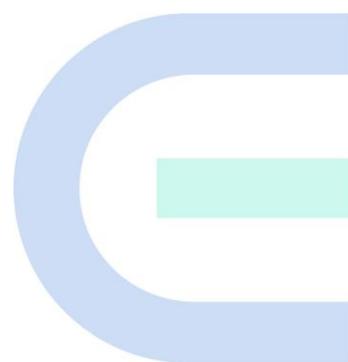


# Ruijie Reyee Home Wi-Fi Router

## Implementation Cookbook



## Copyright

Copyright © 2023 Ruijie Networks

All rights are reserved in this document and this statement.

Without the prior written consent of Ruijie Networks, any organization or individual shall not reproduce, extract, back up, modify, or propagate the content of this document in any manner or in any form, or translate it into other languages or use some or all parts of the document for commercial purposes.



and other Ruijie networks logos are trademarks of 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, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. Except for the agreement in the contract, Ruijie Networks makes no explicit or implicit statements or warranties with respect to the content of this document.

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

This manual is designed merely as a user guide. Ruijie Networks has tried its best to ensure the accuracy and reliability of the content when compiling this manual, but it does not guarantee that the content of the manual is completely free of errors or omissions, and all the information in this manual does not constitute any explicit or implicit warranties.

# Preface

## Technical Support

- The official website of Ruijie Reye: <https://www.ruijienetworks.com/products/reeye>
- Technical Support Website: <https://www.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

This document also uses signs to indicate some important points during the operation. The meanings of these signs are 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.

---

---

 Note

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

---

---

 Instruction

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. Instruction**

This manual is used to guide users to understand the product, install the product, and complete the configuration.

- The example of the port type may be different from the actual situation. Please proceed with configuration according to the port type supported by the product.
- The example of display information may contain the content of other product series (such as model and description). Please refer to the actual display information.
- The routers and router product icons involved in this manual represent common routers and layer-3 switches running routing protocols.

# Contents

Preface .....	1
1 Introduction to Reyee Products.....	1
1.1 Product List.....	1
1.2 LED .....	2
1.3 Button.....	5
2 Reyee Login .....	7
2.1 Connecting to the Router.....	7
2.2 Logging In .....	7
3 Reyee Quick Start.....	9
3.1 Internet Access Modes .....	9
3.2 Primary Router Mode.....	9
3.2.1 Getting Started.....	9
3.2.2 Configuration Steps .....	10
3.2.3 Verification and Testing.....	12
3.2.4 Forgetting the PPPoE Account .....	12
3.3 Secondary Router Mode.....	13
3.3.1 Getting Started.....	13
3.3.2 Configuration Steps .....	13
3.3.3 Verification and Testing.....	20
4 Reyee Wi-Fi Network Settings .....	21
4.1 Changing the SSID and Password.....	21
4.2 Hiding the SSID .....	22
4.2.1 Overview .....	22

4.2.2 Getting Started .....	22
4.2.3 Configuration Steps .....	22
4.3 Adding a Wi-Fi Network .....	23
4.3.1 Overview .....	23
4.3.2 Configuration Steps .....	24
4.3.3 Verification and Testing .....	24
4.4 Configuring a Wi-Fi Blacklist or Whitelist .....	24
4.4.1 Overview .....	24
4.4.2 Configuration Steps .....	24
4.5 Optimizing the Wi-Fi Network .....	27
4.5.1 Overview .....	27
4.5.2 Getting Started .....	27
4.5.3 Configuration Steps .....	27
4.6 Configuring the Healthy Mode .....	30
4.7 Enabling Roaming Optimization .....	31
5 Reye Networks Settings .....	32
5.1 Configuring Internet Connection Type .....	32
5.2 Changing the Address of a LAN Port .....	32
5.3 Changing the MAC Address .....	33
5.4 Changing the MTU .....	34
5.5 Configuring the Repeater Mode .....	35
5.5.1 Wired Repeater .....	35
5.5.2 Wireless Repeater .....	36
5.5.3 WISP .....	38

5.6 Controlling the Internet Access Time Range.....	38
5.7 Configuring XPress.....	39
5.8 Configuring Port Mapping.....	40
5.8.1 Overview.....	40
5.8.2 Getting Started.....	40
5.8.3 Configuration Steps.....	40
5.8.4 Verification and Testing.....	41
5.8.5 Solution to a Test Failure.....	41
5.8.6 DMZ Configuration Steps.....	41
5.9 Configuring the DHCP Server.....	42
5.9.1 Overview.....	42
5.9.2 Configuration Steps.....	42
5.10 Configuring DNS.....	45
5.11 Configuring DDNS.....	46
5.11.1 Overview.....	46
5.11.2 Getting Started.....	46
5.11.3 Configuration Steps.....	46
5.12 Configuring APR Binding and ARP Guard.....	46
5.12.1 Overview.....	46
5.12.2 Configuration Steps.....	46
5.13 Configuring Static Routing.....	47
5.14 Policy-based Routing.....	49
5.15 Connecting to IPTV.....	52
5.15.1 Getting Started.....	52

5.15.2 IPTV Configuration Steps (VLAN Type) .....	52
5.15.3 IPTV Configuration Steps (IGMP Type).....	53
5.16 Configuring Wi-Fi/IGMP .....	54
5.16.1 Overview .....	54
5.16.2 Configuration Steps .....	54
5.17 Configuring IPv6 .....	55
5.17.1 Configuring the IPv6 of the WAN Port .....	55
5.17.2 Configuring the IPv6 of the LAN Port .....	55
5.18 Enabling Smart Flow Control.....	56
5.19 Configuring Firewall .....	57
5.20 Enabling Wi-Fi Switch.....	58
5.21 Configuring UPnP .....	59
5.21.1 Overview .....	59
5.21.2 Configuration Steps .....	59
5.22 Configuring PPTP VPN.....	59
5.22.1 Overview .....	59
5.22.2 Configuring PPTP Server .....	59
5.22.3 Configuring the PPTP Client.....	61
5.23 Configuring OpenVPN .....	62
5.23.1 Overview .....	62
5.23.2 Configuring OpenVPN (Server Mode) .....	63
5.23.3 Configuring OpenVPN (Client Mode) .....	66
5.23.4 Typical Configuration Example .....	67
5.24 Configuring Connectivity Detection .....	74

5.25 Enabling CWMP.....	75
5.25.1 Overview .....	75
5.25.2 Configuration Steps .....	75
5.26 Enabling Reye Mesh.....	76
5.27 Enabling Hardware Acceleration .....	77
5.28 Configuring Console Booster.....	78
5.29 Configuring AP Networking.....	78
5.30 Configuring Reye Mesh 3.0 .....	79
5.30.1 Configuration Steps .....	79
5.31 Diagnosing Network Problems .....	83
6 Reye System Settings.....	84
6.1 Switching to the PC View.....	84
6.2 Configuring the Login Password.....	84
6.3 Remote Access.....	85
6.4 Restoring Factory Settings .....	86
6.5 Configuring the System Time .....	86
6.6 Configuring Scheduled Reboot.....	87
6.6.1 Getting Started .....	87
6.6.2 Configuration Steps .....	87
6.7 Performing Online Upgrade and Displaying the System Version .....	88
6.8 Enabling or Disabling the LED.....	89
6.9 Switching the System Language .....	89
6.10 Network Diagnosis Tools .....	90
6.10.1 Network Test Tool.....	90

6.10.2 Packet Obtaining Tool .....	90
6.11 Configuring Backup and Import .....	91
6.12 Configuring the Session Timeout .....	92
7 Introduction to the Mesh Repeater.....	93
7.1 EW300R.....	93
7.1.1 Network Interface.....	93
7.1.2 System Status LED.....	93
7.1.3 Signal Status LED.....	94
7.1.4 Buttons.....	94
7.2 EW1200R.....	94
7.2.1 Network Interface.....	95
7.2.2 System LED .....	95
7.2.3 Signal LED .....	96
7.2.4 Mesh/WPS Button.....	96
8 Mesh Repeater's Login .....	97
8.1 Connecting to the Device.....	97
8.2 Login .....	99
9 Mesh Repeater's Network Settings.....	100
9.1 Network Settings.....	100
9.1.1 Getting Started.....	100
9.1.2 Configuration Steps .....	100
9.1.3 Verifying the Configuration.....	101
9.2 Network Settings (in Router Mode) .....	102
9.2.1 Getting Started.....	102

9.2.2 Configuration Steps .....	102
9.2.3 Verifying the Configuration.....	105
10 Mesh Repeater's Wi-Fi Network Settings .....	106
10.1 Changing the SSID and Password.....	106
10.2 Hiding the SSID .....	107
10.2.1 Overview .....	107
10.2.2 Getting Started.....	107
10.2.3 Configuration Steps .....	107
10.3 Configuring Wi-Fi .....	108
10.3.1 Overview .....	108
10.3.2 Configuration Steps .....	108
10.4 Configuring a Wi-Fi Blacklist or Whitelist.....	109
10.4.1 Overview .....	109
10.4.2 Configuration Steps .....	109
10.5 Optimizing the Wi-Fi Network .....	111
10.5.1 Overview .....	111
10.5.2 Getting Started.....	111
10.5.3 Configuration Steps .....	111
10.6 Configuring the Healthy Mode .....	115
11 Mesh Repeater's Networks Settings .....	117
11.1 Configuring an Internet Connection Mode.....	117
11.2 Changing the IP Address of a LAN Port.....	117
11.3 Changing the MAC Address .....	118
11.4 Changing the MTU.....	119

11.5 Configuring the Repeater Mode .....	120
11.5.1 Wired Repeater .....	120
11.5.2 Wireless Repeater.....	121
11.5.3 WISP .....	123
11.6 Online Time Control.....	124
11.7 Configuring XPress.....	126
11.8 Configuring the DHCP Server .....	127
11.8.1 Overview .....	127
11.8.2 Configuration Steps.....	127
11.9 Configuring DNS .....	129
11.9.1 Local DNS .....	129
11.9.2 DNS Proxy.....	130
11.10 Enabling Port-based Flow Control.....	130
11.11 Network Problem Diagnosis .....	131
12 Mesh Repeater's System Settings.....	132
12.1 Configuring the Login Password.....	132
12.2 Restoring Factory Settings .....	132
12.3 Configuring the System Time .....	133
12.4 Configuring Scheduled Reboot.....	134
12.4.1 Getting Started.....	134
12.4.2 Configuration Steps .....	134
12.5 Performing Online Upgrade and Displaying the System Version .....	134
12.6 Enabling or Disabling the LED.....	135
12.7 Switching the System Language .....	135

12.8 Network Diagnosis Tools .....	136
12.9 Configuring Backup and Import .....	138
12.10 Configuring the Session Timeout .....	139
12.11 Switching to the PC View.....	139
13 Reyee FAQ.....	141
13.1 Reyee FAQ .....	141
13.1.1 Reyee Password FAQ (Collection) .....	141
13.1.2 Reyee Wireless Repeater FAQ (Collection) .....	141
13.1.3 Reyee Parental Control FAQ (Collection).....	141
13.1.4 Reyee Mesh FAQ (Collection) .....	141
13.1.5 Reyee Self-Organizing Network (SON) FAQ (Collection) .....	141
13.1.6 Reyee series Devices Parameters Tables.....	141
13.1.7 Reyee Parameter Consultation FAQ (Collection).....	141
13.2 Mesh Repeater FAQ.....	141
13.2.1 How Can I Restore Factory Settings? .....	141
13.2.2 How Can I Do If I Forget the Password of the Mesh Repeater?.....	141
13.2.3 How Do I Manage the Mesh Repeater After the Mesh Repeater Is Installed Successfully? .....	141
14 Appendix: Monitoring of Reyee Mesh Wi-Fi Routers.....	142
14.1 Overview .....	142
14.2 Endpoints .....	142
14.3 Internet.....	144

# 1 Introduction to Reyee Products

Reyee EW series products are gigabit dual-band Wi-Fi 6 wireless routers designed for large flat space, villas, small shops, SOHO, and other scenarios. It is designed to meet the needs of high-quality next-generation Wi-Fi services. Reyee EW series products support various local and remote management platforms, such as web and Ruijie Cloud App. This wireless router also provides multiple home-care-based function, including the parental control mode, health mode, and Xpress mode, and is exclusively designed for Smart Life Kit System, meeting needs of all household scenarios.



## 1.1 Product List

Model	Reyee Mesh	Wi-Fi Standards	Maximum Wi-Fi Rate	MIMO	Recommended Users
EW300 PRO	Not supported	Wi-Fi 4 (802.11n)	2.4 GHz: 300 Mbit/s	2.4 GHz: 2x2	8
EW1200	Supported	Wi-Fi 5 (802.11ac)	2.4 GHz: 300 Mbit/s 5 GHz: 867 Mbit/s	2.4 GHz: 2x2 5 GHz: 2x2	2.4 GHz: 8 5 GHz: 16
EW1200G PRO	Supported	Wi-Fi 5 (802.11ac)	2.4 GHz: 400 Mbps 5 GHz: 867 Mbit/s	2.4 GHz: 2x2 5 GHz: 2x2	2.4 GHz: 8 5 GHz: 24
EW1800GX PRO	Supported	Wi-Fi 6 (802.11ax)	2.4 GHz: 573 Mbit/s 5 GHz: 1200 Mbit/s	2.4 GHz: 2x2 5 GHz: 2x2	2.4 GHz: 12 5 GHz: 36
EW3200GX PRO	Supported	Wi-Fi 6 (802.11ax)	2.4 GHz: 800 Mbit/s 5 GHz: 2400 Mbit/s	2.4 GHz: 4x4 5 GHz: 4x4	2.4 GHz: 12 5 GHz: 48
M18	Supported	Wi-Fi 6 (802.11ax)	2.4 GHz: 574 Mbit/s 5 GHz: 1201 Mbit/s	2.4 GHz: 2x2 5 GHz: 2x2	2.4 GHz: 12 5 GHz: 36

Model	Reyee Mesh	Wi-Fi Standards	Maximum Wi-Fi Rate	MIMO	Recommended Users
M32	Supported	Wi-Fi 6 (802.11ax)	2.4 GHz: 800 Mbit/s 5 GHz: 2402 Mbit/s	2.4 GHz: 4x4 5 GHz: 4x4	2.4 GHz: 12 5 GHz: 48
EW3000GX PRO	Supported	Wi-Fi 6 (802.11ax)	2.4 GHz: 573 Mbit/s 5 GHz: 2401 Mbit/s	2.4 GHz: 2x2 5 GHz: 2x2	2.4 GHz: 64 5 GHz: 128

## 1.2 LED

### (a) EW300 PRO

LED	Status	Description
System Status LED	Off	The router is not powered on.
	Solid on	The router is running normally.
	Fast blinking (on for 62 ms, off for 62 ms)	The router is starting up or powered off.
	Slow blinking (on for 250 ms, off for 250 ms)	The Internet is unreachable.
	Fast blinking twice	The router is restored to factory settings. The firmware is upgraded.
	Slow blinking once and fast blinking three times	The firmware is faulty.

### (b) EW1200

LED	Status	Description
System Status LED	Off	The router is not powered on.
	Solid on	The router is running normally.
	Slow blinking (one interval of 1.75 seconds: on for 250 ms, off for 250 ms)	<ul style="list-style-type: none"> <li>● The router is initialized.</li> <li>● The router does not access the Internet.</li> </ul>
	Fast blinking (on for 62.5 ms, off for 62.5 ms)	<ul style="list-style-type: none"> <li>● The router is restored to factory settings.</li> <li>● The router restarts.</li> <li>● The router is initialized.</li> <li>● The firmware is upgraded.</li> </ul>
Wi-Fi LED	Solid on	Reyee mesh router is sunning normally.

LED	Status	Description
	Slow blinking	Reyee mesh router is being paired or the repeater stops.
Port LED	Off	The port is not connected or the cable is disconnected.
	Solid on	The port is connected normally.

**(c) EW1200G PRO**

LED	Status	Description
System Status LED	Off	The router is not powered on.
	Solid on	The router is running normally.
	Fast blinking	The router is restored to factory settings. The router restarts.
	Slow blinking (one interval of 1.75 seconds: on for 250 ms , off for 250 ms)	The router is initialized. The router does not access the Internet.
	Slow blinking (alternately on for 40 ms and off for 150 ms)	Reyee mesh router is being paired or the repeater stops.
Port LED	Off	The port is not connected or the cable is disconnected.
	Solid on	The port is connected normally.
	Blinking	Data is being transmitted.

**(d) EW1800GX and EW3200GX PRO**

LED	Color/Status		Description
Mesh LED	Green	Blinking	The router is being paired.
		Solid on	The router is paired and Wi-Fi signals are normal.
	Orange	Solid on	The router is paired but Wi-Fi signals are weak.
	Red	Solid on	Device pairing is disconnected.
System Status LED	Blue	Solid on	The router is running normally.

		Fast blinking (on for 62.5 ms, off for 62.5 ms)	The router is restored to factory settings. The router restarts. The firmware is upgraded.
		Slow blinking (one interval of 1.75 seconds: on for 250 ms , off for 250 ms)	The router is initialized. The router does not access the Internet.

**(e) M18 and M32**

LED	Status	Description
Reyeer Mesh Indicator	Blinking white	The device is being paired
	Four bars are solid white	The Mesh network signal is excellent.
	Three bars are solid white	The Mesh network signal is good
	Two bars are solid white	The Mesh network signal is average.
	One bar is solid white	The Mesh network signal is poor.
	Off	The Mesh network is disconnected or not set up.
System Status Indicator (Reyeer Mesh Button)	Solid blue	The device is working normally and can access the Internet.
	Solid orange	The device does not access the Internet.
	Blinking blue	The device is starting up or restoring the factory settings.

**(f) EW3000GX PRO**

LED	Color/Status	Description
Reyeer Mesh Indicator	Solid on	Mesh pairing succeeds.
	Off	Mesh pairing is not performed./Mesh network is disconnected.
	Blinking	Mesh pairing is in progress.
System Status Indicator	Green	
	Solid on	The router is functioning properly or is connected to the Internet.
	Blinking	The router is starting up, being reset, or upgrading.

LED	Color/Status		Description
	Orange	Solid on	The signal strength of the mesh link is low (secondary router).
	Red	Solid on	The router is not connected to the Internet.

## 1.3 Button

### (a) EW300 PRO

Button	Function	Operation
Reset	Reset	Press the button for over 3 seconds until the LED starts to blink. Release the button. Then the router is reset.

### (b) EW1200 and EW1200G PRO

Button	Function	Operation
Pairing/Reset	Pair	Press the button for 1 second to pair the router.
	Reset	Press the button for over 10 seconds until the LED starts to blink. Release the button. Then the router is reset.

### (c) EW1800GX and EW3200GX PRO

Button	Function	Operation
Reyee Mesh Button	Pair	Press the button for 1 second to pair the router.
Reset Button	Reset	Press the button for over 10 seconds until the LED starts to blink. Release the button. Then the router is reset.

### (d) M18 and M32

Button	Function	Operation
Reyee Mesh Button	Pair	Press the button for 1 second to pair the router.

Reset Button	Reset	Press the button for over 10 seconds until the LED starts to blink. Release the button. Then the router is reset.
--------------	-------	--

**(e) EW3000GX PRO**

Button	Function	Operation
Reyee Mesh Button	Pair	Press the button for 1 second to pair the router.
Reset Button	Reset	Press the button for over 10 seconds until System Status Indicator starts to blink. Release the button. Then the router is reset.

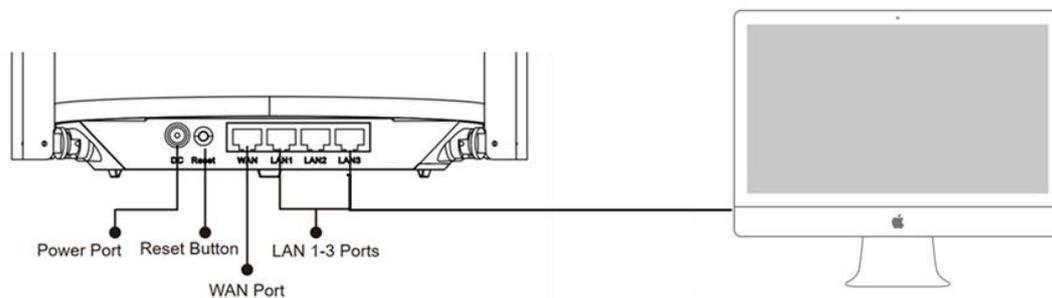
# 2 Reyee Login

## 2.1 Connecting to the Router

You can open the management page and complete Internet access configuration only after connecting a PC or a mobile phone to the router. You can connect a PC to the router in either of the following ways, and connect a mobile phone to the router in wireless connection mode.

- Wired connection

Connect a local area network (LAN) port of the router to the network port of the PC, and configure **Obtain an IP address automatically** on the PC. The EW300 is used as an example. The following figure shows the connection between the router and laptop.



- Wireless connection

On a mobile phone or laptop, search for a Wi-Fi network **@Ruijie-sXXXX** (XXXX is the last four digits of the MAC address of each device). The default SSID and login address can be found on the bottom label of the router.

## 2.2 Logging In

When a PC or a mobile phone connects to a router in initial state, the configuration wizard page appears. If the configuration page does not appear, enter the device IP address into the address bar of the browser to navigate to the login page, and then enter the password for login.

**Table 2-1 Default Configuration**

Item	Default Value
Device IP address	192.168.110.1
Username/Password	No username and password are required at your first login. You can configure the router directly.

If you forget the IP address or password, hold down the **Reset** button for more than 5 seconds to restore factory settings. Then you can use the default IP address and password to log in.

 Note

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

If the router in initial state detects that the IP address of the primary router is 192.168.110.1, the router automatically changes its own IP address to 192.168.111.1 to avoid an IP address conflict. You may fail to log in to the router during the IP address change, but can reconnect to the Wi-Fi network and complete configuration 1 minute later.

---

# 3 Reyee Quick Start

## 3.1 Internet Access Modes

The device supports two Internet access modes: primary router mode and secondary router mode. In secondary router mode, the device can access the Internet through either the wired connection or wireless repeater function.

**Primary Router Mode:** This mode is suitable for network creation. The device connects to the Internet through the wired connection, and can manage secondary routers. You are advised to select the device with the best performance as the primary router. The primary router can work in Point-to-Point Protocol over Ethernet (PPPoE) mode, Dynamic Host Configuration Protocol (DHCP) mode, or static IP address mode.

**Secondary Router Mode:** On an available network, the device can be connected to the primary router through either the wired or wireless connection to expand the Wi-Fi coverage and increase the number of LAN ports and wireless access devices. The wireless repeater mode includes the repeater mode and wireless Internet service provider (WISP) mode.

---

### Instruction

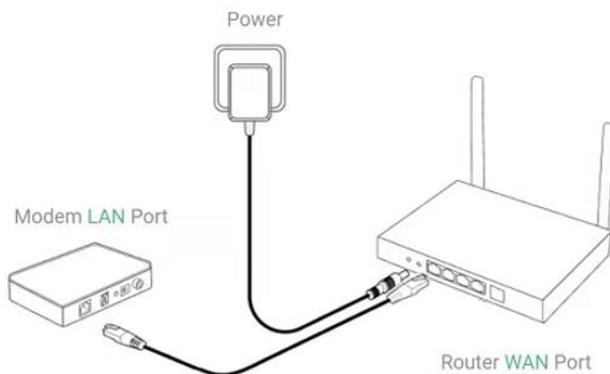
The wired connection mode can greatly improve the network stability. You are advised to use the wired connection.

---

## 3.2 Primary Router Mode

### 3.2.1 Getting Started

Connect the router to a power supply and connect the LAN port of a modem to the WAN port of the router.



Configure the Internet connection mode according to requirements of the local Internet Service Provider (ISP). Otherwise, the Internet may be inaccessible due to improper configuration. You are advised to contact your local ISP to confirm the Internet connection mode.

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

## 3.2.2 Configuration Steps

### 1. Configuring an Internet Connection Mode

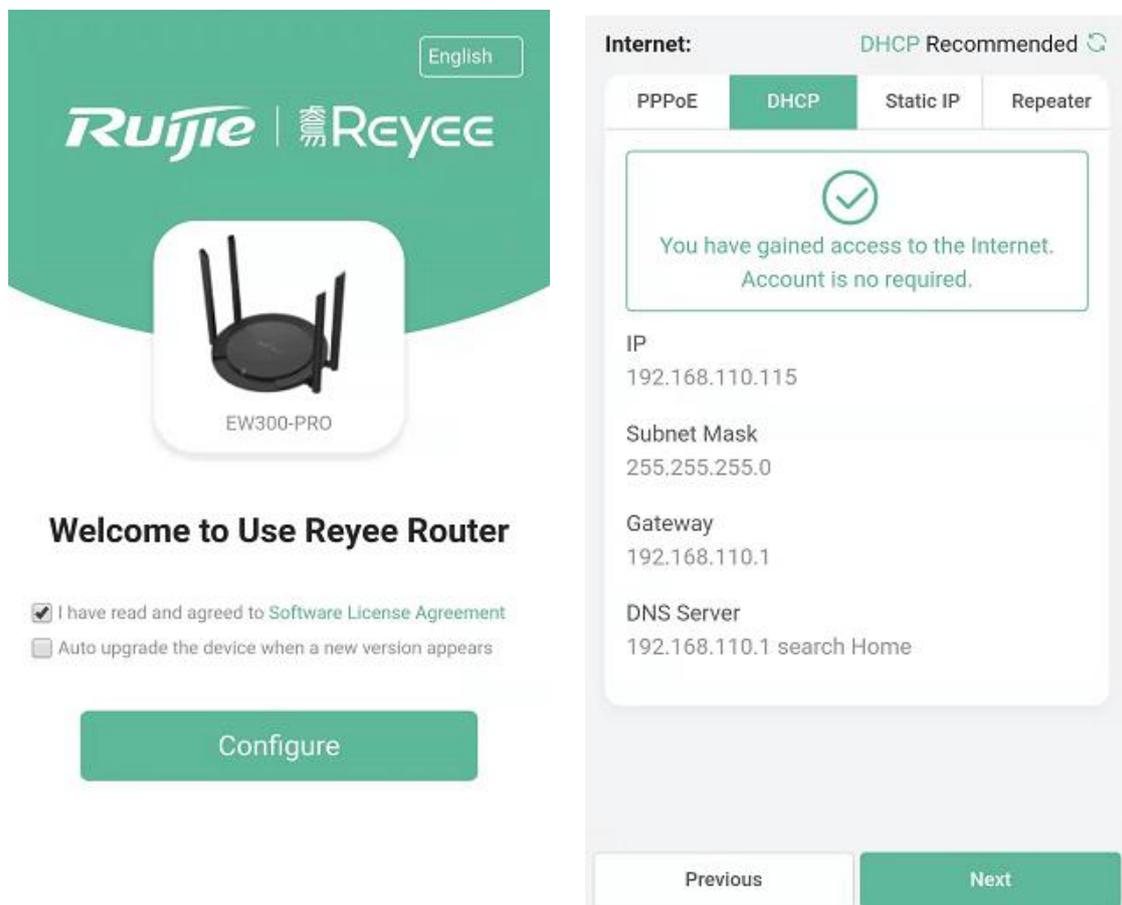
Click **Configure** and select the Internet connection mode confirmed by the carrier.

- **DHCP**: The router detects whether it can obtain an IP address through DHCP by default. If the router connects to the Internet successfully, you can click **Next** without entering an account.

#### Note

If the IP address delivered by the primary router is also 192.168.110.0, the router automatically changes the IP address of its LAN interface to 192.168.111.1 to avoid conflicts. Do not incorrectly change the configuration of the primary router. You can differentiate routers by checking the router model and Wi-Fi information on the home page.

- PPPoE: Click PPPoE, and enter the username, password, and service name. Click Next.
- Static IP: Enter the IP address, subnet mask, gateway, and DNS server, and click Next.



The image displays two screenshots from the Reyee router's web interface. The left screenshot is the 'Welcome to Use Reyee Router' page, featuring the Ruijie and Reyee logos, a router model 'EW300-PRO', and a 'Configure' button. Below the button are two checkboxes: 'I have read and agreed to Software License Agreement' (checked) and 'Auto upgrade the device when a new version appears' (unchecked). The right screenshot shows the 'Internet' configuration page with 'DHCP Recommended' selected. It displays a success message: 'You have gained access to the Internet. Account is no required.' and lists the following settings: IP: 192.168.110.115, Subnet Mask: 255.255.255.0, Gateway: 192.168.110.1, and DNS Server: 192.168.110.1 search Home. There are 'Previous' and 'Next' buttons at the bottom.

### 2. Configuring a Wi-Fi Network

- (1) Setting the SSID and Wi-Fi password: The router 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. The password must be a string of 8 to 64 characters, which can contain uppercase and lowercase letters, digits, and English characters. It cannot contain special characters such as single quotation marks ('), double quotation marks ("), or spaces.

- (2) **Setting the management password:** The password is used for logging in to the management page. The management password must be a string of 8 to 64 characters and contain at least three types among uppercase letters, lowercase letters, digits, and English characters. It cannot contain **admin**, Chinese characters, spaces, or question marks (?). You can select **Same as Wi-Fi Password**.
- (3) **Enabling the Wi-Fi 6:** Wi-Fi 6 can provide a faster and more stable network for Wi-Fi 6-capable clients. You are advised to enable this function.

**⚠ Caution**

Only EW1800GX-PRO and EW3200GX-PRO support Wi-Fi 6.

- (4) **Setting the country or region:** A Wi-Fi channel may vary according to the country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.
- (5) **Setting the time:** The network time server is enabled by default to provide the time service. You are advised to select the actual time zone.
- (6) **Overriding the configuration:** Click **Override**. The Wi-Fi network will restart. You need to enter the new Wi-Fi password to connect to the new Wi-Fi network.

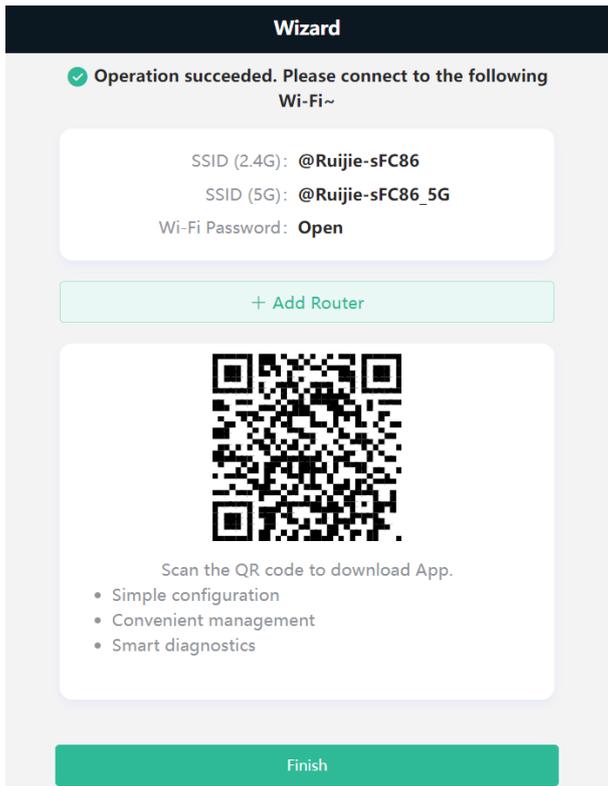
The image displays two side-by-side screenshots of a 'Wizard' configuration interface for Wi-Fi settings.

**Left Screenshot (Wi-Fi Settings):**

- Wi-Fi Settings:** A toggle for 'Dual-Band Single SSID' is turned off.
- SSID (2.4G):** Labeled 'Large Coverage & Slow Rate', the field contains '@Ruijie-sFC86'.
- SSID (5G):** Labeled 'Small Coverage & Fast Rate', the field contains '@Ruijie-sFC86\_5G'.
- Wi-Fi Password:** A toggle is turned on. The field contains 'Please enter a Password.' with a visibility icon.
- Management Password:** A checkbox 'Same as Wi-Fi Password' is unchecked. The field contains 'Please remember the password.' with a note 'The password is 8-31 characters long.' and a visibility icon.
- Buttons:** 'Previous' (grey) and 'Override' (green).

**Right Screenshot (Management Password and Country/Region/Time Zone):**

- Wi-Fi Password:** The field contains '@Ruijie-sFC86\_5G'. A toggle is turned off.
- Management Password:** The field contains 'Please remember the password.' with a note 'The password is 8-31 characters long.' and a visibility icon.
- Country/Region/Time Zone:** A dropdown menu is expanded, showing 'China (CN)' selected for the country and '(GMT+8:00)Asia/Shanghai' selected for the time zone.
- Buttons:** 'Previous' (grey) and 'Override' (green).



### 3.2.3 Verification and Testing

You can access the Internet after connecting to a Wi-Fi network. Log in to the management page (the default address is 192.168.110.1). The main page shows the Internet connection status and real-time uplink and downlink traffic data.



### 3.2.4 Forgetting the PPPoE Account

- (1) Consult your local ISP.
- (2) If you replace the old router with a new one, click **Obtain Account from Old Device**. Connect the old and new routers to a power supply and start them. Insert one end of a network cable into the WAN port of the old router and connect the other end to a LAN port of the new router, and click **Obtain**. The new router automatically obtains the PPPoE account of the old router. Click **Save** to make the configuration take effect.

**Internet** Online (DHCP)

Internet: Online (DHCP)

PPPoE | DHCP | Static IP

\* Username Provided by ISP

Please enter a PPPoE username.

\* Password Obtain Account from Old Device

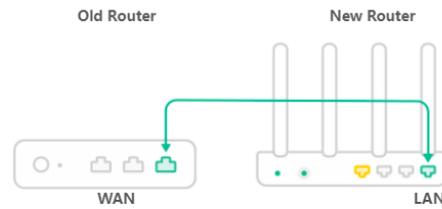
Password

Service Name

(Optional) Provided by ISP

Save

## Obtain PPPoE Account from Old Router



## Steps:

1. Transmit Power on the old router and new router.
2. Connect one end of a cable to the WAN port of the old router and connect the other end to the LAN port of the new router.
3. Click "Obtain".

Obtain

## 3.3 Secondary Router Mode

### 3.3.1 Getting Started

- Before configuring the secondary router, configure the primary router and test that the primary router can access the Internet.
- The router supports both wireless and wired connection modes. If a network cable is available, you are advised to connect the secondary router to the primary router in wired connection mode.
- If no network cable is available, place the secondary router in a place where it can scan at least two-bar Wi-Fi signals of the primary router.

### 3.3.2 Configuration Steps

#### 1. Wired Connection

- (1) Connect to the primary router: Use an Ethernet cable to connect the WAN port of the secondary router to the LAN port of the primary router.
- (2) Wait for the SYS LED on the secondary router to be steady on. Then, press the Reyee Mesh button on the primary router to enable wired connection. The default SSID and password of the secondary router are automatically synchronized to be the same as those on the primary router.

#### **i** Note

Make sure that the secondary router is in the factory default state. If the secondary router has been configured, please first restore it to factory default settings by pressing and holding the reset hole for 10 seconds, and then repeat Step 2.

#### 2. Wireless Connection by using the Reyee Mesh function

- (1) Place the second router within 2 meters of the primary router, power it on and wait for it to start up.
- (2) Press the Reyee Mesh button on the primary router to complete the wireless Reyee Mesh networking in 2 minutes. The SSID and password of the secondary router are automatically synchronized with those of the primary router.
- (3) Place the secondary router in a location where the Wi-Fi signal needs to be extended, and power it on.

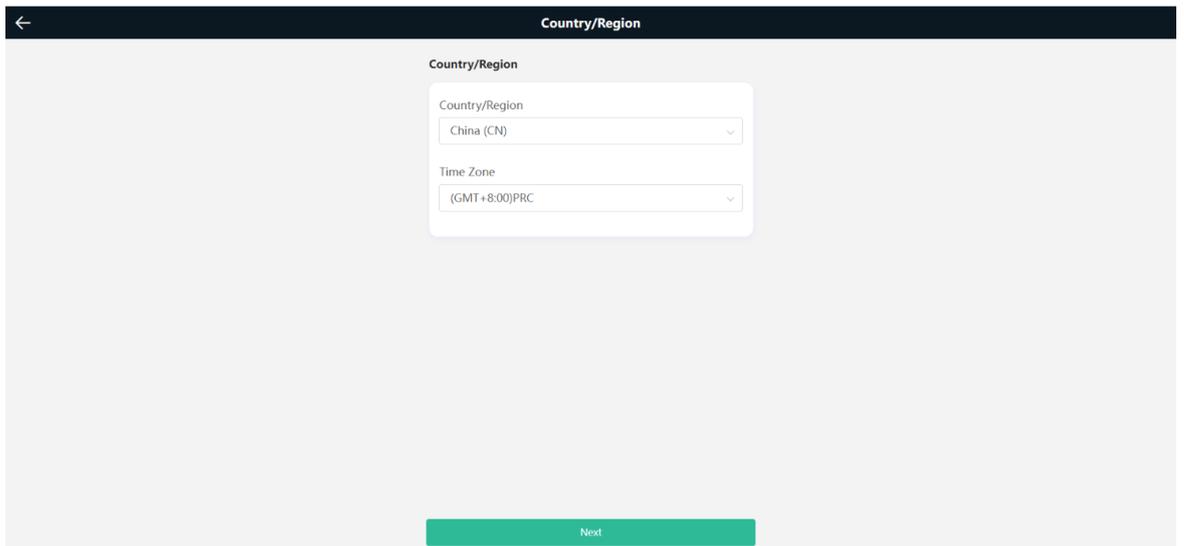
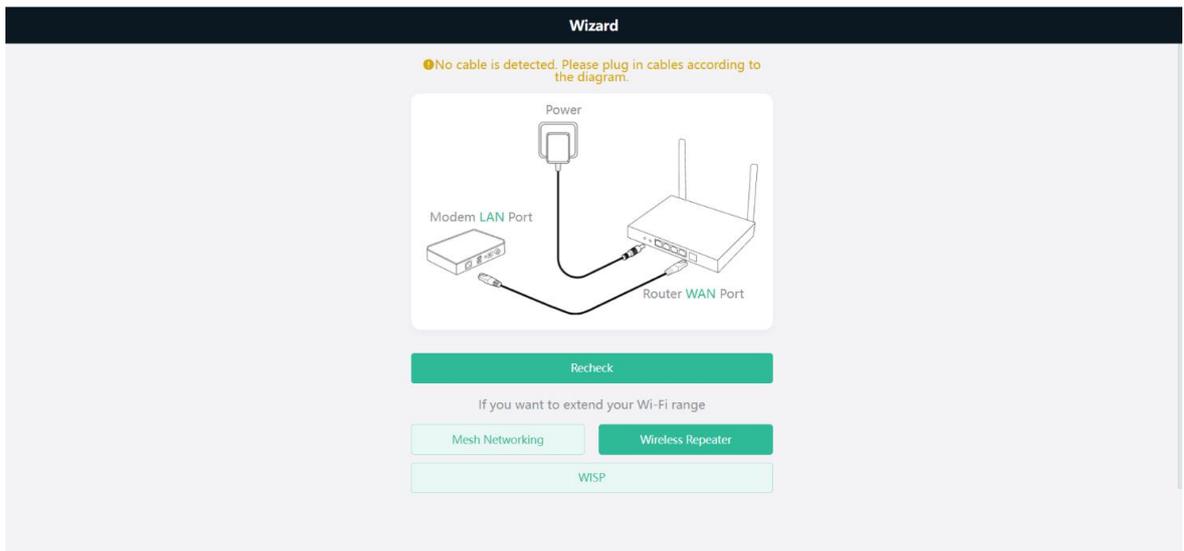
**⚠ Caution**

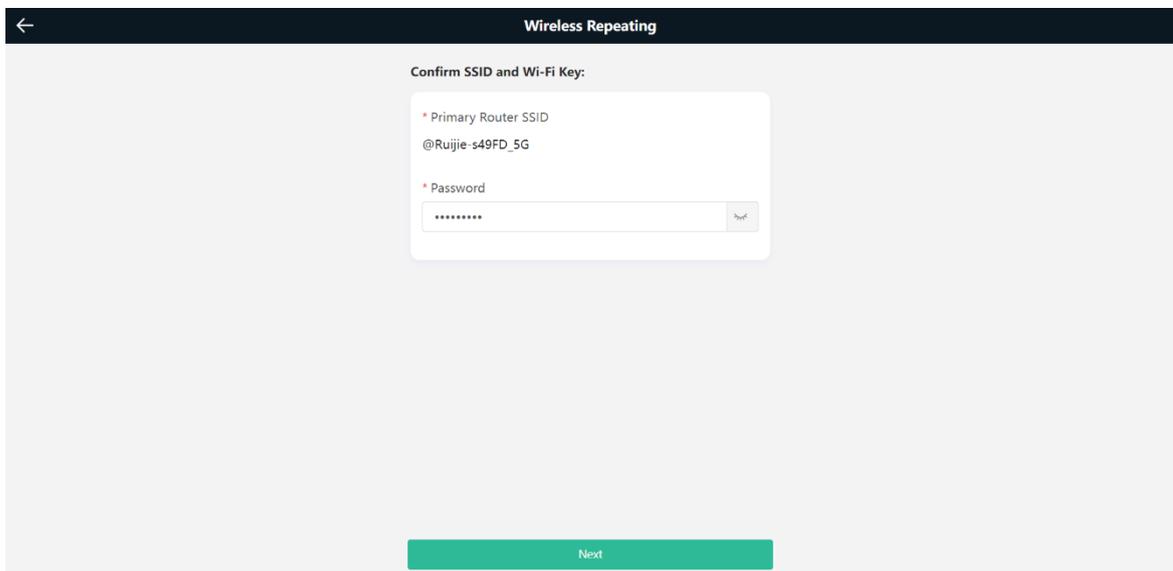
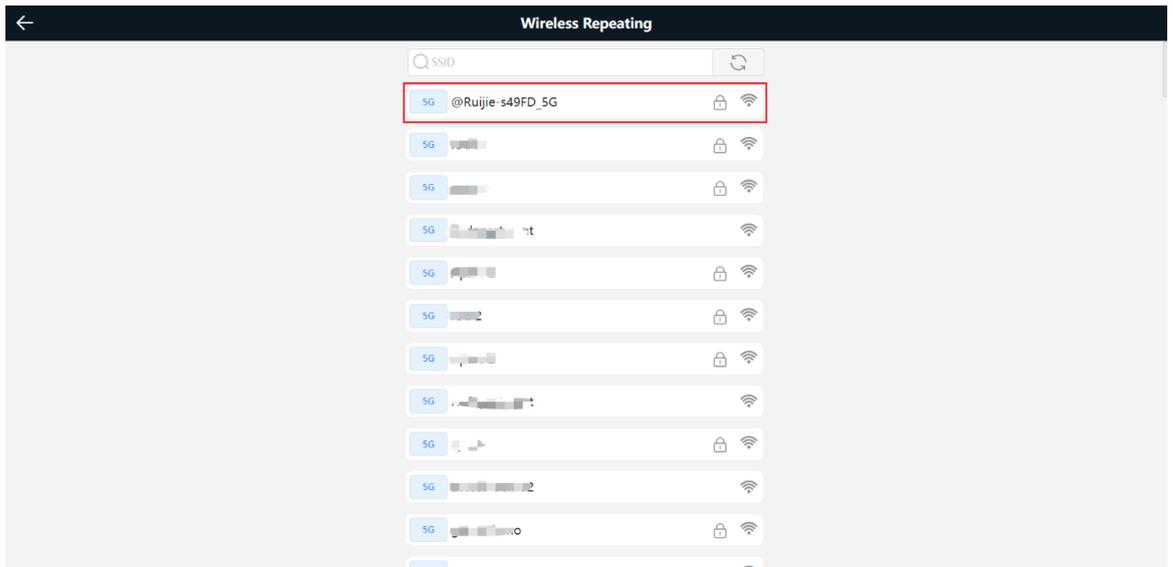
No Ethernet cable is required in the wireless repeater mode. The wireless network stability can be affected by many factors. Therefore, the wired connection is recommended.

