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

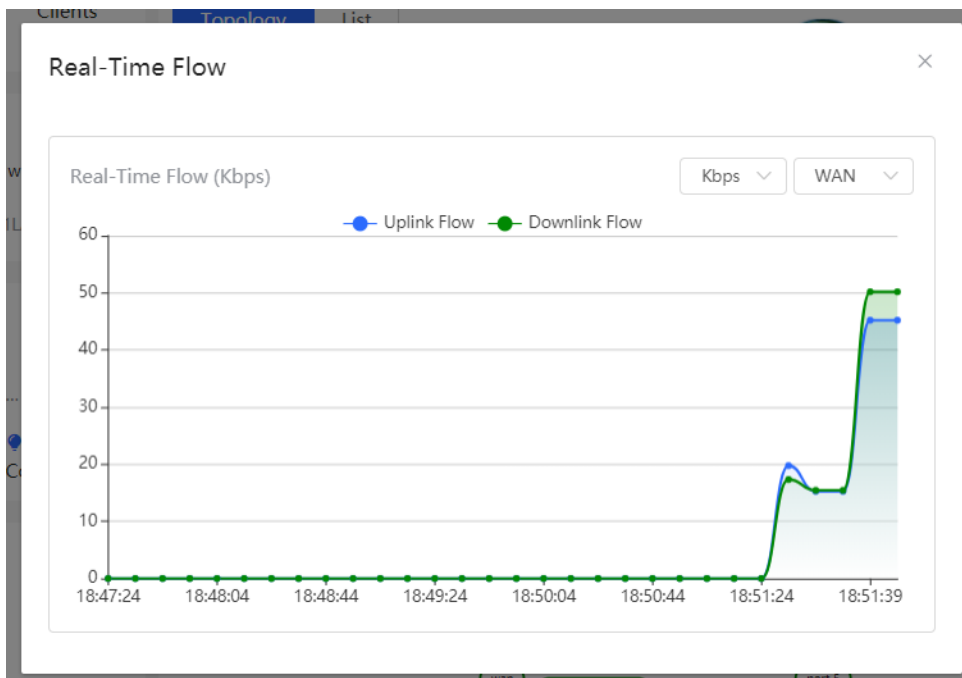



## 2.1 Viewing the Network Information

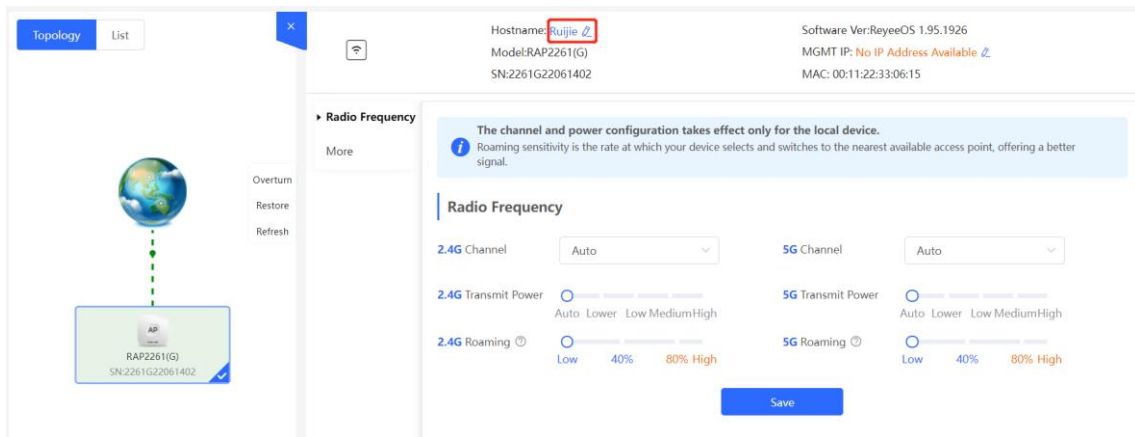
You can view the online device, port ID, device SN as well as the real-time uplink and downlink flow in the network topology.



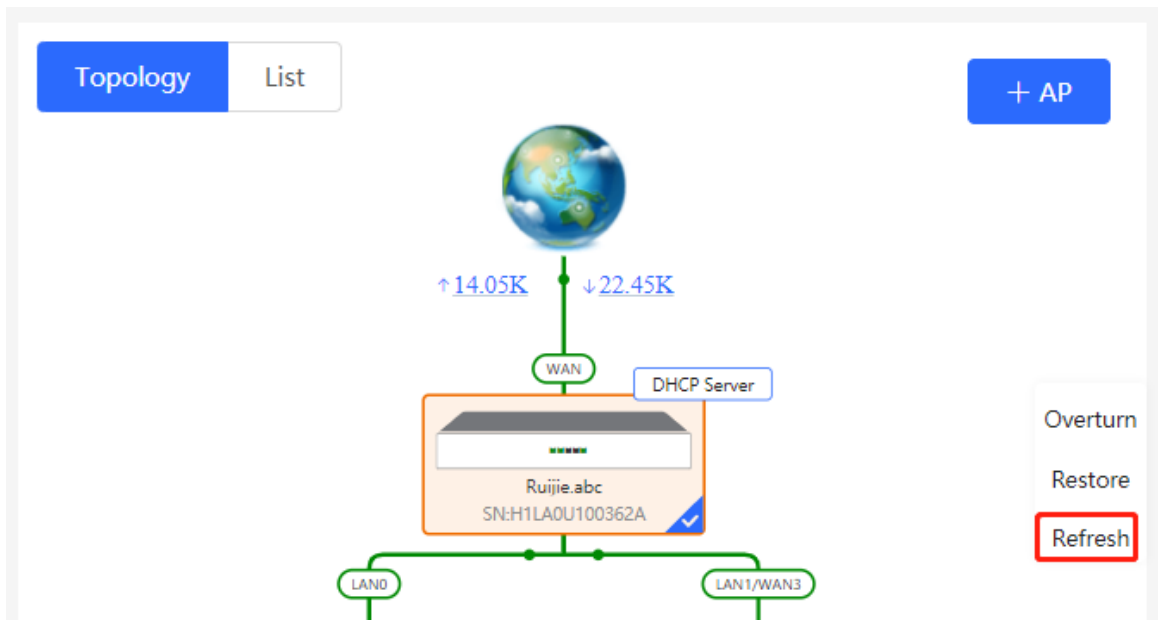
- Click the flow data and view the real-time flow.



