Ruijie Reyee RG-M, EW Series Home Wi-Fi Routers

Implementation Cookbook

Document Version: V1.7
Date: May 17, 2024

Copyright

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 names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

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 Reyee: https://reyee.ruijie.com
- Technical Support Website: https://reyee.ruijie.com/en-global/support
- Case Portal: https://www.ruijienetworks.com/support/caseportal
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Online Robot/Live Chat: https://reyee.ruijie.com/en-global/rita

Conventions

1. GUI Symbols

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

2. Signs

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 I

1 Introduction to Reyee Products 1

1.1 Product List 1

1.2 LED 2

1.2.1 EW300 PRO System LED 2

1.2.2 EW300N System LED 3

1.2.3 EW1200 3

1.2.4 EW1200G PRO 3

1.2.5 EW1800GX and EW3200GX PRO 4

1.2.6 M18 and M32 4

1.2.7 EW3000GX PRO 5

1.2.8 EW1300G 5

1.2.9 EW300T 6

1.3 Button 7

1.3.1 EW300 PRO and EW300N 7

1.3.2 EW1200 and EW1200G PRO 7

1.3.3 EW1800GX and EW3200GX PRO 7

1.3.4 M18 and M32 7

1.3.5 EW3000GX PRO 8

1.3.6 EW1300G 8

1.3.7 EW300T 8

2 Reyee Login 9

2.1 Connecting to the Router 9

2.2 Logging In 9
3 Reyee Quick Start 11
3.1 Internet Access Modes 11
3.2 Primary Router Mode 11
3.2.1 Wireless Router Mode 11
3.2.2 Configuration Steps 12
3.2.3 3G/4G Router Mode 13
3.2.4 Configuring a Wi-Fi Network 15
3.2.5 Configuring IoT Wi-Fi 16
3.2.6 Verification and Testing 17
3.3 Secondary Router Mode 17
3.3.1 Getting Started 17
3.3.2 Configuration Steps 17
3.3.3 Verification and Testing 24
4 Reyee Wi-Fi Network Settings 25
4.1 Changing the SSID and Password 25
4.2 Hiding the SSID 26
4.2.1 Overview 26
4.2.2 Getting Started 26
4.2.3 Configuration Steps 26
4.3 Adding a Wi-Fi Network 27
4.3.1 Overview 27
4.3.2 Configuration Steps 28
4.3.3 Verification and Testing 28

4.4 Configuring a Wi-Fi Blocklist or Allowlist 28
4.4.1 Overview 28
4.4.2 Configuration Steps 28
4.5 Optimizing the Wi-Fi Network 31
4.5.1 Overview 31
4.5.2 Getting Started 31
4.5.3 Configuration Steps 31
4.6 Configuring the Healthy Mode 34
4.7 Enabling Roaming Optimization 35
5 Reyee Networks Settings 36
5.1 Displaying SIM Card Information 36
5.2 Managing the SIM Card 36
5.2.1 Configuring Network Access for a SIM Card 36
5.2.2 Displaying the SIM Card List 38
5.3 Managing the PIN 39
5.4 Managing SMS 40
5.4.1 Creating an SMS Message 40
5.4.2 Displaying the Inbox 41
5.4.3 Displaying the Outbox 41
5.4.4 Displaying the Drafts Box 42
5.5 Configuring Internet Connection Type 42
5.6 Changing the Address of a LAN Port 43
5.7 Changing the MAC Address 43
5.8 Changing the MTU 44

5.9 Configuring the Repeater Mode 45
5.9.1 Wired Repeater 45
5.9.2 Wireless Repeater 46
5.9.3 WISP 48
5.10 Controlling the Internet Access Time Range 48
5.11 Configuring XPress 49
5.12 Configuring Port Mapping 50
5.12.1 Overview 50
5.12.2 Getting Started 50
5.12.3 Configuration Steps 50
5.12.4 Verification and Testing 51
5.12.5 Solution to a Test Failure 51
5.12.6 DMZ Configuration Steps 51
5.13 Configuring the DHCP Server 52
5.13.1 Overview 52
5.13.2 Configuration Steps 52
5.14 Configuring DNS 55
5.15 Configuring DDNS 56
5.15.1 Overview 56
5.15.2 Getting Started 56
5.15.3 Configuration Steps 56
5.16 Configuring APR Binding and ARP Guard 57
5.16.1 Overview 57
5.16.2 Configuration Steps 57

5.17 Configuring Static Routing 58
5.18 Policy-based Routing 60
5.19 Connecting to IPTV 63
5.19.1 Getting Started 63
5.19.2 IPTV Configuration Steps (VLAN Type) 63
5.19.3 IPTV Configuration Steps (IGMP Type) 64
5.20 Configuring Wi-Fi/IGMP 65
5.20.1 Overview 65
5.20.2 Configuration Steps 65
5.21 Configuring IPv6 66
5.21.1 Configuring the IPv6 of the WAN Port 66
5.21.2 Configuring the IPv6 of the LAN Port 66
5.22 Enabling Smart Flow Control 67
5.23 Configuring Firewall 68
5.24 Enabling Wi-Fi Switch 69
5.25 Configuring UPnP 70
5.25.1 Overview 70
5.25.2 Configuration Steps 70
5.26 Configuring PPTP VPN 70
5.26.1 Overview 70
5.26.2 Configuring PPTP Server 70
5.26.3 Configuring the PPTP Client 72
5.27 Configuring OpenVPN 73
5.27.1 Overview 73