**3. Wireless Connection by Web configuration**

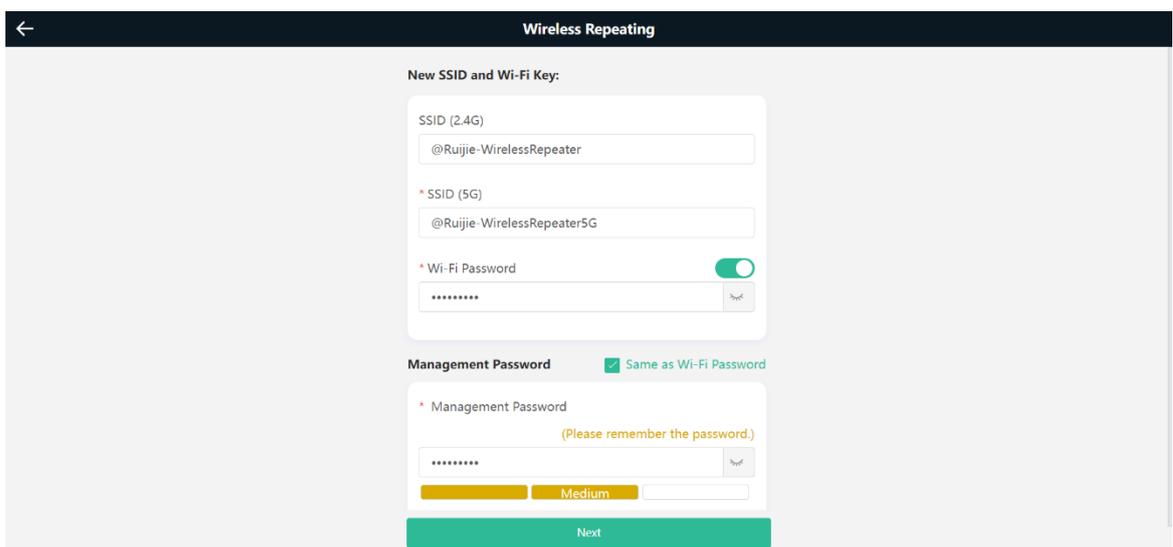
**4. Wireless Repeater Mode**

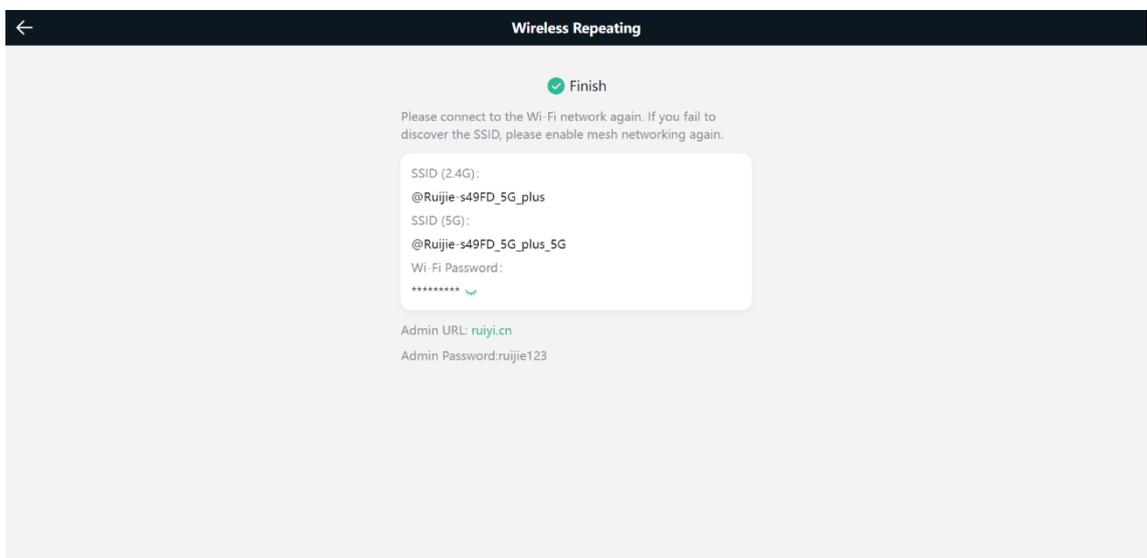
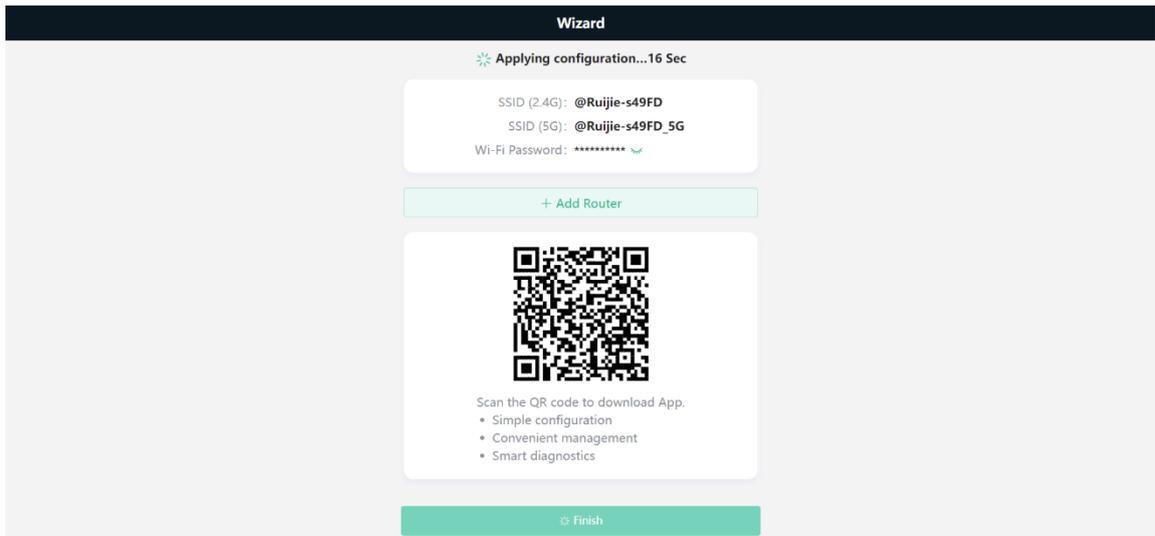
- (1) Click **Wireless Repeater**, select **Country/Region** and **SSID** of the primary router, and enter the Wi-Fi password to connect to the primary router.



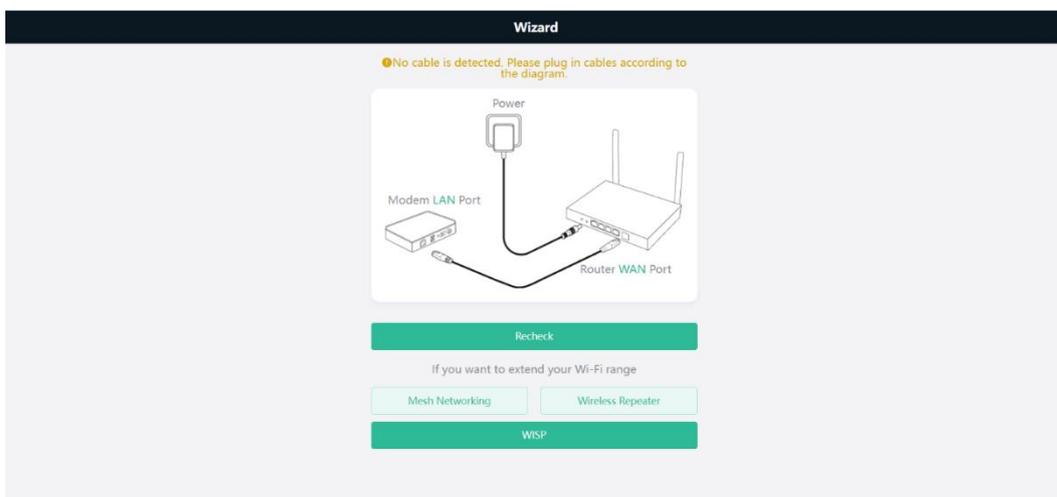


(2) Set the SSID and password and save the settings. Then settings of the Wi-Fi network are reset.



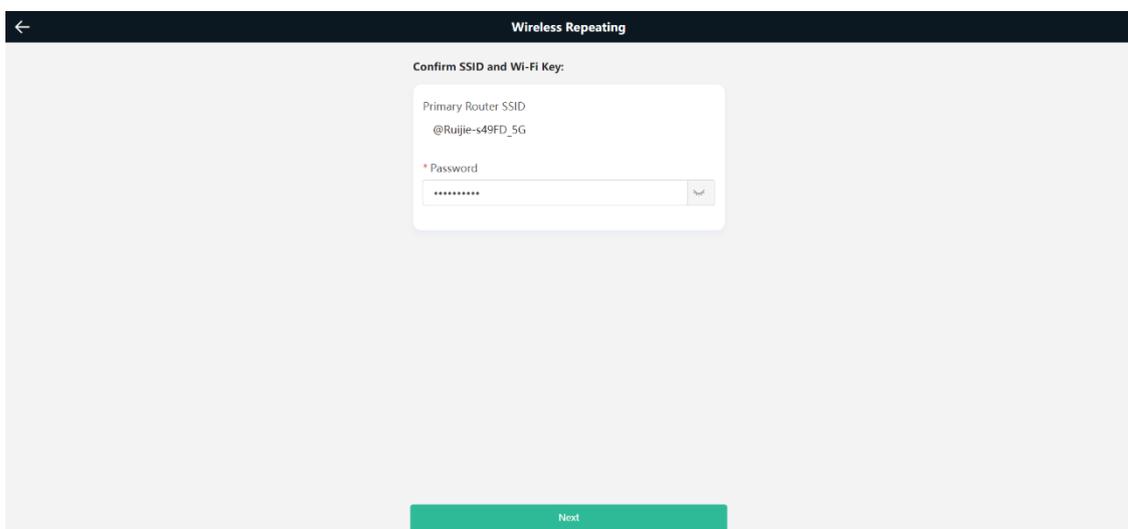
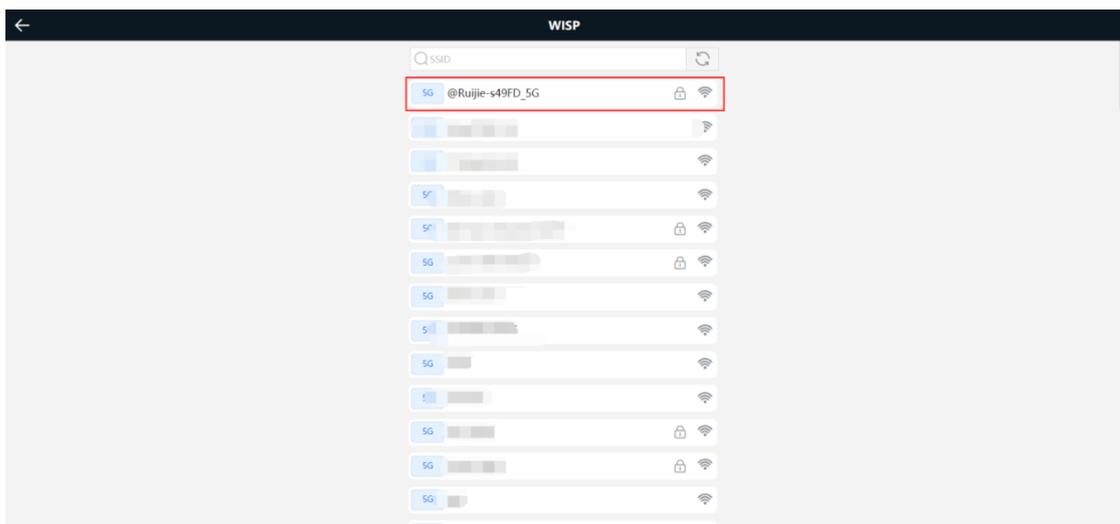
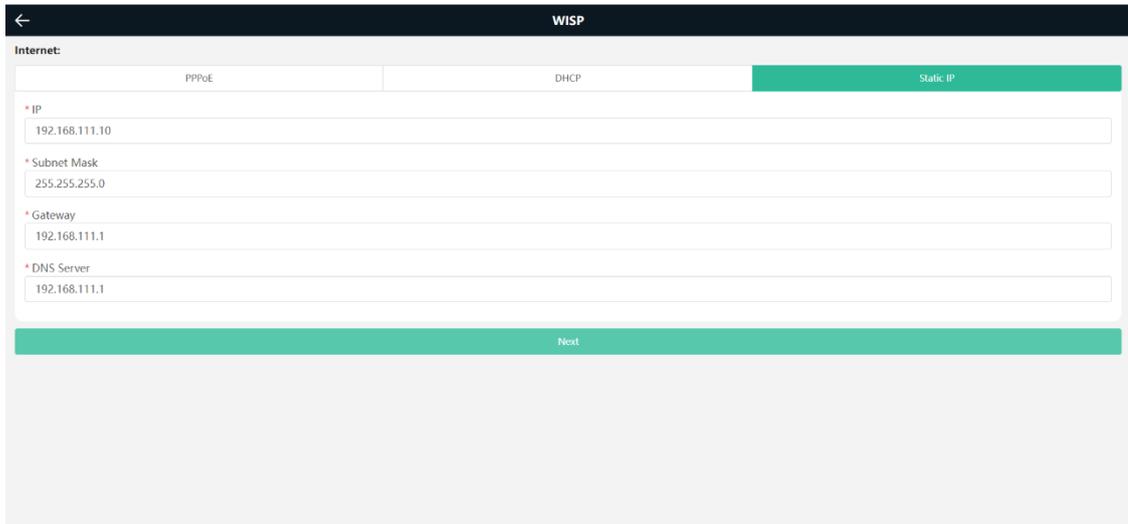


In wireless repeater mode, only Wi-Fi signals are extended and the DHCP function is disabled. IP addresses of all clients connected to the primary and secondary routers are assigned by the primary router. If the device connects to the primary router in wireless repeater mode, the WAN port of the device keeps unchanged. If a WAN cable is installed, the device automatically switches to the wired repeater mode.

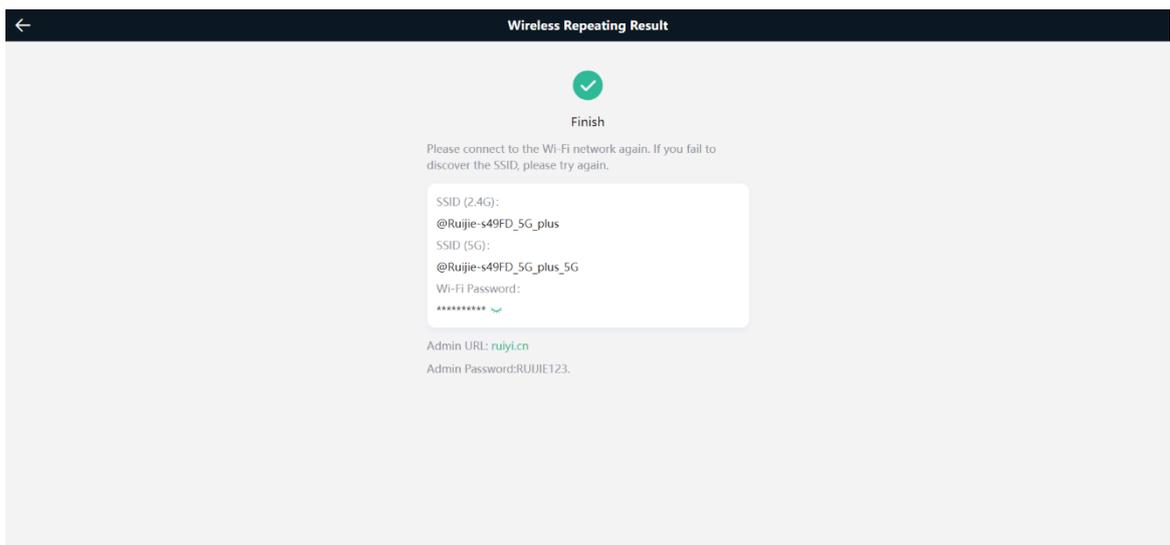
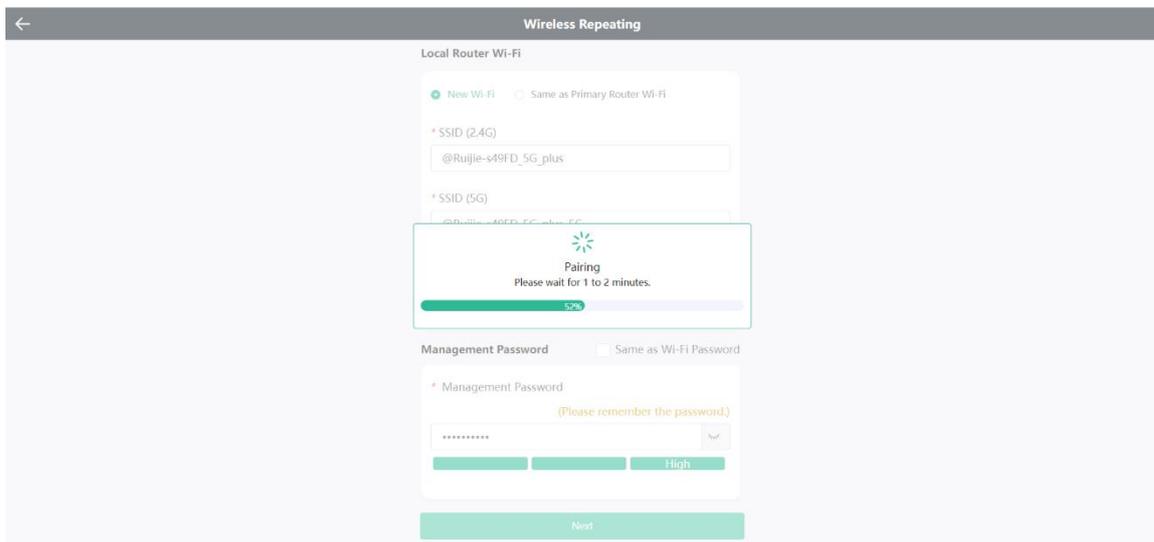
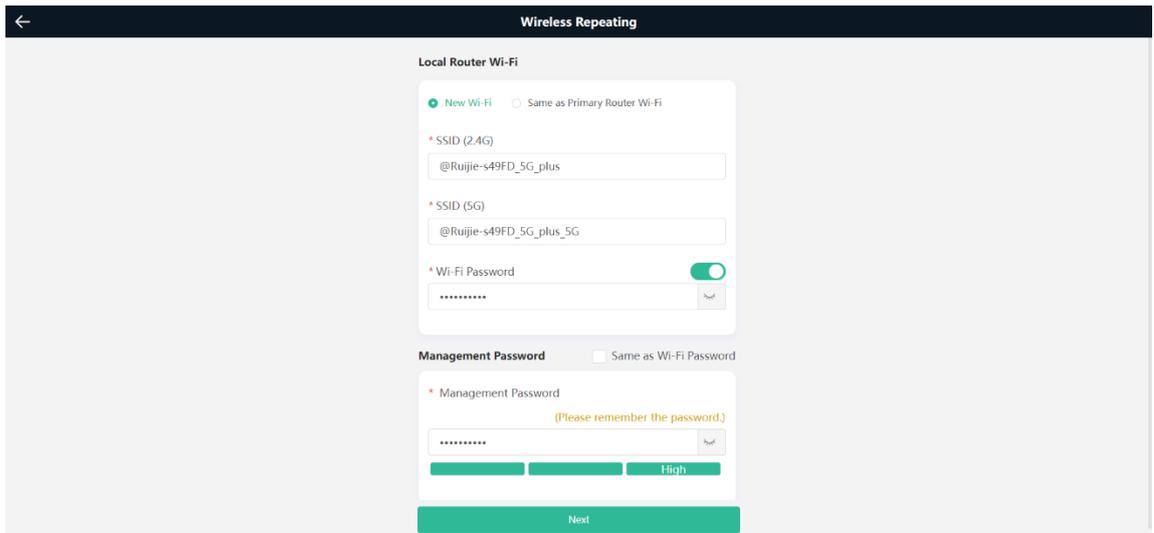


### 5. Wireless ISP Mode

- (1) Click **WISP**. On the displayed network setup page, click **Next** to automatically obtain an IP address. If the primary router cannot deliver an IP address, select **Static IP**. Select the SSID of the primary router and enter the Wi-Fi password to connect to the primary router.



- (2) Set the SSID and password and save the settings. Then settings of the Wi-Fi network are reset.



In wireless ISP mode, the device still supports routing and DHCP functions, IP addresses of clients connected to the primary router are assigned by the primary router and the IP addresses of clients

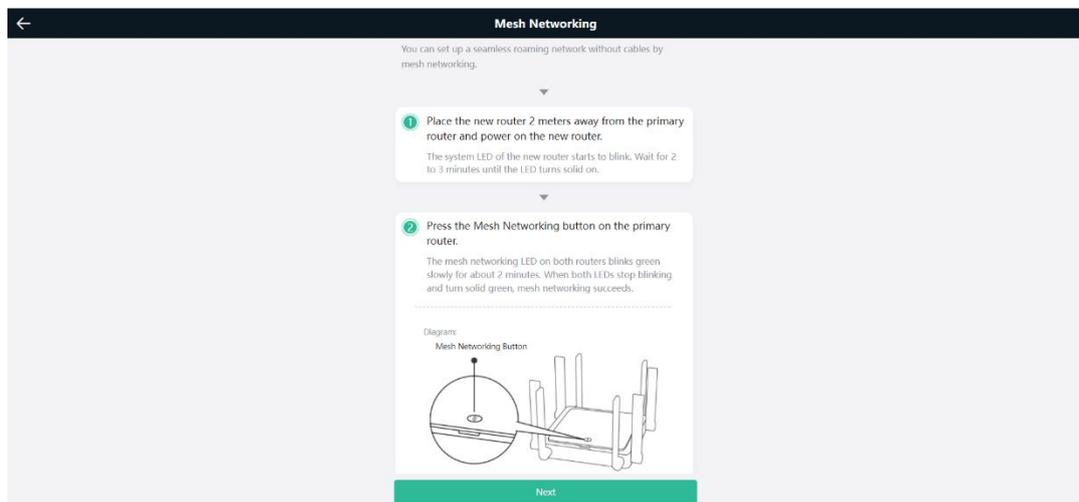
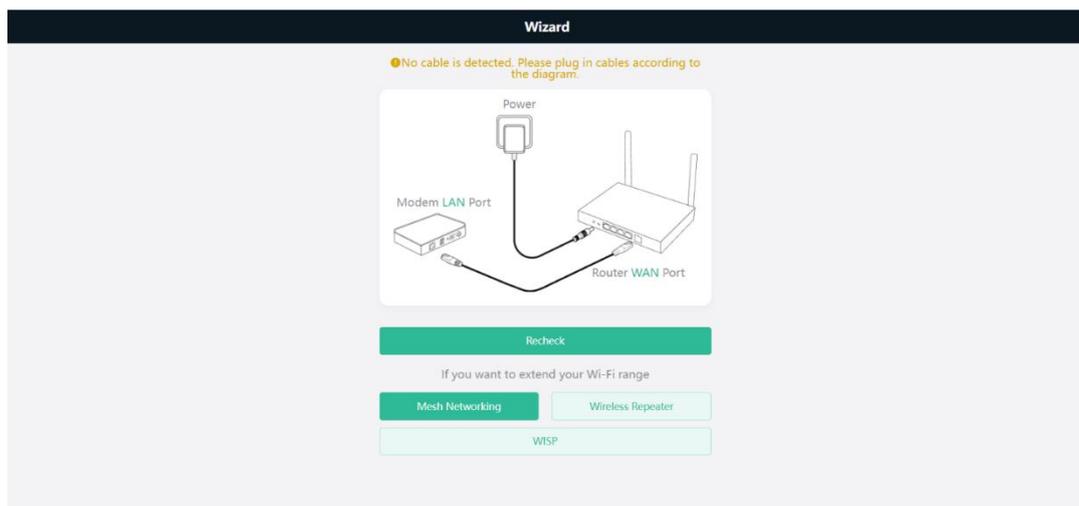
connected to the secondary router are assigned by the secondary router. When the device connects to the Internet in wireless connection mode, the wired WAN port becomes the LAN port and is used by clients.

## 6. Mesh Networking

### ⚠ Caution

This function is not supported by the EW300 PRO.

- (1) Click **Mesh Networking**, then click the **Next** button after accessing the **Mesh Networking** page. According to mesh networking steps on this page, press the **Mesh Networking** button on the primary and second routers.



### ⚠ Caution

The EW1200G PRO and EW1200 do not have the **Mesh Networking** button, press the **Reset** button for less than 2s.

- (2) After the page indicating that the mesh networking is succeeded is displayed, you can view that one new repeater is connected to the primary router.

**Mesh Networking**

✔ Mesh networking succeeded.

Check whether SSID @Ruijie-sC801 disappears. If yes, connect to the Wi-Fi network of the primary router, and you can access the Internet.

Tip:



- Make sure that the new router is around the primary router and there are not too many obstacles between them.
- If there are 3 or more routers, repeat the above steps. Up to 5 (1+4) routers are supported.

Internet    26.67Kbps / 47.41Kbps    EW1200G-PRO    Repeater    Wireless / wired    Clients + Add

### 3.3.3 Verification and Testing

You can access the Internet after connecting to the Wi-Fi network of the primary router.

# 4 Reyee Wi-Fi Network Settings

## 4.1 Changing the SSID and Password

PC view: Choose **Wi-Fi > Wi-Fi Settings**.

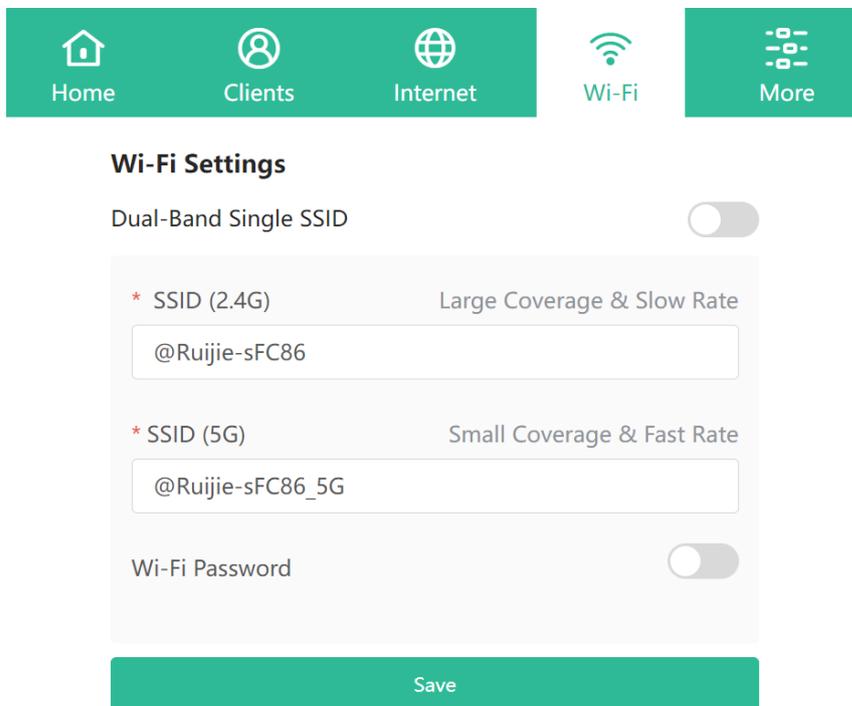
Mobile Phone: Choose **Wi-Fi > Wi-Fi Settings**. Click the target Wi-Fi network, change the SSID and password of the Wi-Fi network, and click **Save**.

---

 Note

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

---



**Wi-Fi Settings**

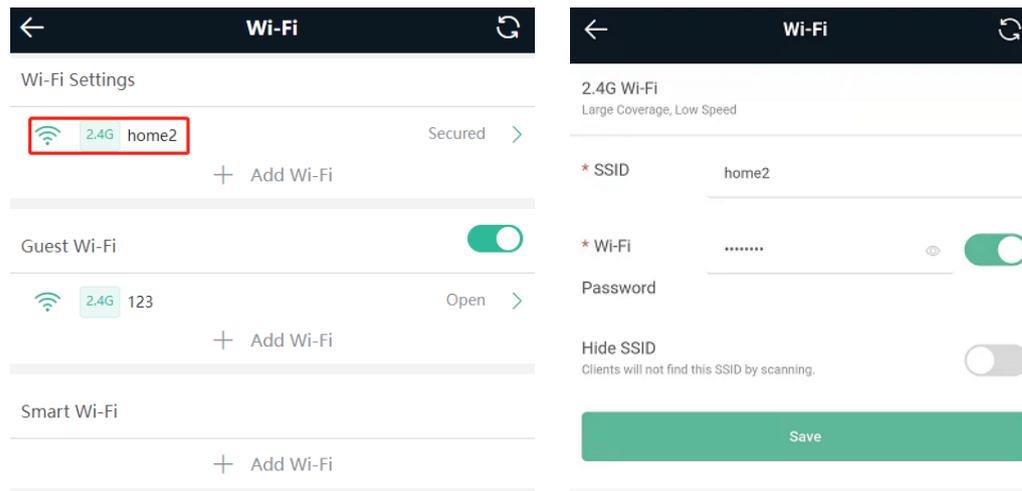
Dual-Band Single SSID

\* SSID (2.4G) Large Coverage & Slow Rate  
@Ruijie-sFC86

\* SSID (5G) Small Coverage & Fast Rate  
@Ruijie-sFC86\_5G

Wi-Fi Password

Save



## 4.2 Hiding the SSID

### 4.2.1 Overview

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

### 4.2.2 Getting Started

Remember the SSID so that you can enter the correct SSID after the function is enabled.

### 4.2.3 Configuration Steps

Choose **More> Wireless> Wi-Fi > Wi-Fi Settings > Expand**.

Enable **Hide SSID** and click **Save**.

---

#### Note

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

---

Wi-Fi Settings
Guest Wi-Fi
Smart Wi-Fi
Healthy Mode

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

### Wi-Fi Settings

\* SSID(2.4G)

Security

..... Collapse .....

Wireless Schedule

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

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

XPress  (The client will experience faster speed.)

---

#### i Instruction

You need to manually enter the SSID and password each time they connect to a hidden Wi-Fi network. An Android-based device is used as an example. To connect it to a hidden Wi-Fi network, choose **WLAN > Add network > Network name**, enter the Wi-Fi name, select **WPA/WPA2/WPA3** from the **Security** drop-down list, enter the password, and click **Connect**.

---

## 4.3 Adding a Wi-Fi Network

### 4.3.1 Overview

The router supports three types of Wi-Fi networks: master, guest, and smart Wi-Fi network. Only one Wi-Fi network type can be configured.

- **Master Wi-Fi:** The master Wi-Fi network is listed in the first line of the page and is enabled by default.
- **Guest Wi-Fi:** The guest Wi-Fi network is provided for guests and is disabled by default. It supports user isolation, that is, access users are isolated from each other. They can only access the Internet through Wi-Fi, but cannot access each other, improving security.

The guest Wi-Fi network can be disabled as scheduled. You can configure the guest Wi-Fi network to be disabled 1 hour later. When the time expires, the guest Wi-Fi network is disabled.

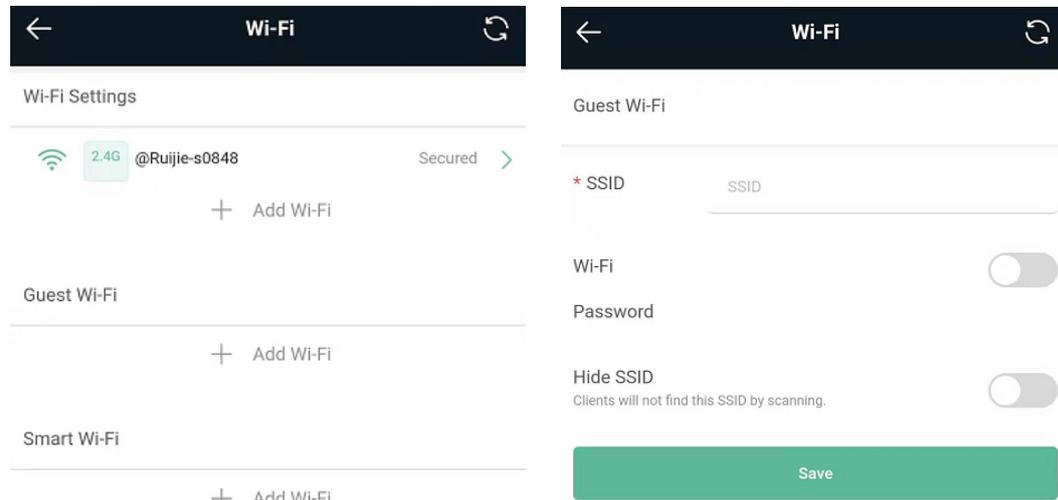
- **Smart Wi-Fi:** The smart Wi-Fi network is disabled by default. Smart clients can connect to the smart Wi-Fi network for a long time. The smart Wi-Fi network cannot be disabled as scheduled.

### 4.3.2 Configuration Steps

Mobile phone view: Choose **Wi-Fi > Wi-Fi Settings**.

The page displays the master Wi-Fi network, guest Wi-Fi network, and smart Wi-Fi network from top to bottom. Click **Add Wi-Fi** and set the SSID and password.

PC view: Choose **More > Wireless > Wi-Fi > Wi-Fi Settings/Guest Wi-Fi/Smart Wi-Fi**.



### 4.3.3 Verification and Testing

A client can search out the new Wi-Fi network, and the Wi-Fi page displays information about the new Wi-Fi network.



## 4.4 Configuring a Wi-Fi Blacklist or Whitelist

### 4.4.1 Overview

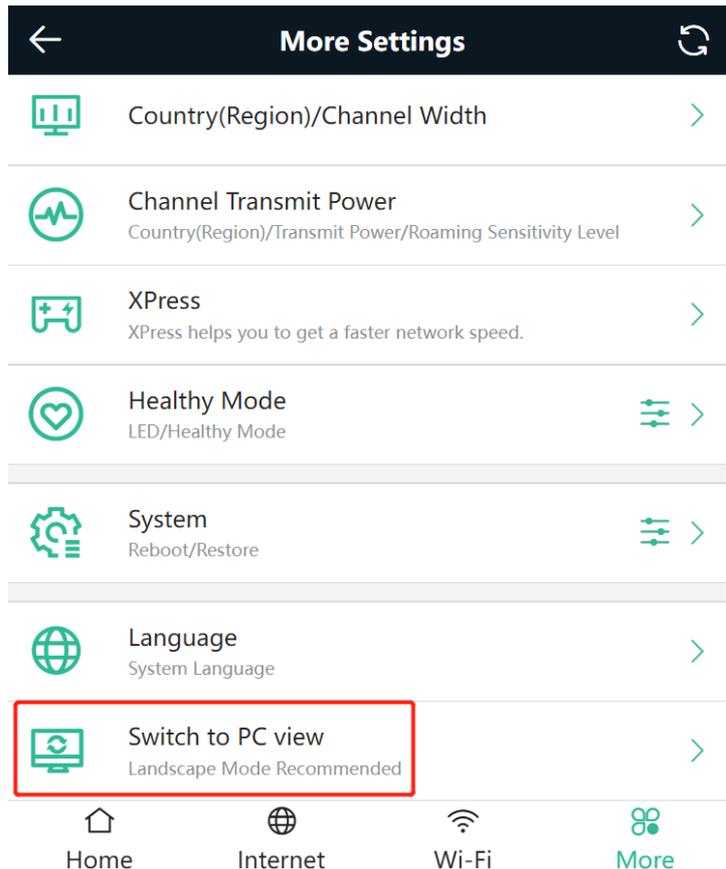
Wi-Fi blacklist: Clients in the Wi-Fi blacklist are prevented from accessing the Internet. Clients that are not added to the Wi-Fi blacklist are free to access the Internet.

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.

### 4.4.2 Configuration Steps

Mobile phone view: Choose **More > Switch to PC view > More > Wireless > Blacklist/Whitelist**.

PC view: Choose **More > Wireless > Blacklist/Whitelist**.



- (1) Select the blacklist mode and click **Add**. The default mode is blacklist.

In the displayed dialog box, enter the MAC address and remarks of the client to be blacklisted. The device displays information about the connected clients. Select a client. The client will be added to the blacklist automatically. Click **OK** to save the configuration. The client will be disconnected and prevented from connecting to the Wi-Fi network.

---

**Note**

The blacklist prevents some devices from connecting to the Wi-Fi network. Exercise caution when performing this operation.

---

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 30 members can be added.

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

< 1 > 10/page Total 0

Add ×

\* MAC

Example: 00:11:22:33:44:55

Please enter a MAC address.

- RainOS (30:0d:9e:3e:7e:be)
- PC-3e7ebe (52:54:00:3e:7e:be)
- ELZ-AN10 (82:26:75:da:ce:73)
- Honor\_10-a96f220e73c0a3f9 (c8:c2:fa:be:55:5d)

Cancel

OK

(2) Click **Delete**. The client can connect to the Wi-Fi network again.

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 30 members can be added.

<input type="checkbox"/>	MAC	Remark	Action
<input type="checkbox"/>	F2:36:1D:EB:20:6 D	test	Edit <span>Delete</span>

< 1 > 10/page Total 1

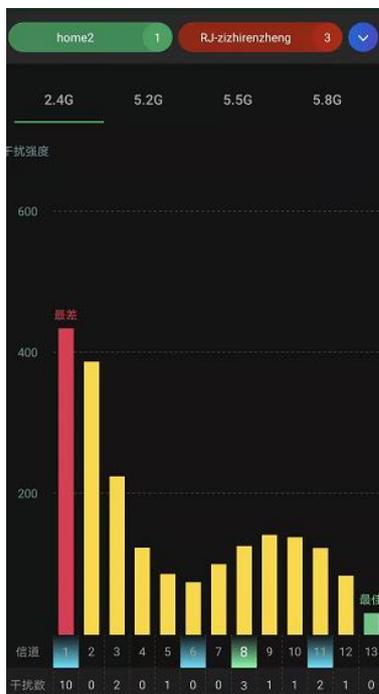
## 4.5 Optimizing the Wi-Fi Network

### 4.5.1 Overview

The device detects the surrounding wireless environment and selects the appropriate configuration upon power-on. However, network freezing caused by wireless environment changes cannot be avoided. Restarting the router is a convenient and effective method to cope with network freezing. The router supports scheduled restart. For details, see [6.6 Configuring Scheduled Reboot](#). You can also analyze the wireless environment around the router and select appropriate parameters.

### 4.5.2 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.



### 4.5.3 Configuration Steps

- Optimizing the radio channel

Mobile phone view: Choose **More** > **Channel Transmit Power**.

PC view: Choose **More** > **Wireless** > **Radio Frequency**.

Select the best channel identified by Wi-Fi Moho or other Wi-Fi scanning app. Click **Save** to make the configuration take effect immediately. Excess clients connected to a channel may result in stronger wireless interference.

---

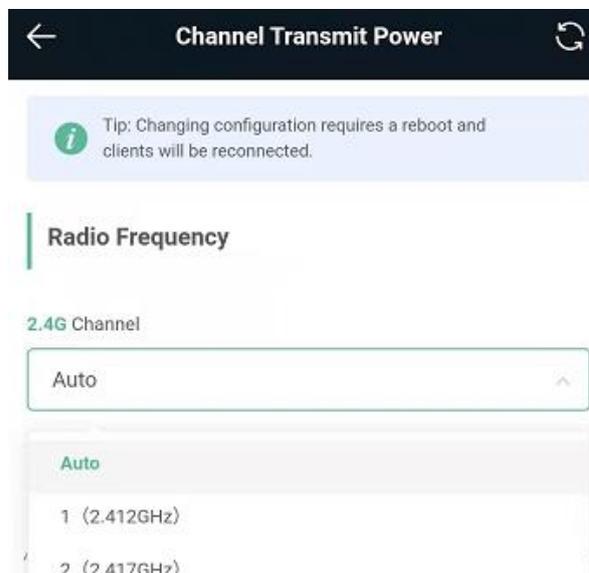
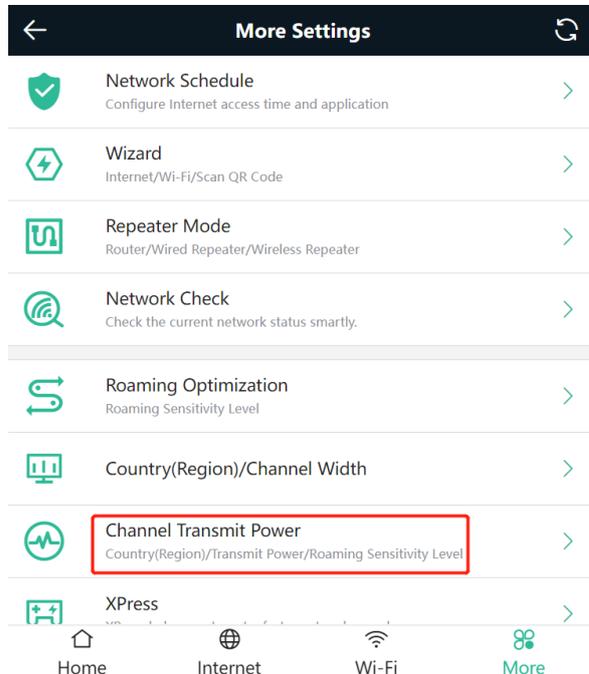
#### Instruction

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

---

**Note**

Settings of settings of the Wi-Fi network are reset after the radio channel is changed. Therefore, exercise caution when performing this operation.