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



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

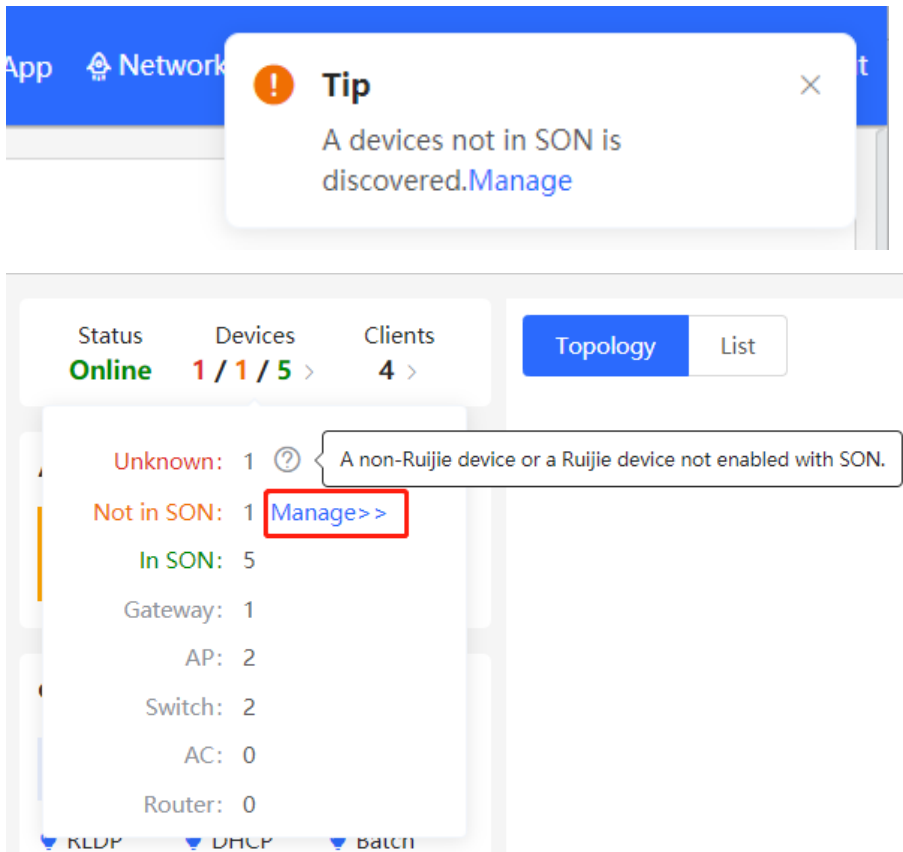


## 2.2 Adding Network Devices

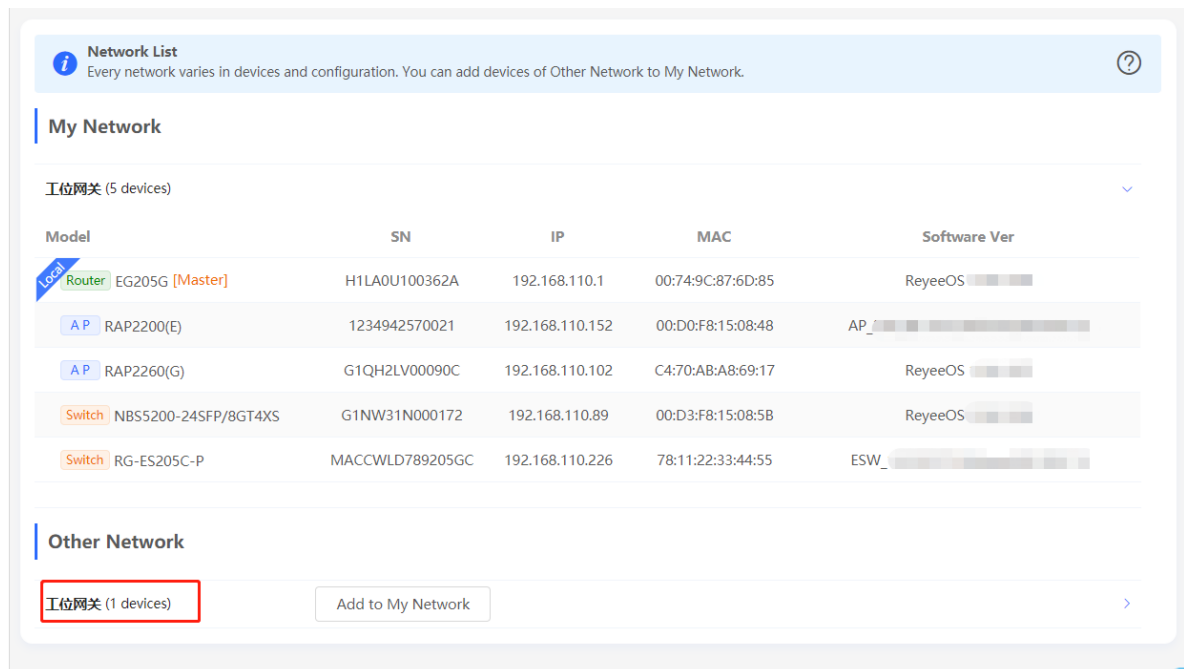
### 2.2.1 Wired Connection

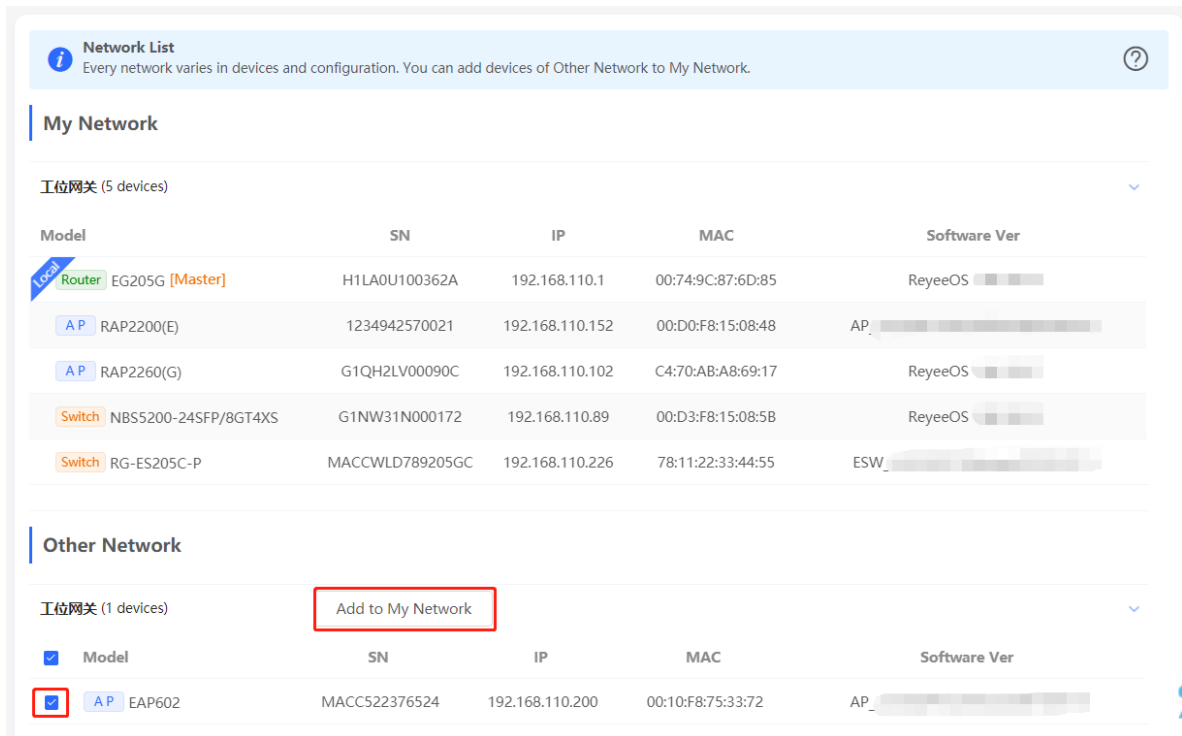
- (1) If a new device is connected to the device in the network through wired connection, a prompt message will pop up, indicating that a device not in SON (Self-Organizing Network) is discovered. The number (in orange) of devices that are not in SON is displayed under the **Devices** at the top left corner of the page. Click **Manage** to add the device to the current network.



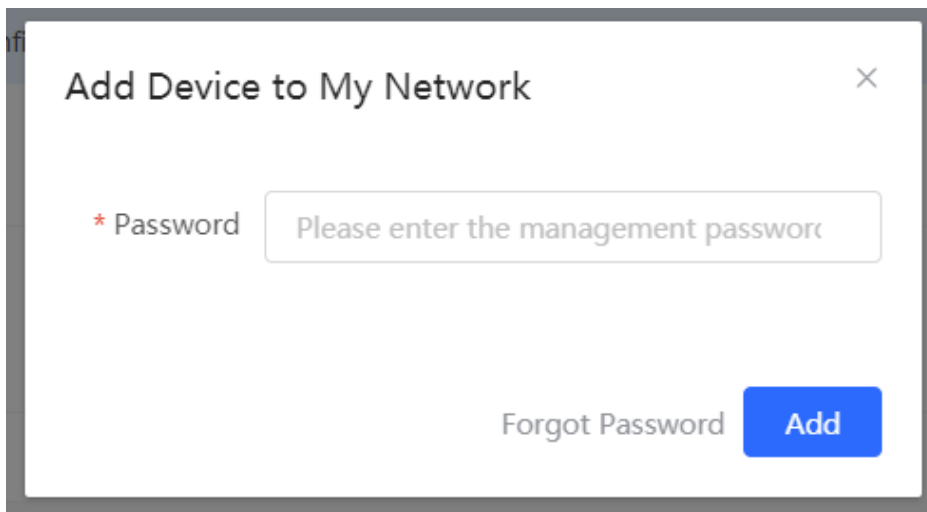


(2) Go to the **Network List** page, click **Other Network** to select the target device and click **Add to My Network**.





If the target device is not configured yet, you can add the device directly without a password. If the device is configured with a password, please enter the management password of the device. If the password is incorrect, the device cannot be added to the network.



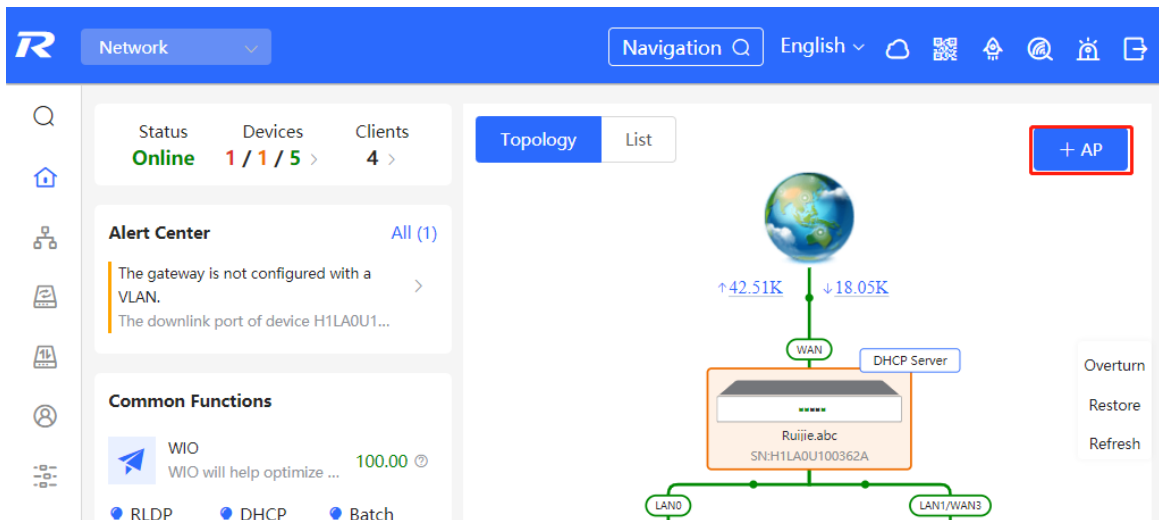
### 2.2.2 AP Mesh

The device supporting the AP Mesh requires no wired connection after power-on. It can be directly added to the current network through Reyee Mesh to perform Mesh networking with other wireless devices, and automatically synchronize the Wi-Fi configuration.

### ⚠ Caution

The device can be discovered only if Reyee Mesh is enabled in the current network (See [3.17 Enabling Reyee Mesh](#) for details). Please place the target AP near the devices already in SON after power-on. If the distance is too far or there are obstacles, the device cannot be discovered.

- (1) Please place the new AP near the devices already in SON after power-on, ensuring that the exiting devices can receive the AP's Wi-Fi signal. Log in to the devices in the self-organizing network, Click **+AP** at the top right corner of the topology on the **Overview** page to discover the target AP that is not added to the current network yet and not connected to an Ethernet cable.



- (2) Select the target AP and add it to the current 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.

## 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.

The screenshot shows the Ruijie RCloud interface. On the left, the 'Devices' menu item is highlighted with a red box. The main area displays a network topology diagram with various devices like switches and APs. A 'List' tab is highlighted with a red box at the top of the main area.

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	rujije	78:11:22:33:44:55	192.168.110.226	ESW_	RG-ES205C-P
<input checked="" type="checkbox"/>	H1LA0U100362A	Online	Rujije.abc [Master]	00:74:9C:87:6D:85	192.168.110.1	ReyeeOS	EG205G
<input type="checkbox"/>	G1NW31N000172	Online	Rujije	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_	RAP2200(E) <span>new</span>
<input type="checkbox"/>	G1QH2LV00090C	Online	Rujije	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.

The screenshot shows the configuration page for a device with SN: 2261G22061402. The 'Radio Frequency' section is expanded, showing settings for 2.4G and 5G channels, transmit power, and roaming. The SN '2261G22061402' is highlighted in the device list on the left.

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

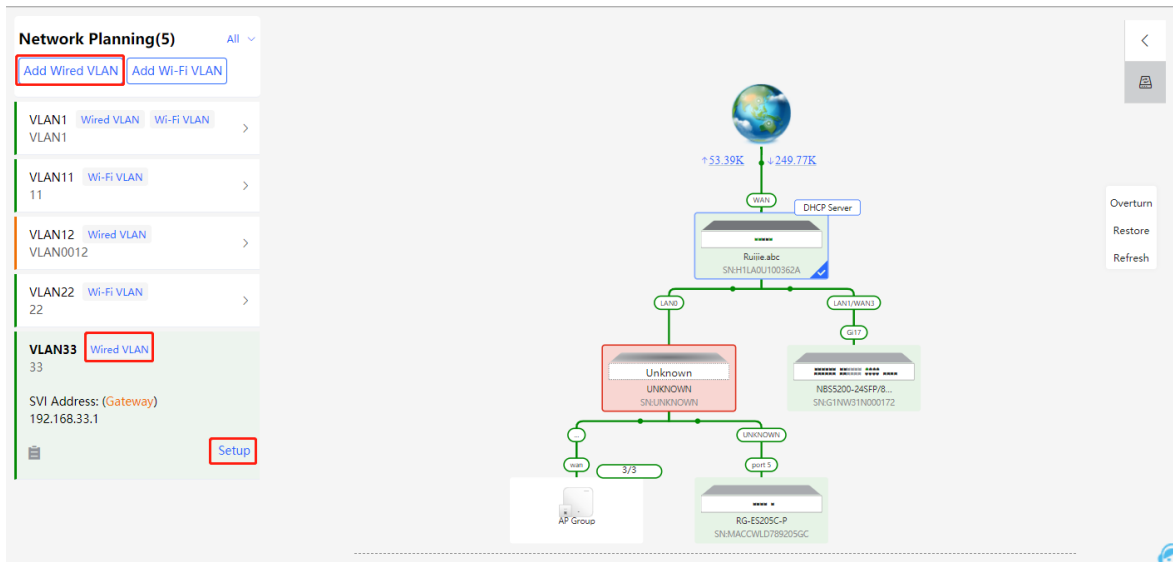
Topology		List	IP/MAC/hostname/SN/S					Delete Offline Devices	Batch Upgrade
SN	Status	Hostname	MAC	IP	Software Ver	Model			
MACCWLD789205GC	Online	rujije	78:11:22:33:44:55	192.168.110.226		RG-ES205C-P			
<span>Local</span> H1LA0U100362A	Online	Rujije.abc [Master]	00:74:9C:87:6D:85	192.168.110.1		EG205G			
G1NW31N000172	Online	Rujije	00:D3:F8:15:08:5B	11.1.1.89		NB55200-245FP/8GT4XS			
<input checked="" type="checkbox"/> G1QH2LV00090C	Offline	Rujije	C4:70:AB:A8:69:17	192.168.110.102		RAP2260(G)			
1234942570021	Online	RAP2200e	00:D0:F8:15:08:48	192.168.110.152		RAP2200(E)			
MACCS22376524	Online	Rujije	00:10:F8:75:33:72	192.168.110.200		EAP602			

## 2.4 Configuring Network Planning

The **Overview** page displays Wi-Fi VLAN and wired VLAN at the bottom left corner. Click **Setup**, and then click **OK** in the displayed dialog box to go to the **Network Planning** page for configurations (**Network > Network Planning**).