- Optimizing the channel width

Mobile phone view: Choose **More**> **Country(Region)/Channel Width**.

PC view: Choose **More** > **Wireless** > **Radio Frequency**.

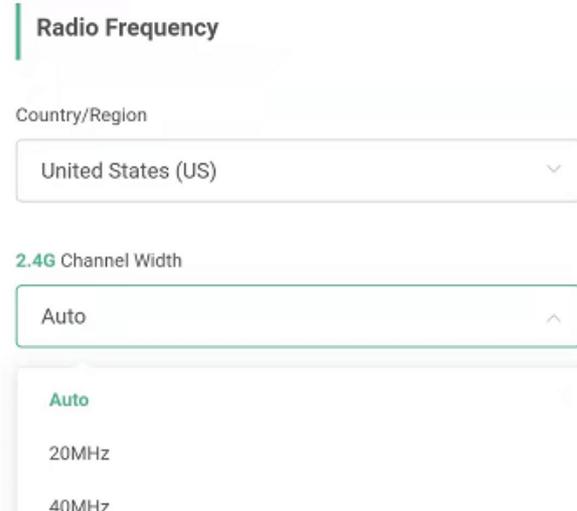
If the interference is severe, select a lower channel width to avoid network freezing. The router supports 20 MHz and 40 MHz channel width. You are advised to select 20 MHz channel width. After changing the channel width, click **Save** to make the configuration take effect immediately.

---

 **Note**

After the change, settings of settings of the Wi-Fi network are reset, and clients need to reconnect to the Wi-Fi network. Therefore, exercise caution when performing this operation.

---



**Radio Frequency**

Country/Region

United States (US)

**2.4G Channel Width**

Auto

Auto

20MHz

40MHz

- Optimizing the transmit power

Mobile phone view: Choose **More > Channel Transmit Power**.

PC view: Choose **More > Wireless > Radio Frequency**.

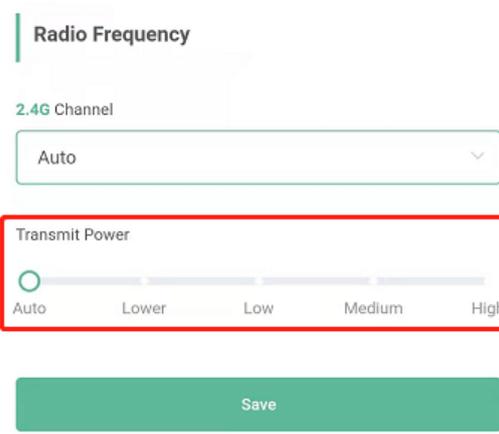
A greater transmit power indicates a larger coverage and brings stronger interference to surrounding wireless routers. The default value is **Auto**, indicating automatic adjustment of the transmit power. In a scenario in which routers are installed in centralized mode, a lower transmit power is recommended.

---

 **Note**

After the change, settings of settings of the Wi-Fi network are reset, and clients need to reconnect to the Wi-Fi network. Therefore, exercise caution when performing this operation.

---



**Radio Frequency**

**2.4G Channel**

Auto

**Transmit Power**

Auto Lower Low Medium High

Save

- (Optional) Configuring the roaming sensitivity

Mobile phone view: Choose **More > Roaming Optimization**.

PC view: Choose **More > Wireless > Radio Frequency**.

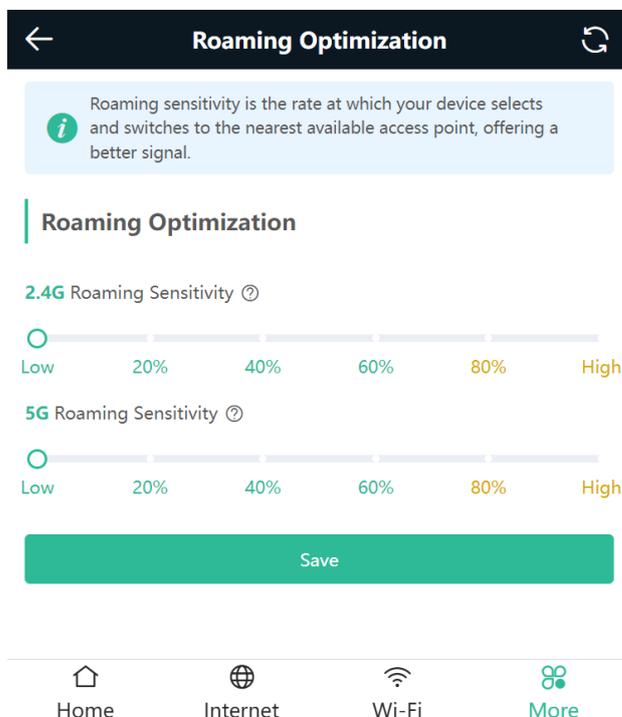
Clients such as mobile phones support the roaming function but the sensitivity level may be not high. The roaming sensitivity enables the device to proactively disconnect a client from the Wi-Fi network when the client is far away, forcing the client to re-select the nearest signal and thus improving the sensitivity of wireless roaming.

A low sensitivity is recommended.

#### Note

After the change, settings of settings of the Wi-Fi network are reset, and clients need to reconnect to the Wi-Fi network.

A high sensitivity may cause Wi-Fi network disconnection. Therefore, exercise caution when performing this operation.



## 4.6 Configuring the Healthy Mode

Mobile phone view: Choose **More > Healthy Mode > Healthy Mode**.

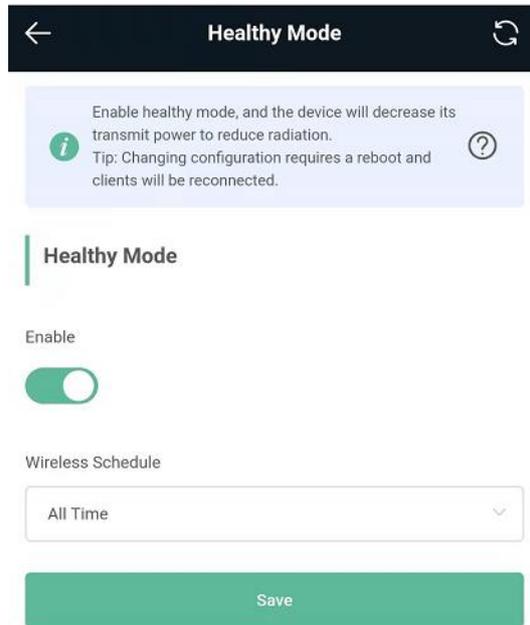
PC view: Choose **More > Wireless > Wi-Fi > Healthy Mode**.

Click **Enable** to enable the healthy mode. You are allowed to set the validity time 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 freezing. You are advised to disable it.

**i** Instruction

All Ruijie wireless routers have undergone stringent radiation detection and evaluation, and comply with IEC/EN62311, EN 50385, and other standards. Wi-Fi networks will not affect human health, and you can use Ruijie wireless routers safely.



## 4.7 Enabling Roaming Optimization

PC View: Choose **More > WLAN > Wi-Fi > Roaming Optimization**.

Mobile Phone View: Choose **More > Switch to PC view > More > WLAN > Wi-Fi > Roaming Optimization**.

Click **Enable** to enable Roaming Optimization. Terminal devices can connect to the new router to maintain their original Internet services.

Wi-Fi Settings   Guest Wi-Fi   Smart Wi-Fi   Healthy Mode   **Roaming Optimization**

### Roaming Optimization

Enable

Save

# 5 Reyee Networks Settings

## 5.1 Configuring Internet Connection Type

Mobile phone view: Choose **More** > **Switch to PC view** > **More** > **Basics** > **WAN**.

PC view: Choose **More** > **Basics** > **WAN**.

The router supports three Internet connection modes: PPPoE, DHCP, and static IP address. For details, see [3.2.1 Getting Started](#).

**Configure WAN settings.**

\* Internet  or DHCP clients.

IP

Subnet Mask

Gateway

DNS Server

[Advanced Settings](#)

**Save**

## 5.2 Changing the Address of a LAN Port

Mobile phone view: Choose **More** > **Switch to PC view** > **More** > **Basics** > **LAN**.

PC view: Choose **More** > **Basics** > **LAN**.

Change the IP address and subnet mask, and click **Save**. After the IP address of a LAN port is changed, you need to log in to Eweb by using the new IP address of the LAN port.

---

**Note**

Changing the IP address and subnet mask will disconnect the Wi-Fi network. You need to reconnect to the Wi-Fi network. Therefore, exercise caution when performing this operation.

---

LAN Settings   DHCP Clients   Static IP Addresses   DNS Proxy

---

**LAN Settings**

 The LAN port is configured with **An address conflict occurs..** The IP address is changed from **192.168.110.1** to **192.168.111.1** to ensure network connection.

\* IP

\* Subnet Mask

Remark

\* MAC

### 5.3 Changing the MAC Address

The ISP may restrict Internet access of devices with unknown MAC addresses to ensure security. In this case, you can change the MAC address of the WAN port to another address. You are advised to use the MAC address of an old router that is allowed to access the Internet (the MAC address can be found on the bottom label of the device).

Mobile phone view: Choose **More > Switch to PC view > More > Basics > WAN**.

PC view: Choose **More > Basics > WAN**.

Click **Advanced Settings**.

Enter the MAC address in the format of 00:11:22:33:44:55.

To change the MAC address of the LAN port, choose **Basics > LAN**.

---

 **Note**

Changing the MAC address of the LAN or WAN port will disconnect the router from the network. You need to reconnect to the router or restart the router. Therefore, exercise caution when performing this operation.

---

Figure 5-1 WAN Port Settings

**Configure WAN settings.**

\* Internet

No username or password is required for DHCP clients.

IP 172.26.1.118

Subnet Mask 255.255.255.0

Gateway 172.26.1.1

DNS Server 192.168.58.94 192.168.58.110

---

Advanced Settings

\* MTU

\* MAC

802.1Q Tag

**Save**

## 5.4 Changing the MTU

Sometimes, the ISP restrict the speed of large data packets or prevent large data packets from passing through. As a result, the network speed is low or even the network is disconnected. In this case, you are required to set the maximum transmission unit (MTU) to a smaller value.

Mobile phone view: Choose **More > Switch to PC view > More > Basics > WAN > Advanced Settings**.

PC view: Choose **More > Basics > WAN > Advanced Settings**.

The default MTU is 1500, which is the maximum value. You are advised to adjust the value to 1492, 1400, or even smaller if necessary.

**Configure WAN settings.**

\* Internet

No username or password is required for DHCP clients.

IP 172.20.141.106

Subnet Mask 255.255.255.0

Gateway 172.20.141.1

DNS Server 172.30.44.20 192.168.5.28

..... Advanced Settings .....

\* MTU

\* MAC

802.1Q Tag

**Save**

## 5.5 Configuring the Repeater Mode

---

**Caution**

Only the EW1200G-PRO and EW300-PRO support the WISP mode.

---

### 5.5.1 Wired Repeater

The wired repeater mode is available when the network cable provides reliable transmission over a more stable Wi-Fi network with less interference. You are advised to use the wired repeater mode. Ensure that the primary router can access the Internet with the DHCP server enabled. Otherwise, the configuration will take ineffective.

Choose **More > Switch to PC view > More > Basics > Repeater/WISP**.

Click **Wired Repeater**, click **Check**, and then click **Save**. The device will run in AP mode, namely, network address translation (NAT) and DHCP-related routing functions will be disabled.

---

**Note**

Ensure that the primary router can access the Internet with the DHCP server enabled. After the configuration is saved, settings of the Wi-Fi network are reset, and clients need to reconnect to the Wi-Fi network.

---

Figure 5-2 Wired Repeater Settings (1/2)

The device is working in **Router** mode. The following three modes are available:

Router
  **Wired Repeater**
 Wireless Repeater
  WISP



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

### Wired Repeater

Check

Figure 5-3 Wired Repeater Settings (2/2)

### Wired Repeater

Status **Cable Plugged**

IP Address: 172.26.1.118

\* Local Router SSID

Password

Save

## 5.5.2 Wireless Repeater

The wireless repeater mode extends the Wi-Fi coverage of the primary router.



#### Instruction

- The wireless repeater mode will affect the network speed and stability. You are advised to install a network cable and select the wired repeater mode if the network cable is available.
- In wireless repeater mode, remove the WAN cable to prevent loops, which may cause network interruption.
- Obtain the SSID and Wi-Fi password of the primary router.

Choose **More > Switch to PC view > More > Basics > Repeater/WISP**.

(1) Click **Wireless Repeater** and then click **Select**. A list of surrounding Wi-Fi signals appears.

The device is working in **Router** mode. The following three modes are available:

Router
  Wired Repeater
  **Wireless Repeater**
 WISP

**i**

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

**Please unplug the cable to avoid loops.**

## Wireless Repeater

### Primary Router

\* SSID

- (2) Select the Wi-Fi signal of the primary router and enter its Wi-Fi password. You can configure a new Wi-Fi network or use the same Wi-Fi network as that of the primary router.
- If you select **Same as Primary Router Wi-Fi**, Wi-Fi settings of the primary router are automatically synchronized to the current router. In most cases, clients merge Wi-Fi signals with the same SSID into one Wi-Fi signal, and they can search out only the Wi-Fi signal of the primary router.
  - If you select **New Wi-Fi**, you can set the local SSID and password. Clients will search out a Wi-Fi signal that is different from the Wi-Fi signal of the primary router.

**⚠ Note**

After the configuration is saved, the Wi-Fi network will be disconnected and you need to connect to the new Wi-Fi network. Exercise caution when performing this operation. Remember the new SSID and password.

**Figure 5-4 Selecting the Wi-Fi Signal of the Primary Router and Connecting to the Wi-Fi Network**

**2.4G Wi-Fi List** Select a target Wi-Fi.

Q SSID 2.4G

SSID	BSSSID	Security	Channel	RSSI
WiFi_77FC				High
<b>xiaoxi</b>	50:64:2b:0e:77:fd	WPA2PSK	3	-28 dBm High
WLS-PRO-140	02:0d:9e:85:bb:11	WPA2PSK	10	-49 dBm High
ruijie-802.1x	06:05:88:c6:65:c8	WPA2PSK	1	-57 dBm High
22222	46:0d:9e:e7:e9:18	WPAPSK	11	-64 dBm Medium
PPSKnettime	20:04:0e:7c:0:18	OPEN	11	-67 dBm

### Wireless Repeater

**Primary Router**

\* SSID

\* Wi-Fi Password

**Local Router**

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

\* SSID(2.4G)

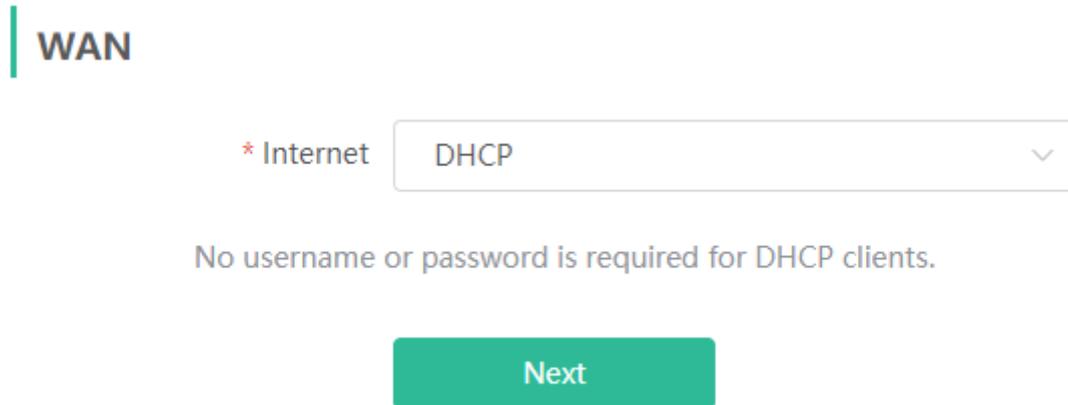
Wi-Fi Password

### 5.5.3 WISP

WISP allows users to establish their own WLANs for Internet access in public spaces, including coffee shops, hotels, airports, or restaurants.

- (1) Choose **More > Switch to PC view > More > Basics > Repeater/WISP**.

Click **WISP**, select an Internet connection mode, and click **Next**.



WAN

\* Internet

No username or password is required for DHCP clients.

Next

- (2) Click **Select**, select a Wi-Fi signal, and click **Save**. See "Selecting and Connecting to the Wi-Fi Network of the Primary Router."

 Note

After you click **Save**, settings of settings of the Wi-Fi network are reset. You need to connect to the new Wi-Fi network. Exercise caution when performing this operation. Remember the SSID and password.

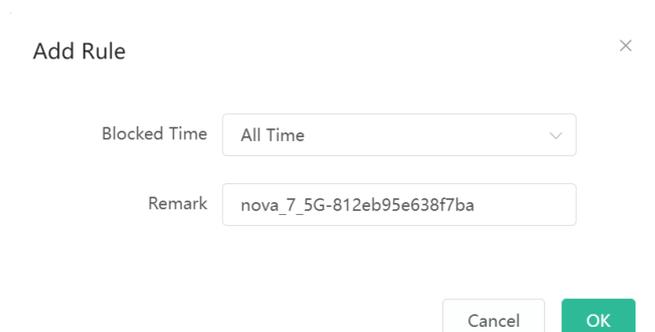
## 5.6 Controlling the Internet Access Time Range

Mobile phone view: Choose **More > Network Schedule**. Select a client and click **Schedule**. Click **Add** and set the time range in which Internet access is blocked. In the specified time range, the client is prevented from accessing the Internet.

PC view: Choose **Clients > Add Blocked Time**.

Select a client and click **Add Blocked Time**.

In the PC view, you can select **Weekdays** or **Weekends** to block Internet access of a client, or set **Blocked Time to Custom** and set a specific time range for blocking Internet access.

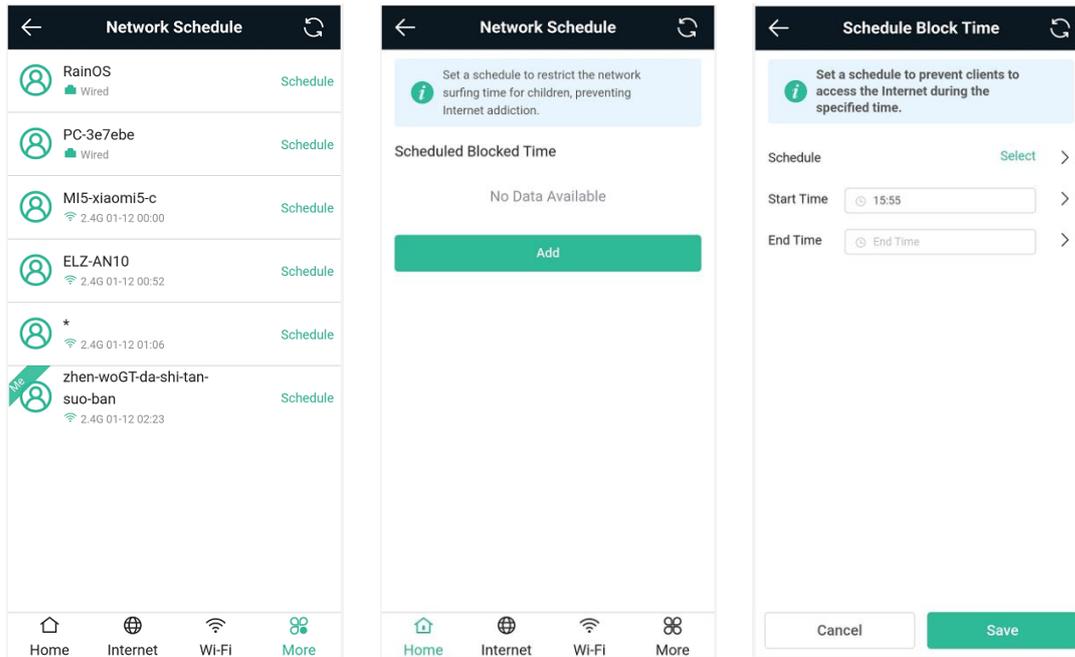


Add Rule ×

Blocked Time

Remark

Cancel OK

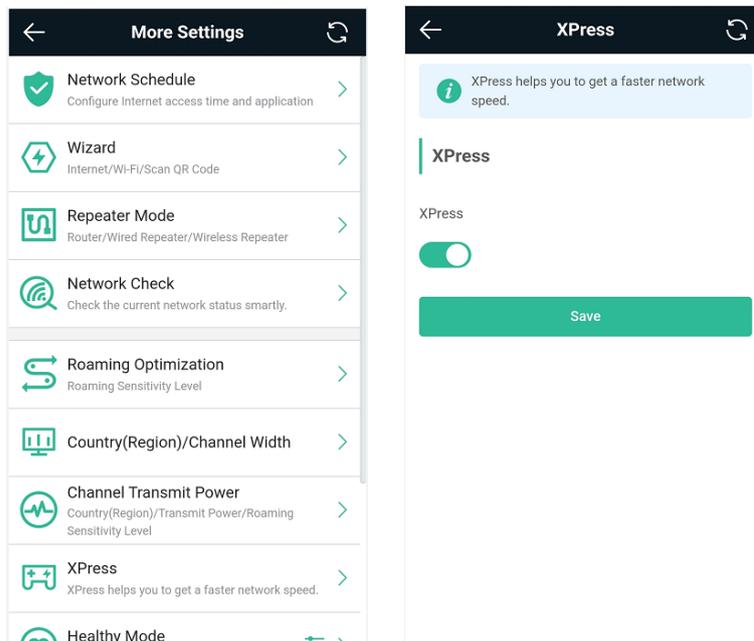


## 5.7 Configuring XPress

Mobile phone view: Choose **More** > **XPress**.

PC view: Choose **More** > **Wireless** > **Wi-Fi** > **Wi-Fi Setting** > **Expand** > **XPress**.

Enable **XPress** and click **Save** to save the configuration. After XPress is enabled, you will have a more stable gaming experience.



In the PC view, enable **XPress** as follows.

**Wi-Fi Settings**

\* SSID(2.4G)

Security

\* Wi-Fi Password

----- Collapse -----

Wireless Schedule

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

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

XPress  (The client will experience faster speed.)

## 5.8 Configuring Port Mapping

### 5.8.1 Overview

Port mapping maps the IP address of a device on the LAN to an external network in the form of a WAN IP address plus a port number, so as to provide the external network access service.

- Scenario 1: When you need to access IP cameras or PCs at home while you are away from home, port mapping needs to be configured.
- Scenario 2: When a server needs to be set up on the home network for Internet access, port mapping or demilitarized zone (DMZ) needs to be configured.

Port mapping maps the WAN port's IP address of a router to an internal network host and port so that Internet users can proactively access hosts on the LAN.

All packets are forwarded from the Internet to DMZ hosts to provide the Internet access service.

### 5.8.2 Getting Started

- Confirm the IP address of the target device on the internal network and service port ID.
- Ensure that port mapping is available on the internal network.

### 5.8.3 Configuration Steps

Mobile phone view: Choose **More > Switch to PC view > More > Advanced > Port Mapping**.

PC view: Choose **More > Advanced > Port Mapping**.

Click **Add**. In the displayed dialog box, enter the name, service type, protocol type, external port/range, internal IP address, and internal port/range. A maximum of 50 port mapping rules can be configured.

**Name:** Enter a name for ease of maintenance.

**Preferred Server:** Select a service to be mapped, such as HTTP or FTP. The device will automatically fill in the internal port number of the service. If the service is uncertain, you can select **Custom**.

**Protocol:** Select the transport-layer protocol used by the selected service, such as **ALL**, **TCP**, or **UDP**. The configuration on the server must be consistent with that on the client.

**External Port/Range:** Enter the port number used for external network access. You need to check the port number in software, such as camera monitoring software.

**Internal IP Address:** Enter the LAN IP address used by an extranet terminal to access the device, such as the IP address of an IP camera.

**Internal Port/Range:** Enter the port number used by an application, such as port 8080 used by the web service.

The screenshot displays the NAT-DMZ configuration interface. On the left, the 'Port Mapping List' is empty, with an 'Add' button highlighted in red. On the right, the 'Add' form is open, showing the following fields:

- Name:** test
- Preferred Server:** HTTP
- Protocol:** TCP
- External IP Address:** 172.26.1.118
- External Port/Range:** Example: X or X-X (Range: 1-6553!). Error: Please enter an external port.
- Internal IP Address:** Example: 1.1.1.1. Error: Please enter an internal IP address.
- Internal Port/Range:** Example: X or X-X (Range: 1-6553!). Error: Please enter an internal port.

Buttons for 'Cancel' and 'OK' are visible at the bottom right of the form.

## 5.8.4 Verification and Testing

Use an external device to test whether the destination service is accessible based on the external IP address and port number.

## 5.8.5 Solution to a Test Failure

- (1) Use a new external port number and perform a test again. The test often fails on the ports blocked by firewalls of some ISPs.
- (2) Enable the remote access permission on a server. The common cause is that remote access is disabled on the server by default. As a result, intranet access is successful but the access across different network segments fails.
- (3) Enable the DMZ service. For details, see [5.8.6 DMZ Configuration Steps](#). The common cause is that port configuration is incorrect or incomplete.

## 5.8.6 DMZ Configuration Steps

Mobile phone view: Choose **More** > **Switch to PC view** > **More** > **Advanced** > **Port Mapping** > **NAT-DMZ**.

PC view: Choose **More** > **Advanced** > **Port Mapping** > **NAT-DMZ**.

Click **Enable**, enter the IP address of the internal server, and click **Save**.

Port Mapping **NAT-DMZ**

---

**i** NAT-DMZ

Enable

\* Dest IP Address

Please enter a destination IP address.

Save

## 5.9 Configuring the DHCP Server

### 5.9.1 Overview

The DHCP server function enables a router to automatically assign IP addresses to clients so that clients connected to the LAN ports or Wi-Fi network of the router obtain IP addresses for Internet access. When multiple routers are connected through LAN ports, a DHCP server conflict may occur. In this case, you need to disable the DHCP server function and enable the DHCP service on one router only. Otherwise, some devices may be disconnected from the network.

### 5.9.2 Configuration Steps

#### 1. Configuring the DHCP Server Function

Mobile phone view: Choose **More > Switch to PC view > More > Basics > LAN > LAN Settings**.

PC view: Choose **More > Basics > LAN > LAN Settings**.

**DHCP Server:** The DHCP server function is enabled by default. You are advised to enable it when only a single router is used. When multiple routers are connected to the primary router through LAN ports, disable this function.

---

 Note

If the DHCP server function is disabled on all routers on the network, clients cannot automatically obtain IP addresses. In this case, you need to enable the DHCP server on a router 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, the client will fail to obtain the IP address.

**IP Count:** Enter the number of IP addresses in the address pool. The default value is **254**.

**Lease Time (Min):** Enter the address lease time. When a client keeps connected, the lease is automatically renewed. If a lease is not renewed due to client disconnection or network instability, the IP address will be reclaimed after the lease time expires. After the client is re-connected, the client requests an IP address again. The default lease time is 30 minutes.

[LAN Settings](#)   [DHCP Clients](#)   [Static IP Addresses](#)   [DNS Proxy](#)

**LAN Settings**

*i* The LAN port is configured with **An address conflict occurs..** The IP address of the LAN port to ensure network connection.

\* IP

\* Subnet Mask

Remark

\* MAC

DHCP Server

\* Start

\* IP Count

\* Lease Time(Min)

[LAN Settings](#)   [DHCP Clients](#)   [Static IP Addresses](#)   [DNS Proxy](#)

**LAN Settings**

\* IP

\* Subnet Mask

\* MAC

DHCP Server

\* Start

\* IP Count

\* Lease Time(Min)

## 2. Displaying Online DHCP Clients

Mobile phone view: Choose **More** > **Switch to PC view** > **More** > **LAN** > **DHCP Clients**.

PC view: Choose **More** > **LAN** > **DHCP Clients**.

Check information about an online client. Click **Convert to Static IP** and click **OK**. Then the client obtains the IP address each time when it connects to the router.

LAN Settings   DHCP Clients   Static IP Addresses   DNS Proxy

*i* View DHCP clients. ?

**DHCP Clients**   Search by Hostname/IP/MAC

Up to 300 IP-MAC bindings can be added.

<input type="checkbox"/>	No.	Hostname	IP	MAC	Remaining Lease Time(Min)	Status
<input type="checkbox"/>	1	RainOS	192.168.111.18	30:0d:9e:3c:d6:be	24	<span style="border: 1px solid red; padding: 2px;">Convert to Static IP</span>
<input type="checkbox"/>	2	PC-3CD6BE	192.168.111.53	52:54:00:3c:d6:be	17	Convert to Static IP
<input type="checkbox"/>	3	*	192.168.111.176	f2:36:1d:eb:20:6d	22	Convert to Static IP

< 1 >   10/page   Total 3

## 3. Displaying the DHCP Static IP Address Table

Mobile phone view: Choose **More** > **Switch to PC view** > **More** > **LAN** > **Static IP Addresses**.

PC view: Choose **More** > **LAN** > **Static IP Addresses**.

Click **Add**. In the displayed static IP address dialog box, enter the MAC address and IP address of the target client, and click **OK**. After a static IP address is bound, the client obtains the IP address each time when it connects to the router.

LAN Settings   DHCP Clients   Static IP Addresses   DNS Proxy

*i* Static IP Address List ?

**Static IP Address List**   Search by IP/MAC

Up to 300 entries can be added.

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

< 1 >   10/page   Total 0

Add ×

\* IP

\* MAC

Cancel

OK

## 5.10 Configuring DNS

The domain name system (DNS) proxy configuration is optional. The device obtains the DNS server address from the uplink device by default.

Mobile phone view: Choose **More** > **Switch to PC view** > **More** > **LAN** > **DNS Proxy**.

PC view: Choose **More** > **LAN** > **DNS Proxy**.

**DNS Proxy:** The function is disabled by default and the DNS configuration delivered by a carrier is used. If the DNS configuration is incorrect, the network is accessible and the mobile app can access the Internet properly, but the web page cannot be opened. You are advised to disable the function.

**DNS Server:** Clients automatically use the DNS service provided by the primary router by default. The default configuration is recommended. When the DNS proxy function is enabled, you can enter the IP address of the DNS server. The available DNS service varies depending on the region. You can consult the local ISP.

LAN Settings   DHCP Clients   Static IP Addresses   **DNS Proxy**

 DNS proxy is not required. The device will obtain the DNS server address from the uplink device by default.

Enable

\* DNS Server

Save

## 5.11 Configuring DDNS

### 5.11.1 Overview

After the dynamic domain name service (DDNS) is enabled, you can use a fixed domain name on the Internet to access service resources of the router without checking the IP address of the WAN port. To make the service available, you need to register an account and domain name with a third-party DNS service provider. The router supports PeanutHull, Dyn DNS, and No-IP DNS.

### 5.11.2 Getting Started

Register an account and domain name at PeanutHull or No-IP official website.

### 5.11.3 Configuration Steps

Mobile phone view: Choose **More > Switch to PC view > More > Advanced > Dynamic DNS > Dynamic DNS**.

PC view: Choose **More > Advanced > Dynamic DNS > Dynamic DNS**.

Peanut Shell NAT is a more advanced version of DDNS and can be used when an intranet IP address is configured for the WAN port. Peanut Shell NAT is recommended. Click **Enable** and then click **Save**. The service status and QR code for login appear in the lower part of the page. Scan the QR code to log in by using WeChat or PeanutHull app (the QR code shown in the figure below is unavailable. Scan the QR code displayed on your device).

If you select **Peanut Shell NAT**, **Dynamic DNS**, **No-IP DNS**, or **DynDNS**, enter the registered account and password, and click **Log In**. The connection status and domain name will be displayed in the lower part of the page.

The screenshot displays the router's configuration interface for Dynamic DNS. It features a navigation bar with tabs for 'Peanut Shell NAT', 'Dynamic DNS', 'No-IP DNS', and 'DynDNS'. The 'Dynamic DNS' tab is selected. Below the tabs, there is a blue information box stating: 'It is recommended to use Peanut Shell for NAT, including TCP, UDP, HTTP and HTTPS mapping.' The main configuration area includes an 'Enable' toggle switch (which is turned on), a green 'Save' button, and a 'Service Status' dropdown menu. A 'Scan to Login' section contains a QR code. Below this, there are input fields for '\* Username' and '\* Password', followed by 'Log In' and 'Delete' buttons. At the bottom, there are 'Link Status' and 'Domain' dropdown menus.

## 5.12 Configuring APR Binding and ARP Guard

### 5.12.1 Overview

The router learns the ARP table from all devices connected to its ports. You can search for a device by its MAC address, perform ARP binding, and enable ARP guard to improve network security.

### 5.12.2 Configuration Steps

- (1) Binding ARP information

Mobile phone view: Choose More > Switch to PC view > More > Security> ARP List

PC view: Choose **More > Security> ARP List**

ARP binding means binding of IP addresses and MAC addresses on the LAN.

**ARP Guard**

Enable  Only the devices configured with IP-MAC binding are allowed to access the Internet.

**ARP List**

Up to **64** IP-MAC bindings can be added.

No.	MAC	IP	Type	Action
1	f2:36:1d:eb:20:6d	192.168.111.176	Dynamic	Bind
2	30:0d:9e:7e:13:a1	172.26.1.1	Dynamic	Bind
3	52:54:00:3c:d6:be	192.168.111.53	Dynamic	Bind

Total 3 | 10/page | 1 | Go to page 1

## (2) Enabling ARP guard

Enable **ARP Guard** and then click **OK**. After ARP guard is enabled, only clients whose IP address and MAC address are bound are allowed to access the Internet.

### Note

Enabling this function will disconnect some devices from the network. Therefore, exercise caution when performing this operation.

## 5.13 Configuring Static Routing

### Note

Only EW3000GX PRO supports this function.

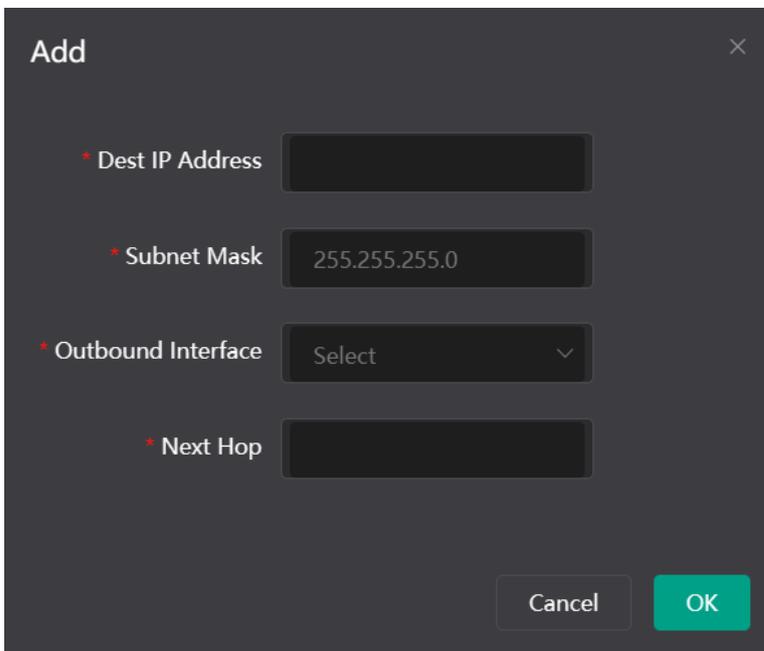
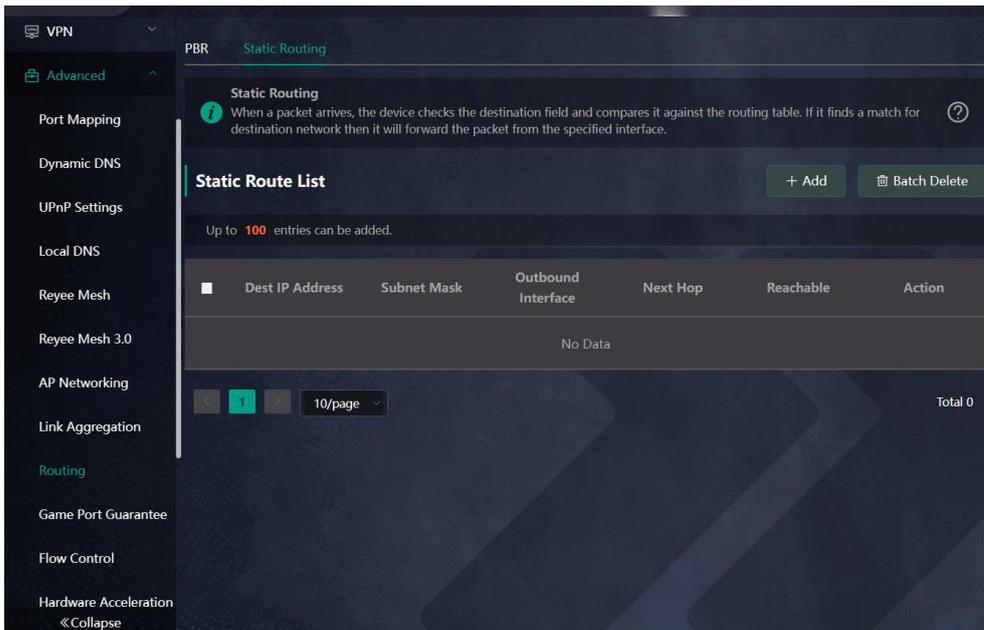
Smartphone View: Choose **More > Switch to PC view > More > Advanced > Routing > Static Routing**.

PC View: Choose **More > Advanced > Routing > Static Routing**.

### Caution

Static routing does not automatically adapt to changes in network topology, and need to be reconfigured manually when the network topology changes.

Click **Add**, enter the destination IP address, subnet mask, outbound interface and next-hop IP address to create a static route.



**Table 5-1 Description of Static Routing Configuration**

Parameter	Description
Dest IP Address	The destination network of the packet. The destination IP address of the packet is matched based on the destination IP address and subnet mask.
Subnet Mask	The subnet mask of the destination network. The destination IP address of the packet is matched based on the destination IP address and subnet mask.
Outbound Interface	Interface over which packets are forwarded.

Parameter	Description
Next Hop	The IP address of the next-hop router to which the packet will be sent. If the outbound interface is a PPPoE interface, there is no need to configure the next-hop IP address.

After a static route is created, you can view the configuration details and reachability of the route in the static route list on the **Static Routing** page. The **Reachable** column indicates whether the next hop is reachable, so as to determine whether the route can take effect normally. If **Unreachable** is displayed, check whether the next-hop address is reachable by the outbound interface of the current route by performing a ping test.

## 5.14 Policy-based Routing

### Note

Only EW3000GX PRO supports this function.

Smartphone View: Choose **More** > **Switch to PC view** > **More** > **Advanced** > **Routing** > **PBR**.

PC View: Choose **More** > **Advanced** > **Routing** > **PBR**.

### 1. Overview

Policy-based routing is a routing mechanism using user-specified policies. When the router forwards a packet, it first filters the packet according to the configured rules, and if the rules are hit, the packet is forwarded according to a certain forwarding policy. You can formulate routing rules based on specific fields (source/destination IP, protocol type) in the packet and forward it from a specific interface.

In the multi-line scenario, if a device is connected to both the Internet and the intranet through different lines, if no routing settings are made, traffic will be routed in a balanced way by default, and packets destined for the intranet may be mistakenly sent to the Internet, and vice versa, which may lead to network abnormality.

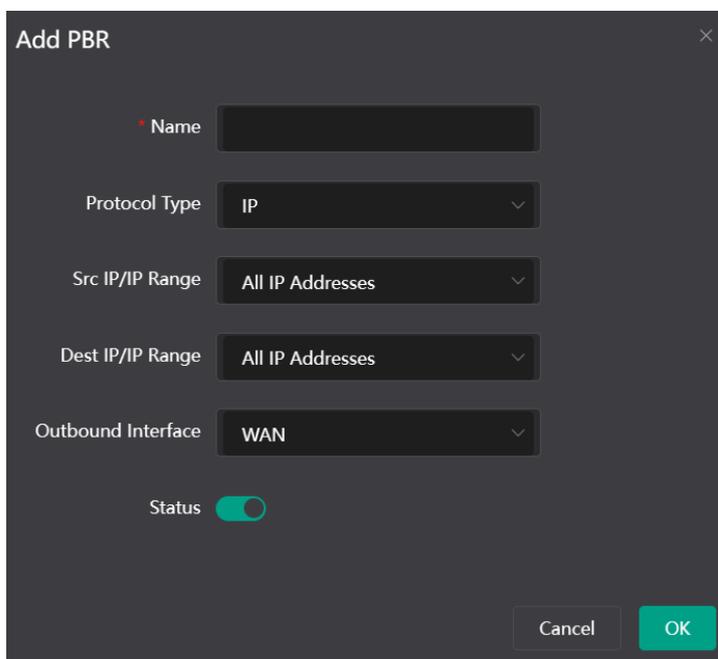
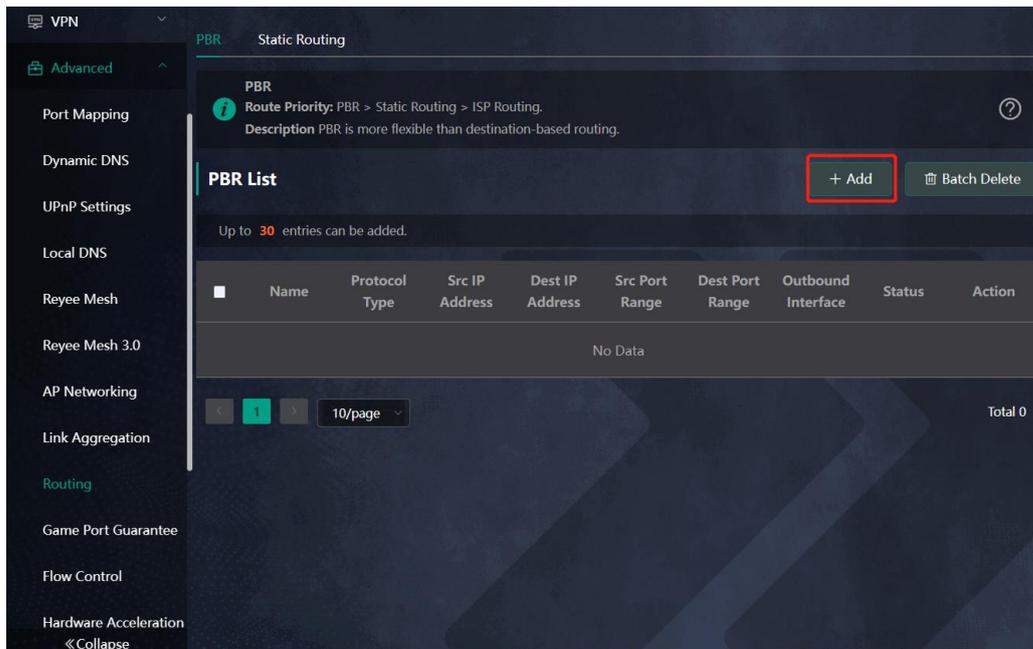
Therefore, it is necessary to configure policy-based routes for segregated packet forwarding between the Internet and the intranet.