### 2.4.1 Configuring Wired VLAN

- (1) Click **Add Wired VLAN** to add the wired VLANs to the current network or select the available wired VLANs. Click **Setup** to edit the wired VLANs.



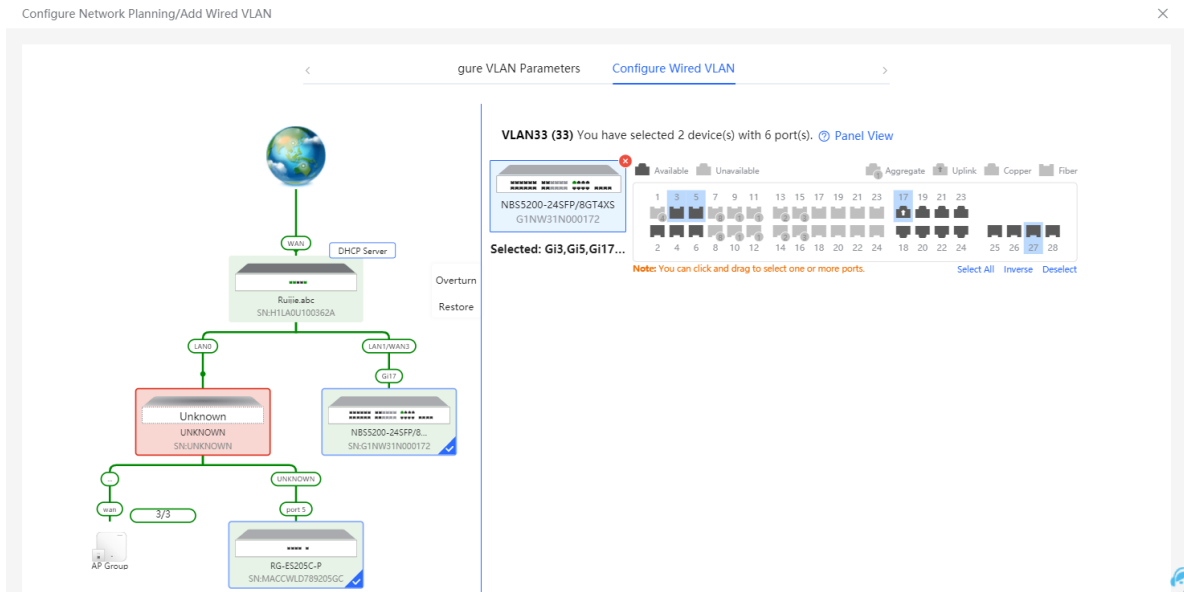
(2) Configure the VLAN ID, address pool server and DHCP pool. The gateway is configured as the address pool server by default to assign IP addresses to clients. If an access switch exists in the network, you can select the access switch as the address pool server. Click **Next** after VLAN parameters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

The image shows a configuration dialog titled 'Configure Network Planning/Add Wired VLAN'. It has three steps: '1 Configure VLAN Parameters', '2 Configure Wired Access', and '3 Confirm Config Delivery'. The '1 Configure VLAN Parameters' step is active. It contains the following fields and options:

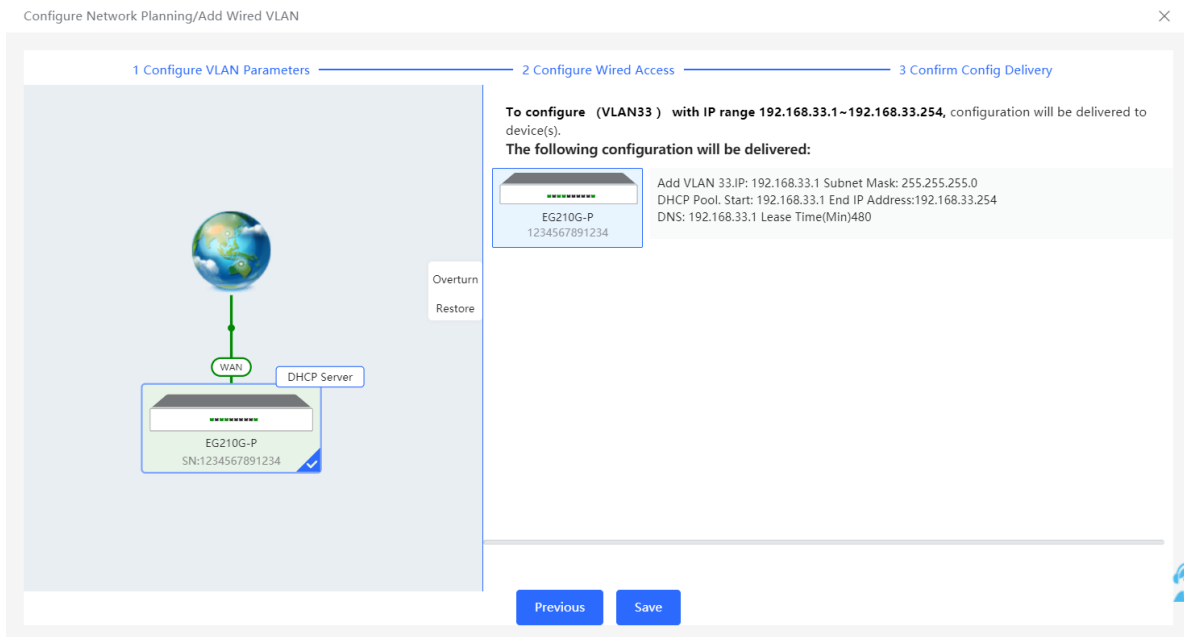
- Description: [Empty text box]
- \* VLAN ID: [33]
- Address Pool:  Gateway
- Server: [Empty text box]
- Gateway/Mask: [192.168.33.1] / [255.255.255.0]
- DHCP Pool:
- IP Range: [192.168.33.1] - [192.168.33.254]

A 'Next' button is located at the bottom center of the dialog.

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

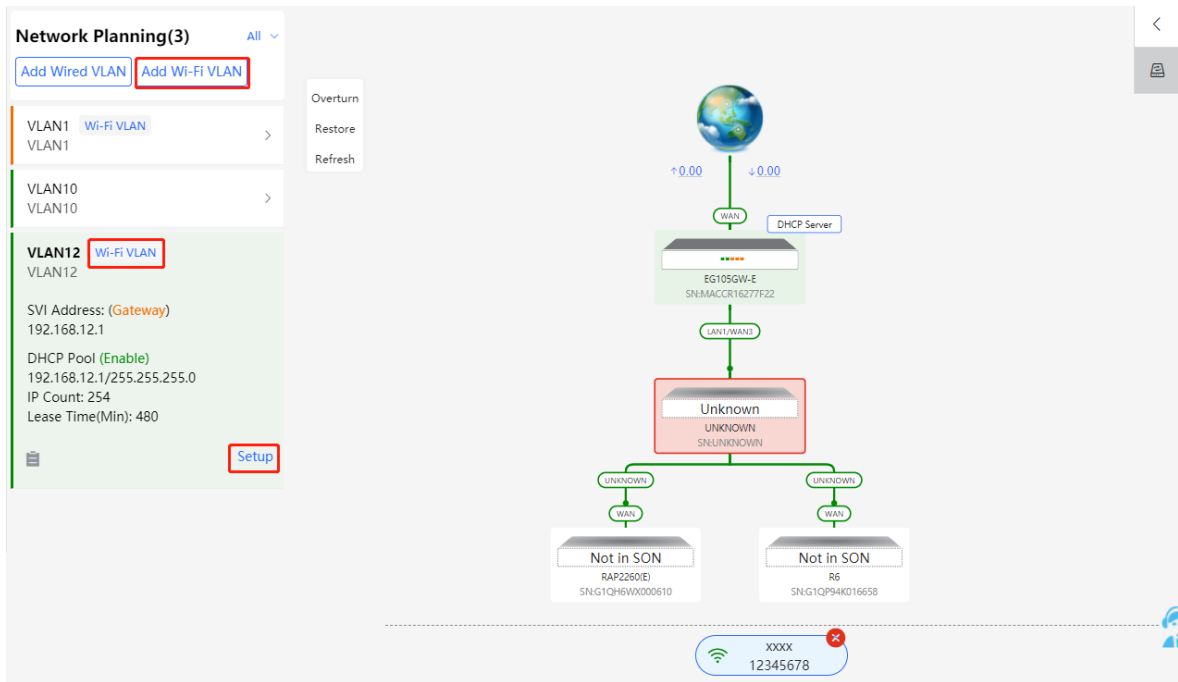


(4) Please confirm the delivered configurations and click **Save**. The configurations will take effect after a few minutes.



### 2.4.2 Configuring Wi-Fi VLAN

(1) Click **Add Wi-Fi VLAN** to add the Wi-Fi VLANs to the current network or select the available Wi-Fi VLANs. Click **Setup** to edit the Wi-Fi VLANs.