This router supports three routing policies, namely, PBR, ISP routing, and static routing. In case all three routing policies are present, the priority is: policy-based routing > static routing > ISP routing.

## 2. Configuration Steps

PC View: Choose **Advanced > Routing > PBR**.

Click **Add** to add a PBR rule.



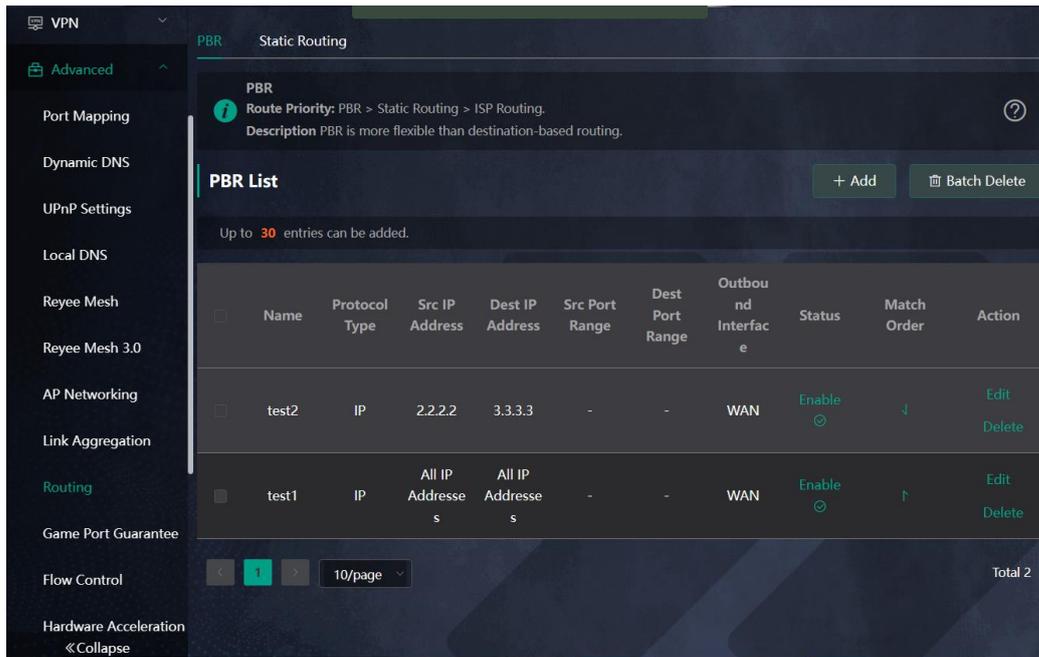
**Table 5-2 Description of Policy-based Routing**

Parameter	Description
Name	The name of the PBR rule, as the identifier of the PBR route. The name must be unique.
Protocol Type	The protocol for the PBR route to take effect, which can be IP, ICMP, UDP, TCP, or a custom protocol type as needed.
Protocol Number	When the protocol type is <b>Custom</b> , the protocol number is required.
Src IP/IP Range	The source IP/IP range to which the PBR rule matches. By default, <b>All IP</b> is selected. <ul style="list-style-type: none"> <li>● All IP: Matches all source IP addresses.</li> <li>● Custom: Matches source IP addresses in the specified range.</li> </ul>
Custom Src IP	The source IP address or range is required when the matching source IP/IP range is <b>Custom</b> .
Dest IP/IP Range	The destination IP/IP range to which the PBR rule matches. By default, <b>All IP</b> is selected. <ul style="list-style-type: none"> <li>● All IP: Matches all destination IP addresses.</li> <li>● Custom: Matches destination IP addresses in the specified range.</li> </ul>
Custom Dest IP	The destination IP address or range is required when the matching destination IP/IP range is <b>Custom</b> .
Src Port Range	This field is displayed only when the protocol type is <b>TCP</b> or <b>UDP</b> . The value in this field is the source port range matching the PBR route.
Dest Port Range	This field is displayed only when the protocol type is <b>TCP</b> or <b>UDP</b> . The value in this field is the destination port range matching the PBR route.
Outbound Interface	Interface over which packets hit the PBR rule are forwarded.
Status	You can enable or disable the toggle switch next to <b>Status</b> to enable or disable the PBR rule.

**Note**

To restrict an access device to access only a specific intranet, you can specify the outbound interface of the PBR route as the WAN port for the private network.

The **PBR List** shows the created PBR routes, which are prioritized from top to bottom. Newly added PBR routes are at the top of the list and are prioritized. You can manually adjust the priority of PBR routes in the **Match Order** column, or click **Match Order** to set the priority for a PBR route.



## 5.15 Connecting to IPTV

Internet Protocol Television (IPTV) is provided by ISPs.

### 5.15.1 Getting Started

- Check whether the IPTV service has been provisioned.
- Check whether the local IPTV service is of the VLAN or Internet Group Management Protocol (IGMP) type. If the VLAN type is used, confirm the VLAN ID. If the IPTV type is unknown, contact your local ISP.

### 5.15.2 IPTV Configuration Steps (VLAN Type)

Mobile phone view: Choose **More > Switch to PC view > More > Basics > IPTV/VLAN**

PC view: Choose **More > Basics > IPTV/VLAN**

Select the local ISP mode, click the drop-down list of the target port, select **IPTV** from the drop-down list, and enter the VLAN ID provided by the ISP. For example, connect an IPTV set top box (STB) to LAN3 and set the VLAN ID to 2. The configuration is shown in the figure below.

**Internet VLAN:** If a VLAN ID needs to be set for the Internet access service, enable the Internet VLAN function and enter a VLAN ID. The VLAN tag function is disabled by default. You are advised to disable the function unless in special cases.

After the configuration, confirm that the IPTV STB is connected to the specified port properly. In the following figure, the IPTV STB is connected to LAN3.

#### Note

Enabling this function will disconnect some devices from the network. Therefore, exercise caution when performing this operation.

 IPTV/VLAN settings.

### IPTV/VLAN

\* Mode

\* LAN1

\* LAN2

\* LAN3

Internet VLAN  802.1Q Tag

### 5.15.3 IPTV Configuration Steps (IGMP Type)

Mobile phone view: Choose **More** > **Switch to PC view** > **More** > **Basics** > **IPTV**.

PC view: Choose **More** > **Switch to PC view** > **More** > **Basics** > **IPTV**.

The configuration applies to Vietnam FPT ISP. After IPTV of the IGMP type is enabled, connect the IPTV STB to any LAN port of the router.

[IPTV/VLAN](#) [IPTV/IGMP](#)

 IPTV/IGMP (for Vietnam FPT ISP)

### IPTV/IGMP

Enable

---

 **Caution**

The EW1200 does not support the IGMP type.

---

## 5.16 Configuring Wi-Fi/IGMP

### 5.16.1 Overview

In China Broadnet's centralized procurement, IPTV services rely on multicast streaming. However, when it comes to wireless drivers, multicast packets are forwarded at a lower fixed rate of either 6 Mbps or 24 Mbps. This means that if a large number of multicast packets are forwarded at this lower rate, they can end up using up a significant amount of air interface resources and causing congestion, which in turn leads to an abundance of packet loss. All of this can significantly impact the user experience and make streaming slow.

When it comes to routers, the terminals connected to them are fixed, so multicast packets only need to be forwarded to specific terminals. By enabling WIFI/IGMP and converting the multicast packets into unicast packets, the packets can then be forwarded to the designated terminals in the multicast group table. This approach minimizes congestion caused by low rate multicast.

### 5.16.2 Configuration Steps

Mobile phone view: Choose **More > Switch to PC view > More > Basics > IPTV> Wi-Fi/IGMP**.

PC view: Choose **More > Basics > IPTV> Wi-Fi/IGMP**.

#### Note

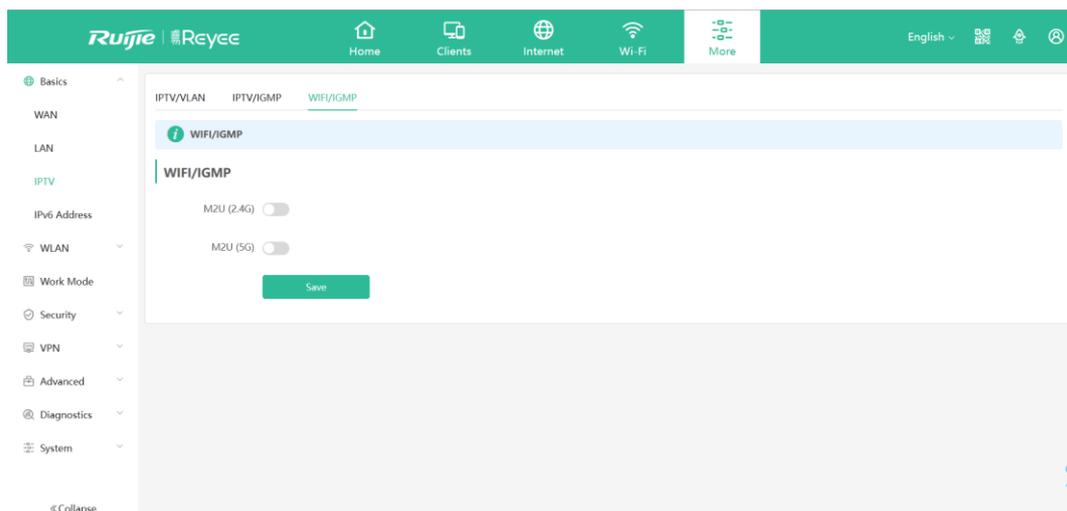
Select the method to configure EW3000GX PRO:

Smartphone View: Choose More > Switch to PC view > More >  WLAN > Wi-Fi > Wi-Fi/IGMP.

PC View: Choose **More >  WLAN > Wi-Fi > Wi-Fi/IGMP**

Click M2U(2.4G) to enable WIFI/IGMP for 2.4G wireless clients.

ClickM2U(5G) to enable WIFI/IGMP for 5G wireless clients.



## 5.17 Configuring IPv6

### Caution

This feature is supported in router mode.

With the popularity of the network, the IPv4 address fails to meet demands. The 128-bit IPv6 solves the problem of IPv4 address exhaustion.

Smartphone View: Choose **More** > **Switch to PC** > **More** >  **Basics** > **IPv6 Address**

PC View: **More** >  **Basics** > **IPv6 Address**

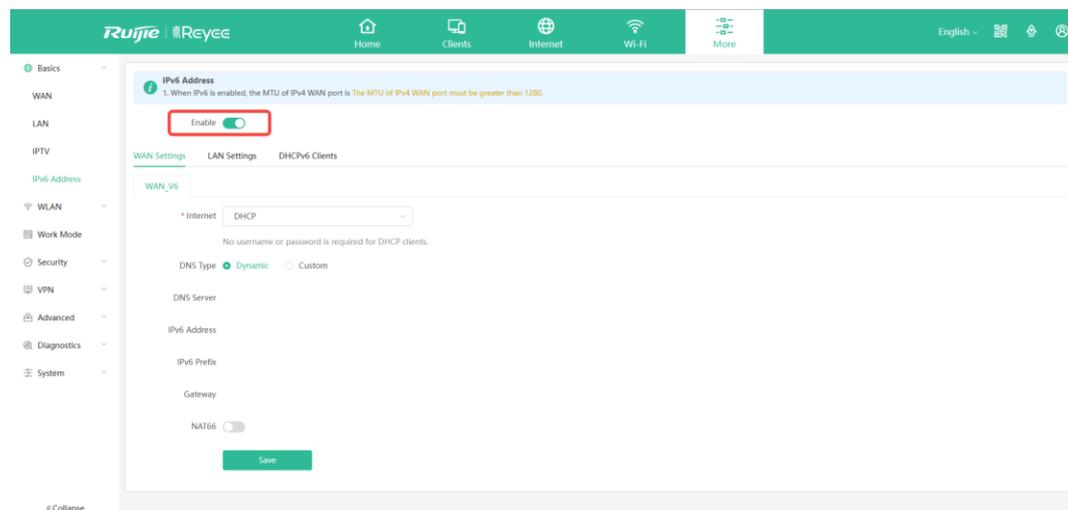
### 5.17.1 Configuring the IPv6 of the WAN Port

Internet Connection Type: If you select **DHCP**, and the device will get an IPv6 from the upstream device. If you select **Static IP**, please configure the IPv6, gateway address and DNS server address manually. If you select **NULL**, the IPv6 function will be disabled on the WAN port.

If the DHCP mode fails, turn on **NAT66** and try again. If the fault persists, you are advised to consult the local ISP about the IPv6 status of the network.

### Caution

- When IPv6 is enabled, The MTU of IPV4 WAN port need higher than 1280.



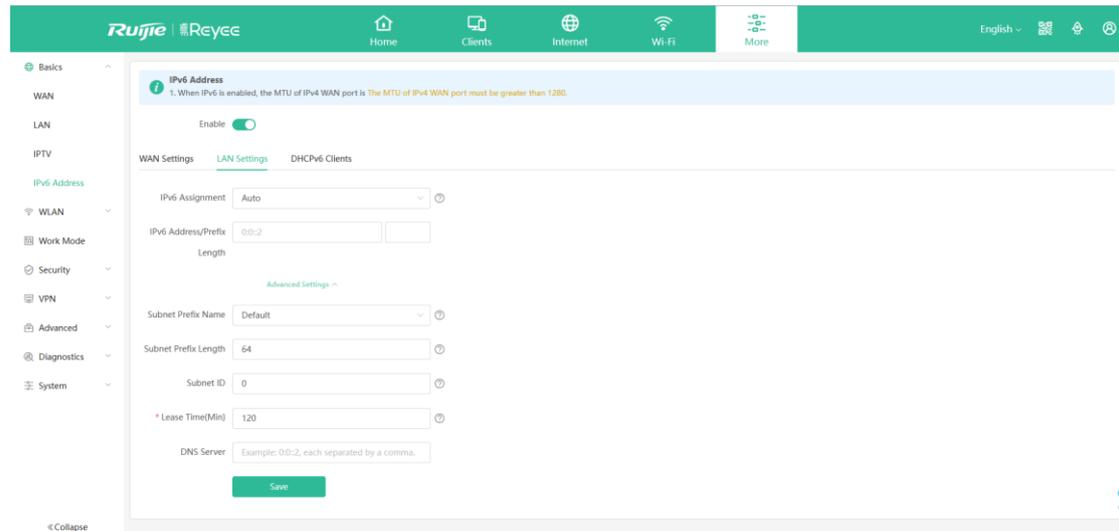
### 5.17.2 Configuring the IPv6 of the LAN Port

Click **LAN Settings**.

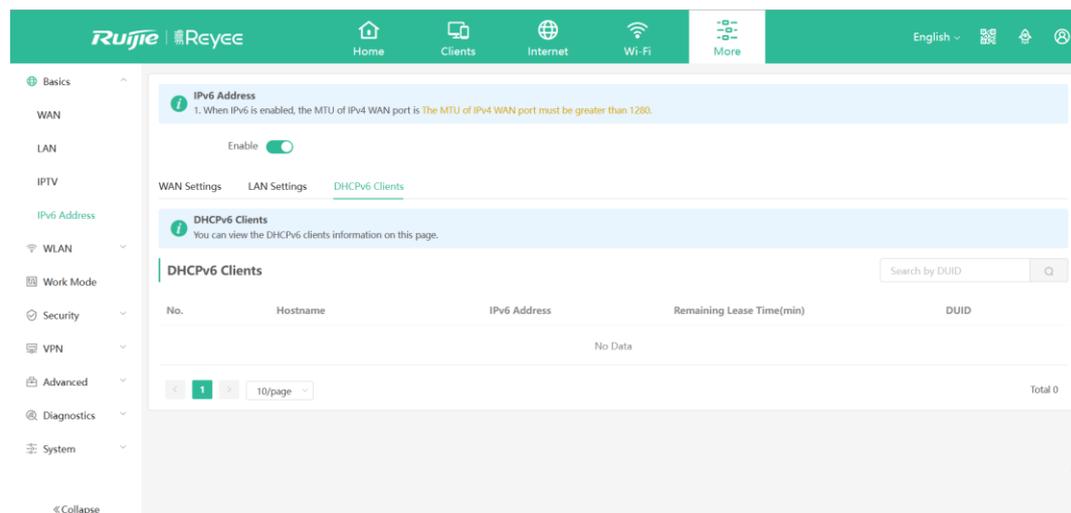
**IPv6 Assignment:** Choose **Auto** to use both DHCPv6 mode and SLAAC mode to allocate address. Choose **Null** to assign no address. You are advised to choose **Auto**.

**IPv6/Prefix Length:** If the router fails to obtain an IPv6 prefix, you can configure one manually. Set the subnet prefix length to a value smaller than or equal to 64.

Click **Advanced Settings** to perform the advanced settings. See the following figure for the recommended configuration.



Click **DHCPv6 Clients** to view the list of clients that have obtained IPv6 from the router.



## 5.18 Enabling Smart Flow Control

Smartphone View: Choose **More** > **Switch to PC view** > **More** >  **Advanced** > **Flow Control** > **Smart Flow Control**.

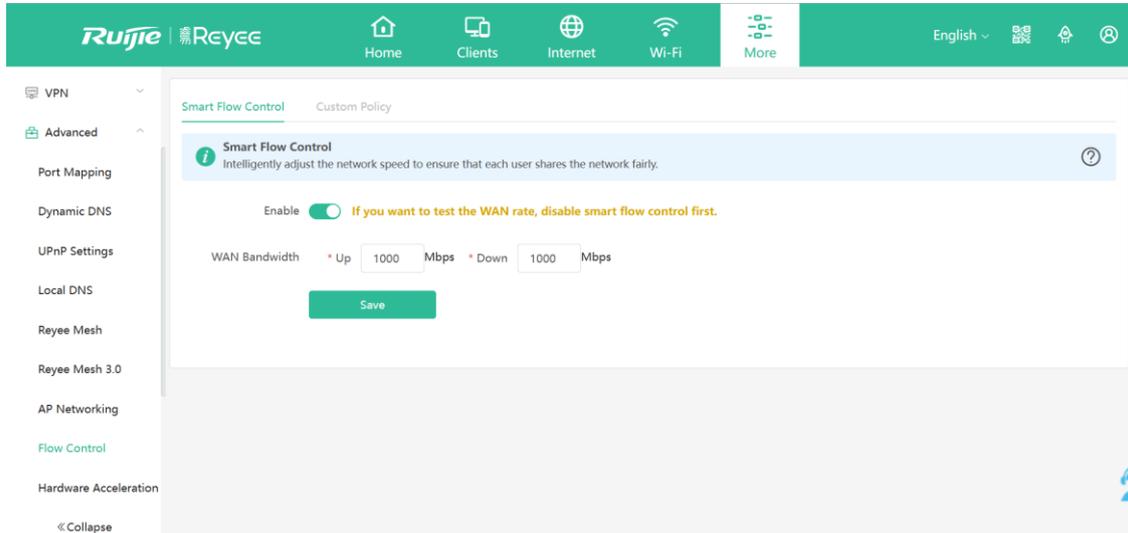
PC View: Choose **More** >  **Advanced** > **Flow Control** > **Smart Flow Control**.

### 1. Enabling Smart Flow Control

Click **Enable** and set the network bandwidth provided by the ISP. After the configuration is saved, the router adjusts the bandwidth of each client based on the total bandwidth to prevent any one client from occupying too much bandwidth.

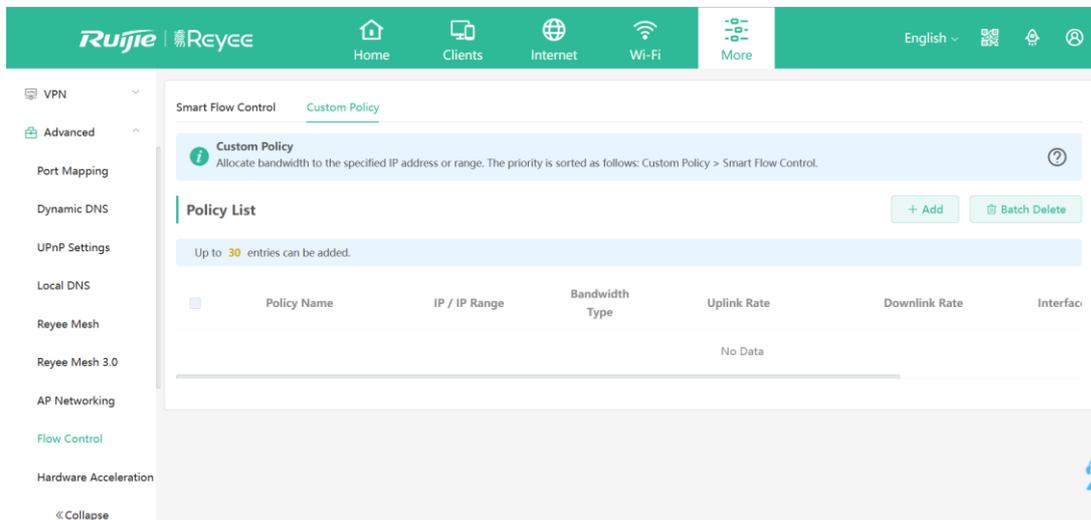
**⚠ Caution**

After smart flow control is enabled, speed measurement will be affected. Disable flow control if you want to do speed measurement.



## 2. Custom Policy

You can configure custom policies to allocate bandwidth to specific IP addresses/ranges to meet the bandwidth needs of specific users or servers. Click **Add** on the **Custom Policy** page to set the policy name, specific IP address/range, bandwidth type, and uplink/downlink rates.



## 5.19 Configuring Firewall

**⚠ Caution**

This feature is supported in router mode.

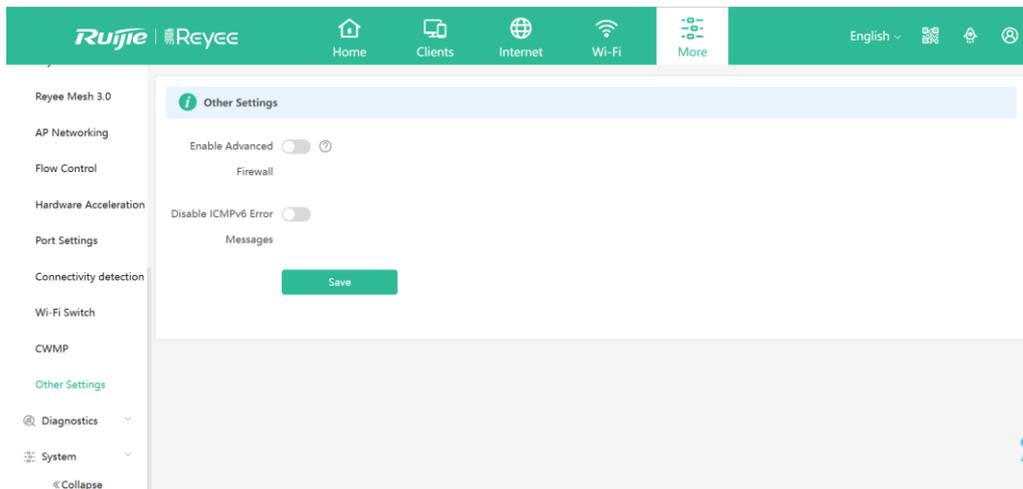
Smartphone View: Choose **More** > **Switch to PC view** > **More** >  **Advanced** > **Other Settings**.

PC View: Choose **More** >  **Advanced** > **Other Settings**.

The functions are disabled by default. You are advised to keep them disabled if there are no special requirements.

**Enable Advanced Firewall:** Advanced firewall is enabled to prevent attacks and check the IP protocol.

**Disable ICMPv6 Error Messages:** You can choose to disable four types of error messages so that ICMPv6 error messages cannot be sent, which saves system resources and prevents ICMPv6 attacks.



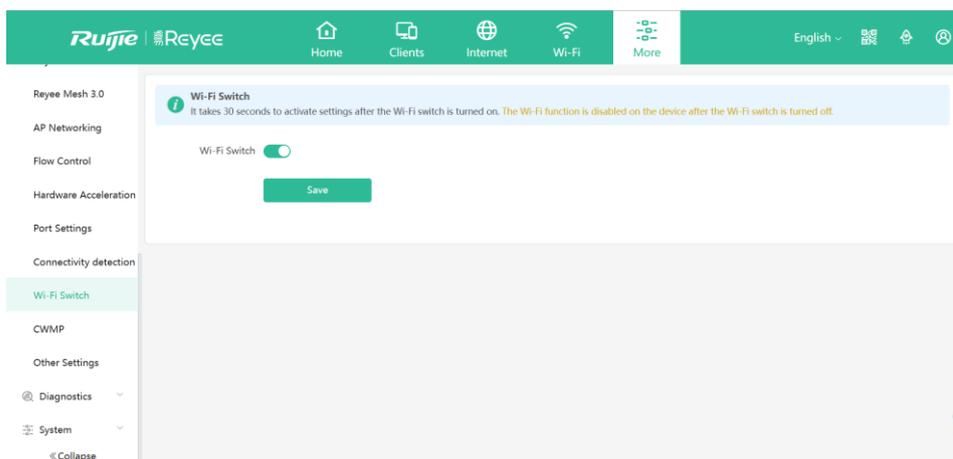
## 5.20 Enabling Wi-Fi Switch

Smartphone View: Choose **More** > **Switch to PC view** > **More** >  **Advanced** > **Wi-Fi Switch**.

PC View: Choose **More** >  **Advanced** > **Wi-Fi Switch**.

The Wi-Fi function is disabled on the device after the Wi-Fi switch is turned off.

The Wi-Fi function is disabled on the device after the Wi-Fi switch is turned off.



## 5.21 Configuring UPnP

### 5.21.1 Overview

The Universal Plug and Play (UPnP) function can map the port used by a client for Internet access according to the client's request so that related applications run more fast or stably. Common applications that support UPnP include MSN Messenger, Xunlei, BT, and PPLive.

### 5.21.2 Configuration Steps

Mobile phone view: Choose **More > Switch to PC view > More > Advanced > UPnP Settings**.

PC view: Choose **More > Advanced > UPnP Settings**.

Click **Enable**, and then click **OK**. You are advised to disable the function. Any applications that use UPnP to map ports will be listed below.



## 5.22 Configuring PPTP VPN

### Caution

The EW1800GX PRO and EW3200GX PRO support this function. The EW1200G PRO only supports the PPTP client.

### 5.22.1 Overview

The device supports the Point-to-point Tunneling Protocol (PPTP) server or client, enabling enterprises to connect to branch offices on the public network through private tunnels. A VPN connection can be established with other network devices that support PPTP.

### 5.22.2 Configuring PPTP Server

Mobile phone view: Choose **More > Switch to PC view-> More->  VPN > PPTP**.

PC view: Choose **More->  VPN > PPTP**.

(1) Click **Enable** to enable PPTP and select **Server**.

**Local Address:** Enter the local address. It is used as the local virtual IP address of the VPN tunnel for the client to access the server after dial-up.

**IP Range:** Enter the range of IP addresses. IP addresses in this range will be assigned to clients.

**DNS Server:** Enter the address of the DNS server pushed to the client.

**PPP Hello Interval:** Enter the interval for sending hello packets. You are advised to set the value to 10.

Click **Save**. The device will receive and process VPN requests.

PPTP Settings   Tunnel List

**PPTP Settings**

Enable

PPTP Type  Server  Client

\* Local Address

\* IP Range  ?

\* DNS Server

\* PPP Hello Interval  seconds

**Save**

**VPN Client List** + Add Delete Selected

Up to **32** entries can be added.

<input type="checkbox"/>	Username	Password	Network Mode	Peer Subnet	Status	Action
--------------------------	----------	----------	--------------	-------------	--------	--------

(2) Add a PPTP user.

Click + Add to enter a username and a password for authentication during client dial-up.

Select the network connection mode. **PC to Router** indicates dial-up from a PC to a router. **Router to Router** indicates dial-up from one router to the other router.

Enable **Status** and click **OK**.

Add User×

\* Username

\* Password  👁

Network Mode  ▾

Status

### 5.22.3 Configuring the PPTP Client

Choose **More** > **Switch to PC view**-> **More**->  **VPN**-> **PPTP**.

PC view: Choose **More**->  **VPN**-> **PPTP**.

Click **Enable** to enable PPTP. Select **Client** and enter the username and password configured on the server, which must be consistent with the server configuration.

**Tunnel IP:** Enter the virtual IP address used to create a VPN tunnel. You are advised to select **Dynamic** to obtain the IP address assigned by the server. You can also set static IP addresses in the address pool, which does not cause conflicts.

**Server Address:** Enter the WAN port's IP address (public IP address is required) or domain name of the server.

**Peer Subnet:** Enter the destination network segment of the server, which must be different from that of the client.

**Work Mode:** The **NAT** mode only allows a client to access the Internet on the server and does not allow the server to access the Internet on the client. The **Router** mode allows the server to access the Internet on the client.

**PPP Hello Interval:** Enter the interval for sending hello packets. You are advised to set the value to 10.

Click **Save**. The device will send VPN tunnel requests to the WAN port.

## PPTP Settings

## Tunnel List

 PPTP SettingsEnable PPTP Type  Server  Client\* Username \* Password  Interface Tunnel IP  Dynamic  Static\* Server Address \* Peer Subnet Work Mode  NAT  Router\* PPP Hello Interval  seconds

## 5.23 Configuring OpenVPN

### 5.23.1 Overview

OpenVPN can be used to establish a secure virtual private tunnel between different sites, or between a client and a site, allowing users to access the intranet over ISP networks. It is a VPN that enables layer 2 and layer 3 tunneling through virtual network cards, supporting various devices such as PCs, mobile phones, and routers to establish VPN connections.

Credentials provide security support for OpenVPN. The VPN client must use a credential generated by the server, which verifies the credential and the pre-shared key. Only after verification can a connection be established. After completing the verification, the VPN client obtains an IP address from the server, and establishes a VPN connection through that IP address.

Reyee mesh routers support server mode and client mode. In server mode, a Reyee mesh router can act as an OpenVPN server to generate credentials and verify the credential and the pre-shared key. In client mode, a Reyee mesh router works as an OpenVPN client to connect to the VPN server.

## 5.23.2 Configuring OpenVPN (Server Mode)

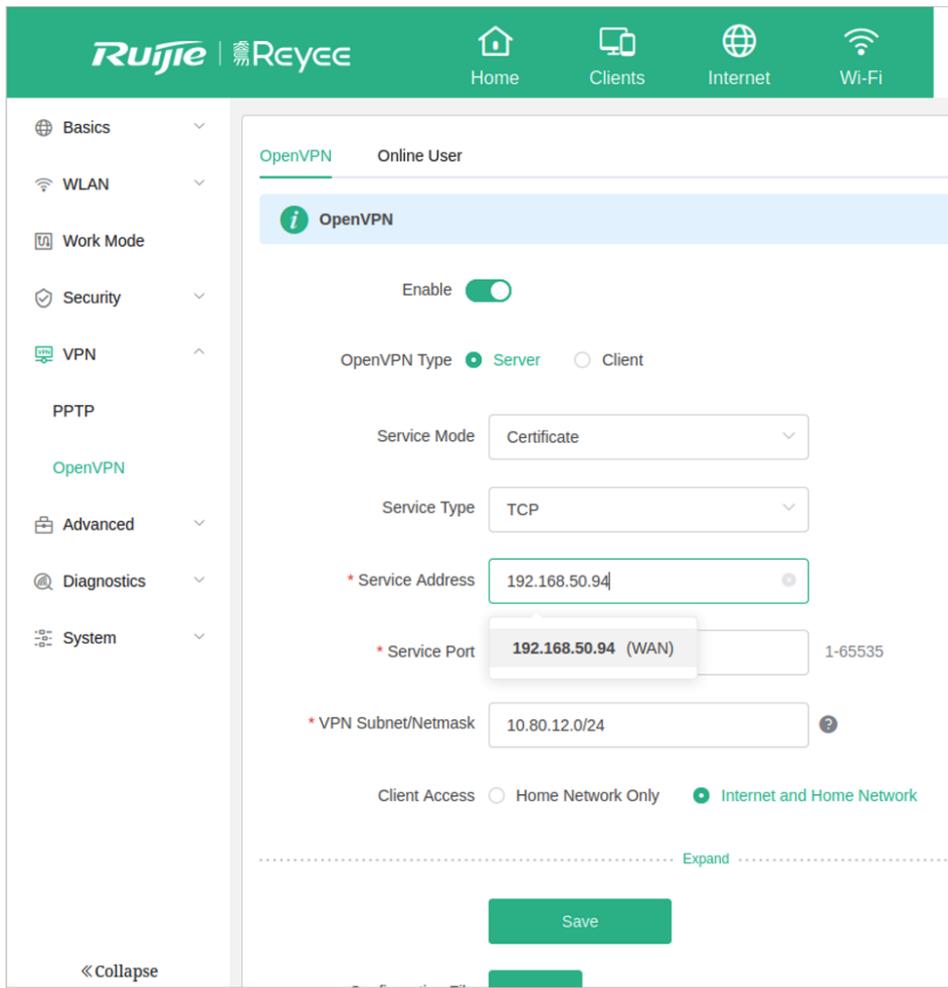
Mobile Phone View: Choose **More** > **Switch to PC view**-> **More**->  **VPN**-> **OpenVPN**.

PC View: Choose **More**->  **VPN**-> **OpenVPN**.

### 1. Configuring OpenVPN

- (1) Click **Enable** to enable the OpenVPN feature.
- (2) Select **Server** for the **OpenVPN Type**.
- (3) Select the protocol, and enter the server address, port number and other information.

Figure 5-5 Configuring OpenVPN Server



The screenshot displays the Ruijie Reyee web management interface for configuring an OpenVPN server. The interface is divided into a sidebar and a main configuration area. The sidebar on the left contains navigation menus for Basics, WLAN, Work Mode, Security, VPN, PPTP, OpenVPN, Advanced, Diagnostics, and System. The main configuration area is titled "OpenVPN Online User" and features an "OpenVPN" section with an information icon. The "Enable" toggle is turned on. The "OpenVPN Type" is set to "Server". The "Service Mode" is "Certificate", and the "Service Type" is "TCP". The "Service Address" is "192.168.50.94". The "Service Port" is "192.168.50.94 (WAN)" with a range of "1-65535". The "VPN Subnet/Netmask" is "10.80.12.0/24". The "Client Access" is set to "Internet and Home Network". A "Save" button is located at the bottom of the configuration area.

- (4) (Optional) Advanced settings.

Click **Expand** to perform the following advanced settings. If there are no special requirements, use the default settings, as shown in the following figure.

----- Collapse -----

TLS Authentication  ?

Allow Data Compression Yes ▾ ?

Cipher AES-128-CBC ▾ ?

Deliver DNS Example: 1.1.1.1 ? +

Authentication SHA2

(5) Click **Save** and the device will receive and process the VPN request.

(6) Once the basic configurations are completed, you can view the server tunnel information in the **Tunnel List**.

**Table 5-3 Configuration Items of OpenVPN Server Mode**

Item	Description
Server Mode	<p>The device supports Account, Certificate and Account &amp; Certificate authentication modes:</p> <ul style="list-style-type: none"> <li>● Account mode: The correct account name, password, and CA certificate are required to connect to the server. The configuration is simple.</li> <li>● Certificate mode: The client needs the correct CA certificate, client certificate, and pre-shared key to connect to the server.</li> <li>● Account &amp; Certificate mode: The client needs the correct account name, password, CA certificate, client certificate, and pre-shared key to connect to the server. This mode is suitable for scenarios with high security requirements.</li> </ul>
Service Type	<p>All communication on OpenVPN is based on a single IP port, using UDP or TCP protocols.</p> <p>The default value is UDP. You can select TCP for higher performance. TCP protocol can be used to improve the stability of VPN channels in high latency or unstable network conditions.</p>
Service Address	The server address used for client docking, which can be a domain name.
Service Port	The port used by the OpenVPN service process. The official port assigned to OpenVPN is 1194. If the port is occupied or disabled on the local network, the server log will prompt a log indicating port binding failure. In this case, the port number needs to be changed.
VPN Subnet/Netmask	<p>The IP address pool delivered to VPN clients, in the form of a network segment.</p> <p>The first address in that segment is reserved by the server. For example, if 10.80.12.0/24 is set, then the VPN server address is 10.80.12.1.</p>

Item	Description
Client will access	<p>You can choose <b>Home Network Only</b> or <b>Internet and Home Network</b></p> <ul style="list-style-type: none"> <li>● <b>Home Network Only:</b> The client can only access the LAN segment on the server.</li> <li>● <b>Internet and Home Network:</b> The client can access the LAN and WAN segments on the server. In this mode, all traffic from the client will be forwarded to the server.</li> </ul>
TLS Authentication	TLS Authentication can enhance the security of OpenVPN. Once enabled, the client must import the TLS key. (The version of the peer OpenVPN client must be later than 2.40.)
Allow Data Compression	Once enabled, the device will compress the transmitted data to save bandwidth, but it will occupy a certain amount of CPU resources. This configuration must be consistent on the client and the server to avoid any potential connection failures.
CIPher	Encrypts the data to prevent it from being intercepted midway. The default encryption standard is AES-128-CBC. If the server is configured in auto mode, the client can be configured with any data encryption algorithm, which will be automatically matched by the server. If a specific encryption method is configured on the server, the client must be configured with the same encryption method. Otherwise, the connection between the server and the client cannot be established.
Deliver DNS	The information pushed by the server to the client's DNS. Currently only Windows clients are supported.
Authentication	The digest algorithm informed by the server to the client. The default value is SHA256.

## 2. Adding OpenVPN clients

Click **+ Add** to enter a username and a password for authentication when the client dials in.

Enable **Status** and click OK.

**VPN Client List**

Up to **30** entries can be added.

<input type="checkbox"/>	Username	Password	Status	Action
No Data				

< **1** >
10/page
Total 0

## Add User ×

\* Username

\* Password  

Status

### 5.23.3 Configuring OpenVPN (Client Mode)

Mobile Phone View: Choose **More** > **Switch to PC view**-> **More**->  **VPN**-> **OpenVPN**.

PC View: Choose **More**->  **VPN**-> **OpenVPN**.

Currently, this device supports Import Config, through which the configuration file is manually imported for docking with the server that is similar to this device. The client configuration file client.ovpn can be directly exported from the docked OpenVPN server.

- (1) Click **Enable** to enable the **OpenVPN** function. Configure **OpenVPN Type** as **Client**.
- (2) Configure the Server Mode, and click **Browse** to import the client configuration file. Click **Save** to save the configuration.

The device supports three authentication modes: Account, Certificate, and Account & Certificate.

**Account mode:** The correct account, password, and CA certificate is required to connect to the server, where the CA certificate information is embedded in the client's configuration file.

**Certificate mode:** The client needs the correct CA certificate, client certificate, and pre-shared key to connect to the server, which are all embedded in the client's configuration file.

**Account & Certificate mode:** The client needs the correct account, password, CA certificate, client certificate, and pre-shared key to connect to the server, where the CA certificate information, client certificate, and pre-shared key are embedded in the client's configuration file.

OpenVPN
Tunnel List

---

i OpenVPN

Enable

OpenVPN Type  Server  Client

Server Mode Account & Certificate

\* Username Username of OpenVpn user ?

\* Password Password of OpenVpn user ?

\* Client Config .ovpn Browse

Save

**Table 5-4 Configuration Items of OpenVPN Client Web Setting Configuration Mode**

Parameter	Description
Server Mode	The device supports Account, Certificate and Account & Certificate authentication modes: <ul style="list-style-type: none"> <li>● Account mode: The correct account, password, and CA certificate is required to connect to the server. The configuration is simple.</li> <li>● Certificate mode: The client needs the correct CA certificate, client certificate, and pre-shared key to connect to the server.</li> <li>● Account &amp; Certificate mode: The client needs the correct account, password, CA certificate, client certificate, and pre-shared key to connect to the server. This mode is suitable for scenarios with high security requirements.</li> </ul>
Username and password	Enter the username and password configured on the server. This parameter can be left blank if the <b>Server Mode</b> is <b>Certificate</b> .
Client Config	Click <b>Browse</b> and select the client configuration file with the suffix .ovpn.

### 5.23.4 Typical Configuration Example

#### 1. Requirements

Through OpenVPN, a client can establish a secure connection to a server over the Internet, and access resources on the server's internal network or access the Internet through the server's network proxy.

## 2. Topology



## 3. Notes

- Configure Device A as the OpenVPN server.
- Install the OpenVPN client on Device B. (<https://openvpn.net/>)

## 4. Configuring OpenVPN Server (Device A)

- (1) Log in to the Eweb management system of the device, and choose **VPN > OpenVPN**. Then, flip on the toggle switch next to **Enable** to enable the OpenVPN function. On the page that is displayed, enter the IP address of the WAN port as the service address, as well as other required parameters.

Use the default settings unless there are specific requirements.

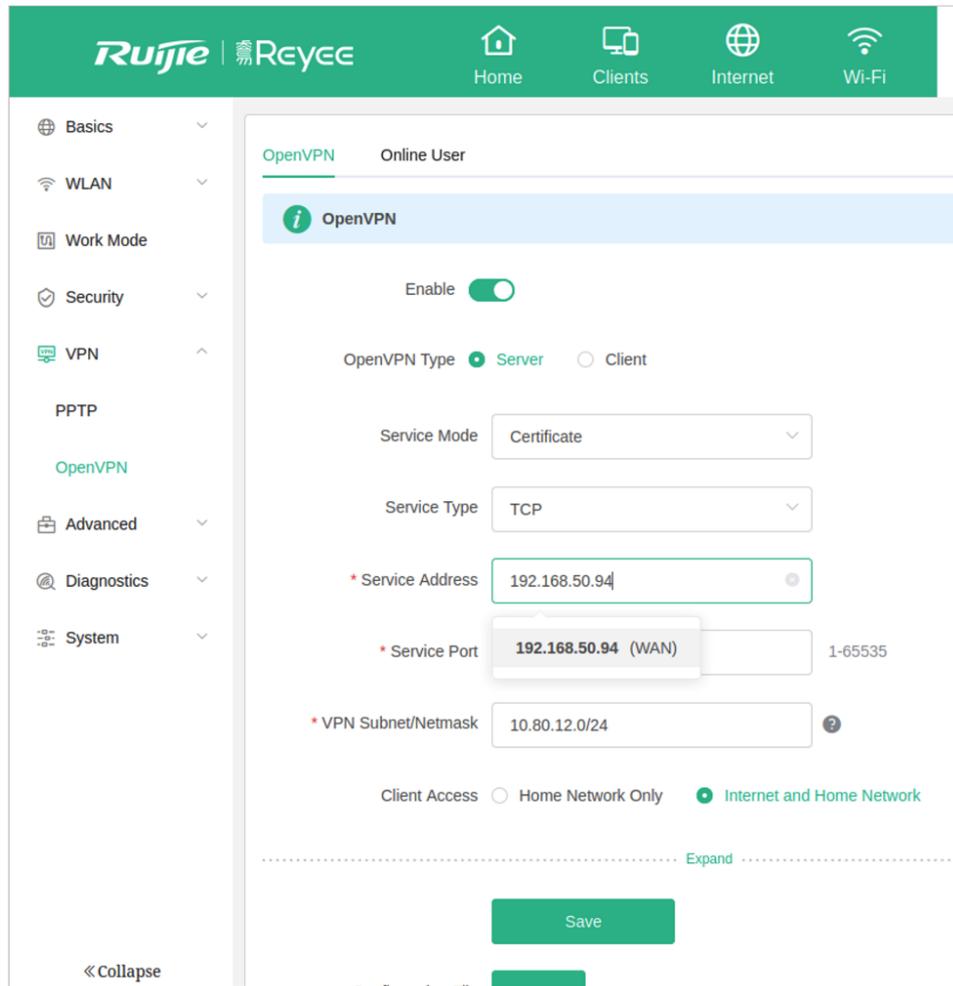
---

### Note

The WAN IP address must be a public IP address or a DDNS domain name that is accessible from outside the local network.

If the router does not have a public IP address, contact the ISP to obtain a public IP address.

---



(2) Click **Save**. The OpenVPN settings are saved.

(3) The following table describes the OpenVPN server configuration.

Parameter	Description
Service Mode	Account: Authentication based on password. Certificate: Authentication based on client certificate. Account & Certificate: Authentication based on password and client certificate.
Service Type	Use the default value unless there are specific requirements. Both UDP and TCP are supported. If the network connection between the two ends of an encrypted tunnel is poor, for example due to high latency or heavy packet loss, then select <b>TCP</b> .
Service Address	The IP address of the WAN port is automatically populated.

Parameter	Description
Service Port	Indicates the port for OpenVPN service. Use the default value unless there are specific requirements.
VPN Subnet/Netmask	Indicates the network segment of the OpenVPN address pool. The first available IP address in the address pool is reserved for the server, while other addresses can be allocated to clients. For example, if this parameter is set to <b>10.80.12.0/24</b> , then the virtual IP address of the VPN server is 10.80.12.1.
Client Access	Home Network Only: If this access mode is selected, then the client can only access resources on the server's internal network, but is unable to access the Internet through the server's network proxy.  Internet and Home Network: If this access mode is selected, then the client not only can access resources on the server's internal network, but also can access the Internet through the server's network proxy.

(4) Click **Expand** to show advanced settings. Use the default values unless there are specific requirements.

..... Collapse .....

TLS Authentication  ?

Allow Data Compression  ?

Cipher  ?

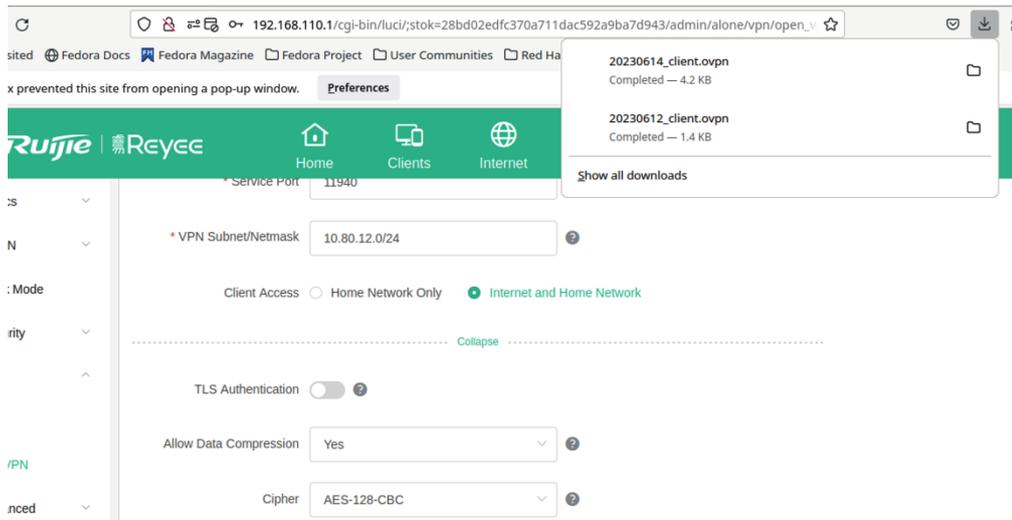
Deliver DNS  ? +

Authentication

Configuration File

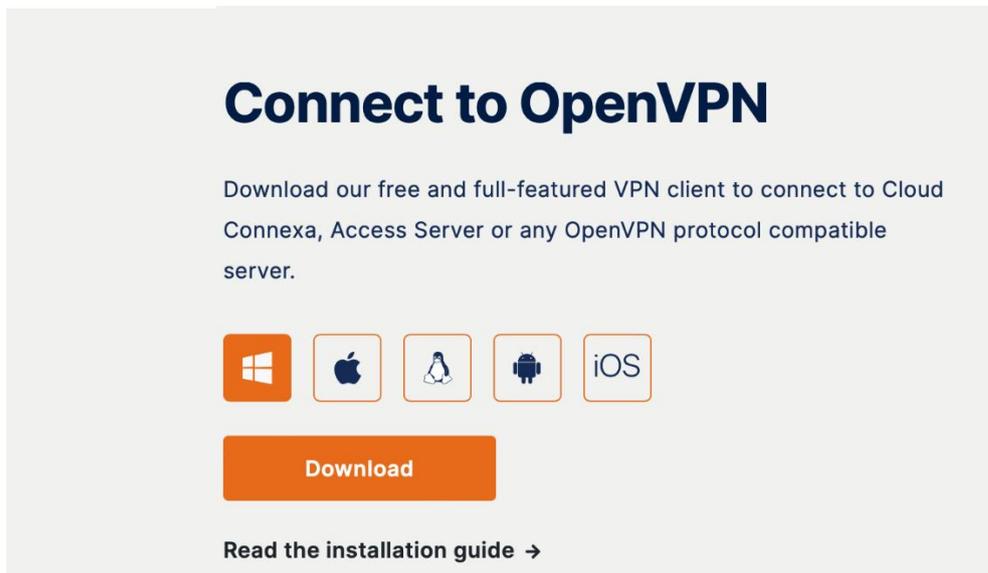
CA Certificate

(5) Click **Export** next to **Configuration File** to export the .ovpn file which can be imported on the client side. Unless there are specific requirements, you do not need to export the CA certificate.

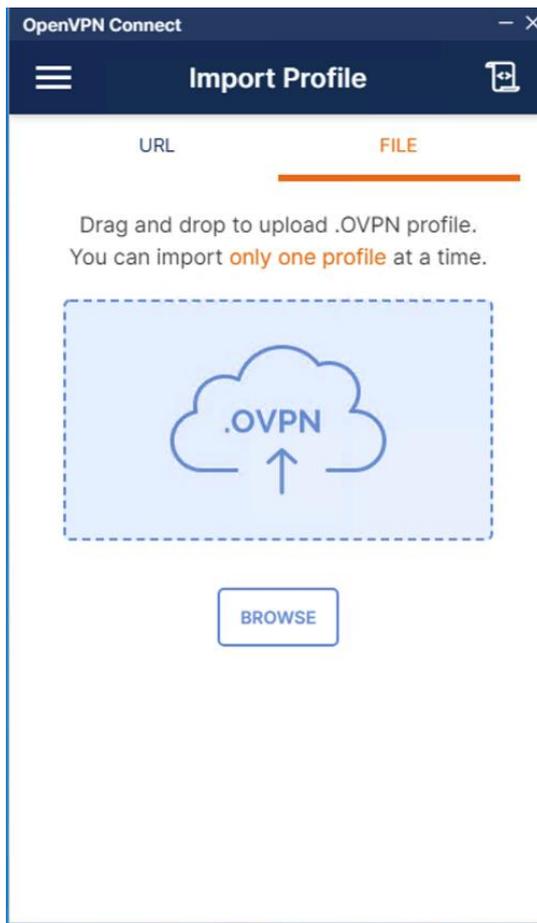


## 5. Configuring OpenVPN Client (Use Windows Client as an Example)

- (1) download the OpenVPN client (<https://openvpn.net>).



- (2) Open the Windows OpenVPN client and choose the **File** tab.



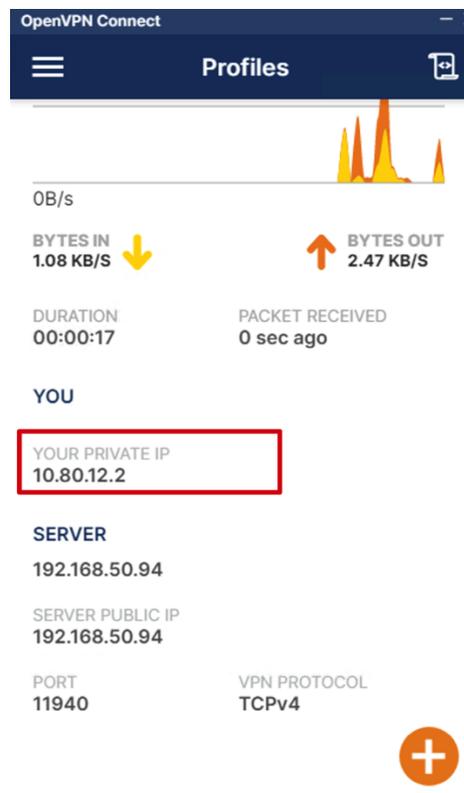
(3) Click **BROWSE** and select the .ovpn file exported from the server side.



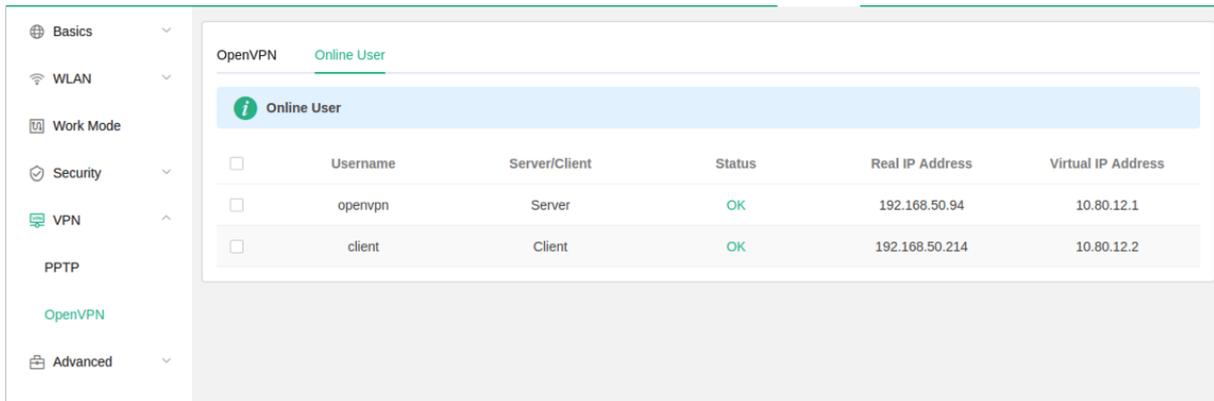
(4) Click **CONNECT** to connect to the OpenVPN server.



Check the obtained virtual IP addresses.



- (5) Log in to the Eweb management system of the device, and choose **More > VPN > OpenVPN > Online User** to find the connected client.



## 5.24 Configuring Connectivity Detection

Smartphone View: Choose **More > Switch to PC view > More >  Advanced > Connectivity detection**.

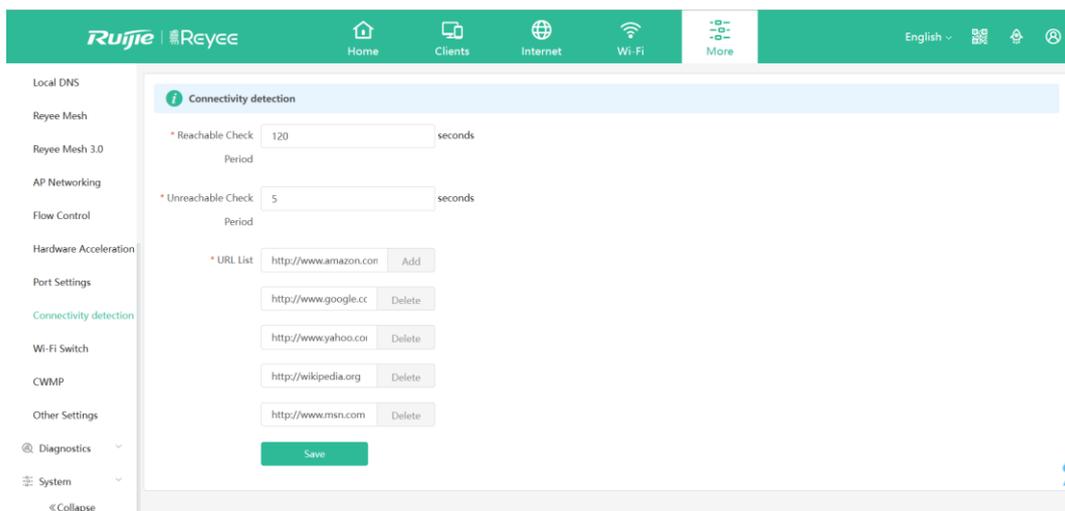
PC View: Choose **More >  Advanced > Connectivity detection**.

Enter the values in the **Reachable Check Period**, **Unreachable Check Period** and **URL List** fields, and click **Save** to save the settings.

**Reachable Check Period:** Interval for network connectivity detection when the network is reachable. The value range is 3 to 120 seconds.

**Unreachable Check Period:** Interval for network connectivity detection when the network is unreachable. The value range is 1 to 30 seconds.

**URL List:** Domain name for network connectivity detection. A maximum of 5 URLs are supported.



## 5.25 Enabling CWMP

PC View: Choose **More** >  **Advanced** > **CWMP**

Mobile Phone View: Choose **More** > **Switch to PC view** > **More** >  **Advanced** > **CWMP**

### 5.25.1 Overview

CPE WAN Management Protocol (CWMP) provides a general framework and protocol for management and configuration of home network devices in the next generation network. It is used for remote centralized management of gateways, routers, set-top boxes and other home network devices from the network side.

CWMP uses ACS and CPE models to manage devices. With CWMP, CPE can perform mandatory initialization and O&M actions such as service activation, function settings, file upload and download, and system detection.

With CWMP, ACS can remotely manage the software and firmware of user devices, monitor the status and performance of user devices, realize automatic configuration of user devices and dynamic service configuration, and perform communication fault troubleshooting.

### 5.25.2 Configuration Steps

Click to enable **CWMP**, and configure the ACS account, password, address, and other information.

If NAT is enabled on the router, then enable STUN for NAT traversal. Click to enable **STUN**, and configure the STUN server port, account, password, and other information. Click **Save** to complete the configuration.

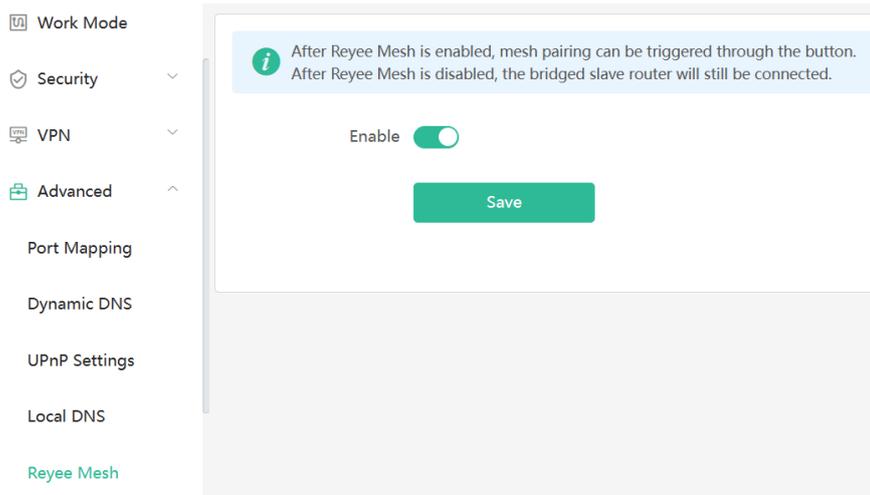
CWMP \* Inform Interval \* ACS Address \* ACS Account \* ACS Password STUN \* STUN Server Address \* STUN Server Port \* STUN Server Account \* STUN Server Password 

## 5.26 Enabling Reyee Mesh

Smartphone View: Choose **More** > **Switch to PC view** > More >  **Advanced** > **Reyee Mesh**

PC View: Choose **More** >  **Advanced** > **Reyee Mesh**

When Reyee Mesh is enabled, you can press the **Reyee Mesh** button to start mesh pairing. When Reyee Mesh is disabled, no action will be triggered by pressing the **Reyee Mesh** button.



### **i** Note

When Reyee Mesh is disabled, bridged mesh repeaters will not be disconnected.

## 5.27 Enabling Hardware Acceleration

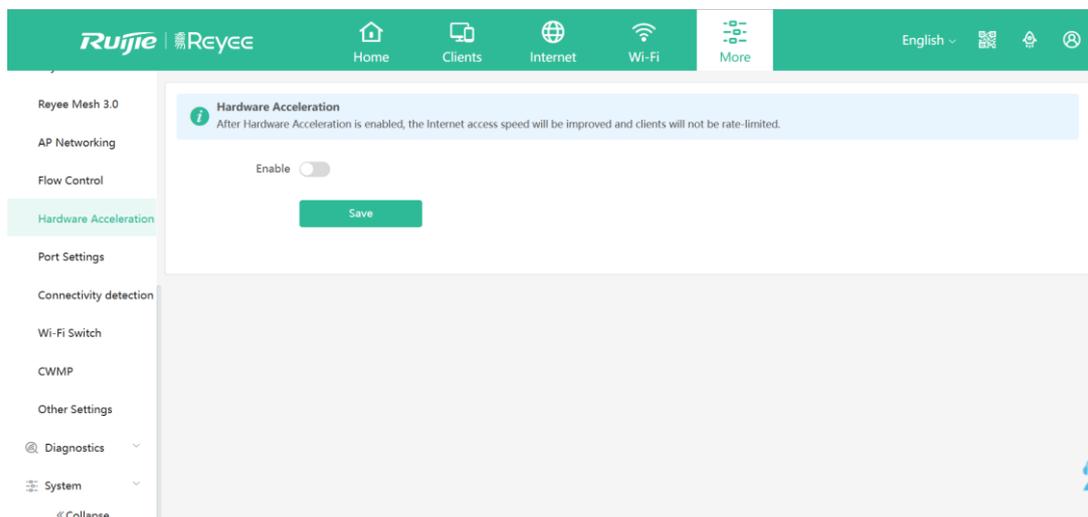
### **!** Caution

This feature is supported in router mode.

Smartphone View: Choose **More** > **Switch to PC view** > **More** > **Advanced** > **Hardware Acceleration**.

PC View: Choose **More** > **Advanced** > **Hardware Acceleration**.

After Hardware Acceleration is enabled, the Internet access speed will be improved and clients will not be rate-limited. You are advised to enable hardware acceleration when doing speed measurement.



---

**⚠ Caution**

After hardware acceleration is enabled, IPv6 and smart flow control will be disabled.

---

## 5.28 Configuring Console Booster

---

**i Note**

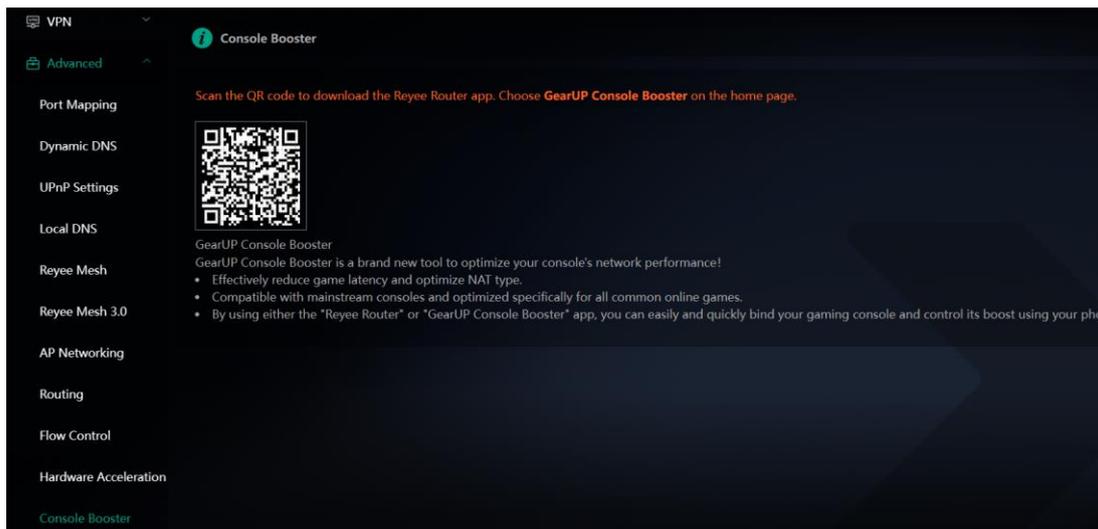
Only EW3000GX PRO supports this function.

---

Smartphone View: Choose **More** > **Switch to PC view** > **More** >  **Advanced** > **Console Booster** .

PC View: Choose **More** >  **Advanced** > **Console Booster** .

GearUP Console Booster is a brand new tool to optimize your console's network performance. By using either the "Reyee Router" or "GearUP Console Booster" app, you can easily and quickly bind your gaming console and control its boost using your phone.

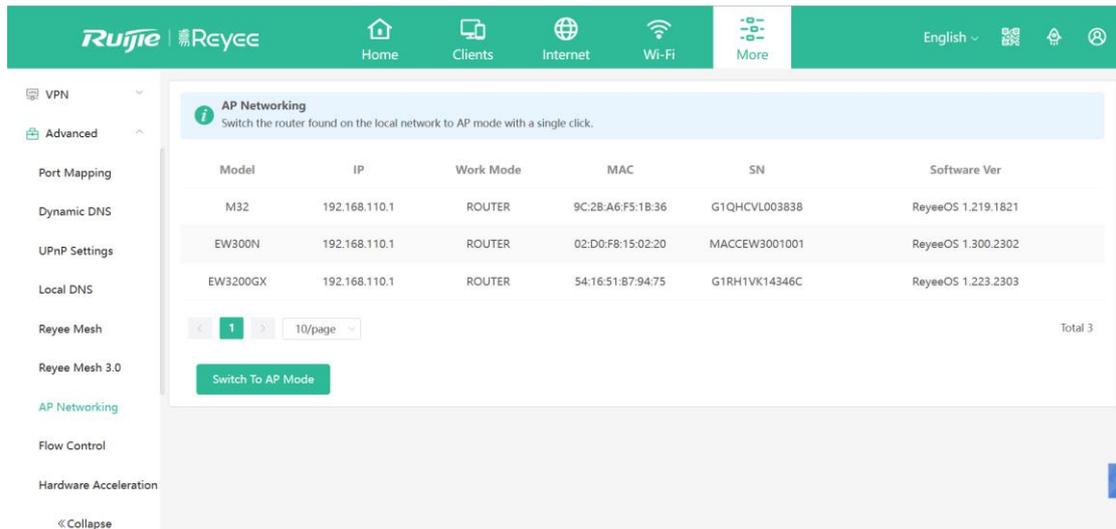


## 5.29 Configuring AP Networking

PC View: Choose **More** >  **Advanced** > **AP Networking**

Smartphone View: Choose **More** > **Switch to PC view** > **More** >  **Advanced** > **AP Networking**

Click **Switch To AP Mode**, switch the router found on the local network to AP mode with a single click.



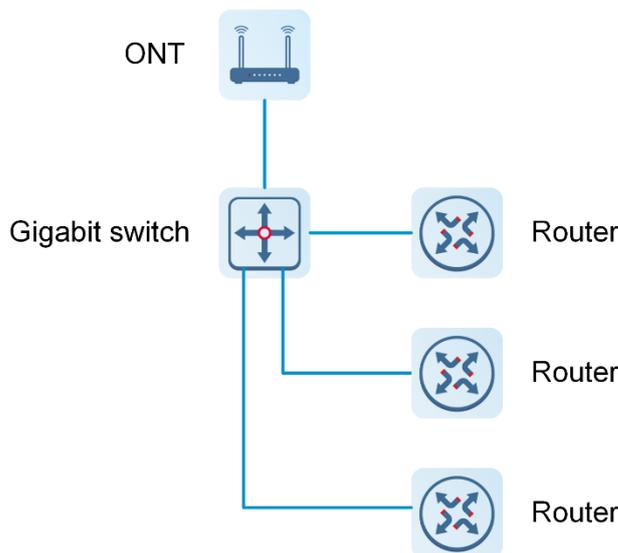
## 5.30 Configuring Reyee Mesh 3.0

### 5.30.1 Configuration Steps

PC View: Choose **More** > **Advanced** > **Reyee Mesh 3.0**

Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Advanced** > **Reyee Mesh 3.0**

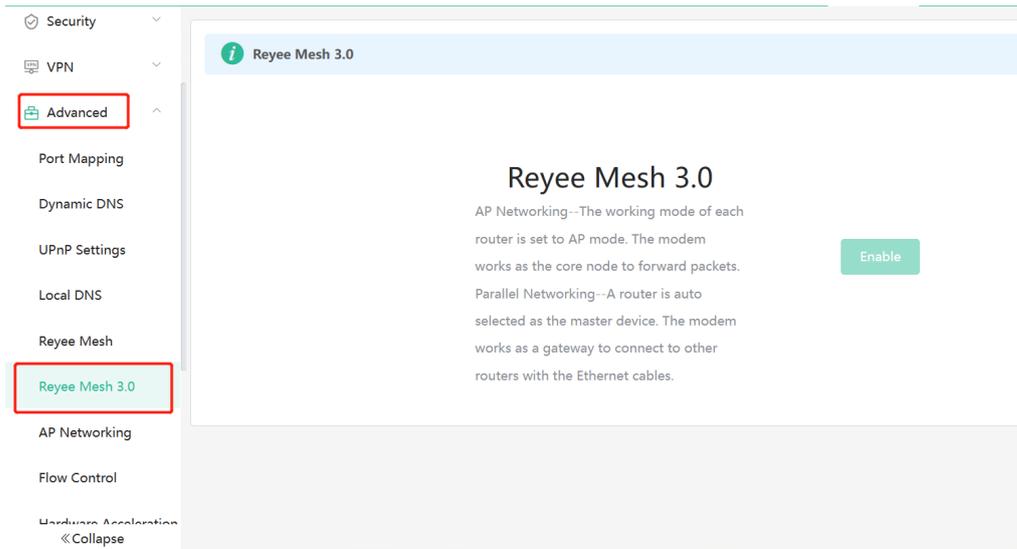
Connect the routers as indicated in the following figure:



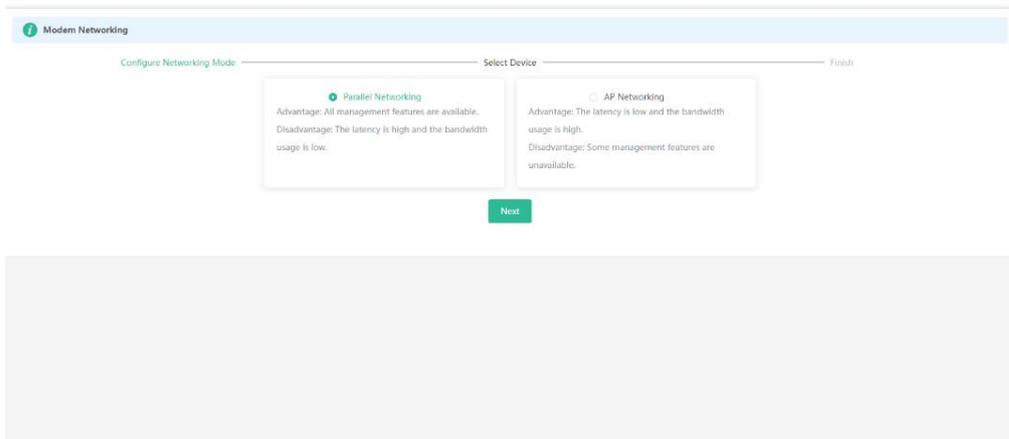
#### 1. Parallel Networking

Parallel networking refers to connecting multiple routers in a wired manner to a modem or switch (Gigabit switch), with the modem as the network bridge, and one router elected as the master router. Other routers forward packets to the master router through the modem to access the internet, achieving network-wide unified management.

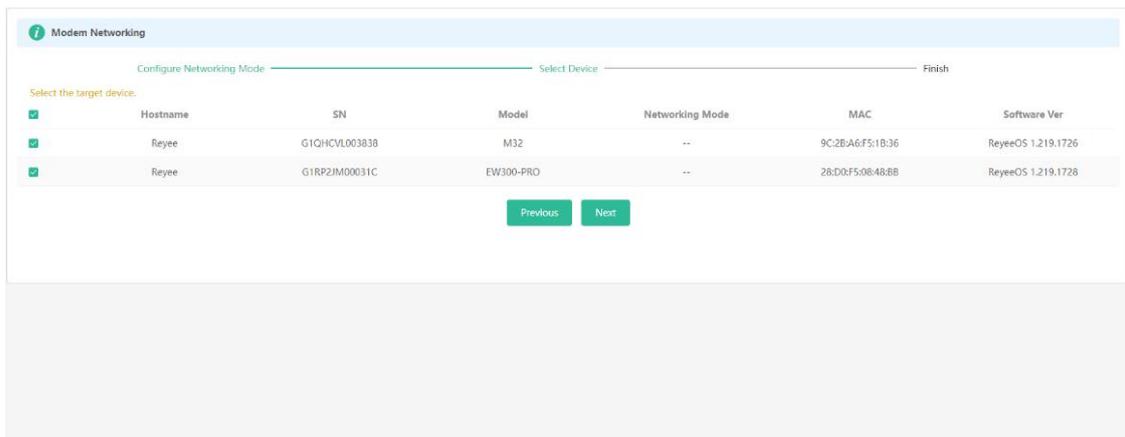
- (1) Click **Enable** to enable Reyee Mesh 3.0.



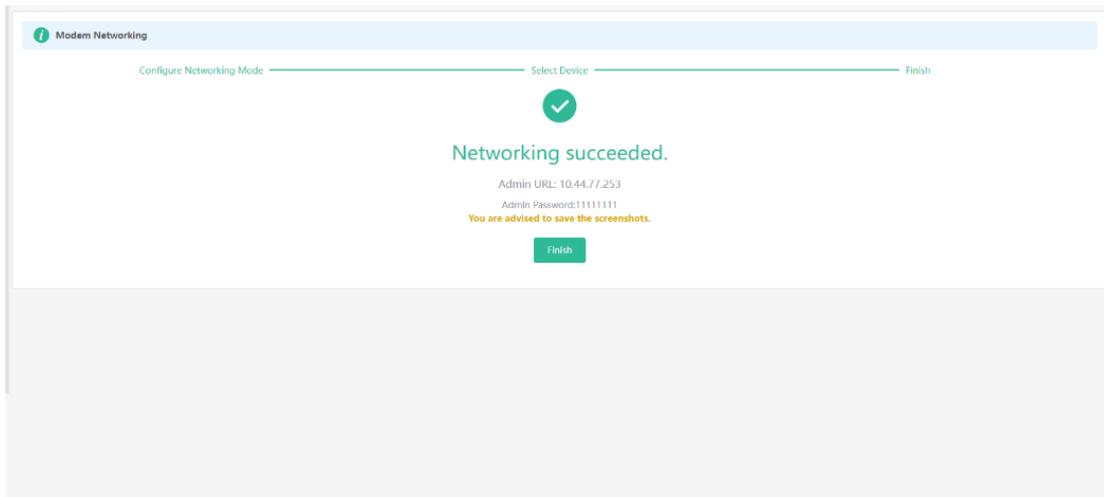
(2) Choose **Parallel Networking**, and click **Next**.



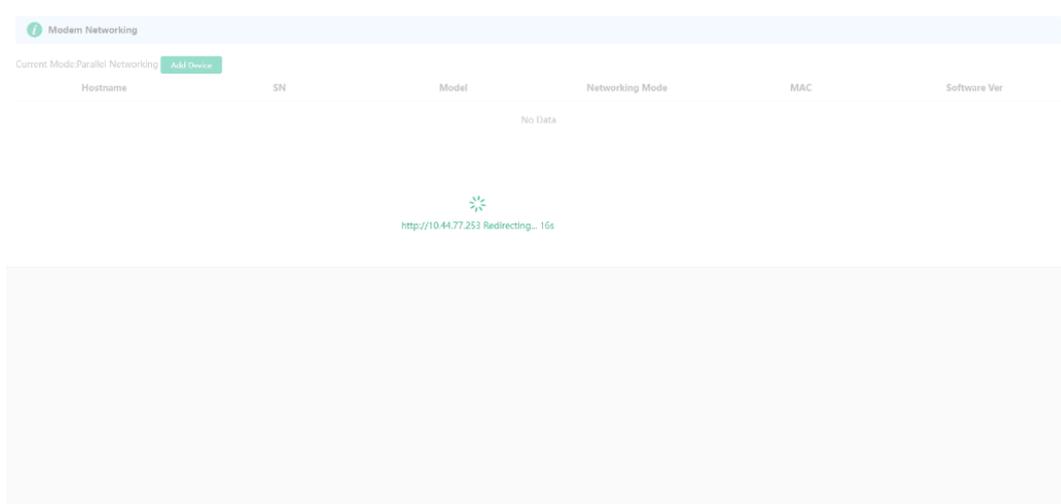
(3) Check routers for the networking.



(4) Click **Next**.



(5) Click **Finish**. You will be redirected to a new page.

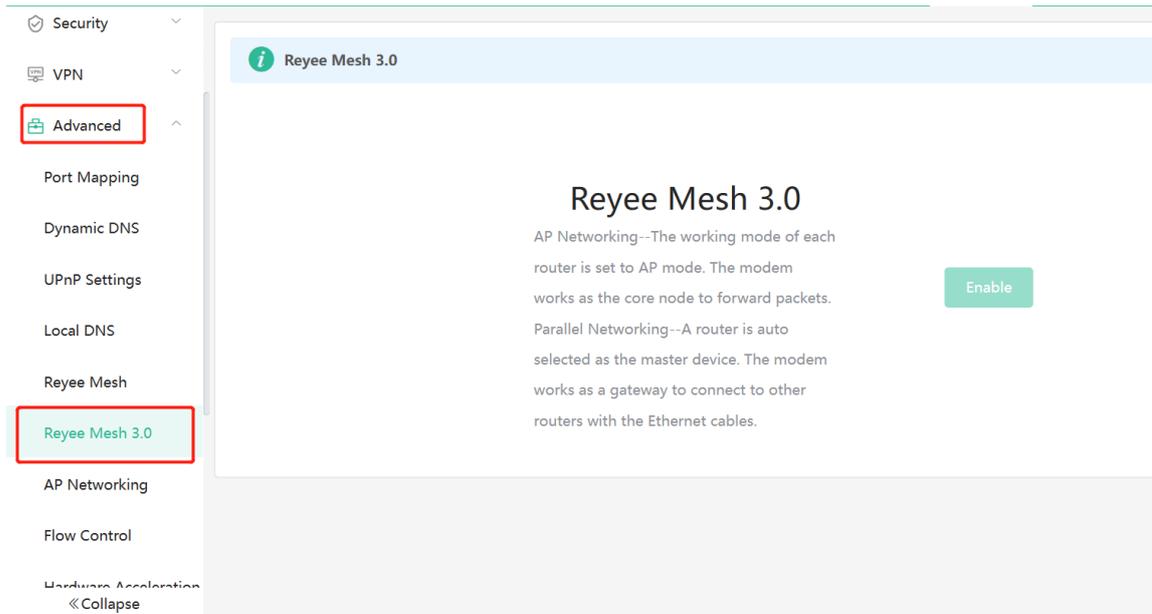


(6) On the master router page that is displayed, enter the password to log in.

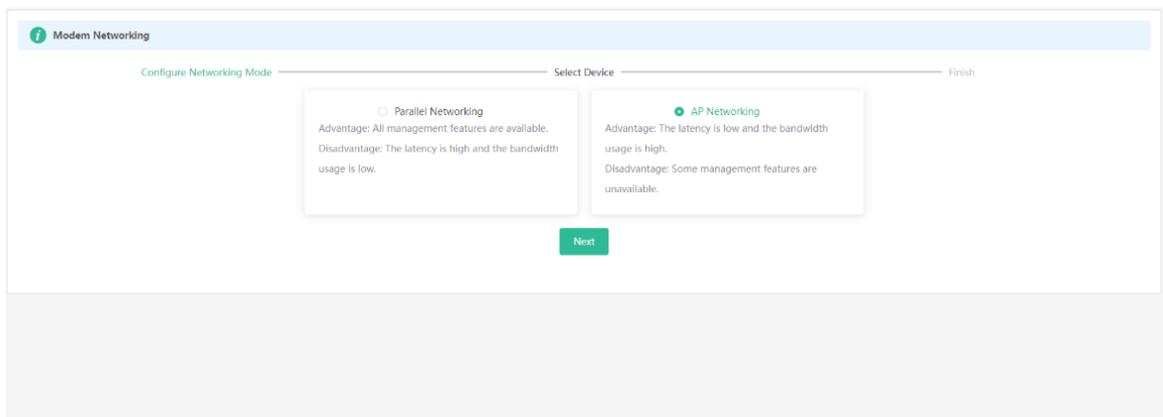
## 2. AP Networking

AP networking refers to connecting multiple routers in a wired manner to a modem or switch, with all routers working in AP mode. The modem acts as the core node for data forwarding.

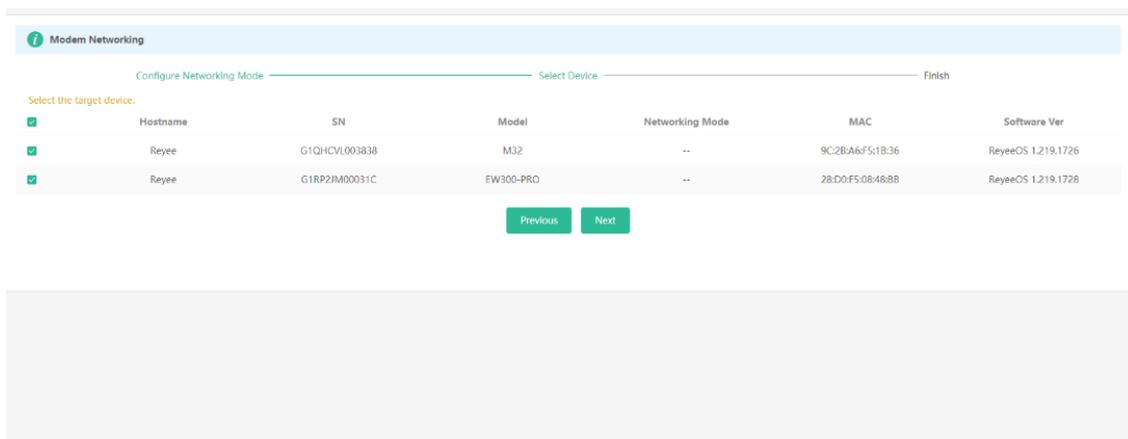
(1) Click **Enable** to enable Reyee Mesh 3.0.



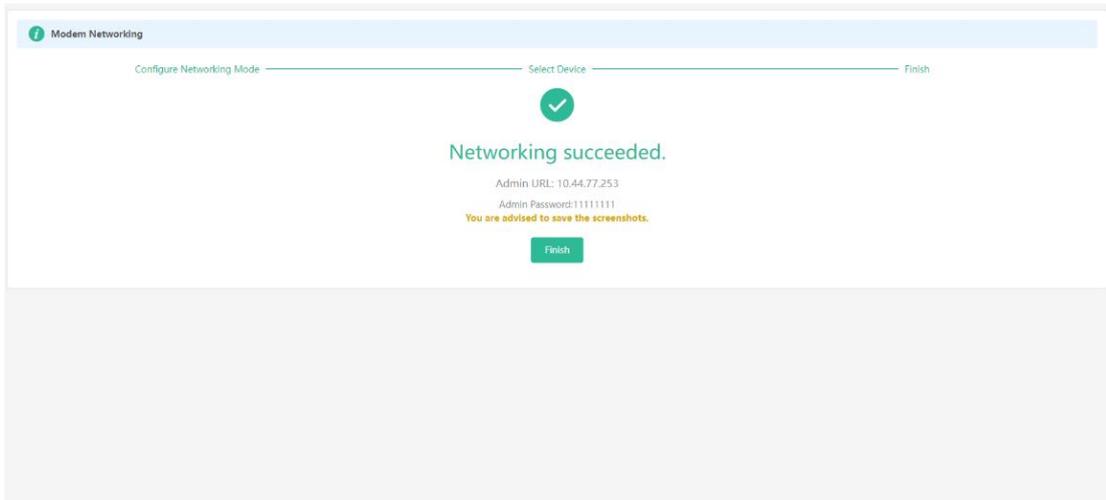
(2) Choose **AP networking**, and click **Next**.



(3) Check routers for AP networking, and click **Next**.



(4) Click **Finish**. You will be redirected to a new page.