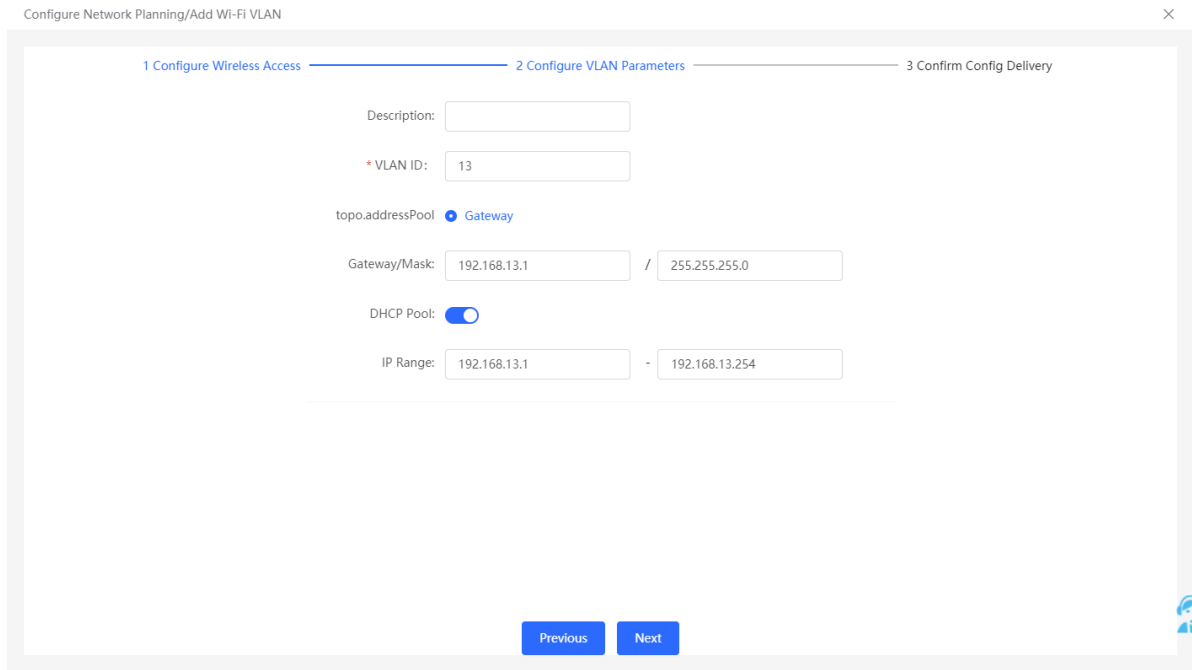


(2) Configure the SSID, Wi-Fi password and band. Then, click **Next**.

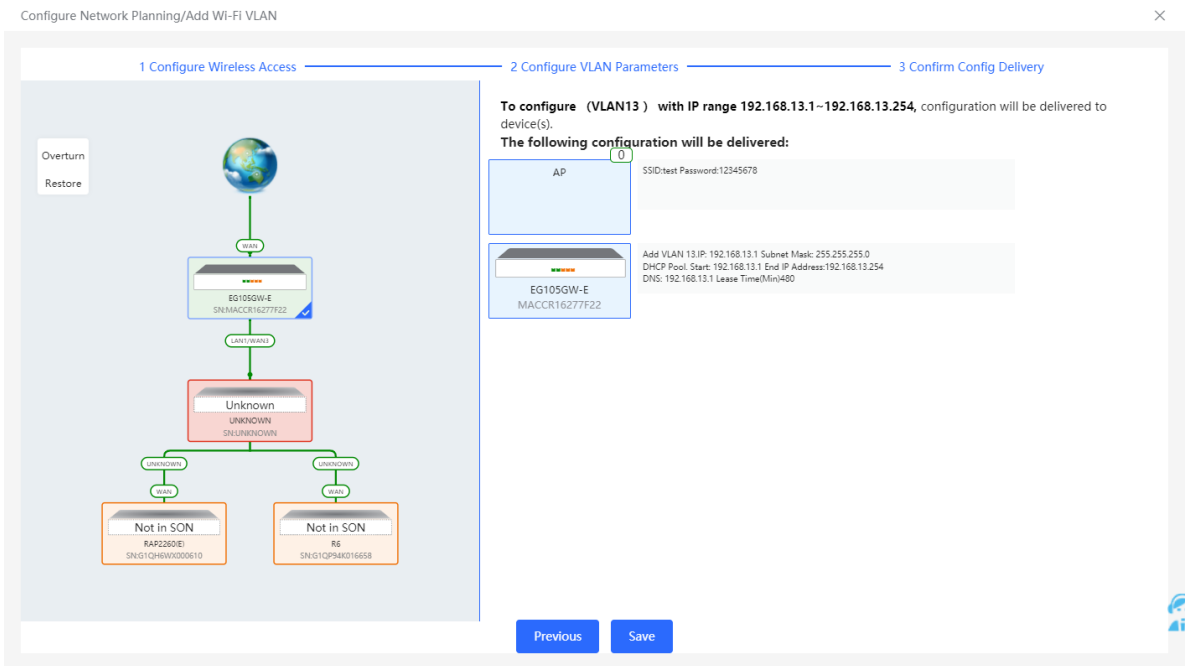
The configuration screen is titled 'Configure Network: Planning/Add Wi-Fi VLAN'. It has three steps: 1. Configure Wireless Access, 2. Configure VLAN Parameters, and 3. Confirm Config Delivery. Under step 1, there is a field for '\* SSID:' which is empty. Below it, 'Security:' has radio buttons for 'Security' and 'Open', with 'Open' selected. 'Band:' has radio buttons for '2.4G + 5G', '2.4G', and '5G', with '2.4G + 5G' selected. A blue 'Next' button is at the bottom center.

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





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



## 2.5 Troubleshooting Fault Alerts

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

The screenshot shows a network monitoring interface with a blue header. On the left, there are navigation icons and a sidebar with sections: Alert Center (highlighted with a red box), Common Functions, and Network Planning. The main area displays a network topology diagram with a central Gateway device (Ruijie abc, SN:H1LA0U100362A) connected to a WAN interface. Below it, there are LAN and LAN1/WAN3 interfaces. The LAN1/WAN3 interface is connected to a Switch (NB55200-24SFP/8...), which is further connected to another Switch (RG-ES205C-P). An AP Group is also shown connected to the LAN interface. A DHCP Server is connected to the WAN interface. The Alert Center on the left shows a message: "The gateway is not configured with a VLAN. The downlink port of device H1LA0U1...".

The screenshot shows the Alerts section of the network monitoring interface. It features a blue header with an information icon and the word "Alerts". Below the header, there is a "Current Alert" section with a red border. The alert message reads: "The downlink port LAN1/WAN3 of device H1LA0U100362A is not allowed to be configured with allowed VLAN 12." Below the alert, there is a "Solution:" section with the text: "Please configure the LAN IP address." Below the solution, there is a detailed network topology diagram showing the Gateway device (Ruijie abc, SN:H1LA0U100362A) connected to a WAN interface. The LAN1/WAN3 interface is connected to a Switch (NB55200-24SFP/8...). The LAN interface is connected to an AP Group (RAP2200b, SN:1234842570021). The Switch (RG-ES205C-P, SN:MACCWLD789205GC) is connected to the LAN1/WAN3 interface. The diagram also shows other devices like "Not in SON" (EAP802, SN:MACCS22376524) and another AP (RAP2260(G), SN:G1QJ2L100090C).

# 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 3.1 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.

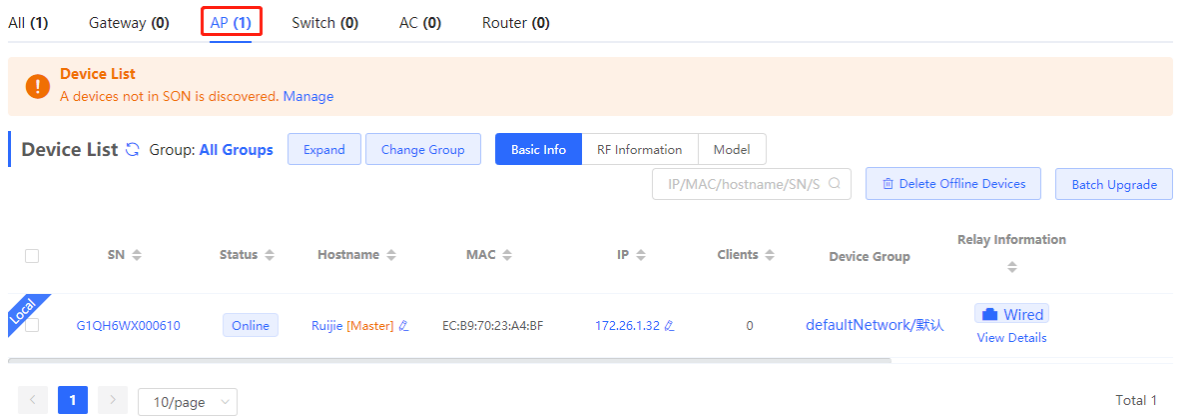
## Note

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



In **Network** mode, choose  **Devices > AP**.

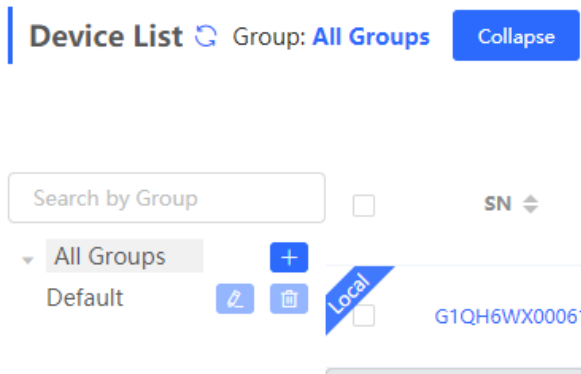
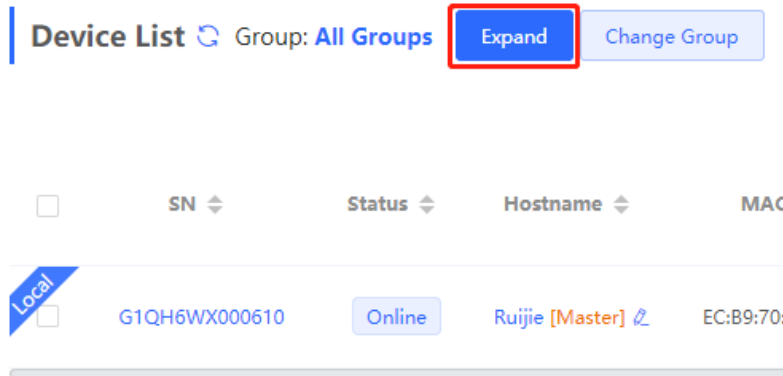
- View the information of all APs in the current network, including the basic information, RF information and models. You can click **SN** to configure the device.