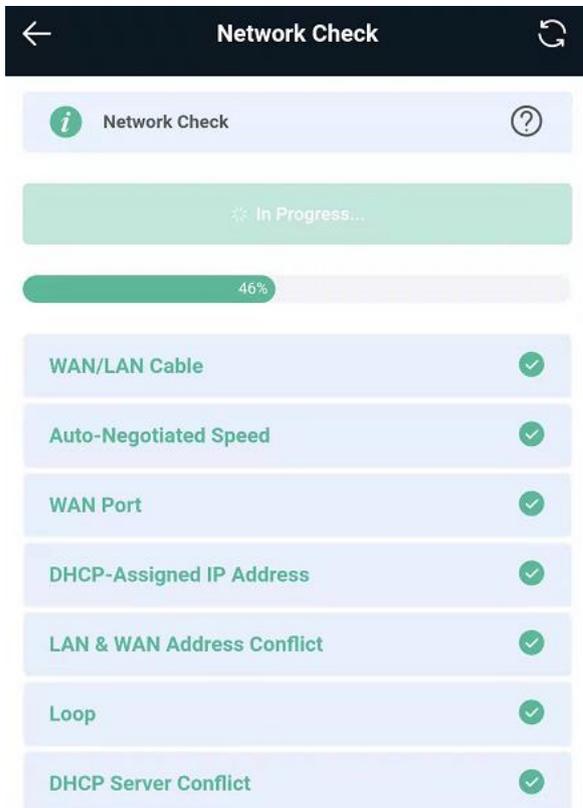
(5) On the master router page that is displayed, enter the password to log in.

### 5.31 Diagnosing Network Problems

Mobile phone view: Choose **More > Network Check**.

PC view: Choose **More > Diagnostics > Network Check**.

Click **Start** and then click **OK**. The device will check the network for problems, including interfaces, routing, flow control, and Ruijie Cloud platform, and provide solutions and suggestions for risk items.



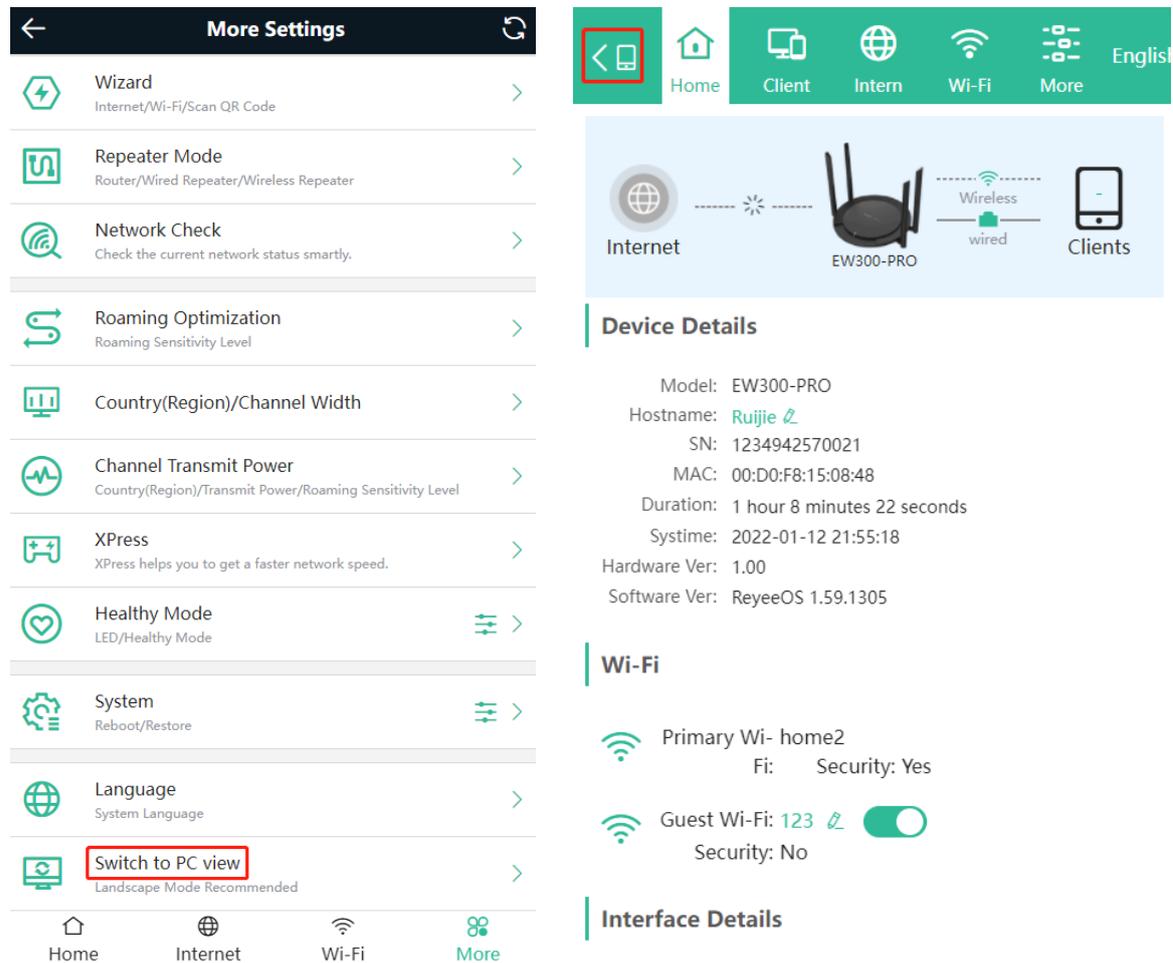
# 6 Reyee System Settings

## 6.1 Switching to the PC View

Choose **More** > **Switch to PC view**.

The PC view is the screen displayed after you log in from a PC. The page layout is different from that on a mobile phone.

You can click  in the upper left corner to return to the mobile phone view or drag the page to the narrowest position on the PC to enter the mobile phone view.



The screenshot displays the Reyee System Settings mobile application interface. On the left, the 'More Settings' menu is visible, with the 'Switch to PC view' option highlighted by a red box. The right side of the screen shows the main dashboard, which includes a navigation bar at the top with icons for Home, Client, Intern, Wi-Fi, and More. Below the navigation bar is a network diagram showing the connection between the Internet, the EW300-PRO router, and Clients. The 'Device Details' section lists information such as Model (EW300-PRO), Hostname (Ruijie), SN (1234942570021), MAC (00:D0:F8:15:08:48), Duration (1 hour 8 minutes 22 seconds), System time (2022-01-12 21:55:18), Hardware Ver (1.00), and Software Ver (ReyeeOS 1.59.1305). The 'Wi-Fi' section shows Primary Wi-Fi (home2) with Security: Yes and Guest Wi-Fi (123) with Security: No and a toggle switch. The 'Interface Details' section is also visible at the bottom.

## 6.2 Configuring the Login Password

Mobile phone view: Choose **More** > **System** > **Password**.

PC view: Choose **More** > **System** > **Login** > **Login Password**.

Enter the old password and new password. After saving the configuration, log in again with the new password.

The screenshot shows a mobile application interface for changing a password. At the top, there is a dark header with a back arrow on the left, the title "Password" in the center, and a refresh icon on the right. Below the header is a light blue informational banner with an 'i' icon, the text "Change the login password. Please log in again with the new password later.", and a question mark icon. The main content area contains three input fields, each with a red asterisk and a label: "\* Old Password", "\* New Password", and "\* Confirm Password". At the bottom of the form is a large green button labeled "Save".

## 6.3 Remote Access

Smartphone View: Choose **More** > **Switching to PC View** > **More** >  **System** > **Login** > **Remote Access**.

PC View: Choose **More** >  **System** > **Login** > **Remote Access**.

Click **Enable** to enable the remote access.

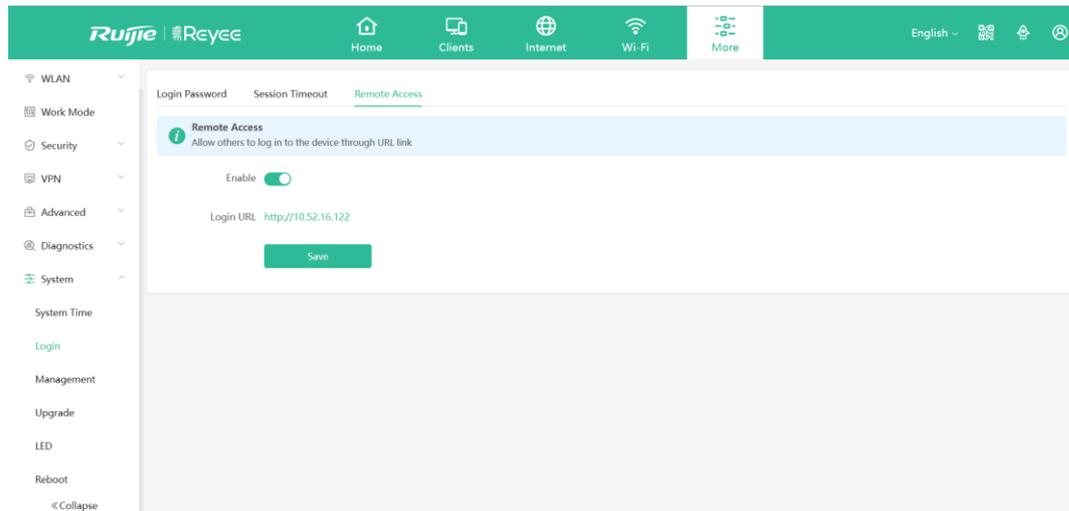
---

### Caution

This this may cause attack. Therefore, exercise caution when performing this operation.

This function cannot be enabled if the device management password has a weak security strength, such as being purely numerical or alphabetical. See [6.2 Configuring the Login Password](#) to configure a strong and secure device management password.

---



## 6.4 Restoring Factory Settings

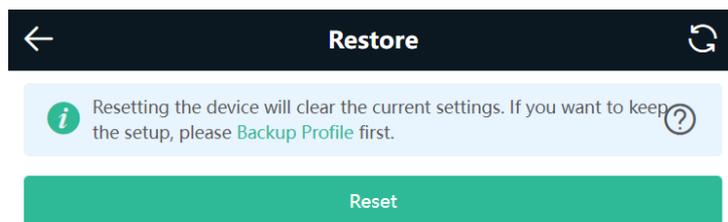
Mobile phone view: Choose **More** > **System** > **Restore**.

PC view: Choose **More** > **System** > **Management** > **Reset**.

Click **Reset** to restore factory settings.

### Note

This operation will clear existing settings and restart the device. Therefore, exercise caution when performing this operation.

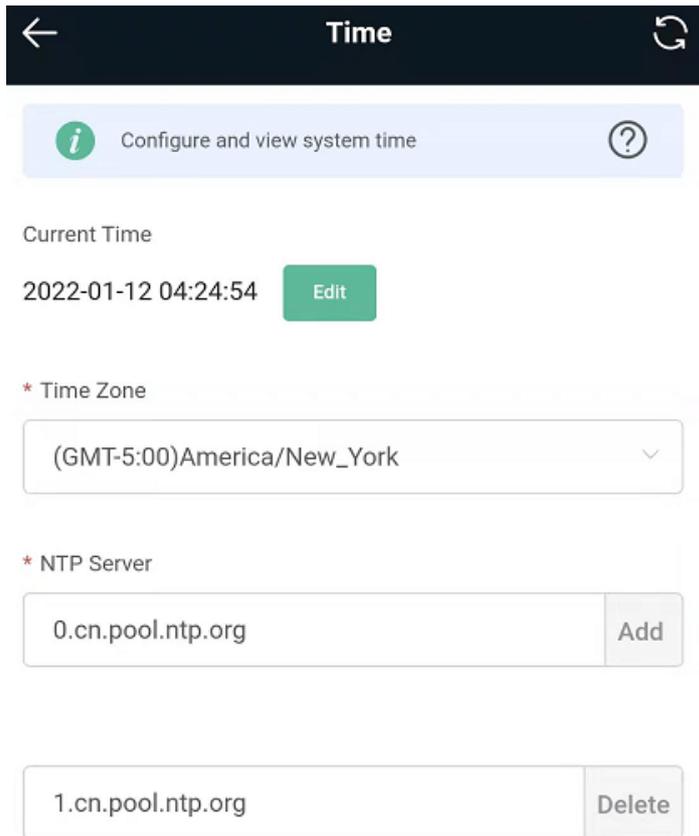


## 6.5 Configuring the System Time

Mobile phone view: Choose **More** > **System** > **Time**.

PC view: Choose **More** > **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 the time is still incorrect, click **Edit** to manually set the time. In addition, the router supports Network Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete local servers as required.



## 6.6 Configuring Scheduled Reboot

### 6.6.1 Getting Started

Confirm that the system time is accurate to avoid network interruption caused by device reboot at the incorrect time point. For details, see [6.5 Configuring the System Time](#).

### 6.6.2 Configuration Steps

Mobile phone view: Choose **More > System > Scheduled Reboot**.

PC view: Choose **More > System > Reboot > Scheduled Reboot**.

Click **Enable**, and select the date and time of weekly scheduled reboot. Click **Save**. When the system time matches the scheduled reboot time, the device will restart.

← **Scheduled Reboot** ↻

Enable

Day

Mon  Tue  Wed  Thu

Fri  Sat  Sun

Time

03 : 00

Save

## 6.7 Performing Online Upgrade and Displaying the System Version

Mobile phone view: Choose **More** > **System** > **Online Upgrade**.

PC view: Choose **More** > **System** > **Upgrade** > **Online Upgrade**.

You can check the current system version. If the version needs to be upgraded, you can click it for the upgrade. The upgrade time can be set. You are advised to set the upgrade time to the idle network time, for example, 4:15 a.m.

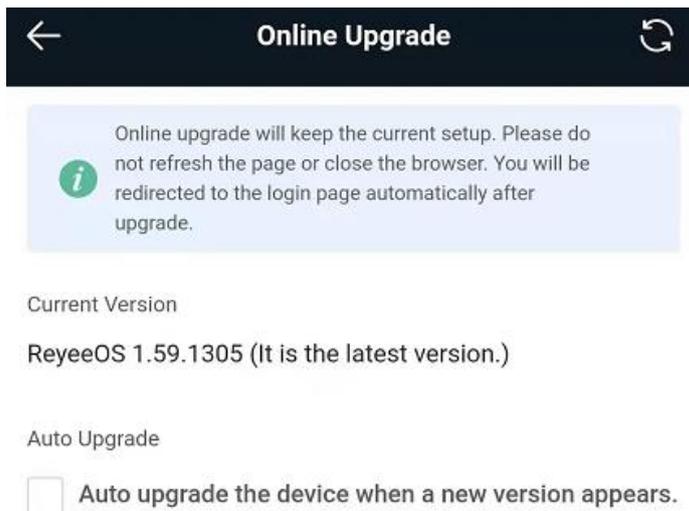
---

### Note

After being upgraded, the device will restart. Therefore, exercise caution when performing this operation. You are advised to set the scheduled upgrade time to an early morning time to avoid Internet access from being affected.

If no version upgrade is detected and online upgrade cannot be performed, check whether the DNS configuration is correctly obtained or go to **More** > **Advanced** > **Local DNS** to set the DNS server for the router.

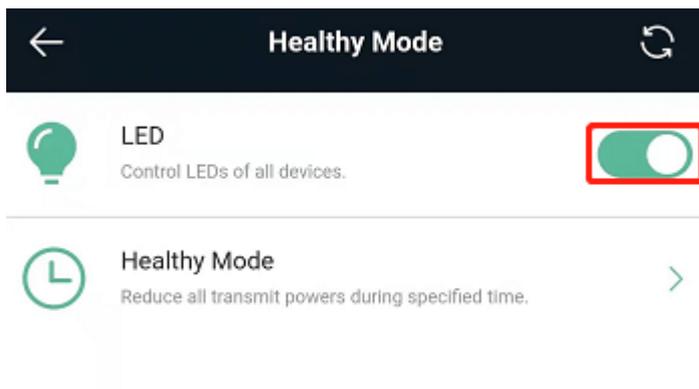
---



## 6.8 Enabling or Disabling the LED

Mobile phone view: Choose **More** > **System** > **Healthy Mode**.

PC view: Choose **More** > **System** > **LED**.



## 6.9 Switching the System Language

Mobile phone view: Choose **More** > **Language**.

PC view: Click  in the upper right corner of the page.

Click a required language to switch the system language.



## 6.10 Network Diagnosis Tools

### 6.10.1 Network Test Tool

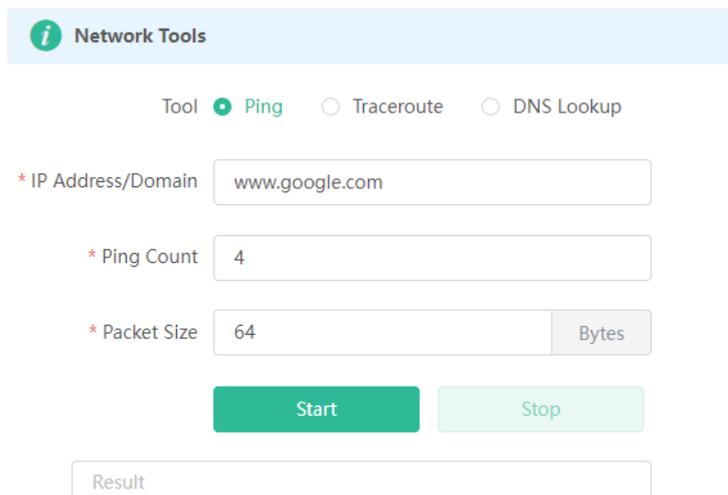
Mobile phone view: Choose **More > System > Network Tools**.

PC view: Choose **More > Diagnostics > Network Check**.

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

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

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



### 6.10.2 Packet Obtaining Tool

Mobile phone view: Choose **More > Switch to PC view > More > Diagnostics > Packet Capture**.

PC view: Choose **More > Diagnostics > Packet Capture**.

Configure the interface, protocol, IP address whose packets need to be obtained, file size limit, and packet count limit to limit the volume of packets obtained. Click **Start**. Packet obtaining can be stopped at any time and a link to the generated file is generated. You can use Wireshark and other analysis software to open and view the file.

**Note**

Packet obtaining may occupy many system resources and cause network freezing. Exercise caution when performing this operation.

i
Packet Capture

Interface

Protocol

IP Address

File Size Limit  Available Memory 26.61 M

Packet Count Limit

Start
Stop

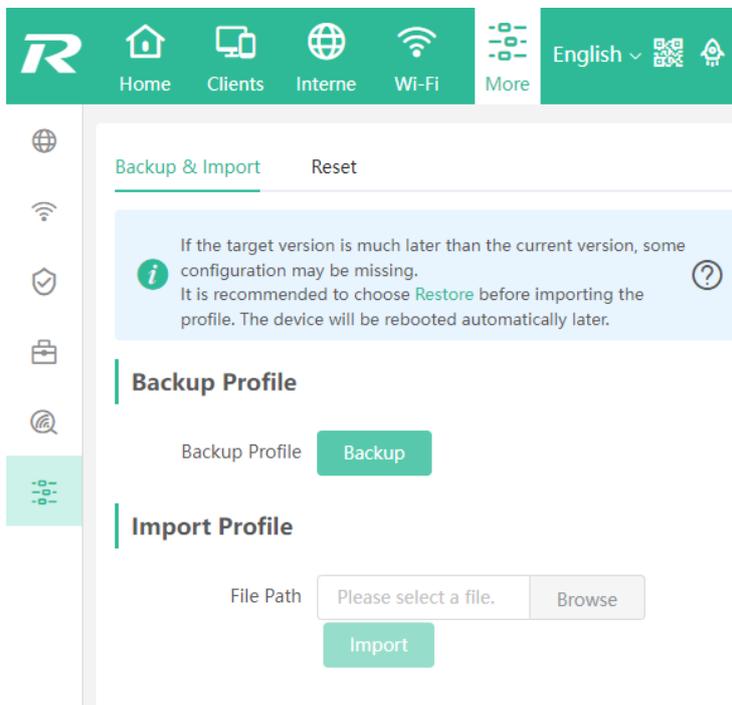
## 6.11 Configuring Backup and Import

Mobile phone view: Choose **More** > **Switch to PC view** > **More** > **System** > **Management**.

PC view: Choose **More** > **System** > **Management** > **Backup&Import**.

To configure backup, click **Backup** to download a configuration file locally.

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



## 6.12 Configuring the Session Timeout

Mobile phone view: Choose **More** > **Switch to PC view** > **More** > **System** > **Login**.

PC view: Choose **More** > **System** > **Login**.

If no operation is performed on the page within a given period of time, the session will ended. When you need to perform operations again, enter the password to open the configuration page. The default timeout is 3600 seconds, that is, 1 hour.

< .ogin Password    Session Timeout >

*i* Session Timeout ?

\* Session Timeout

3600

Save

# 7 Introduction to the Mesh Repeater

## 7.1 EW300R

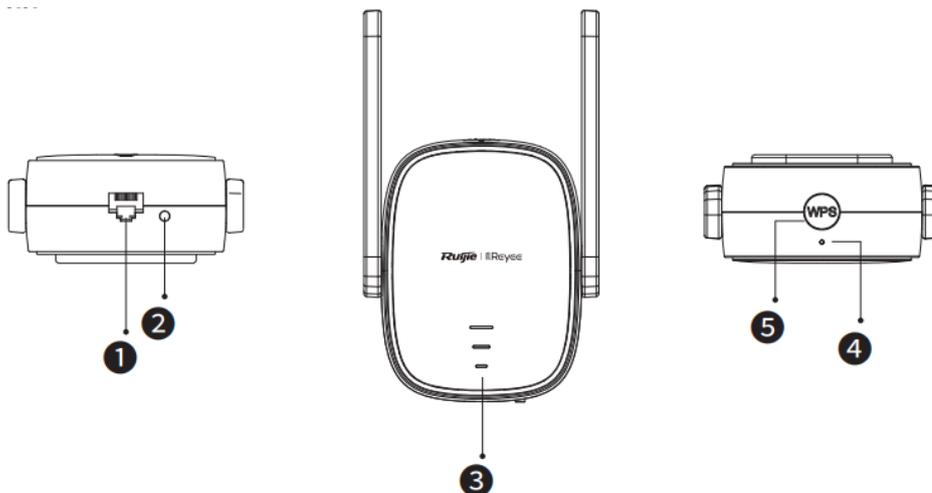
The EW300R mesh repeater uses binaural antennas to support 2.4 GHz dual bands and is equipped with two independent signal amplification chips. It can extend the dual-band Wi-Fi coverage. The maximum wireless rate of the entire device is 1200 Mbps. The EW300R can extend the signals of other devices, and can also connect to the Internet independently.

The signals that the EW300R can extend are:

- Wi-Fi of any model from Reyee.
- Wi-Fi of other vendors' devices. The compatibility problem may exist.
- For the open hotspots in the merchant stores, the repeater function may be denied. The signals may not be extended. In addition, open networks have security risks, so it is not recommended to extend such signals.

### Caution

The supported encryption types include WPA-PSK, WPA2-PSK, and WPA-PSK/WPA2-PSK. If you want to extend encrypted signal, please enter the correct Wi-Fi password.



### 7.1.1 Network Interface

In the factory settings state, the network interface works in WAN mode, which can be connected to an optical modem as a router. To log in to the web page of the mesh repeater, connect to the Wi-Fi of mesh repeater.

### 7.1.2 System Status LED

Status		Description
Blue	Solid on	The device is functioning properly. / The port has made a successful link.

Status		Description
	Blinking	The device is starting up. / The device is restoring factory settings.
Red	Solid on	The network is unreachable.

### 7.1.3 Signal Status LED

Status		Description
Blinking alternately		The device is accessing the Wi-Fi network of the primary router.
White	Three bars on	The signal strength is high.
	Two bars on	The signal strength is medium.
	One bar on	The signal strength is low.
Off		<ol style="list-style-type: none"> <li>The device is set to the router mode.</li> <li>The device fails to access the Wi-Fi network of the primary router.</li> </ol>

### 7.1.4 Buttons

Button		Description
WPS Button	Short press for less than 2s	Establish a WPS network with other routers.
Reset Button	Short press for less than 2s	Turn on or off the signal status LED.
	Long press for more than 5s	The device restores factory settings.

## 7.2 EW1200R

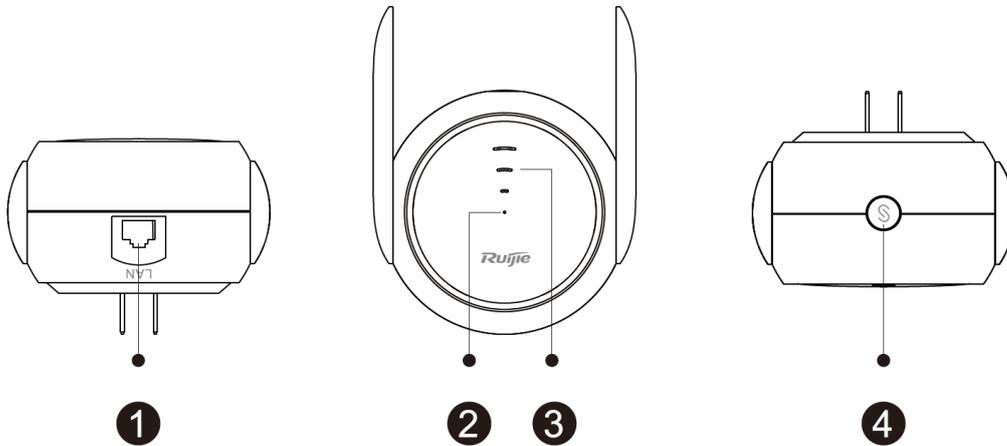
The EW1200R mesh repeater uses circular binaural antennas to support 2.4 GHz and 5 GHz dual bands and is equipped with two independent signal amplification chips. It extends the dual-band Wi-Fi coverage and provides a maximum of 1200 Mbit/s wireless rate. Furthermore, the EW1200R can extend signals of other devices, and can also connect to the Internet independently.

The EW1200R can extend the following signals:

- Wi-Fi of any model from Ruijie.
- Wi-Fi of other vendors' devices. However, there may be compatibility issues.
- Open hotspots such as CMCC, Chinanet, and merchant stores. The repeater function may be forbidden. Such signals may fail to be extended. In addition, open networks have security risks, so extending such signals is not recommended.

**⚠ Caution**

The EW1200R supports WPA-PSK, WPA2-PSK, and WPA-PSK/WPA2-PSK. If you want to extend encrypted signals, enter the correct Wi-Fi password.



No.	Name
1	Ethernet interface
2	System LED
3	Signal LED
4	Mesh/WPS button

### 7.2.1 Network Interface

When the EW1200R uses factory settings, the network interface works in WAN mode, which can be connected to an optical modem as a router. In this situation, you cannot log in to the web page of the mesh repeater through the network interface. To log in to the web page of the mesh repeater, connect to Wi-Fi of the mesh repeater.

### 7.2.2 System LED

Color/Status		Description
Green	Solid on	The device is functioning properly.
	Blinking	The device is starting up or restoring factory settings.
Orange	Solid on	The device fails to access the Wi-Fi network of the primary router.
	Blinking	The device is accessing the Wi-Fi network of the primary router.
Red	Solid on	The network is unreachable.

### 7.2.3 Signal LED

Color/Status		Description
Blinking alternately		The device is accessing the Wi-Fi network of the primary router.
White	Three bars on	The signal strength is strong.
	Two bars on	The signal strength is medium.
	One bar on	The signal strength is low.
Off		<p>The device is set to work in router mode.</p> <p>The device fails to access the Wi-Fi network of the primary router.</p>

### 7.2.4 Mesh/WPS Button

Mesh/WPS Button	Description
Long-press for more than 5s	The device restores factory settings.
Short-press for less than 2s	<p>Three functions are triggered simultaneously:</p> <p>Turn on or off the signal LED.</p> <p>Perform mesh networking as the Reyee primary device.</p> <p>Establish a WPS network with other routers.</p>

# 8 Mesh Repeater's Login

## 8.1 Connecting to the Device

- **Connecting the Device to a Reyee Router (Reyee Mesh)**

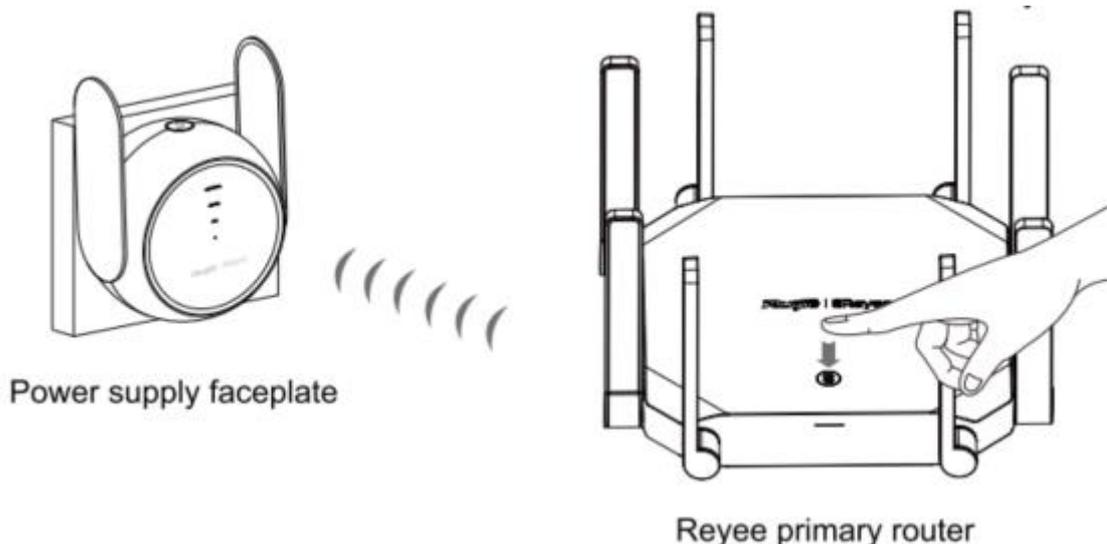
- Connect the mesh repeater to a power source, and wait for 1-2 minutes until the status of the center green LED changes from blinking to solid on. The mesh repeater is started.
- Press the Reyee mesh button on the primary Reyee router or connect the network cable to the primary Reyee router for automatic networking. When the three bars of the LED are on, Reyee mesh is successfully set up. Then the default Wi-Fi disappears, and the Wi-Fi name and password are synchronized with the primary router. When the signal LED is solid white, the network connection is successful. Clients can connect to the amplified Wi-Fi of the primary router to access the Internet.
- If the center dot LED is solid red, the network connection fails. Check whether the primary router can access the Internet. If the center dot is solid orange, the connection with the primary router fails. Move the mesh repeater to a position closer to the primary router, remove obstacles, and press the Reyee mesh button on the primary router again.

---

**⚠ Caution**

When you connect a network cable to the Reyee router, the router will automatically connect to the network. After the network connection is successfully set up, the default signal of the mesh repeater disappears. In this situation, the mesh repeater is successfully connected and managed by the Reyee primary router. The default address of the mesh repeater is unreachable.

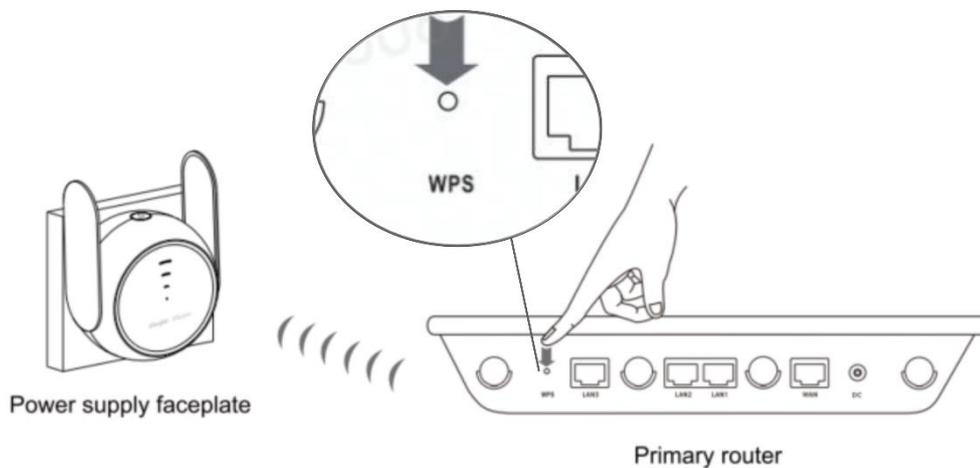
---



- **Connecting the Device to a Primary Router (WPS)**

- Connect the mesh repeater to a power source, and wait for 1-2 minutes until the status of the center green LED changes from blinking to solid on. The mesh repeater is started.

- b Press the WPS button on the primary router.
- d Press the Reyee mesh button of the mesh repeater within 2 minutes. When the three bars of the LED are on, the mesh repeater is connecting to the primary router. When the signal LED is solid white, the network connection is successful. In this situation, the default Wi-Fi disappears, and the Wi-Fi name and password are synchronized with the primary router. Clients can connect to the amplified Wi-Fi of the primary router to access the Internet.
- e If the center dot LED is solid red, the network connection fails. Check whether the primary router can access the Internet. If the center dot is solid orange, the connection with the primary router fails. Move the mesh repeater to a position closer to the primary router, remove obstacles, and repeat the preceding operations.



### ● Connect the Device to a Modem or the Other Router

Before performing this step, you need to connect the device to the Internet. Search for the wireless network with the Wi-Fi name **@Ruijie-sXXXX** by using a mobile phone or laptop. The mobile phone or laptop can log in to the web management page through a browser.

---

#### Note

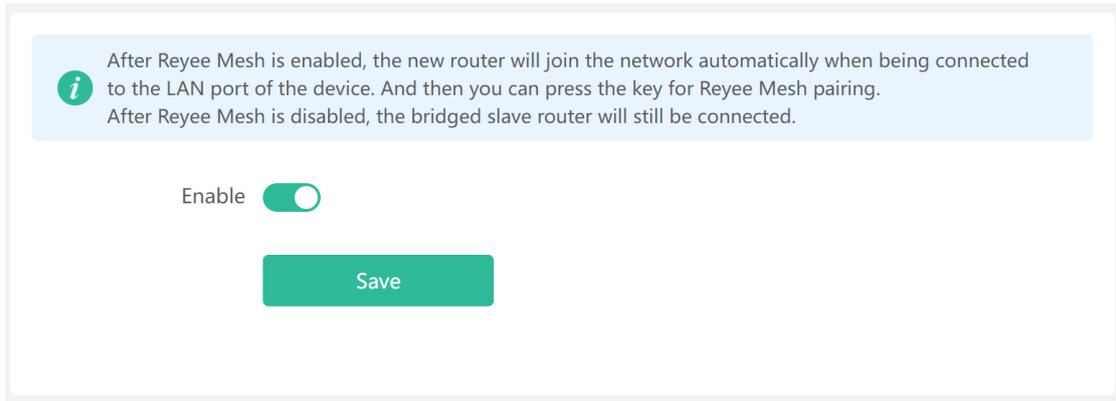
In the Wi-Fi name, XXXX in the Wi-Fi name is the last four digits of the MAC address of each device. You can find the default wireless network name and web login address at the bottom of the device.

---

#### Caution

When an EW1200R is connected to a Reyee router, the EW1200R is automatically connected and functions as a mesh repeater without any manual configurations. If you want to use an EW1200R as a router, disable the Reyee mesh discovery function of the primary router.

---



## 8.2 Login

The configuration wizard page will pop up automatically if you log in for the first time. If no configuration page pops up, enter the IP address into the address bar of the browser and press **Enter** to navigate to the login page.

**Table 8-1 Default Configuration**

Item	Default
IP address	192.168.110.1
Username/Password	Username and password are not required at your first login and you can configure the access point directly.

If you forget the IP address or password, press the  button for over 5 seconds to restore the default settings. Then log in again with the default IP address and password.

 **Caution**

Restoring the factory settings will clear the current configuration and require a re-login. Exercise caution when performing this operation.

# 9 Mesh Repeater's Network Settings

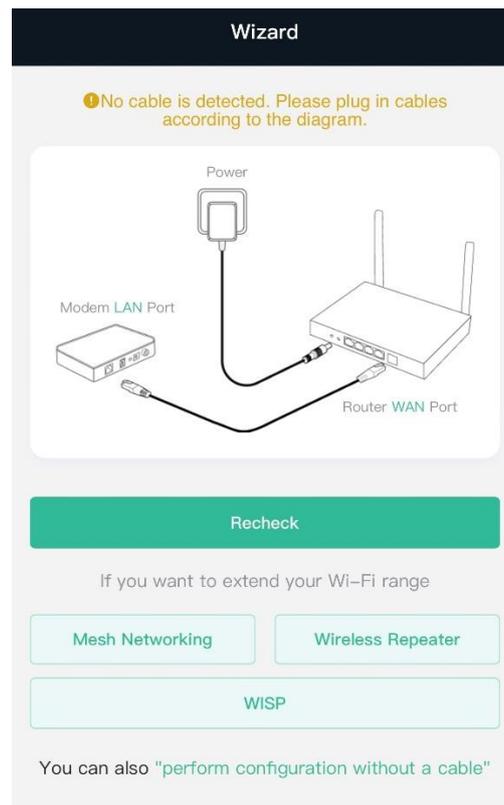
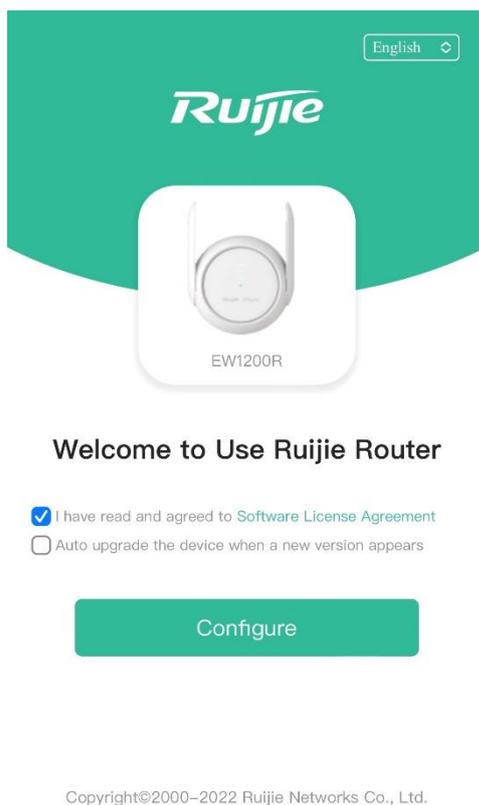
## 9.1 Network Settings

### 9.1.1 Getting Started

- Ensure that the primary router can connect to the Internet successfully.
- To use the device as a mesh repeater, remove the network cable from the device first.

### 9.1.2 Configuration Steps

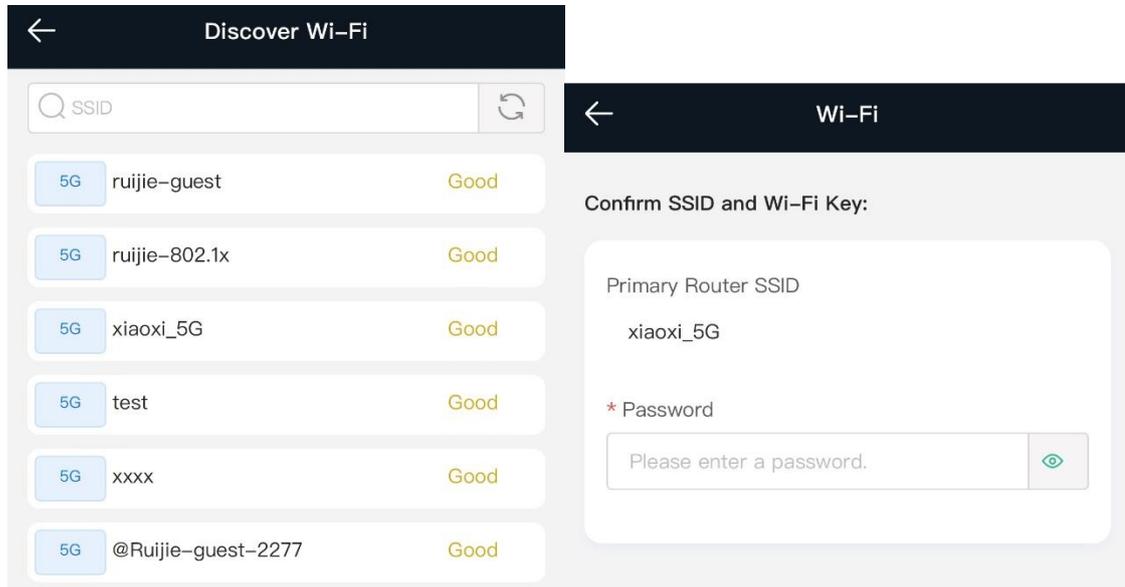
- To extend the Wi-Fi of the Reyeer router by using the Reyeer mesh function, press the Reyeer mesh button of the Reyeer router for automatic networking. For details, see [8.1 Connecting to the Device](#).
- To extend the Wi-Fi of the WPS-supported router, press the WPS button of the primary router and then the Reyeer Mesh button of the mesh repeater for networking. For details, see [8.1 Connecting to the Device](#).
- To extend the Wi-Fi of other routers, click **Configure**. The wireless repeater mode and wireless ISP mode are available.



(1) Select Wireless Repeater or WISP.

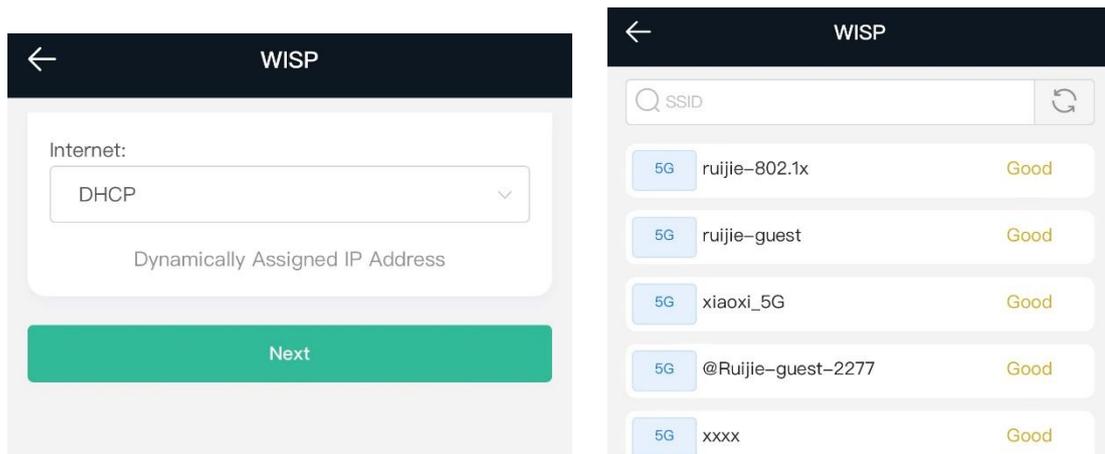
- Wireless repeater mode: Click **Wireless Repeater**, select the Wi-Fi of the primary router, and enter the Wi-Fi password of the primary router to connect to the Wi-Fi.