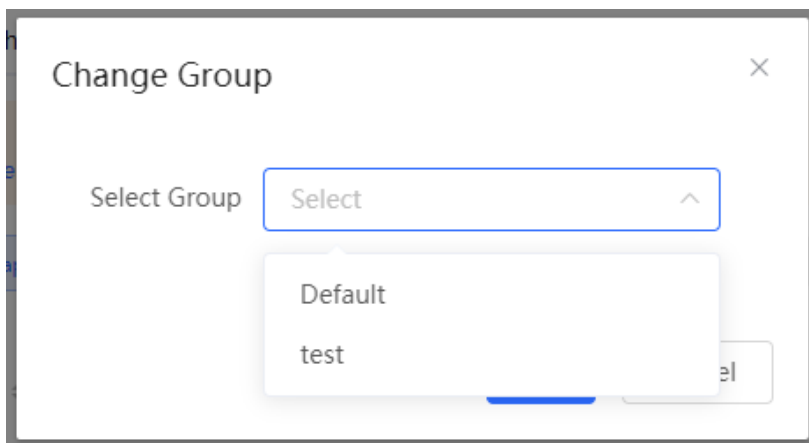
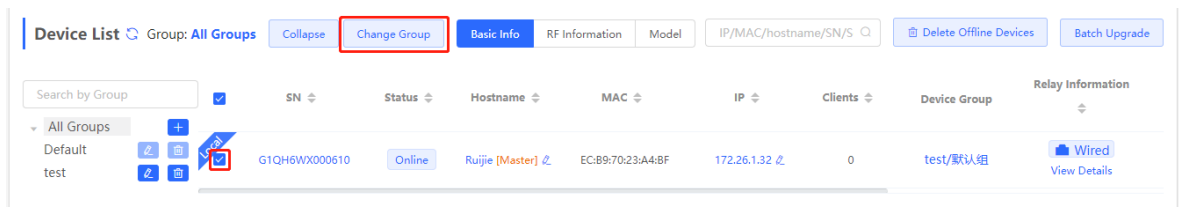
The screenshot shows the 'Device List' page in the web-based configuration interface. At the top, there are tabs for 'All (1)', 'Gateway (0)', 'AP (1)', 'Switch (0)', 'AC (0)', and 'Router (0)'. Below the tabs is a 'Device List' section with a warning message: 'Device List: A devices not in SON is discovered. Manage'. There are buttons for 'Expand', 'Change Group', 'Basic Info', 'RF Information', and 'Model'. A search bar for 'IP/MAC/hostname/SN/S' and buttons for 'Delete Offline Devices' and 'Batch Upgrade' are also present. The main table has columns for 'SN', 'Status', 'Hostname', 'MAC', 'IP', 'Clients', 'Device Group', and 'Relay Information'. One device is listed with SN 'G1QH6WX000610', Status 'Online', Hostname 'Ruijie [Master]', MAC 'EC:B9:70:23:A4:BF', IP '172.26.1.32', and 0 clients. The device group is 'defaultNetwork/默认' and it is 'Wired'. At the bottom, there is a pagination control showing '1' of 10 pages and a 'Total 1' count.

- 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. For created groups, you can click  to edit the group name and click  to delete the group. The default group cannot be deleted and its name cannot be edited.



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



## 3.2 Configuring SSID and Wi-Fi Password

To edit the master Wi-Fi, choose  **Network** (  **WLAN**) > **Wi-Fi** > **Wi-Fi Settings**.


To edit other Wi-Fi, choose  **Network** (  **WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action bar.

Enter the SSID, select the security type (WPA\_WPA2-PSK is recommended), enter the Wi-Fi password, and click **OK**. If the security type is **No Encryption**, the Wi-Fi is an open network and wireless clients can access the Internet without a password. A Wi-Fi password is a string of 8 to 16 characters, which can contain letter, numbers and special characters, such as <=>[!]@#\$.().

### 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](#)   [Guest Wi-Fi](#)   [Wi-Fi List](#)   [Healthy Mode](#)


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

### Wi-Fi Settings

\* SSID

Band

Security

\* Wi-Fi Password  

[Expand](#)

**Save**

## 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

To edit the master Wi-Fi, choose  **Network** (  **WLAN**) > **Wi-Fi** > **Wi-Fi Settings**.

To edit other Wi-Fi, choose  **Network** (  **WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action bar.

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

\* SSID

Band

Security

\* Wi-Fi Password  

----- Collapse -----

Wireless Schedule

VLAN

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

AP Isolation  (The client joining this Wi-Fi network will be isolated.)

### 3.4 Checking Wireless Clients

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**

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.

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

To edit the master Wi-Fi, choose **Network** ( **WLAN** ) > **Wi-Fi** > **Wi-Fi Settings**.

To edit other Wi-Fi, choose  **Network** (  **WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action bar.

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.

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

### Wi-Fi Settings

Device Group:

\* SSID

Band

Security

Expand

Save

## 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.

To edit the master Wi-Fi, choose  **Network** (  **WLAN**) > **Wi-Fi** > **Wi-Fi Settings**.

To edit other Wi-Fi, choose  **Network** (  **WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action bar.

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.



**Wi-Fi Settings** Device Group:

\* SSID

Band

Security

----- Collapse -----

Wireless Schedule

VLAN

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

AP Isolation  (The client joining this Wi-Fi network will be isolated.)

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

XPress  (The client will experience faster speed.)

### 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.

To edit the master Wi-Fi, choose  **Network** (  **WLAN** ) > **Wi-Fi** > **Wi-Fi Settings**.

To edit other Wi-Fi, choose  **Network** (  **WLAN** ) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action bar.

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.)

AP Isolation  (The client joining this Wi-Fi network will be isolated.)

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 his IP address unchanged in this Wi-Fi network.)

Wi-Fi6  (802.11ax High-Speed Wireless Connectivity.) ?

### 3.8 Configuring Layer-3 Roaming

To edit the master Wi-Fi, choose  **Network** (  **WLAN**) > **Wi-Fi** > **Wi-Fi Settings**

To edit other Wi-Fi, choose  **Network** (  **WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action bar.

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.)

AP Isolation  (The client joining this Wi-Fi network will be isolated.)

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 his IP address unchanged in this Wi-Fi network.)

Wi-Fi6  (802.11ax High-Speed Wireless Connectivity.) ⓘ

### 3.9 Configuring AP Isolation

To edit the master Wi-Fi, choose  **Network** (  **WLAN** ) > **Wi-Fi** > **Wi-Fi Settings**

To edit other Wi-Fi, choose  **Network** (  **WLAN** ) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action bar.

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.

**Wi-Fi Settings** Device Group: Default

\* SSID

Band 2.4G + 5G

Security Open

---

[Collapse](#)

Wireless Schedule All Time

VLAN Default VLAN

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

AP Isolation  (The client joining this Wi-Fi network will be isolated.)



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

### 3.10 Adding a Wi-Fi Network

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

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.

Wi-Fi Settings   Guest Wi-Fi   Wi-Fi List   Healthy Mode

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

**Wi-Fi List** Device Group: Default  + Add

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
test	2.4G + 5G	OPEN	No	Default VLAN	<a href="#">Edit</a> <a href="#">Delete</a>

Add×

\* SSID

Band

Security

---

[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** > **Guest Wi-Fi**.

Turn on **Guest Wi-Fi** and enter the SSID and Wi-Fi password. 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   **Guest Wi-Fi**   Wi-Fi List   Healthy Mode

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


**Guest Wi-Fi** Device Group:

Enable

\* SSID

Band

Security

\* Wi-Fi Password  

----- Expand -----

## 3.12 Configuring Wi-Fi Blacklist or Whitelist

### 3.12.1 Overview

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

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

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

#### Caution

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

### 3.12.2 Configuration Steps

#### 1. Configuring a Global Blacklist/Whitelist

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

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

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.

+ Add
Delete Selected

**Blocked WLAN Clients**

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

	MAC	Remark	Action
<input type="checkbox"/>	00:E0:4C:36:0B:EA	forbidden	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	00:11:22 <span style="background-color: #d4edda; padding: 2px 5px; font-size: 0.8em;">OUI</span>		<a href="#">Edit</a> <a href="#">Delete</a>

Add



Match Type  Full  Prefix (OUI)

\* MAC

Remark

## 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.

	MAC	Remark	Action
No Data			

### 3.13 Optimizing Wi-Fi Network

#### 3.13.1 Overview

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

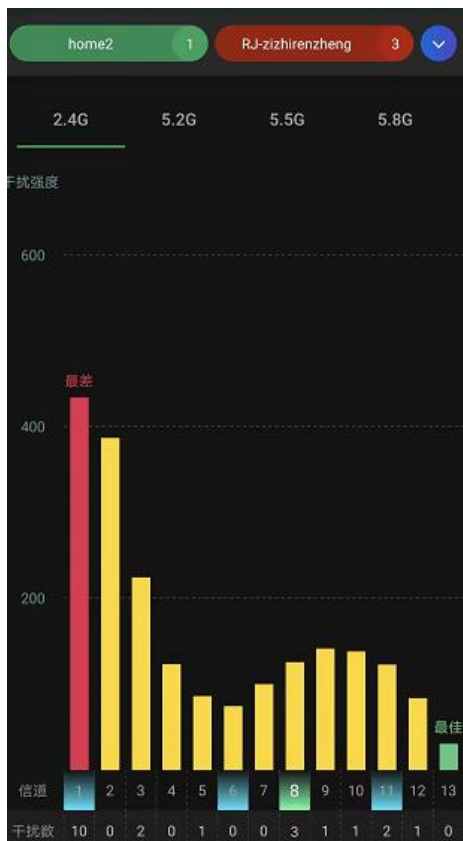
 **Caution**

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

#### 3.13.2 Getting Started

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





### 3.13.3 Optimizing the Radio Channel

- 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**.

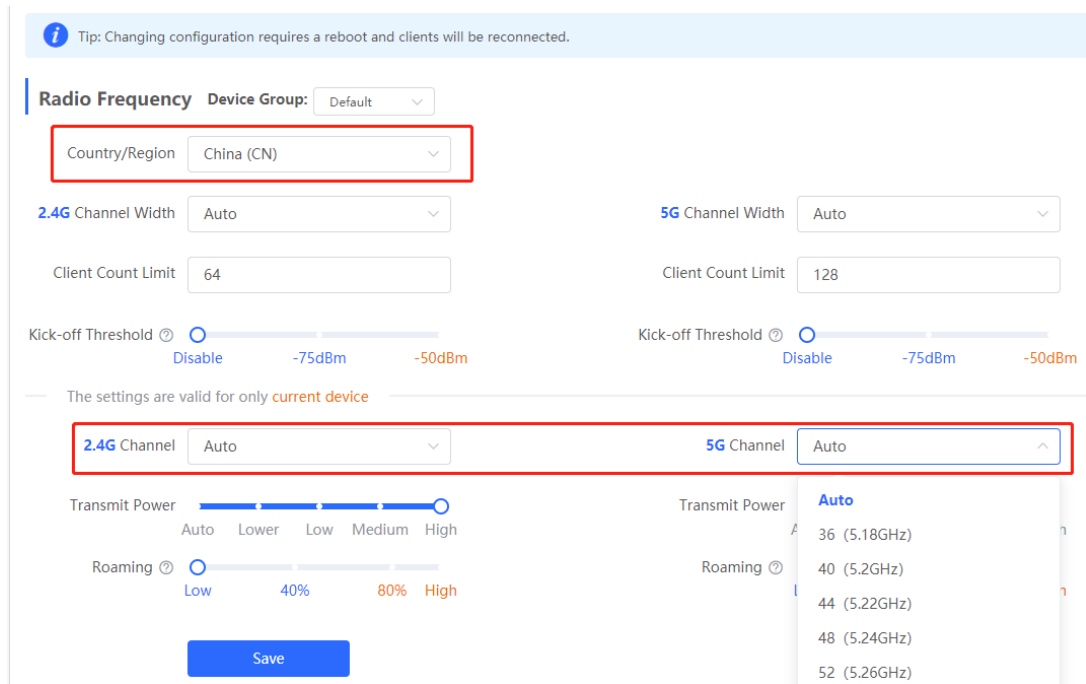
Choose the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. The more devices in a channel, the greater the interference.

---

**Note**

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

---



### 3.13.4 Optimizing the Channel Width

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

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

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

**Caution**

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

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

**Radio Frequency** Device Group: Default

Country/Region: China (CN)

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



Client Count Limit: 64 Client Count Limit: Auto

Kick-off Threshold Disable -75dBm -50dBm Kick-off Threshold Di 80MHz 160MHz

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

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

### 3.13.5 Optimizing the Transmit Power

- 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**

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.

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

**Radio Frequency** Device Group: Default

Country/Region: China (CN)

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

Client Count Limit: 64 Client Count Limit: 128

Kick-off Threshold Disable -75dBm -50dBm Kick-off Threshold Disable -75dBm -50dBm

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

**Roaming** Low 40% 80% High **Roaming** Low 40% 80% High


**Save**

### 3.13.6 Configuring the Kick-off Threshold

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

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

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

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

**Radio Frequency** Device Group: Default

Country/Region China (CN)

2.4G Channel Width Auto  5G Channel Width Auto

Client Count Limit 64  Client Count Limit 512

When the client's RSSI is lower than the threshold, it will be kicked off.

Kick-off Threshold  Disable -75dBm -50dBm Kick-off Threshold  Disable -75dBm -50dBm

The settings are valid for only current device

2.4G Channel Auto  5G Channel Auto

 **Caution**

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

### 3.13.7 Configuring the Client Limit

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

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

### Radio Frequency

Country/Region	<input type="text" value="China (CN)"/>		
<b>2.4G</b> Channel Width	<input type="text" value="Auto"/>	<b>5G</b> Channel Width	<input type="text" value="Auto"/>
Client Count Limit	<input type="text" value="32"/>	Client Count Limit	<input type="text" value="32"/>
Kick-off Threshold	<input type="text" value="Disable"/> <input type="text" value="-75dBm"/> <input type="text" value="-50dBm"/>	Kick-off Threshold	<input type="text" value="Disable"/> <input type="text" value="-75dBm"/> <input type="text" value="-50dBm"/>
<b>2.4G</b> Channel	<input type="text" value="Auto"/>	<b>5G</b> Channel	<input type="text" value="Auto"/>
Transmit Power	<input type="text" value="Auto"/> <input type="text" value="Lower"/> <input type="text" value="Low"/> <input type="text" value="Medium"/> <input type="text" value="High"/>	Transmit Power	<input type="text" value="Auto"/> <input type="text" value="Lower"/> <input type="text" value="Low"/> <input type="text" value="Medium"/> <input type="text" value="High"/>
Roaming Sensitivity	<input type="text" value="Low"/> <input type="text" value="20%"/> <input type="text" value="40%"/> <input type="text" value="60%"/> <input type="text" value="80%"/> <input type="text" value="High"/>	Roaming Sensitivity	<input type="text" value="Low"/> <input type="text" value="20%"/> <input type="text" value="40%"/> <input type="text" value="60%"/> <input type="text" value="80%"/> <input type="text" value="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.

### 3.13.8 Configuring the Roaming Sensitivity

- 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**.

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.

**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

Client Count Limit: 64  Client Count Limit: 128

Kick-off Threshold  Disable -75dBm -50dBm Kick-off Threshold  Disable -75dBm -50dBm

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

Roaming  Low 40% 80% High Roaming  Low 40% 80% High

**Save**

### 3.13.9 Configuring WIO

In **Network** mode, choose  **Network >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

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.

Notes:  
1. During network optimization, the APs will switch channels, forcing the clients to go offline. The process will last for a while, subject to the quantity of devices. It is recommended you enable network optimization at night.  
2. If dynamic channel allocation is running in the backend, network optimization will fail. Please try again later.  
3. The configuration cannot be rolled back once optimization starts.

I have read the notes.

**Network Optimization**

### Scheduled Optimization

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

Enable

Day

Time  :

**Save**


## 3.14 Configuring Healthy Mode

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

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.

Wi-Fi Settings   Guest Wi-Fi   Wi-Fi List   Healthy Mode

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

## Healthy Mode

Enable

Wireless Schedule

Save

### 3.15 Configuring Xpress

To edit the master Wi-Fi, choose  **Network** (  **WLAN**) > **Wi-Fi** > **Wi-Fi Settings**.

To edit other Wi-Fi, choose  **Network** (  **WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action bar.

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.



## Wi-Fi Settings

\* SSID

Band

Security

[Collapse](#)

Wireless Schedule

VLAN

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

AP Isolation  (The client joining this Wi-Fi network will be isolated.)

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 his IP address unchanged in this Wi-Fi network.)

## 3.16 Configuring Wireless Schedule

To edit the master Wi-Fi, choose  **Network** (  **WLAN**) > **Wi-Fi** > **Wi-Fi Settings**.

To edit other Wi-Fi, choose  **Network** (  **WLAN**) > **Wi-Fi** > **Wi-Fi List**. Select the target Wi-Fi in the list and click **Edit** in the action bar.

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.

### Wi-Fi Settings

\* SSID

Band

Security


[Collapse](#)

Wireless Schedule


VLAN

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

## 3.17 Enabling Reye Mesh

In **Network** mode, choose  **Network > 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 Reye Mesh, you can set up a Mesh network through Mesh pairing between the devices that support Reye Mesh.

Enable

# 4 Network Settings

## 4.1 Switching Work Mode

### 4.1.1 Work Mode

See [1.3](#) Work Mode for details.

### 4.1.2 Self-Organizing Network Discovery

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

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

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


### 4.1.3 Configuration Steps

---

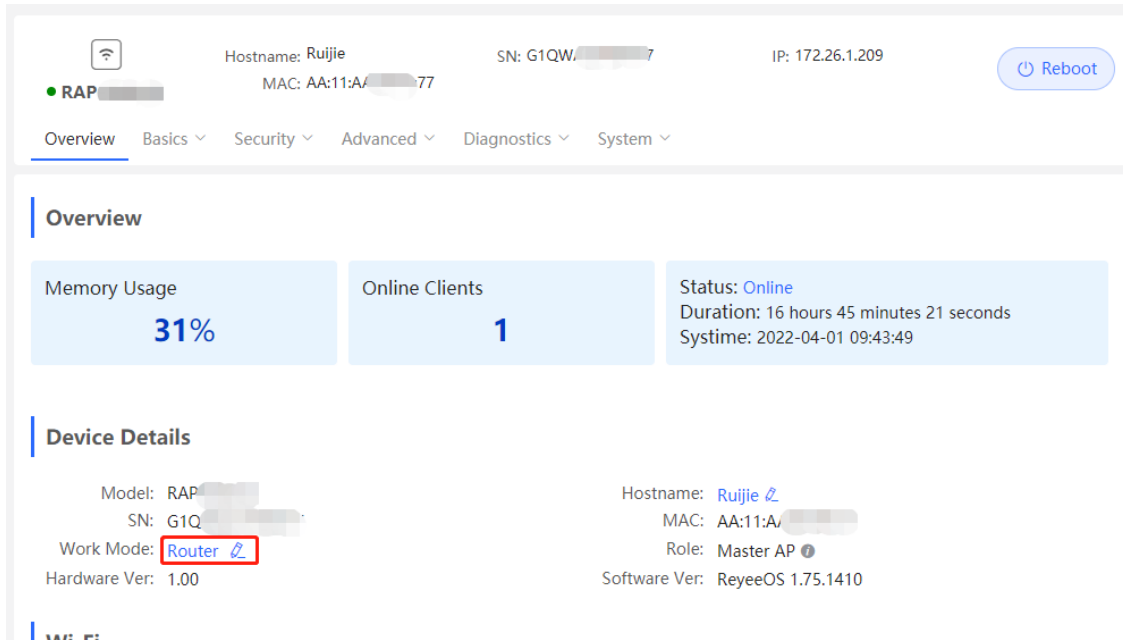
#### Note

If you need to switch the work mode to wireless repeater mode, please see [4.4.2](#) Wireless Repeater for details.

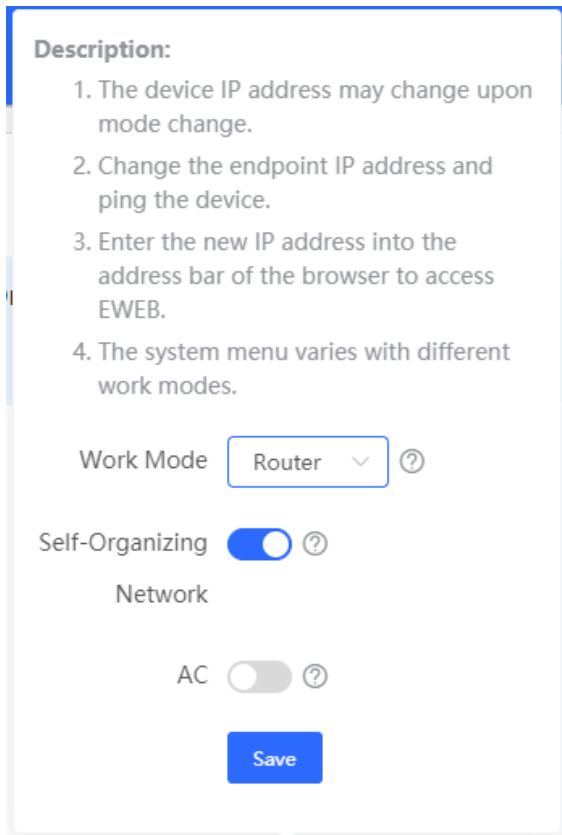
---

In **Local Device** mode, choose  **Overview > Device Details**.

Click the current work mode to change the work mode.




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



**⚠ Caution**

- After the self-organizing network discovery is enabled, you can check the role of the device in self-organizing network mode. For details, see 4.1.4 Viewing Device Role.
- After switching to the router mode, the device's LAN IP address will change to 192.168.120.1 and enable DHCP service. 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 and configure the router mode again.

## 4.1.4 Viewing Device Role

In **Local Device** mode, choose  **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.

### 设备详细信息

设备型号: RAP	设备名称: <a href="#">Ruijie</a>
SN号: G1QH6WX000610	MAC地址: EC:B9:70:23:A4:BF
工作模式: <a href="#">AP模式</a>	自组网角色: <b>从AP</b> (主AC: 172.26.1.244)
硬件版本: 1.00	软件版本: ReyeeOS 1.86

## 4.2 Configuring Internet Type

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

- If the device works in the router mode, select the Internet connection type after confirming with the ISP. For detailed configuration, see [1.4 Configuration Wizard \(Router Mode\)](#).
- If the device works in the AP mode, select the Internet connection type (**DHCP** or **Static IP**) without confirming with the ISP. For detailed configuration, see [1.5 Configuration Wizard \(AP Mode\)](#).