In wireless repeater mode, the device extends Wi-Fi signals and disables its DHCP function. When clients connect to the wireless network, the primary router assigns addresses to them. When the device in wireless repeater mode extends the network of the primary router, the WAN interface is unchanged. If you connect the network cable to the WAN interface, the device automatically switches to the wired repeater mode.



- WISP mode: Click **WISP**, select a networking mode on the pop-up network settings page, and click **Next**. The device automatically obtains an IP address. If the primary router cannot assign IP addresses, select **Static IP**. Select the Wi-Fi of the primary router, and enter the Wi-Fi password to connect to the primary router.

In wireless ISP mode, the device still supports routing and DHCP. The clients connected to the primary router are assigned IP addresses by the primary router; the clients connected to the secondary router are assigned IP addresses by the secondary router. When the device connects to the Internet wirelessly, the network interface functions as a LAN interface.



- (2) Set the Wi-Fi name and password for the router. When the settings are saved, Wi-Fi settings are reset.

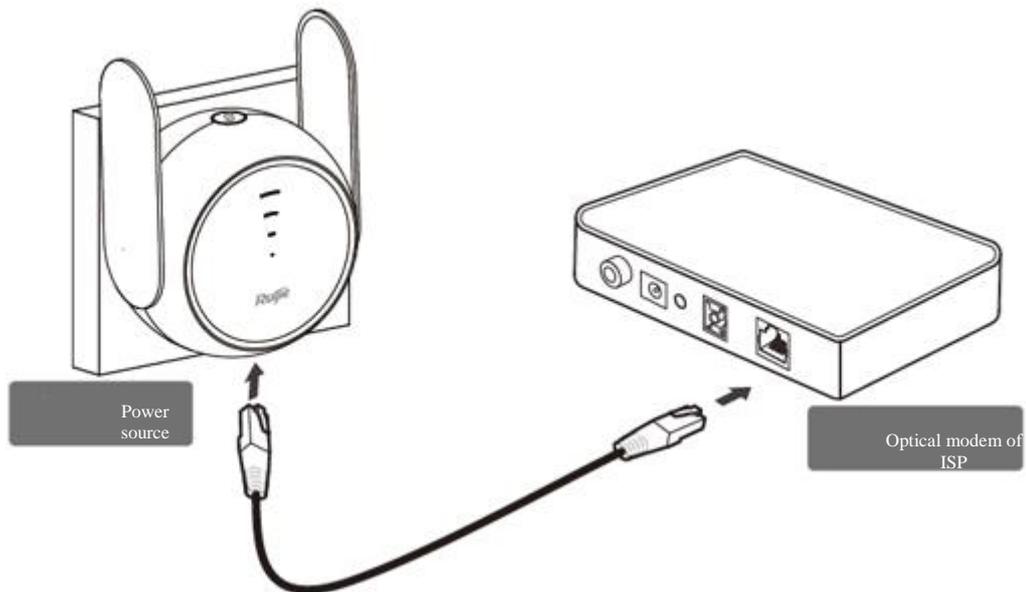
### 9.1.3 Verifying the Configuration

The device can access the Internet after connecting to the Wi-Fi network of the primary router.

## 9.2 Network Settings (in Router Mode)

### 9.2.1 Getting Started

- (1) Connect the mesh repeater to a power source.
- (2) Connect the LAN interface of the optical modem to the network interface of the mesh repeater through a network cable. If the network cable is not connected, the wireless repeater page is automatically displayed.
- (3) Log in to the web management interface of the mesh repeater. For details, see [8.2 Login](#).



- (4) Configure the Internet connection mode according to requirements of the local ISP. Otherwise, the Internet may fail to be accessed due to improper configuration. You are advised to contact your local ISP to confirm the Internet connection mode.
  - o Check whether the Internet connection mode is PPPoE, DHCP mode, or static IP address.
  - o In PPPoE mode, a username, a password, and possibly a service name are needed.
  - o In static IP address mode, an IP address, a subnet mask, a gateway address, and a DNS server address need to be configured.

### 9.2.2 Configuration Steps

#### 1. Configuring an Internet Connection Mode

Click **Configure** and select the Internet mode confirmed with the ISP.

- **DHCP**: The device detects whether it can obtain an IP address through DHCP by default. If the device connects to the Internet successfully, you can click **Next** without entering an account.

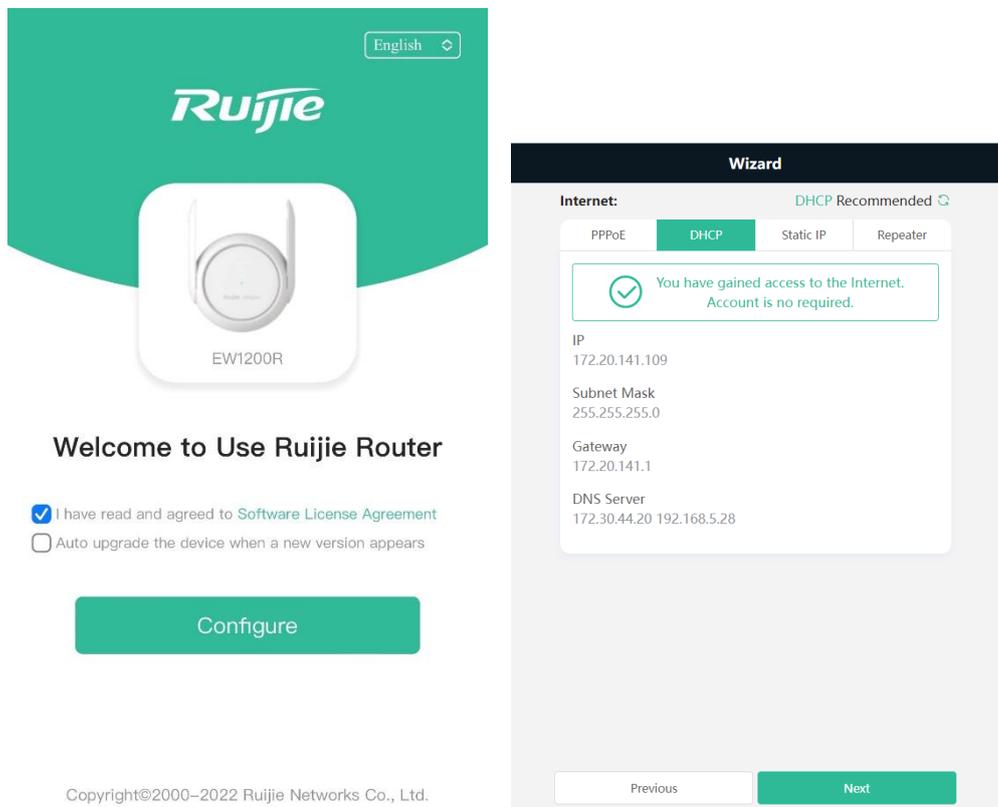
---

#### ⚠ Caution

If the primary router assigns an IP address from 192.168.110.0 to the mesh repeater, the mesh repeater will change the IP address of its LAN port to 192.168.111.1 automatically. If the mesh repeater is incorrectly considered as the primary router and the configuration is changed, the device may be disconnected from the network. You are advised to refer to the model and Wi-Fi information on the home page.

---

- **PPPoE:** Click **PPPoE**, and enter the username, password, and service name. Click **Next**.
- **Static IP:** Enter the IP address, subnet mask, gateway address, and DNS server address, and click **Next**.



## 2. Configuring the Wi-Fi Network

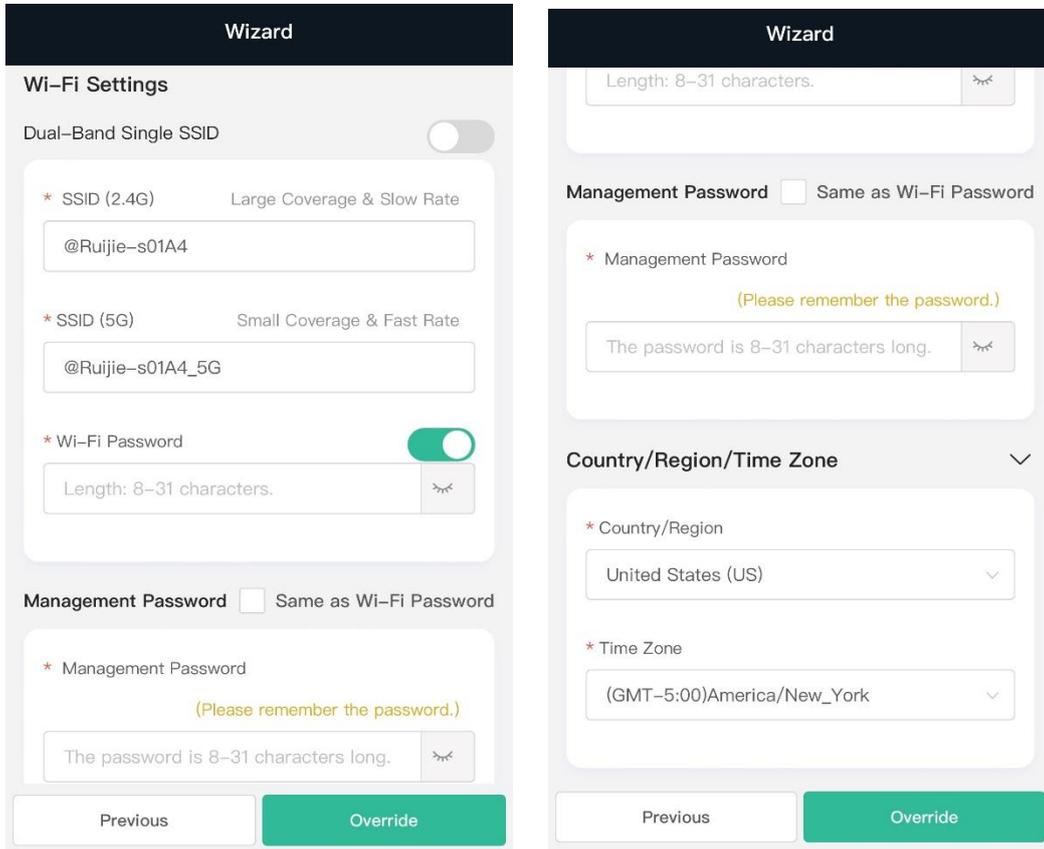
- (1) Dual-band integration: When dual-band integration is enabled, the 2.4 GHz SSID will be consistent with the 5 GHz SSID. The 2.4 GHz signal is strong but is easily interfered by various wireless signals. The 5 GHz band delivers fast speed, low latency, and less interference. Dual-band integration is disabled by default. You are advised to disable this feature. After configuring a 5 GHz SSID, you can enjoy better Internet experience by accessing the 5 GHz band in an unobstructed location near the device.

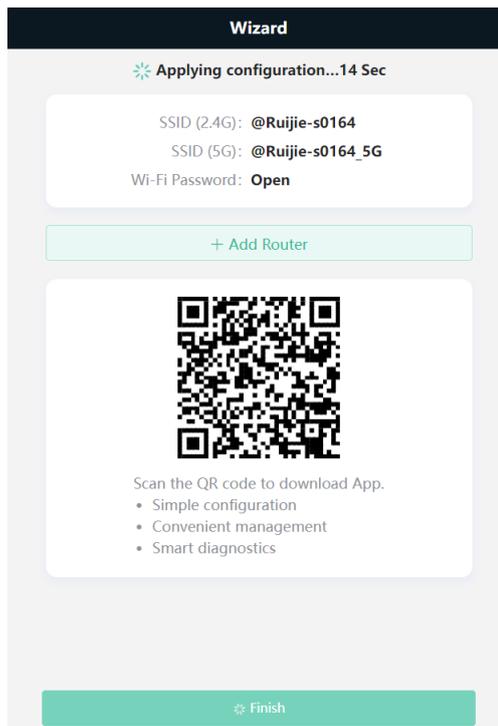
### **Note**

2.4 GHz and 5 GHz mentioned in this document only refer to the channels with the frequency of 2.4 GHz and 5 GHz, and are irrelevant to Fifth Generation (5G) Mobile Communication Technology.

- (2) Setting the 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 network security. The password must be a string of 8 to 64 characters, which can contain uppercase and lowercase letters, digits, and English characters. It cannot contain special characters such as single quotation marks ('), double quotation marks ("), or spaces. The SSID (5 GHz) is the name of the 5 GHz radio. If dual-band integration is enabled, you need to configure only one SSID.
- (3) Setting the management password: The password is used for logging in to the management page. The management password must be a string of 8 to 64 characters, which must contain at least three types among uppercase letters, lowercase letters, digits, and English characters. It cannot contain admin, Chinese characters, spaces, or question marks (?). You can select **Same as Wi-Fi Password**.

- (4) Setting the country or region: The Wi-Fi channel may vary depending on countries. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.
- (5) Setting the time: The network time server is enabled by default to provide the time service. You are advised to select the actual time zone.
- (6) Overriding the configuration: Click **Override**. Settings of the Wi-Fi network are reset. You need to enter the new Wi-Fi password to connect to the new Wi-Fi network.





### 9.2.3 Verifying the Configuration

The device can access the Internet after connecting to the Wi-Fi network.

# 10 Mesh Repeater's Wi-Fi Network Settings

## 10.1 Changing the SSID and Password

Choose **Wi-Fi > Wi-Fi Settings**.

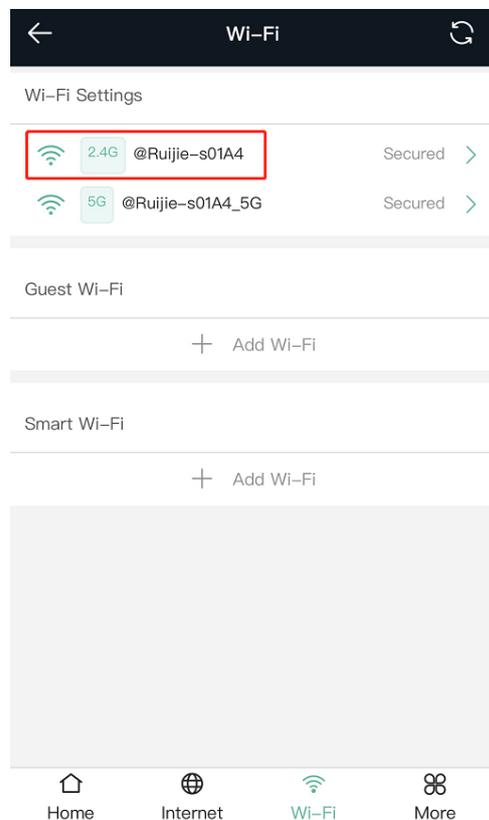
Click the target, change **SSID** and **password** of the Wi-Fi network, and click **Save**.

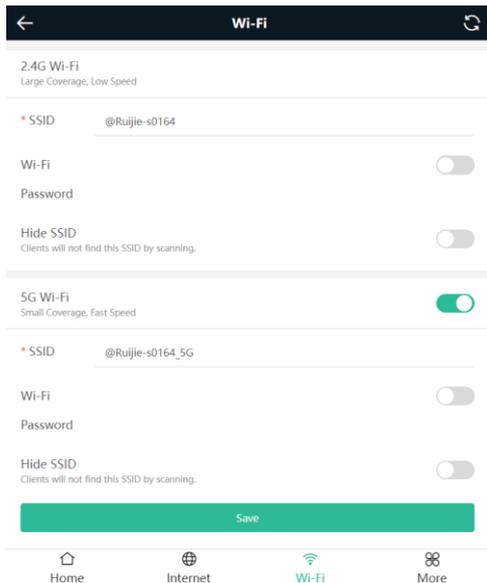
---

 Caution

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

---





## 10.2 Hiding the SSID

### 10.2.1 Overview

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

### 10.2.2 Getting Started

Remember the SSID so that you can enter the correct SSID after the function is enabled.

### 10.2.3 Configuration Steps

PC view: Choose **More > WLAN > Wi-Fi > Wi-Fi Settings**.

Click to expand **Advanced Settings**. Enable **Hide SSID** and click **Save**.

Mobile phone view: Choose **Wi-Fi > Wi-Fi Settings**.

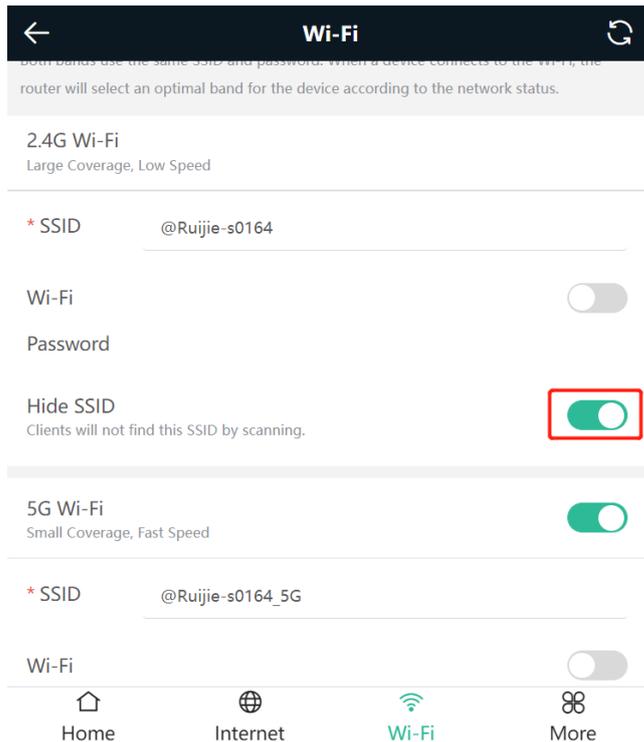
Click the target, enable **Hide SSID**, and click **Save**.

---

#### Caution

After **Hide SSID** is enabled, all clients need to enter the SSID and password manually to search for the Wi-Fi network. Exercise caution when performing this operation.

---



#### Note

Users need to manually enter the SSID and password each time they connect to a hidden Wi-Fi network. An Android-based device is used as an example: To connect it to a hidden Wi-Fi network, choose **WLAN > Add network > Network name**, enter the Wi-Fi name, select **WPA/WPA2/WPA3** from the **Security** drop-down list, enter the password, and click **Connect**.

## 10.3 Configuring Wi-Fi

### 10.3.1 Overview

The mesh repeater supports three types of Wi-Fi: primary Wi-Fi, guest Wi-Fi, and smart Wi-Fi.

- **Primary Wi-Fi:** The primary Wi-Fi network is listed in the first line of the page and is enabled by default.
- **Guest Wi-Fi:** The guests Wi-Fi network is provided for guests and is disabled by default. It supports user isolation, that is, access users are isolated from each other. They can only access the Internet through Wi-Fi, but cannot access each other, improving security.

The guest Wi-Fi network can be disabled as scheduled. You can configure to enable the guest Wi-Fi network 1 hour later. When the time expires, the guest Wi-Fi network is disabled.

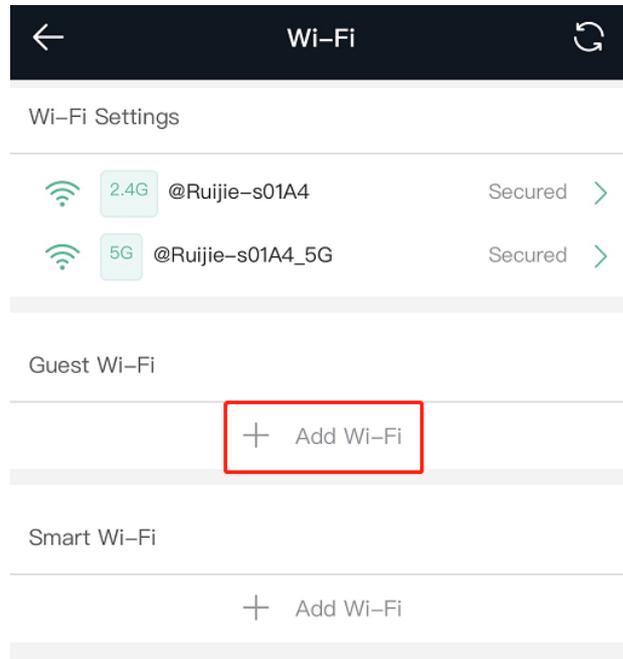
- **Smart Wi-Fi:** The smart Wi-Fi network is disabled by default. Smart clients can connect to the smart Wi-Fi network for a long period of time. The smart Wi-Fi network cannot be disabled as scheduled.

### 10.3.2 Configuration Steps

Mobile phone view: Choose **Wi-Fi > Wi-Fi Settings**.

The page displays the primary Wi-Fi network, guest Wi-Fi network, and smart Wi-Fi network from top to bottom. Click **Add Wi-Fi** and set the SSID and password.

PC view: Choose **More** >  **WLAN** > **Wi-Fi** > **Wi-Fi Settings** > **Guest Wi-Fi/Smart Wi-Fi**.



## 10.4 Configuring a Wi-Fi Blacklist or Whitelist

### 10.4.1 Overview

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.

### 10.4.2 Configuration Steps

Mobile phone view: Choose **More** > **Switch to PC view** > **More** >  **WLAN** > **Blacklist/Whitelist**.

PC view: Choose **More** >  **WLAN** > **Blacklist/Whitelist**.

The blacklist configuration is used as an example. If you want to configure a whitelist, perform the same steps.

(1) Select the blacklist mode and click **Add**. The default mode is blacklist.

In the displayed dialog box, enter the MAC address and remarks of the client to be blacklisted. The device displays information about the connected clients. Select a client. Then the client will be added to the blacklist automatically. Click **OK** to save the configuration. The client will be disconnected and prevented from connecting to the Wi-Fi network.

#### Caution

This configuration prevents some devices from connecting to the Wi-Fi network. Exercise caution when performing this operation.

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 30 members can be added.

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

< 1 > 10/page Total 0

Add ×

\* MAC

Example: 00:11:22:33:44:55

Please enter a MAC address.

- RainOS (30:0d:9e:3e:7e:be)
- PC-3e7ebe (52:54:00:3e:7e:be)
- ELZ-AN10 (82:26:75:da:ce:73)
- Honor\_10-a96f220e73c0a3f9 (c8:c2:fa:be:55:5d)

Cancel

OK

(2) Click **Delete** and then click **OK**. The client can connect to the Wi-Fi network again.

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 30 members can be added.

<input type="checkbox"/>	MAC	Remark	Action
<input type="checkbox"/>	F2:36:1D:EB:20:6 D	test	Edit <a href="#">Delete</a>

< 1 > 10/page Total 1

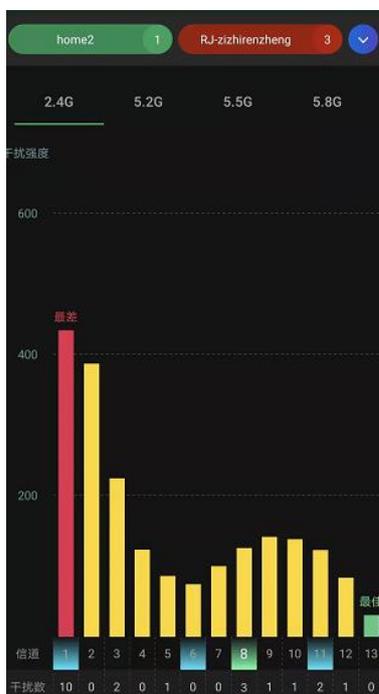
## 10.5 Optimizing the Wi-Fi Network

### 10.5.1 Overview

The device detects the surrounding wireless environment and selects the appropriate configuration upon power-on. However, network freezing caused by wireless environment changes cannot be avoided. Restarting the mesh repeater is a convenient and effective method to cope with this issue. The mesh repeater supports scheduled restart. For details, see [12.4 Configuring Scheduled Reboot](#). You can also analyze the wireless environment around the mesh repeater and select appropriate parameters.

### 10.5.2 Getting Started

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



### 10.5.3 Configuration Steps

#### 1. Optimizing the Radio Channel

Mobile phone view: Choose **More** > **Channel Transmit Power**.

PC view: Choose **More** >  **WLAN** > **Radio Frequency**.

Select the best channel identified by Wi-Fi Moho or other Wi-Fi scanning app. Click **Save** to make the configuration take effect immediately. Excess clients connected to a channel may result in stronger wireless interference.

---

#### Note

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

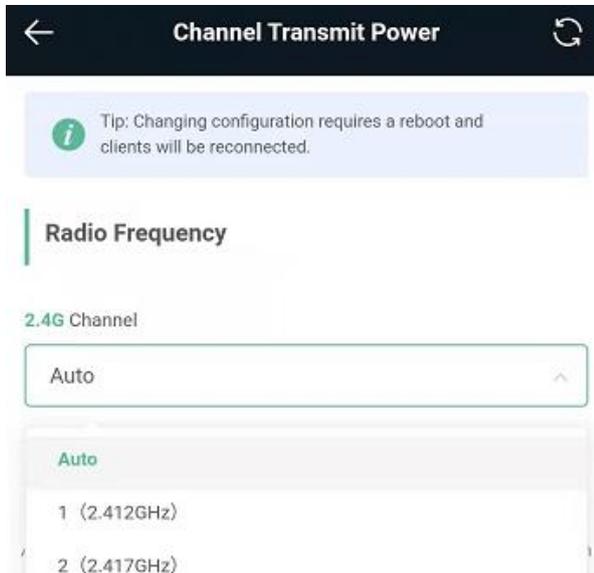
---

---

**⚠ Caution**

Settings of settings of the Wi-Fi network are reset after the radio channel is changed. Therefore, exercise caution when performing this operation.

---



## 2. Optimizing the Channel Width

Mobile phone view: Choose **More > Country(Region)/Channel Width**.

PC view: Choose **More >  WLAN > Radio Frequency**.

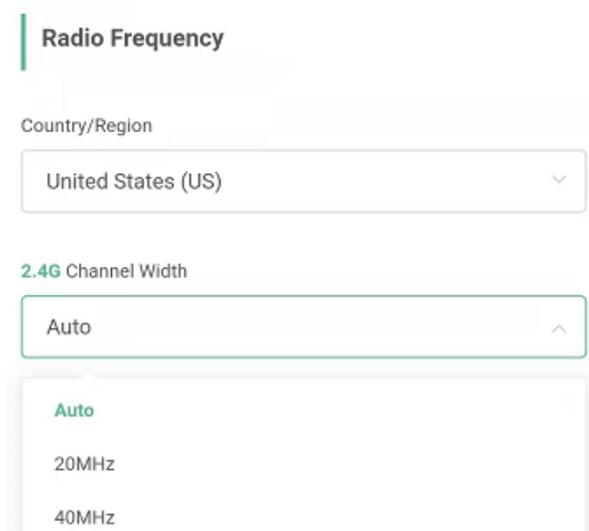
If the interference is severe, select a lower channel width to avoid network freezing. The mesh repeater supports 20 MHz and 40 MHz channel width. The Wi-Fi network speed is more stable when the channel width is smaller, and a larger channel width makes the device more prone to interference. You are advised to select 20 MHz for the 2.4 GHz radio and Auto for the 5 GHz radio. A channel width of 80 MHz at 5 GHz radio is recommended for a speed test. After changing the channel width, click Save to make the configuration take effect immediately.

---

**⚠ Caution**

After the change, settings of settings of the Wi-Fi network are reset, and clients need to reconnect to the Wi-Fi network. Therefore, exercise caution when performing this operation.

---



**Radio Frequency**

Country/Region

United States (US) ▾

2.4G Channel Width

Auto ▲

Auto

20MHz

40MHz

### 3. Optimizing the Transmit Power

Mobile phone view: Choose **More > Channel Transmit Power**.

PC view: Choose **More >  WLAN > Radio Frequency**.

A greater transmit power indicates a larger coverage and brings stronger interference to surrounding wireless routers. The default value is **Auto**, indicating automatic adjustment of the transmit power. In a scenario in which routers are installed in centralized mode, a lower transmit power is recommended.

---

 **Caution**

After the change, settings of the Wi-Fi network are reset, and clients need to reconnect to the Wi-Fi network. Therefore, exercise caution when performing this operation.

---

← Channel Transmit Power ↻

Radio Frequency

2.4G Channel

Auto

Transmit Power

Auto Lower Low Medium High

5G Channel

Same as Master AP

Transmit Power

Auto Lower Low Medium High

Save

#### 4. Configuring the roaming sensitivity (optional)

Mobile phone view: Choose **More > Roaming Optimization**.

PC view: Choose **More >  WLAN > Radio Frequency**.

Clients such as mobile phones support the roaming function but the sensitivity level may be not high. The roaming sensitivity enables the device to proactively 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.

A low sensitivity is recommended.

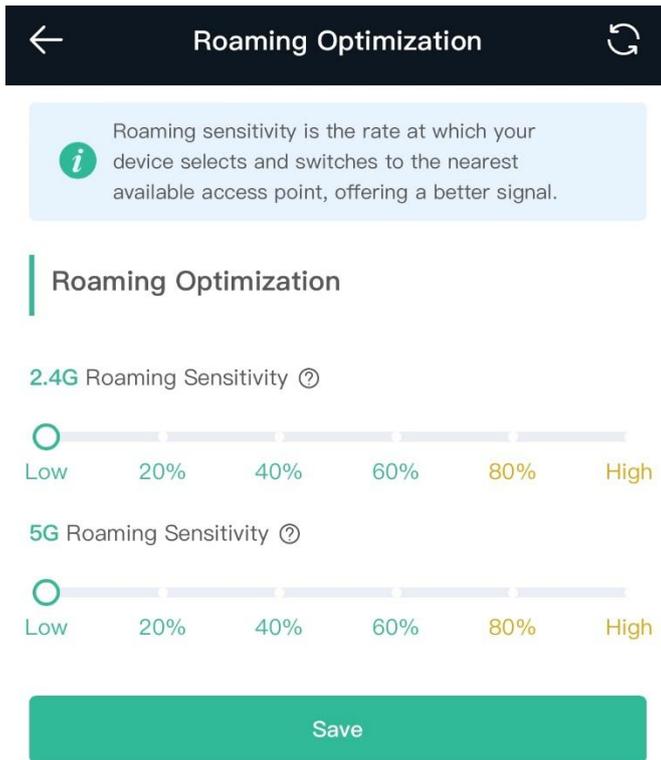
---

#### Caution

After the change, settings of the Wi-Fi network are reset, and clients need to reconnect to the Wi-Fi network.

A high sensitivity may cause Wi-Fi network disconnection. Therefore, exercise caution when performing this operation.

---



## 10.6 Configuring the Healthy Mode

Mobile phone view: Choose **More** > **Healthy Mode** > **Healthy Mode**.

PC view: Choose **More** > **WLAN** > **Wi-Fi** > **Healthy Mode**.

Click **Enable** to enable the healthy mode. You are allowed to set the validity time for the healthy mode.

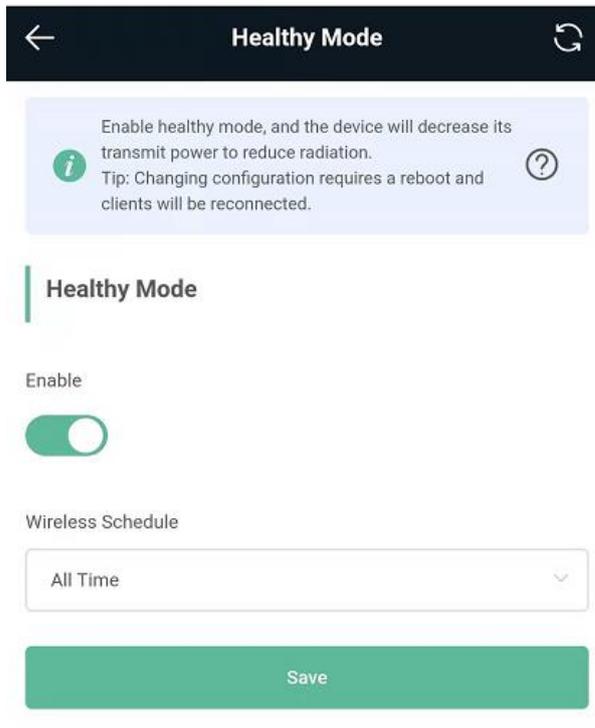
After the healthy mode is enabled, the transmit power and the Wi-Fi coverage area will decrease. The healthy mode may reduce signal strength and cause network freezing. You are advised to disable it.

---

**i** Note

All Ruijie mesh repeaters have undergone stringent radiation detection and evaluation, and comply with IEC/EN62311, EN 50385 and other standards. Wi-Fi networks will not affect human health, and you can use Ruijie wireless routers safely.

---



# 11 Mesh Repeater's Networks Settings

## 11.1 Configuring an Internet Connection Mode

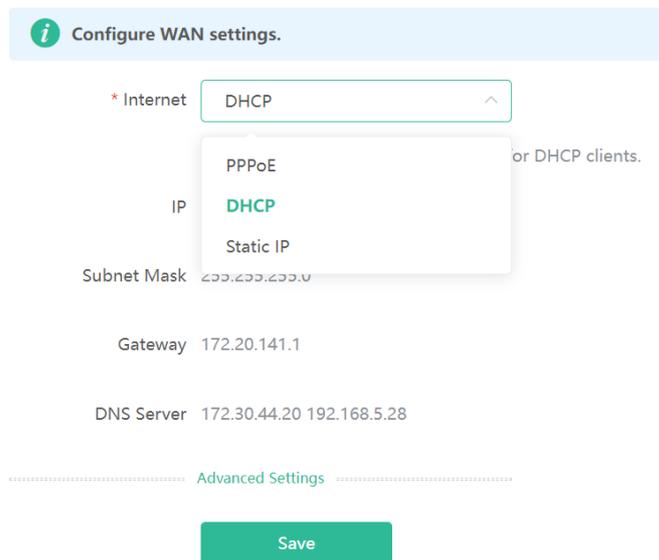
 Caution

This feature is supported by only the router and WISP modes.

Mobile phone view: Choose **More** > **Switch to PC view** > **More** >  **Basics** > **WAN**.

PC view: **More** >  **Basics** > **WAN**.

For details, see [9.2 Network Settings \(in Router Mode\)](#).



## 11.2 Changing the IP Address of a LAN Port

 Caution

This feature is supported by only the router and WISP modes.

Mobile phone view: Choose **More** > **Switch to PC view** > **More** >  **Basics** > **LAN**.

PC view: Choose **More** >  **Basics** > **LAN**.

Change the IP address and subnet mask, and click **Save**. After changing the IP address of the LAN port, log in again with the new IP address.

 Caution

Changing the IP address and subnet mask will disconnect the device from the Wi-Fi network. You need to reconnect to the Wi-Fi network. Therefore, exercise caution when performing this operation.

[LAN Settings](#)   [DHCP Clients](#)   [Static IP Addresses](#)   [DNS Proxy](#)

---

**LAN Settings**

 The LAN port is configured with **An address conflict occurs..** The IP address is **192.168.110.1** to **192.168.111.1** to ensure network connection.

\* IP

\* Subnet Mask

Remark

\* MAC

## 11.3 Changing the MAC Address

---

 **Caution**

This feature is supported by only the router and WISP modes.

---

The ISP may restrict Internet access of devices with unknown MAC addresses to ensure security. In this case, you can change the MAC address of the WAN port to another address. You are advised to use the MAC address of an old router that is allowed to access the Internet (the MAC address can be found on the bottom label of the device).

Mobile phone view: Choose **More > Switch to PC view > More >**  **Basics > WAN > Advanced Settings.**

PC view: Choose **More >**  **Basics > WAN > Advanced Settings.**

Enter the MAC address in the format of 00:11:22:33:44:55.

To change the MAC address of the LAN port, choose  **Basics > LAN.**

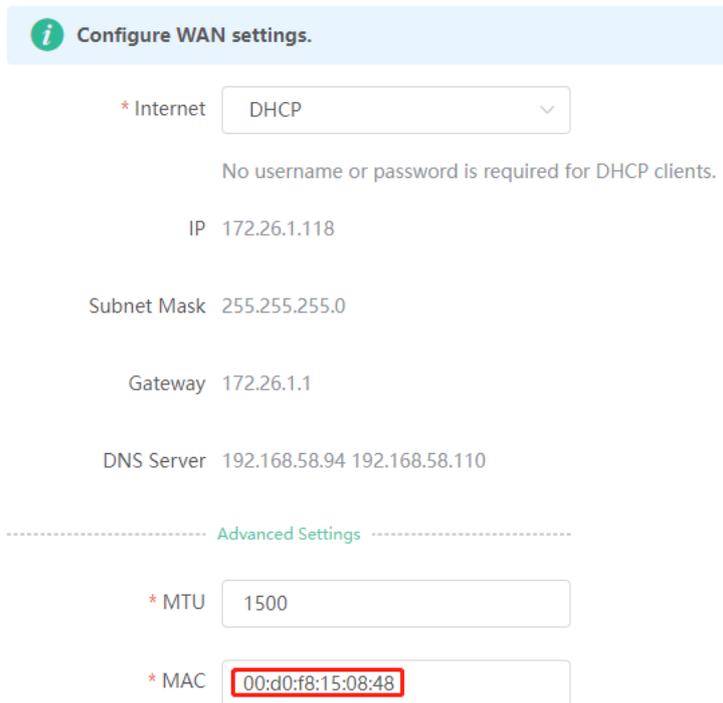
---

 **Caution**

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

---

Figure 11-1 WAN Port Settings



**Configure WAN settings.**

\* Internet

No username or password is required for DHCP clients.

IP 172.26.1.118

Subnet Mask 255.255.255.0

Gateway 172.26.1.1

DNS Server 192.168.58.94 192.168.58.110

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

\* MTU

\* MAC

## 11.4 Changing the MTU

### Caution

This feature is supported by only the router and WISP modes.

Sometimes, the ISP restrict the speed of large data packets or prevent large data packets from passing through. As a result, the network speed is low or even the network is disconnected. In this case, you are required to set the maximum transmission unit (MTU) to a smaller value.

Mobile phone view: Choose **More** > **Switch to PC view** > **More** >  **Basics** > **WAN** > **Advanced Settings**.

PC view: Choose **More** >  **Basics** > **WAN** > **Advanced Settings**.

The default MTU is 1500, which is the maximum value. You are advised to adjust the value to 1492, 1400, or even smaller if necessary.

[Figure 11-1](#) displays the settings.

**Configure WAN settings.**

\* Internet

No username or password is required for DHCP clients.

IP 172.20.141.109

Subnet Mask 255.255.255.0

Gateway 172.20.141.1

DNS Server 172.30.44.20 192.168.5.28

---

Advanced Settings

\* MTU

\* MAC

**Save**

## 11.5 Configuring the Repeater Mode

### 11.5.1 Wired Repeater

Mobile phone view: Choose **More > Repeater Mode**.

PC view: **More >**  **Basics > Repeater/WISP**.

Connect the network interface of the mesh repeater to the LAN interface of primary router through a network cable.

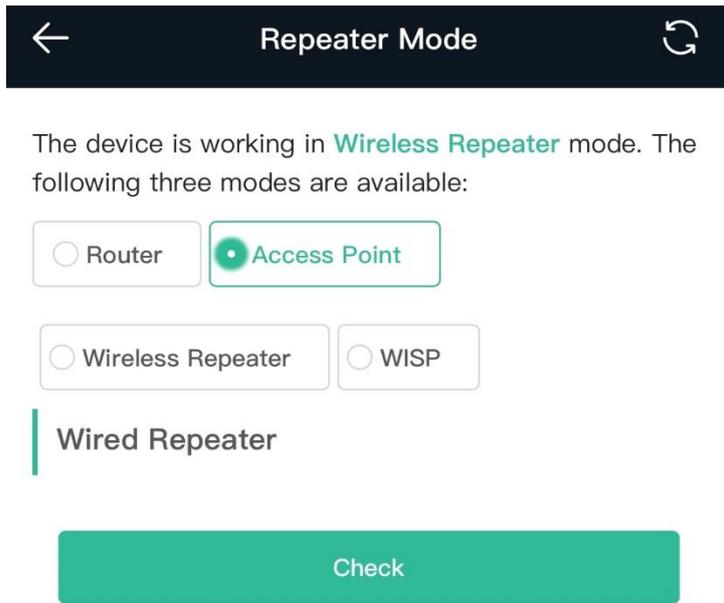
Select **Access Point** and click **Check**. After confirming the Wi-Fi settings of the mesh repeater, click **Save**. The network coverage range is extended.

---

 **Caution**

After the configuration is saved, the connected clients are disconnected from the network for a short time and need to be connected to Wi-Fi again.

---



### 11.5.2 Wireless Repeater

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

---

 Note

- Before using the wireless repeater function, remove the network cable from the mesh repeater.
  - Confirm the Wi-Fi name and password of the primary router before performing the configuration.
- 

Mobile phone view: Choose **More > Repeater Mode**.

PC view: **More >**  **Basics > Repeater/WISP**.

- (1) Click **Wireless Repeater**, and click the search box next to the Wi-Fi name (5G). The list of surrounding Wi-Fi signals is displayed.

←
Repeater Mode
↻

The device is working in **Router** mode. The following three modes are available:

Router

Access Point

**Wireless Repeater**

WISP

### Wireless Repeater

— Primary Router —

SSID (5G)

Please select an SSID for the primary router. ▾

SSID (2.4G)

Please select an SSID for the primary router. ▾

- (2) Select the Wi-Fi signal of the primary router you want to extend. The setting options of this router are displayed. If the signal of selected primary router is encrypted, enter the Wi-Fi password of the primary router. You can configure both 5 GHz and 2.4 GHz signals of the primary router as backup.
- (3) Configure Wi-Fi of this router. You can choose whether Wi-Fi is the same as Wi-Fi of the primary router.
  - If the same Wi-Fi network is used, Wi-Fi settings of the mesh repeater will be automatically synchronized with the primary router. In most cases, clients consider Wi-Fi networks with the same name as one network; therefore, they can find only Wi-Fi of the primary router.
  - If you different Wi-Fi networks are used, configure the local Wi-Fi name and password. Then clients will find different Wi-Fi networks.

---

**⚠ Caution**

After the configuration is saved, the Wi-Fi network is disconnected. The clients need to connect to the new Wi-Fi network. Remember the configured Wi-Fi name and password, and exercise caution when performing the configuration.

You are advised to install the mesh repeater in a position where more than two grids of signals are available to prevent serious signal loss during working. If the signal at the installation position is weak, Wi-Fi signals may fail to be extended or the signal quality is poor after amplification.