**Configure WAN settings.**

\* Internet

No username or password is required for DHCP clients.

IP 192.168.110.240

Subnet Mask 255.255.255.0

Gateway 192.168.110.1

DNS Server 192.168.110.1

[Advanced Settings](#)

### 4.3 Configuring LAN Port

 **Caution**

This function is supported only when the device works in router mode.

In **Local Device** mode, choose  **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 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

Cancel OK

## 4.4 Configuring Repeater Mode

### 4.4.1 Wired Repeater

In **Local Device** mode, choose **Network > Work 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 **Access Point** mode.

Router
  **Access Point**
 Wireless Repeater

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.  
 Note: If you repeat the Wi-Fi signal of a Ruijie device, the local router Wi-Fi settings may be overridden.

**Access Point**

Check


## 4.4.2 Wireless Repeater

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

---

### Note


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

In **Local Device** mode, choose  **Network > Work 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**

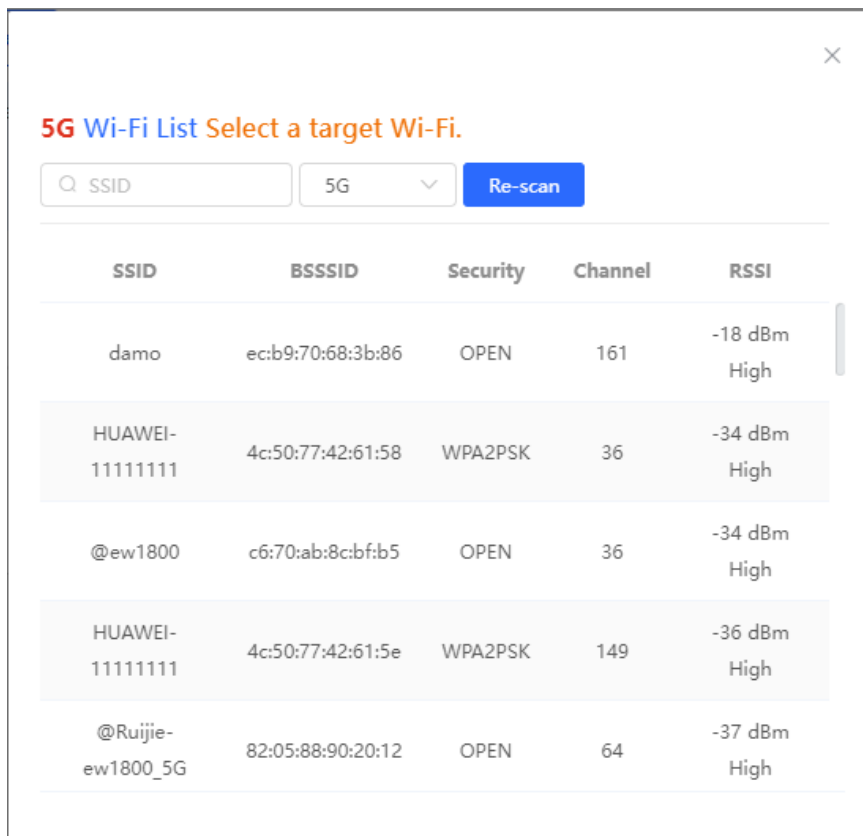
-  • This mode allows you to establish a wireless connection between the primary device and the local device that works as the secondary device, extending network coverage.  
• You are advised to select a 5G Wi-Fi of the primary device for better Internet experience.

### 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

- (2) Select the Wi-Fi signal of the upper-layer device that you want to extend. The configuration items of the local device are displayed. If the signal of the upper-layer device is encrypted, enter the Wi-Fi password of the upper-layer device.
- (3) Configure **Local Router Wi-Fi**. You can select **New Wi-Fi** or **Same as Primary Router Wi-Fi**.
  - 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.

**Primary Device**

\* SSID @ew1800 Select

---

**Local Device**

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

\* SSID(2.4G) @ew1800\_plus

\* SSID(5G) @ew1800\_plus\_5G

Wi-Fi Password A blank value indicates no encryption.

Save

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

## 4.5 Creating a VLAN

- Caution**
- This function is supported only when the device works in router mode.

In **Local Device** mode, choose  **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	<a href="#">Edit</a> <a href="#">Delete</a>

×

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.
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 4.9 Configuring DHCP Server.


 **Caution**

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

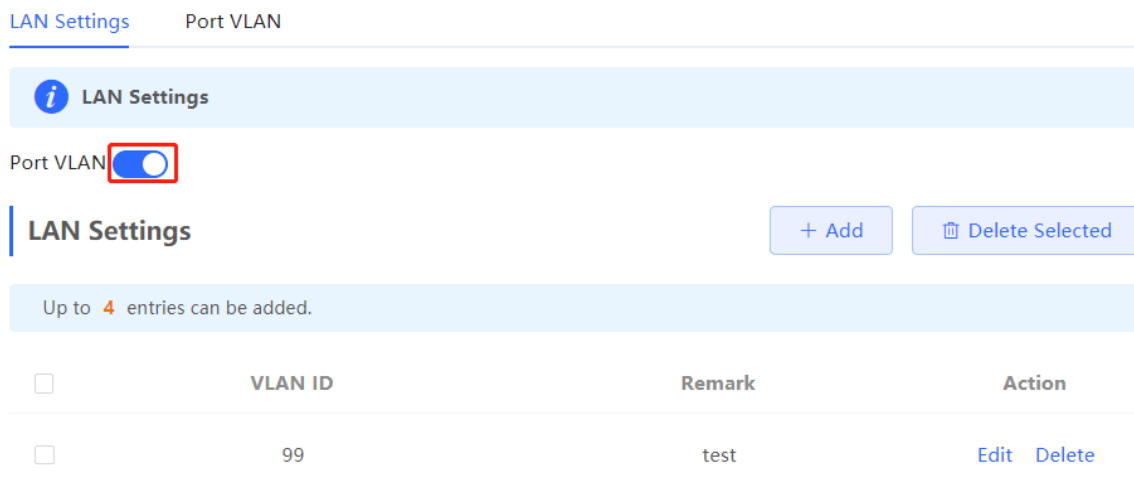
## 4.6 Configuring Port VLAN

### Caution

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

In **Local Device** mode, choose  **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

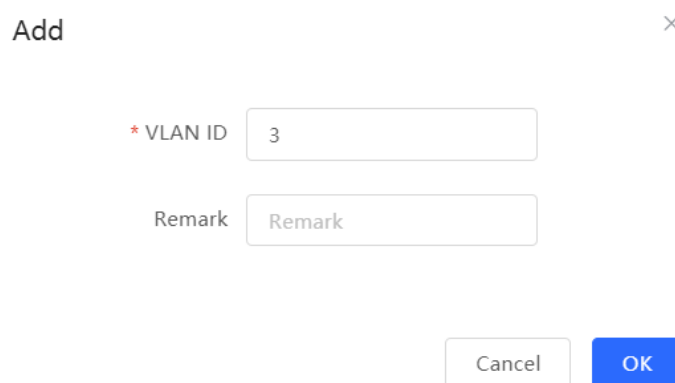
Port VLAN

LAN Settings + Add Delete Selected

Up to 4 entries can be added.

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

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



Add ×

\* VLAN ID

Remark

Cancel OK

- (3) Switch to the **Port VLAN** tab page and configure VLANs for the port. Click the option box below the port, select the mapping between a VLAN and the port from the drop-down list box, and click **Save**.
- **UNTAG**: Configure the VLAN as the native VLAN of the port. That is, when receiving a packet from this VLAN, the port removes the VLAN tag from the packet and forwards the packet. When receiving an untagged packet, the port adds the VLAN tag to the packet and forwards the packet through the VLAN. Only one VLAN can be configured as an untagged VLAN on each port.

- o **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.
- o **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 Join ▾

## 4.7 Changing MAC Address

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

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

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

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

---

**Caution**

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

---

**Configure WAN settings.**

\* Internet

No username or password is required for DHCP clients.

IP 192.168.110.240

Subnet Mask 255.255.255.0

Gateway 192.168.110.1

DNS Server 192.168.110.1

---


[Advanced Settings](#)

VLAN ID

\* MTU

\* MAC

## 4.8 Changing MTU

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

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

---

[Advanced Settings](#)

VLAN ID

\* MTU

\* MAC

## 4.9 Configuring DHCP Server

---

### Caution

This function is supported only when the device works in router mode.

---

### 4.9.1 DHCP Server

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

### 4.9.2 Configuring the DHCP Server Function

In **Local Device** mode, choose  **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)

### 4.9.3 Displaying Online DHCP Clients

In **Local Device** mode, choose  **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

 View DHCP clients. 

**DHCP Clients**

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-97	192.168.120.172	42:11:26:...	23	<a href="#">Convert to Static IP</a>
<input type="checkbox"/>	2	no-7d2c-12	192.168.120.35	72:26:e8:...	13	<a href="#">Convert to Static IP</a>
<input type="checkbox"/>	3	R12	192.168.120.236	00:e0:4:...	19	<a href="#">Convert to Static IP</a>





### 4.9.4 Displaying the DHCP Static IP Address List

In **Local Device** mode, choose  **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

---

 Static IP Address List 

---

**Static IP Address List**

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	<a href="#">Edit</a> <a href="#">Delete</a>


### 4.10 Link Aggregation

 **Caution**

The function is only supported by the 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




LAN2




LAN1



## 4.11 Configuring DNS

In **Local Device** mode, choose  **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**

## 4.12 Hardware Acceleration

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**

## 4.13 Configuring Port Flow Control

In **Local Device** mode, choose  **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**

## 4.14 Configuring ARP Binding

### Caution



This function is supported only when the device works in router 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.

In **Local Device** mode, choose  **Security > ARP List**.

ARP mappings can be bound in two ways:

- 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.

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

ARP List

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

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

- 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)

## 4.15 Configuring LAN Ports

---

 **Caution**


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

---

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

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


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

**LAN Port Settings**  
 The configuration takes effect only for the AP with a LAN port, e.g., EAP101.  
**Note:** The configured LAN port settings prevail. **The AP device with no LAN port settings will be enabled with default settings.**

**Default Settings**

VLAN ID  [Add VLAN](#)

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

Applied to AP device with no LAN port settings 

[Save](#)

**LAN Port Settings**

[+ Add](#)

[Delete Selected](#)

Up to 8 VLAN IDs or 32 APs can be added (1 APs have been added).


<input type="checkbox"/>	VLAN ID ↕	Applied to	Action
<input type="checkbox"/>	5	<a href="#">Ruijie</a>	<a href="#">Edit</a> <a href="#">Delete</a>

# 5 System Settings

## 5.1 PoE Settings


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.

 **PoE Settings**

Power Mode


Current Mode IEEE 802.3bt


Energy Saving  

Band  2.4G  5G  2.4G+5G

Current Power 51W

## 5.2 Setting the Login Password

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**.

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.

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

\* Old Password

\* New Password


\* Confirm Password

Save

### 5.3 Setting the Session Timeout Duration

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.**


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.


**i** Session Timeout

\* Session Timeout  seconds

Save

### 5.4 Setting and Displaying System Time


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**.

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 as required.

### **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 Edit

\* Time Zone  ▼

\* NTP Server

0.cn.pool.ntp.org	Add
1.cn.pool.ntp.org	Delete
cn.pool.ntp.org	Delete
pool.ntp.org	Delete
asia.pool.ntp.org	Delete
europe.pool.ntp.org	Delete
ntp1.aliyun.com	Delete

Save


## 5.5 Configuring Reboot

### **Caution**

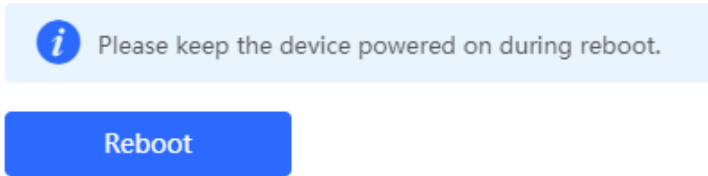
- Do not cut off power during system reboot to avoid device damage.
- Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the Web service becomes available, the device automatically jumps to the login page.
- Rebooting the device affects the network.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



### 5.5.1 Rebooting the Current Device

In **Local Device** mode, choose  **System > Reboot > Reboot**.

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

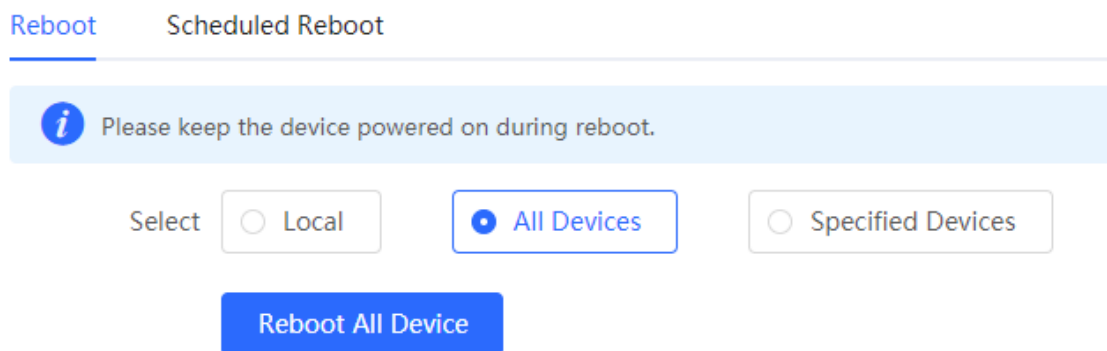


### 5.5.2 Rebooting All Devices in the Network

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

In **Network** mode, choose  **System > Reboot > Reboot**.

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



#### Caution

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

### 5.5.3 Rebooting the Specified Device

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

In **Network** mode, choose  **System > Reboot > 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

## 5.6 Configuring Scheduled Reboot

### 5.6.1 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 5.4 Setting and Displaying System Time.


Choose  **System > Reboot > 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 03 : 00

Save

## 5.7 Configuring Backup and Import



Choose  **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

**Import Profile**

File Path

## 5.8 Restoring Factory Settings


### 5.8.1 Restoring the Current Device to Factory Settings

In **Local Device** mode, choose  **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.

#### **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 5.7 [Configuring Backup and Import](#)). Therefore, exercise caution when performing this operation.

### 5.8.2 Restoring All Devices to Factory Settings


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

In **Network** mode, choose **System > Management > Reset**.

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.

---


## 5.9 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.
- 

### 5.9.1 Online Upgrade

In **Local Device** mode, choose  **System > Upgrade > Online Upgrade**.

You can view the current system version. If there is a new version available, you can click **Upgrade Now** for an update. If your device cannot access the Internet, click **Download File** and choose **Local Upgrade** to upload the file for local upgrade.

Online Upgrade

Local Upgrade

**i** 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

### 5.9.2 Local Upgrade

In **Local Device** mode, choose  **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

**i** Please do not refresh the page or close the browser.

Model RAP

Current Version ReyeeOS 1.86.

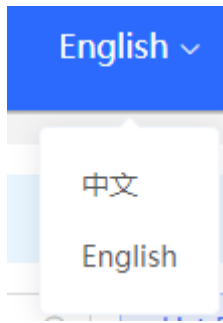
Keep Config  (If the target version is much later than the current version, it is recommended not to keep the configuration.)

File Path

### 5.10 Switching System Language

Choose **English** in the upper right corner of the Web page.

Click a required language to switch the system language.



## 5.11 Configuring LED Status Control

### Caution

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

Choose  **Network > 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

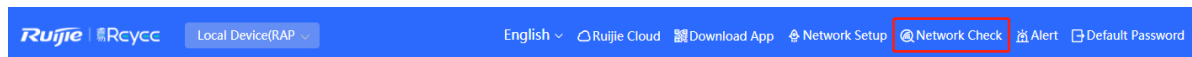
Save

# 6 Network Diagnosis Tools

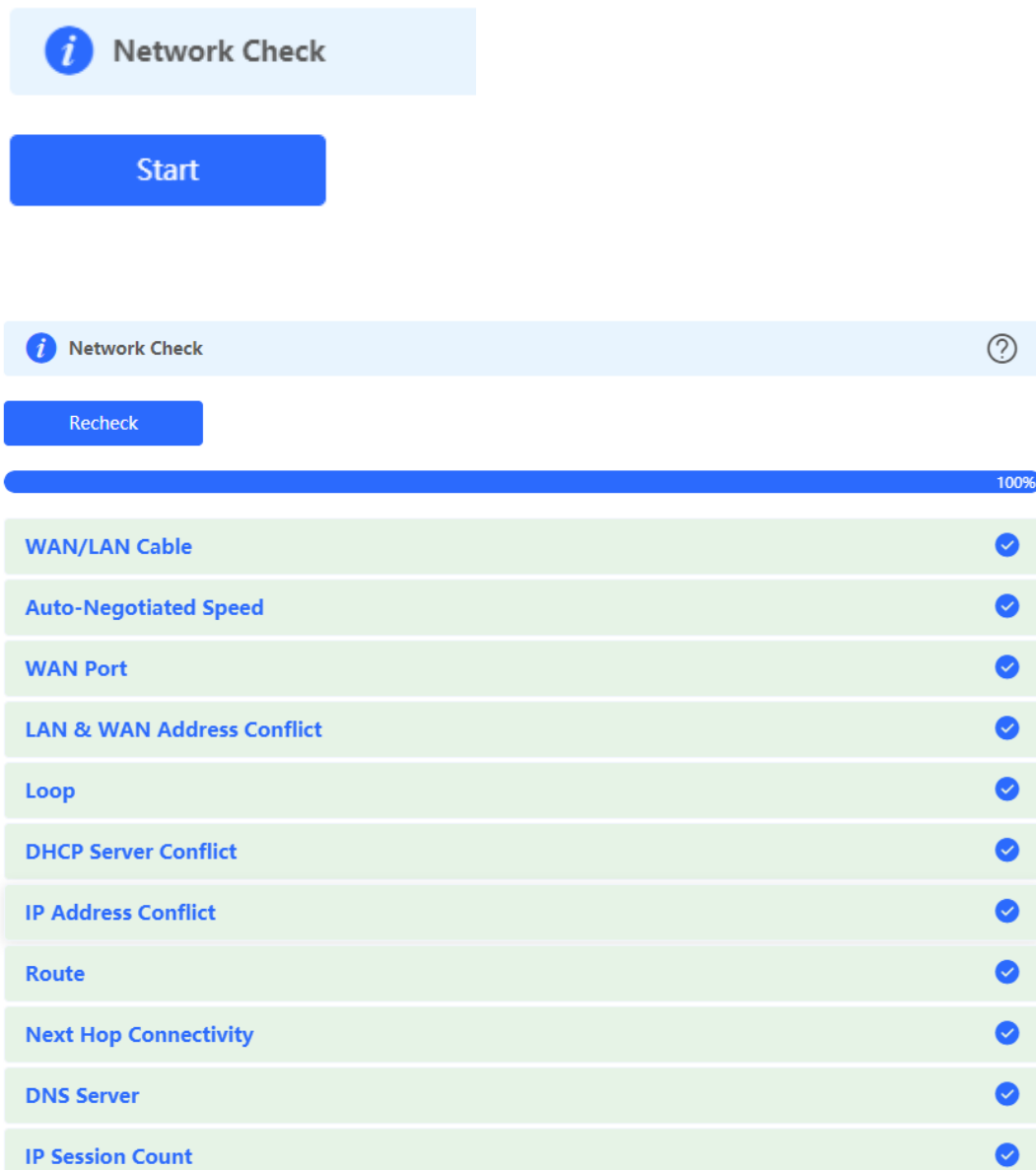
## 6.1 Network Check

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.



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



The screenshot 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. Underneath is a '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

In **Local Device** mode, choose  **Diagnostics > Network Tools**.

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

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

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

**Network Tools**

Tool  Ping  Traceroute  DNS Lookup

\* IP Address/Domain

\* Ping Count


\* Packet Size  Bytes

```

PING 172.26.1.1 (172.26.1.1): 64 data bytes
72 bytes from 172.26.1.1: seq=0 ttl=64 time=2.155 ms
72 bytes from 172.26.1.1: seq=1 ttl=64 time=2.141 ms
72 bytes from 172.26.1.1: seq=2 ttl=64 time=2.043 ms
72 bytes from 172.26.1.1: seq=3 ttl=64 time=2.163 ms

--- 172.26.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.043/2.125/2.163 ms
                    
```

## 6.3 Alarms

In **Network** mode, choose  **Network > 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
<input type="checkbox"/>	There is more than one DHCP server in the LAN network.	Please disable the extra DHCP server in the LAN network.	<a href="#">Delete</a> <a href="#">Unfollow</a>

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	<a href="#">Delete</a>

**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](#)

Cancel

## 6.4 Fault Collection

In **Local Device** mode, choose  **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.

**Start**

# 7 FAQs

## 7.1 What can I do when I failed to log in to the Eweb management system?

Perform the following steps:

- (1) Check that the Ethernet cable is properly connected to the LAN port of the device.
- (2) Before accessing the setup page, you are advised to choose **Auto** for the device enabled with DHCP service to assign an IP address to the PC. If you want to configure a static IP address for the PC, please make sure the IP address of the PC and the LAN port are in the same IP range. The default IP address of the LAN port is 10.44.77.254, and the subnet mask is 255.255.255.0. The IP address of the PC should be set to 10.44.77.X (X is an integer between 2 and 254), and the subnet mask is 255.255.255.0.)
- (3) Run the **Ping** command to check the connectivity between the PC and the device. If the ping fails, please check the network settings.
- (4) If the login failure persists, restore the device to factory settings.

## 7.2 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 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.