---

Figure 11-2 Selecting and Connecting to the Wi-Fi Network of the Primary Router

Local Router

Local Router Wi-Fi

New Wi-Fi  Same as Primary Router Wi-Fi

\* SSID (2.4G)

xiaoxi\_5G\_plus

\* SSID (5G)

xiaoxi\_5G\_plus\_5G

Wi-Fi Password

A blank value indicates no encryption.

Save

### 11.5.3 WISP

WISP allows users to establish their own WLANs for Internet access in public spaces, including coffee shops, hotels, airports, or restaurants.

- (1) Choose **More** > **Switch to PC view** > **More** > **Basics** > **Repeater/WISP**.

Click **WISP** and select an Internet connection mode. Click **Next**.

WAN

\* Internet DHCP

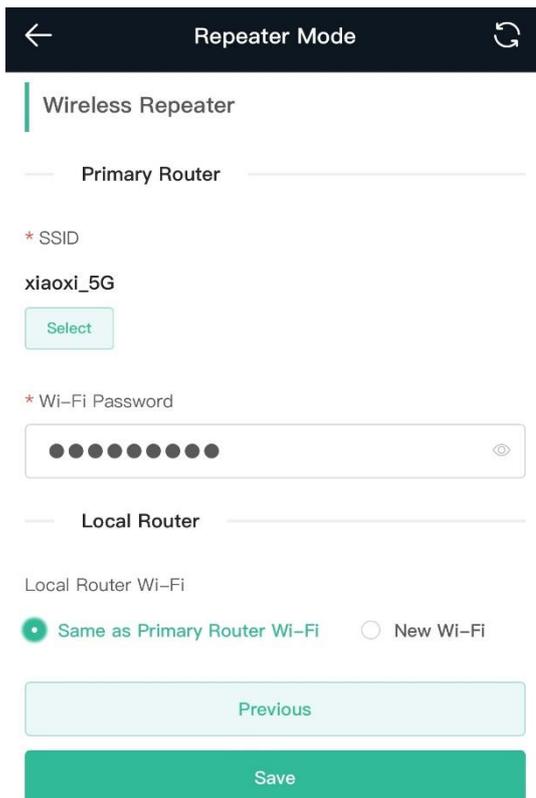
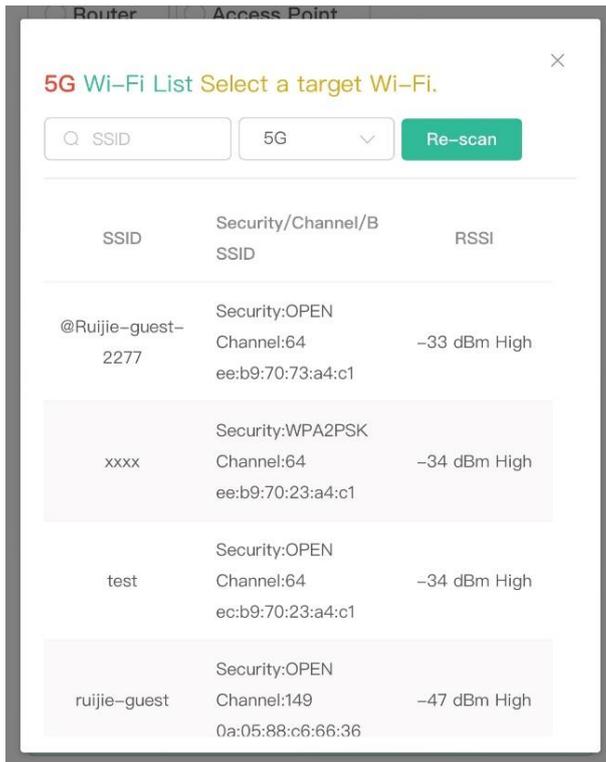
No username or password is required for DHCP clients.

Next

- (2) Click **Select**, select a network signal, enter the password, and click **Save**.

#### Caution

After the configuration is saved, settings of the Wi-Fi network are reset. The clients need to connect to the new Wi-Fi network. Remember the configured Wi-Fi name and password, and exercise caution when performing the configuration.



## 11.6 Online Time Control

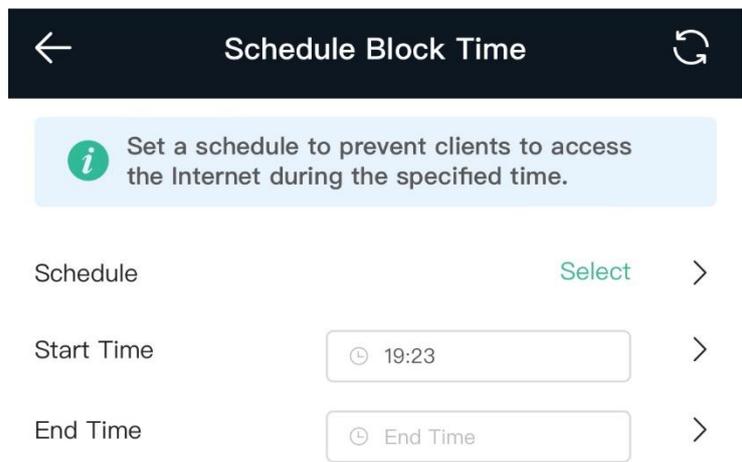
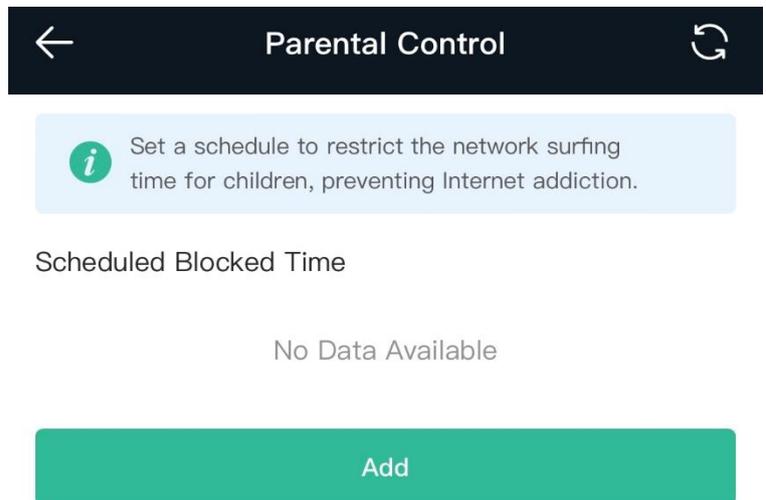
 Caution

This feature is supported by only the router and WISP modes.

Mobile phone view: Choose **More > Parental Control**. Select a client and click **Schedule**, click **Add**, and set the restriction time. The client cannot access the network from the start time to the end time.

PC view: Choose **Clients > Add Blocked Time**.

In the PC view, you can select **Weekdays** or **Weekends** to prevent a client from accessing the Internet all day long, or set **Blocked Time** to **Custom** and set a restriction period.

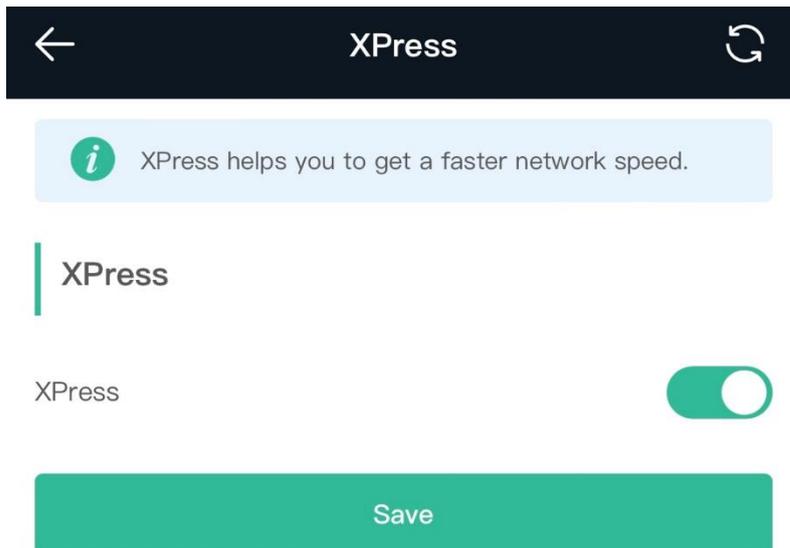


## 11.7 Configuring XPress

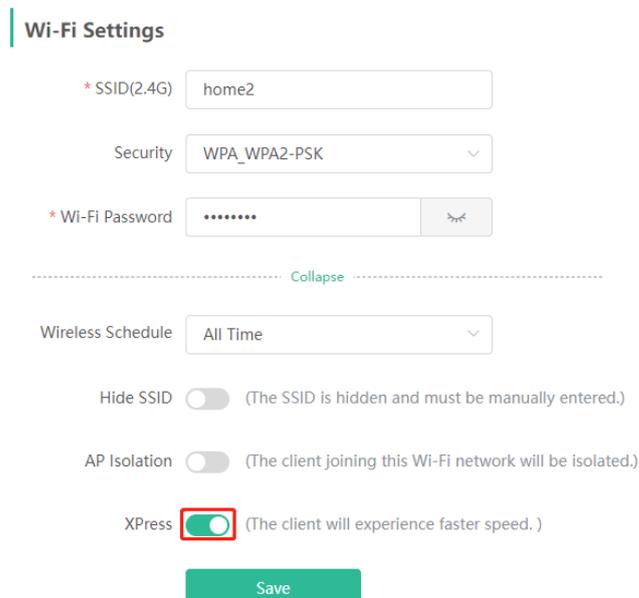
Mobile phone view: Choose **More** > **XPress**.

PC view: Choose **More** >  **WLAN** > **Wi-Fi** > **Wi-Fi Settings** > **Expand** > **XPress**.

Enable **XPress** and click **Save** to save the configuration. After XPress is enabled, you will have a more stable gaming experience.



In the PC view, enable **XPress** as follows.



## 11.8 Configuring the DHCP Server

---

 Caution

This feature is supported by only the router and WISP modes.

---

### 11.8.1 Overview

A DHCP server is responsible for assigning dynamic IP addresses to clients on the Wi-Fi network for Internet access.

### 11.8.2 Configuration Steps

#### 1. Configuring the DHCP Server

Mobile phone view: Choose **More** > **Switch to PC view** > **More** >  **Basics** > **LAN** > **LAN Settings**.

PC view: Choose **More** >  **Basics** > **LAN** > **LAN Settings**.

**DHCP Server:** The DHCP server function is enabled by default. You are advised to enable it when only a single router is used.

---

 Caution

If all DHCP servers on a network are disabled, all clients will fail to obtain dynamic IP addresses. In this case, you need to enable the DHCP server on a router 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, the client will fail to obtain the IP address.

**IP Count:** Enter the number of IP addresses in the address pool. The default value is **254**.

**Lease Time (Min):** Enter the address lease time. When a client keeps connected, the lease is automatically renewed. If a lease is not renewed due to client disconnection or network instability, the IP address will be reclaimed after the lease time expires. After the client is re-connected, the client requests an IP address again. The default lease time is 30 minutes.

LAN Settings DHCP Clients Static IP Addresses DNS Proxy

**LAN Settings**

*i* The LAN port is configured with **An address conflict occurs..** The IP address of the LAN port to ensure network connection.

\* IP

\* Subnet Mask

Remark

\* MAC

DHCP Server

\* Start

\* IP Count

\* Lease Time(Min)

## 2. Viewing DHCP Clients

Mobile phone view: Choose **More** > **Switch to PC view** > **More** >  **Basics** > **LAN** > **DHCP Clients**.

PC view: Choose **More** >  **Basics** > **LAN** > **DHCP Clients**.

Check information about an online client. Click **Convert to Static IP**. The client will be assigned with the specified IP address.

LAN Settings DHCP Clients Static IP Addresses DNS Proxy

*i* View DHCP clients. ?

**DHCP Clients**

Up to 300 IP-MAC bindings can be added.

No.	Hostname	IP	MAC	Remaining Lease Time(Min)	Status
1	RainOS	192.168.111.18	30:0d:9e:3c:d6:be	24	<a href="#">Convert to Static IP</a>
2	PC-3CD68E	192.168.111.53	52:54:00:3c:d6:be	17	<a href="#">Convert to Static IP</a>
3	*	192.168.111.176	f2:36:1d:eb:20:6d	22	<a href="#">Convert to Static IP</a>

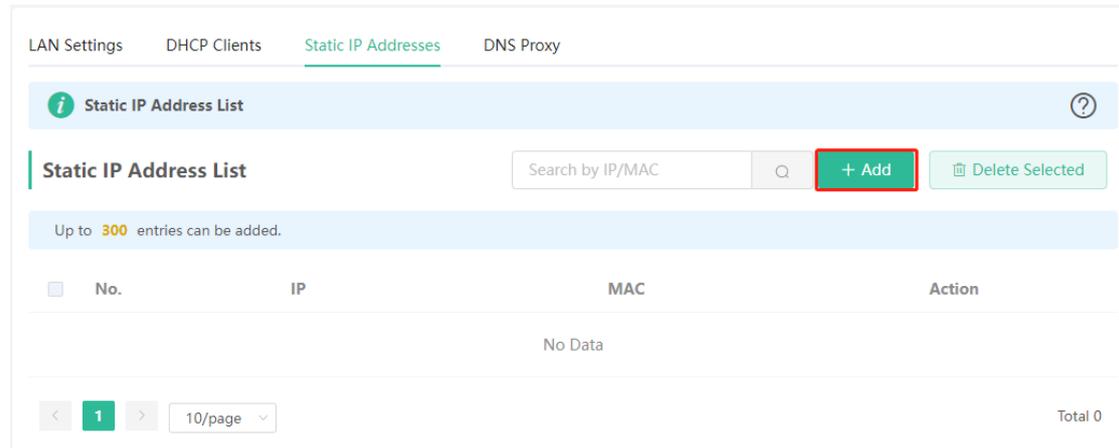
< 1 > 10/page Total 3

### 3. Binding a Static IP Address

Mobile phone view: Choose **More** > **Switch to PC view** > **More** >  **Basics** > **LAN** > **Static IP Addresses**.

PC view: Choose **More** >  **Basics** > **LAN** > **Static IP Addresses**.

Click **Add**. In the displayed static IP address dialog box, enter the MAC address and IP address of the target client, and click **OK**. After a static IP address is bound, the client will be assigned with the specified IP address.



## 11.9 Configuring DNS

### 11.9.1 Local DNS

When the WAN interface runs DHCP or PPPoE, the device automatically obtains the DNS server address. If the primary router does not deliver the DNS server address or the DNS server needs to be changed, you can manually configure a new DNS server.

Mobile phone view: Choose **More** > **Switch to PC view** > **More** >  **Advanced** > **Local DNS**.

PC view: Choose **More** >  **Advanced** > **Local DNS**.

**Local DNS server:** Configure the DNS server address used by the local device. If there are multiple DNS server addresses, separate them with spaces.

 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

## 11.9.2 DNS Proxy

### Caution

This feature is supported by only the router and WISP modes.

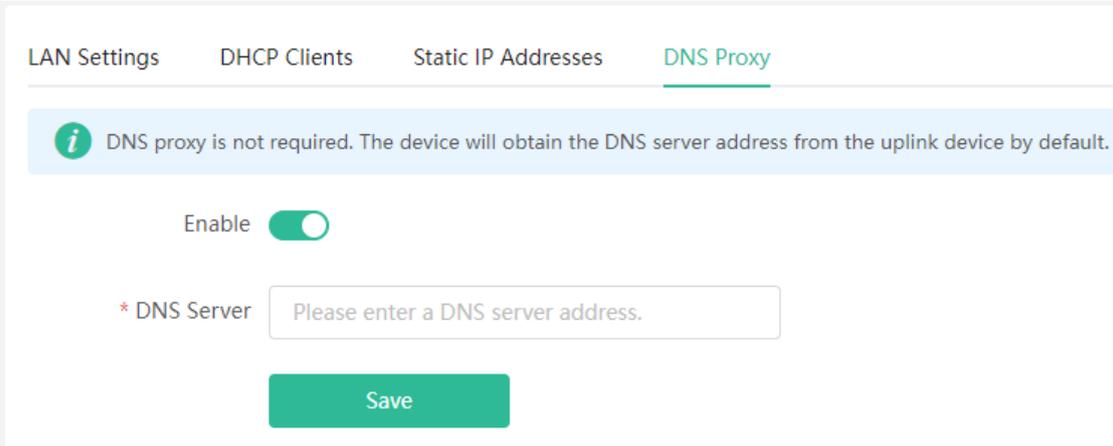
DNS proxy is optional. By default, the device obtains the DNS server address from the uplink device.

Mobile phone view: Choose **More** > **Switch to PC view** > **More** >  **Basics** > **LAN** > **DNS Proxy**.

PC view: Choose **More** >  **Basics** > **LAN** > **DNS Proxy**.

DNS proxy: By default, DNS proxy is disabled, and the DNS server address delivered by the ISP is used. If the DNS configuration is incorrect, the network may be successfully connected and mobile phones can access the Internet by using apps. However, web pages cannot be opened. You are advised to keep the DNS proxy disabled.

**DNS Server:** By default, clients use the DNS service provided by the primary router when accessing the Internet. The default settings are recommended. After DNS proxy is enabled, you can enter the IP address of the DNS server. The DNS server address varies according to regions, and you can consult the local ISP.



LAN Settings   DHCP Clients   Static IP Addresses   **DNS Proxy**

 DNS proxy is not required. The device will obtain the DNS server address from the uplink device by default.

Enable

\* DNS Server

Save

## 11.10 Enabling Port-based Flow Control

Mobile phone view: Choose **More** > **Switch to PC view** > **More** >  **Advanced** > **Port Settings**.

PC view: Choose **More** >  **Advanced** > **Port Settings**.

Flow control can resolve the data congestion problem when wired ports work at different rates, thus improving network speed.

### Port Settings

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

Flow Control

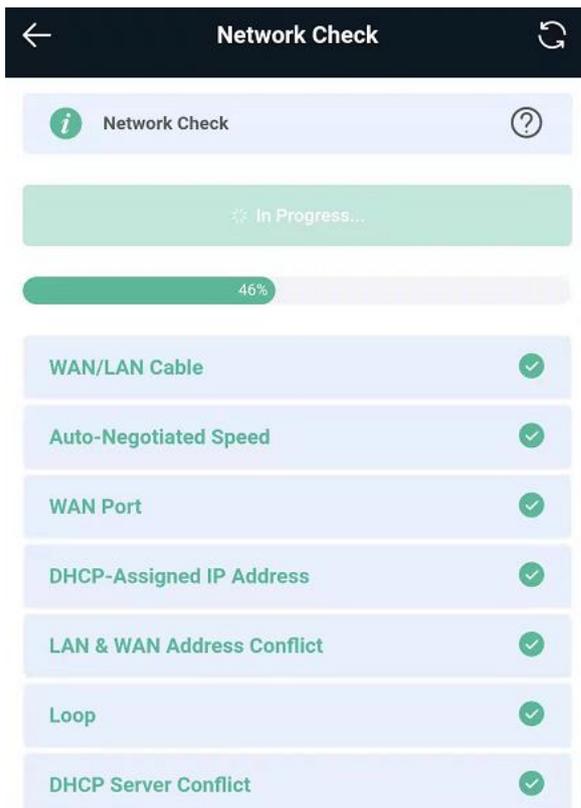
[Save](#)

## 11.11 Network Problem Diagnosis

Mobile phone view: Choose **More** > **Network Check**.

PC view: Choose **More** >  **Diagnostics** > **Network Check**.

Click **Start**. Then the device will check the problems on the network, including problems of interfaces, routing, flow control, and Ruijie Cloud platform, and provides solutions and suggestions on the risks.



**Network Check**

 Network Check 

 In Progress...

46%

- WAN/LAN Cable 
- Auto-Negotiated Speed 
- WAN Port 
- DHCP-Assigned IP Address 
- LAN & WAN Address Conflict 
- Loop 
- DHCP Server Conflict 

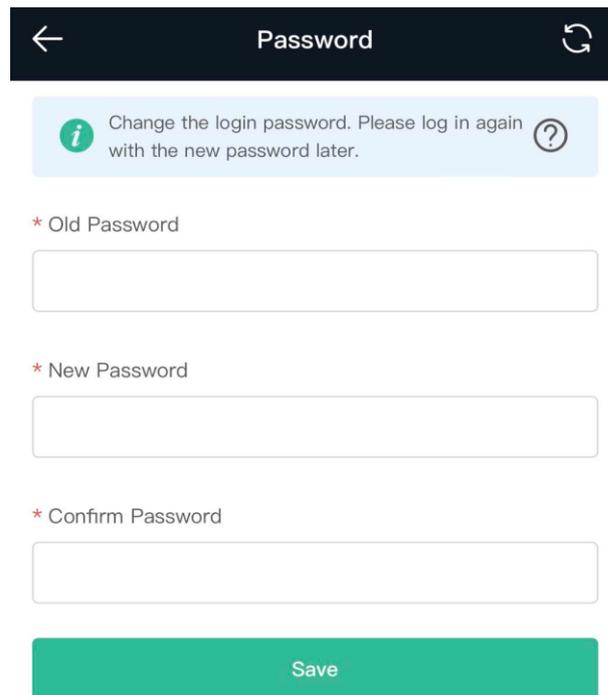
# 12 Mesh Repeater's System Settings

## 12.1 Configuring the Login Password

Mobile phone view: Choose **More** > **System** > **Password**.

PC view: Choose **More** >  **System** > **Login** > **Login Password**.

Enter the old password and new password. After saving the configuration, log in again with the new password.



The screenshot shows a mobile application interface for changing the login password. At the top, there is a dark header bar with a back arrow on the left, the title "Password" in the center, and a refresh icon on the right. Below the header is a light blue information banner with a green 'i' icon on the left and a question mark icon on the right. The banner text reads: "Change the login password. Please log in again with the new password later." Below the banner are three input fields, each with a red asterisk and a label: "\* Old Password", "\* New Password", and "\* Confirm Password". At the bottom of the form is a green "Save" button.

## 12.2 Restoring Factory Settings

Mobile phone view: Choose **More** > **System** > **Reset**.

PC view: Choose **More** >  **System** > **Management** > **Reset**.

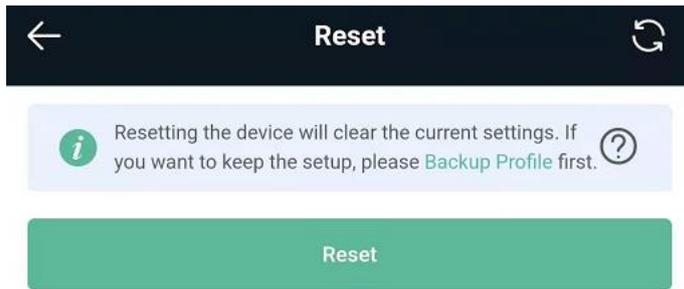
Click **Reset** to restore factory settings.

---

### Caution

This operation will clear existing settings and restart the device. Therefore, exercise caution when performing this operation.

---

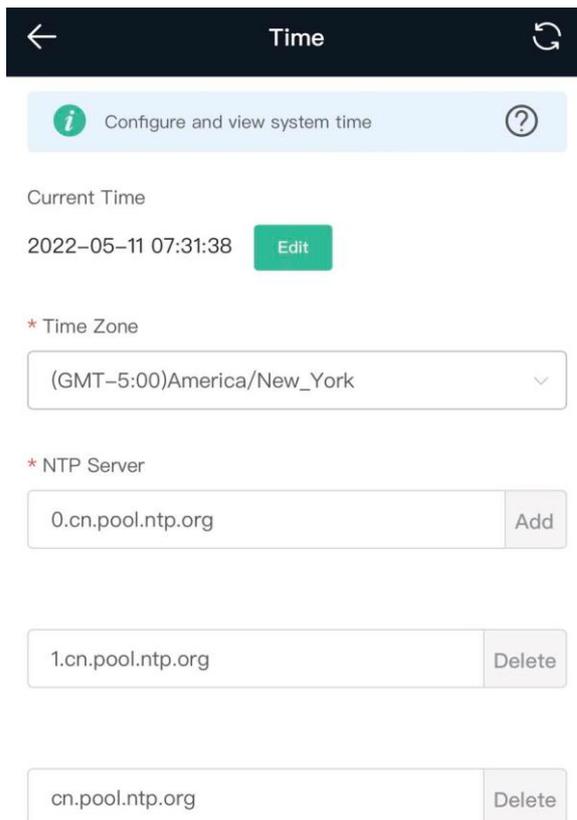


## 12.3 Configuring the System Time

Mobile phone view: Choose **More** > **System** > **Time**.

PC view: Choose **More** >  **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 the time is still incorrect, click **Edit** to manually set the time. In addition, the mesh repeater supports Network Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete local servers as required.



## 12.4 Configuring Scheduled Reboot

### 12.4.1 Getting Started

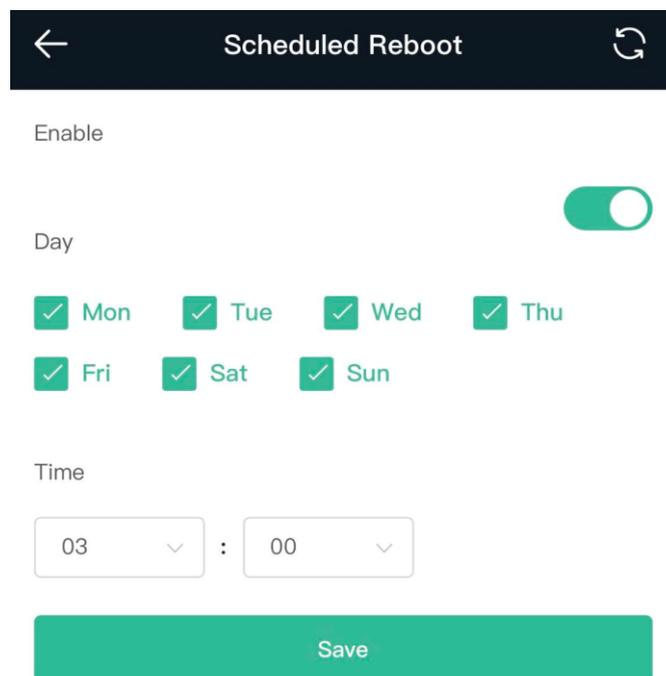
Confirm that the system time is accurate to avoid network interruption caused by device reboot at the incorrect time point. For details, see [12.3 Configuring the System Time](#).

### 12.4.2 Configuration Steps

Mobile phone view: Choose **More** > **System** > **Scheduled Reboot**.

PC view: Choose **More** >  **System** > **Reboot** > **Scheduled Reboot**.

Click **Enable**, and select the date and time of weekly scheduled reboot. Click **Save**. When the system time matches the scheduled reboot time, the device will restart.



← Scheduled Reboot ↻

Enable

Day

Mon  Tue  Wed  Thu

Fri  Sat  Sun

Time

03 : 00

Save

## 12.5 Performing Online Upgrade and Displaying the System Version

Mobile phone view: Choose **More** > **System** > **Online Upgrade**.

PC view: Choose **More** >  **System** > **Upgrade** > **Online Upgrade**.

You can check the current system version. If there is a new version, you can click it for an upgrade. The upgrade time can be set. You are advised to set the upgrade time to the idle network time, for example, 4:15 a.m.

---

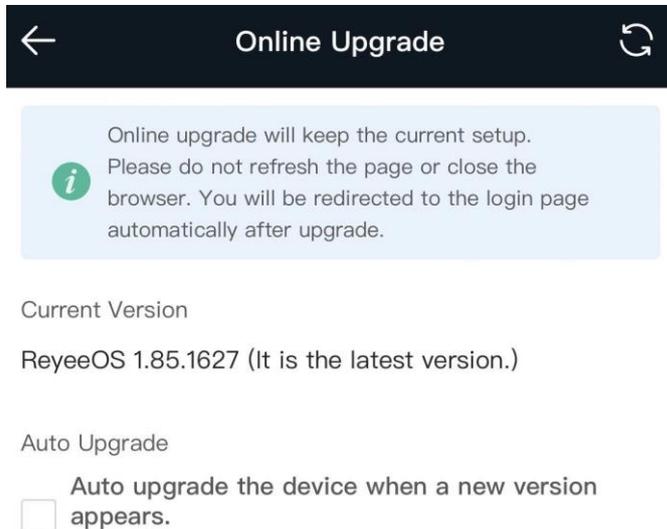
 Caution

After being upgraded, the device will restart. Therefore, exercise caution when performing this operation. You are advised to set the scheduled upgrade time to an early morning time to avoid Internet access from being affected.

---

If no new version is detected and online upgrade cannot be performed, check whether the DNS configuration is correctly obtained or go to **More** >  **Advanced** > **Local DNS** to set the DNS server for the mesh repeater.

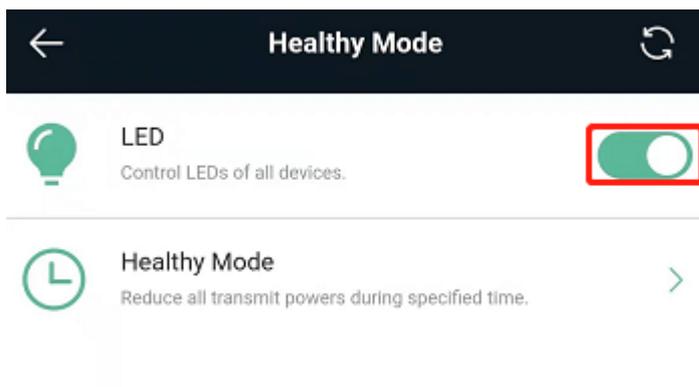
---



## 12.6 Enabling or Disabling the LED

Mobile phone view: Choose **More** > **Healthy Mode**.

PC view: Choose **More** >  **System** > **LED**.



## 12.7 Switching the System Language

Mobile phone view: Choose **More** > **Language**.

PC view: Click  in the upper right corner of the page.

Click a required language to switch the system language.



## 12.8 Network Diagnosis Tools

### 1. Network Test Tool

Mobile phone view: Choose **More > System > Network Tools**.

PC view: Choose **More >  Diagnostics > Network Check**.

When you select the ping tool, you can enter the IP address or URL and click **Start** to test the connectivity between the mesh repeater and the IP address or URL. The message "Ping failed" indicates that the IP address or URL cannot be pinged from the mesh repeater.

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 ↻

*i* Network Tools *?*

Tool

Ping  Traceroute  DNS Lookup

\* IP Address/Domain

www.google.com

\* Ping Count

4

\* Packet Size

64 Bytes

Start

Stop

## 2. Packet Obtaining Tool

---

### Caution

This feature is only supported by only the router and WISP modes.

---

Mobile phone view: Choose **More** > **Switch to PC view** > **More** >  **Diagnostics** > **Packet Capture**.

PC view: Choose **More** >  **Diagnostics** > **Packet Capture**.

Set the interface, protocol, IP address whose packets need to be obtained, file size limit, and packet count limit to limit the volume of packets obtained. Click **Start**. Packet obtaining can be stopped at any time and a link to the generated file is generated. You can use Wireshark and other analysis software to open and view the file.

---

### Caution

Packet obtaining may occupy many system resources and cause network freezing. Exercise caution when performing this operation.

---

**Packet Capture**

Interface:

Protocol:

IP Address:

File Size Limit:  Available Memory **38.78 M**

Packet Count Limit:

PCAP file: [Click to download the PCAP file.](#) i

[Click to delete the file.](#)

## 12.9 Configuring Backup and Import

Mobile phone view: Choose **More** > **Switch to PC view** > **More** > **System** > **Management** > **Backup & Import**.

PC view: Choose **More** > **System** > **Management** > **Backup & Import**.

To configure backup, click **Backup** to download a configuration file locally.

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

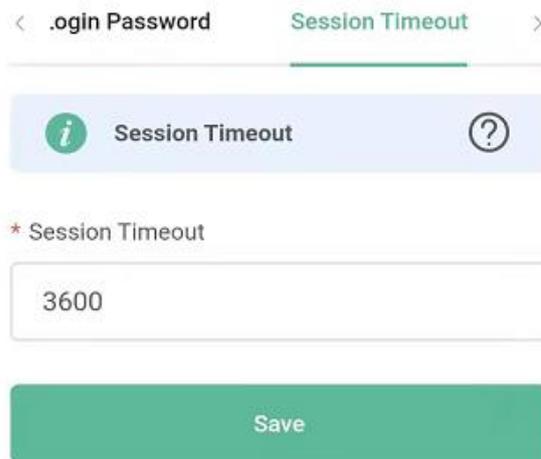
The screenshot shows the Mesh Repeater's System Settings interface. At the top, there is a navigation bar with icons for Home, Clients, Internet, Wi-Fi, and More. The 'More' menu is open, showing 'English' and a QR code. Below the navigation bar, the 'Backup & Import' section is active. It features a 'Reset' button and a warning message: '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.' Below the warning, there are two sections: 'Backup Profile' with a 'Backup' button, and 'Import Profile' with a 'File Path' field containing 'Please select a file.', a 'Browse' button, and an 'Import' button.

## 12.10 Configuring the Session Timeout

Mobile phone view: Choose **More** > **Switch to PC view** > **More** >  **System** > **Login** > **Session Timeout**.

PC view: Choose **More** >  **System** > **Login** > **Session Timeout**.

If no operation is performed on the page within a given period of time, the session will be ended. When you need to perform operations again, enter the password to open the configuration page. The default timeout is 3600 seconds, that is, 1 hour.



< .ogin Password > Session Timeout >

**i** Session Timeout **?**

\* Session Timeout

3600

Save

## 12.11 Switching to the PC View

Mobile phone view: Choose **More** > **Switch to PC view**.

The PC view is the screen displayed after you log in from a PC. The page layout is different from that on a mobile phone.

You can click  in the upper left corner to return to the mobile phone view or drag the page to the narrowest position on the PC to enter the mobile phone view.

The screenshot displays the 'More Settings' menu on the left and the 'Device Details' section on the right. In the 'More Settings' menu, the 'Switch to PC view' option is highlighted with a red box. The 'Device Details' section provides technical information for the EW1200R device, including its model, hostname, serial number, MAC address, and various version numbers. The 'Wi-Fi' section below shows the primary Wi-Fi network name and security status.

**More Settings**

- Roaming Optimization  
Roaming Sensitivity Level
- Country(Region)/Channel Width
- Channel Transmit Power  
Country(Region)/Transmit Power/Roaming Sensitivity Level
- XPress  
XPress helps you to get a faster network speed.
- Healthy Mode  
LED/Healthy Mode
- System  
Reboot/Restore
- Language  
System Language
- Switch to PC view**  
Landscape Mode Recommended

**Device Details**

Model: EW1200R  
Hostname: Ruijie  
SN: G1RP2ER025888  
MAC: 9C:2B:A6:DA:01:A4  
Duration: 1 hour 21 minutes 26 seconds  
System: 2022-05-12 03:43:58  
Hardware Ver: 1.00  
Software Ver: ReyeeOS 1.85.1709

**Wi-Fi**

Primary Wi- @Ruijie-s01A4  
Fi: Security: Yes

# 13 Reyee FAQ

## 13.1 Reyee FAQ

### 13.1.1 [Reyee Password FAQ \(Collection\)](#)

### 13.1.2 [Reyee Wireless Repeater FAQ \(Collection\)](#)

### 13.1.3 [Reyee Parental Control FAQ \(Collection\)](#)

### 13.1.4 [Reyee Mesh FAQ \(Collection\)](#)

### 13.1.5 [Reyee Self-Organizing Network \(SON\) FAQ \(Collection\)](#)

### 13.1.6 [Reyee series Devices Parameters Tables](#)

### 13.1.7 [Reyee Parameter Consultation FAQ \(Collection\)](#)

## 13.2 Mesh Repeater FAQ

### 13.2.1 How Can I Restore Factory Settings?

Press and hold the Reyee Mesh button  for more than 5 seconds. When the LED starts blinking, the device is restoring factory settings. The device will automatically restart after the restoration is completed. After the device is started, that is, the LED is solid on, reconfigure Internet access. The wireless signal name in the factory settings is @Ruijie-sXXXX.

### 13.2.2 How Can I Do If I Forget the Password of the Mesh Repeater?

- If you forget the management password of the web page, try to log in with the Wi-Fi password. If the error still occurs, restore the factory settings.
- If you forget the Wi-Fi password and the mesh repeater is configured to extend the signals of other routers, the Wi-Fi password is usually the same as the primary router's password. You can check the configuration of the primary router. If the Wi-Fi password of the primary router is incorrect, you can restore factory settings and reconfigure the password.

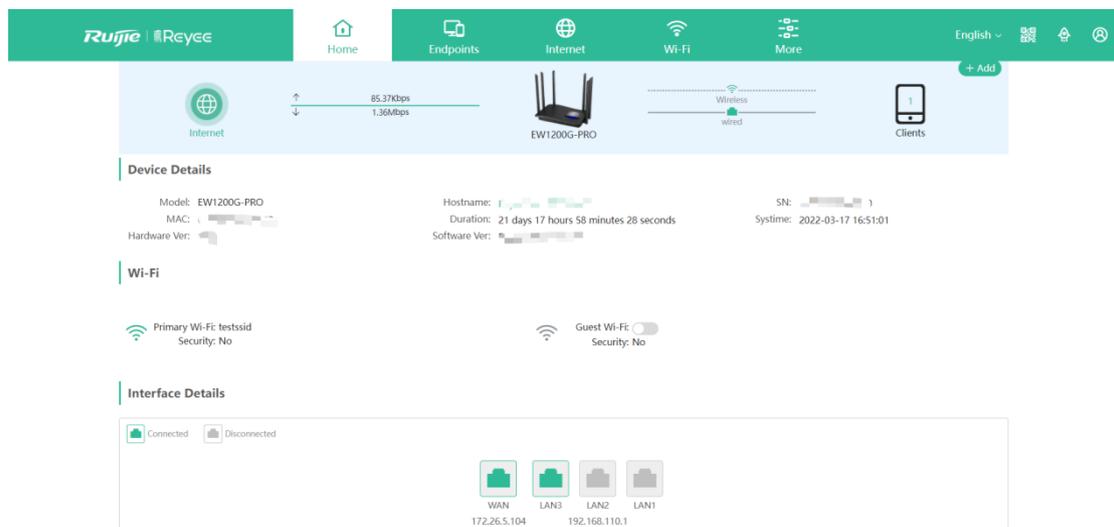
### 13.2.3 How Do I Manage the Mesh Repeater After the Mesh Repeater Is Installed Successfully?

You are advised to use the Reyee router App to manage the mesh repeater, or access the mesh repeater's IP address in a browser to manage it (the default IP address is 192.168.110.1). When working as a mesh repeater, the device obtains a new IP address. In this situation, the default IP address cannot be accessed. You are advised to manage the mesh repeater by using the Reyee router App.

# 14 Appendix: Monitoring of Reyee Mesh Wi-Fi Routers

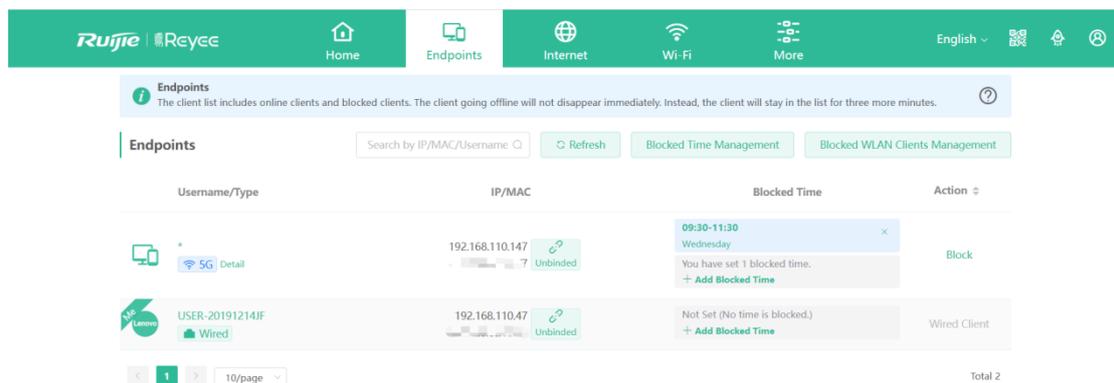
## 14.1 Overview

The **Overview** page displays the local connection and information of **Device Details**, **Wi-Fi** and **Interface Details**. The information of the download speed, upload speed, local device, and connected clients is displayed on the top of this page. **Device Details** includes the model, host name, SN, and MAC address. **Interface Details** displays connections of the WAN and LAN.



## 14.2 Endpoints

This page displays all connected endpoints on this network, including wired and wireless users. The **Clients** page allows you to bind static IP addresses, manage blocked time, and block WLAN clients.



Click **Blocked Time Management** to customize the time to block users.

### Blocked Time Management

**Blocked Time List** + Add Delete Selected

Set a time to prevent clients accessing the Internet. Up to 32 entries can be added.

<input type="checkbox"/>	Blocked Time	Blocked MAC	Remark	Action
<input type="checkbox"/>	00:00-23:59 Monday Tuesday Wednesday Thursday Friday	[MAC]	test	Edit Delete
<input type="checkbox"/>	09:30-11:30 Wednesday	[MAC]	app_C... F...	Edit Delete

< 1 > 10/page Total 2

### Add Rule

Blocked Time: Custom

\* Date: Please Select Day

\* Time: 18:54 - 19:54

Remark: USER-20191214JF

Cancel OK

Click **Blocked WLAN Clients Management** and add the MAC address to prevent WLAN users from connecting the SSID.

Blocked WLAN Clients Management ×

**Blocked WLAN Clients** + Add 🗑️ Delete Selected

Up to 30 members can be added.

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

< 1 > 10/page ▼ Total 0

Blocked WLAN Clients Management ×

**Blocked WLAN Clients** + Add 🗑️ Delete Selected

Up to 30 members can be added.

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

< 1 > 10/page ▼ Total 0

### 14.3 Internet

This page displays the mode where the device access the Internet, including **PPPoE**, **DHCP**, and **Static IP**.

The screenshot shows the Ruijie Reyee web interface. The top navigation bar includes the Ruijie Reyee logo, Home, Endpoints, Internet, Wi-Fi, and More. The Internet section is active, showing a status of 'Online (DHCP)'. Below this, there are three tabs: PPPoE, DHCP (selected), and Static IP. The DHCP tab displays the following information:

IP	172.26.5.104
Subnet Mask	255.255.252.0
Gateway	172.26.4.1
DNS Server	192.168.58.110 192.168.58.94

A 'Save' button is located at the bottom of the configuration area.

**DHCP:** The router detects whether the IP address can be obtained through DHCP by default. If the router connects to the Internet successfully, you can click **Next** without entering an account.

**PPPoE:** Click **PPPoE**, and enter the username, password, and service name. Click **Next**.

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