5.27.2 Configuring OpenVPN (Server Mode) 74
5.27.3 Configuring OpenVPN (Client Mode) 77
5.27.4 Typical Configuration Example 78
5.28 Configuring Connectivity Detection 84
5.29 Enabling CWMP 85
5.29.1 Overview 85
5.29.2 Configuration Steps 85
5.30 Enabling Reyee Mesh 86
5.31 Enabling Hardware Acceleration 87
5.32 Configuring Console Booster 88
5.33 Configuring AP Networking 89
5.34 Configuring Reyee Mesh 3.0 89
5.34.1 Configuration Steps 89
5.35 Diagnosing Network Problems 93
6 Reyee System Settings 95
6.1 Switching to the PC View 95
6.2 Configuring the Login Password 95
6.3 Remote Access 96
6.4 Restoring Factory Settings 97
6.5 Configuring the System Time 97
6.6 Configuring Scheduled Reboot 98
6.6.1 Getting Started 98
6.6.2 Configuration Steps 98
6.7 Performing Online Upgrade and Displaying the System Version 99

6.8 Enabling or Disabling the LED 100
6.9 Switching the System Language 100
6.10 Network Diagnosis Tools 101
6.10.1 Network Test Tool 101
6.10.2 Packet Obtaining Tool 101
6.11 Configuring Backup and Import 102
6.12 Configuring the Session Timeout 103
7 Reyee FAQ 104
7.1 Reyee Password FAQ (Collection) 104
7.2 Reyee Wireless Repeater FAQ (Collection) 104
7.3 Reyee Parental Control FAQ (Collection) 104
7.4 Reyee Mesh FAQ (Collection) 104
7.5 Reyee Self-Organizing Network (SON) FAQ (Collection) 104
7.6 Reyee series Devices Parameters Tables 104
7.7 Reyee Parameter Consultation FAQ (Collection) 104
8 Appendix: Monitoring of Reyee Mesh Wi-Fi Routers 105
8.1 Overview 105
8.2 Endpoints 105
8.3 Internet 108

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 Mbps	2.4 GHz: 2×2	8
EW300N	Not supported	Wi-Fi 4 (802.11n)	2.4 GHz: 300 Mbps	2.4 GHz: 2×2	8
EW1200	Supported	Wi-Fi 5 (802.11ac)	2.4 GHz: 300 Mbps 5 GHz: 867 Mbps	2.4 GHz: 2×2 5 GHz: 2×2	2.4 GHz: 8 5 GHz: 16
EW1200G PRO	Supported	Wi-Fi 5 (802.11ac)	2.4 GHz: 400 Mbps 5 GHz: 867 Mbps	2.4 GHz: 2×2 5 GHz: 2×2	2.4 GHz: 8 5 GHz: 24
EW1800GX PRO	Supported	Wi-Fi 6 (802.11ax)	2.4 GHz: 573 Mbps 5 GHz: 1200 Mbps	2.4 GHz: 2×2 5 GHz: 2×2	2.4 GHz: 12 5 GHz: 36

Model	Reyee Mesh	Wi-Fi Standards	Maximum Wi-Fi Rate	MIMO	Recommended Users
EW3200GX PRO	Supported	Wi-Fi 6 (802.11ax)	2.4 GHz: 800 Mbps 5 GHz: 2400 Mbps	2.4 GHz: 4×4 5 GHz: 4×4	2.4 GHz: 12 5 GHz: 48
M18	Supported	Wi-Fi 6 (802.11ax)	2.4 GHz: 574 Mbps 5 GHz: 1201 Mbps	2.4 GHz: 2×2 5 GHz: 2×2	2.4 GHz: 12 5 GHz: 36
M32	Supported	Wi-Fi 6 (802.11ax)	2.4 GHz: 800 Mbps 5 GHz: 2402 Mbps	2.4 GHz: 4×4 5 GHz: 4×4	2.4 GHz: 12 5 GHz: 48
EW3000GX PRO	Supported	Wi-Fi 6 (802.11ax)	2.4 GHz: 573 Mbps 5 GHz: 2401 Mbps	2.4 GHz: 2×2 5 GHz: 2×2	2.4 GHz: 12 5 GHz: 48
EW1300G	Supported	Wi-Fi 5 (802.11ac)	2.4GHz: 400 Mbps 5GHz: 867 Mbps	2.4 GHz: 2×2 5 GHz: 2×2	2.4 GHz: 8 5 GHz: 24
EW300T	Not supported	Wi-Fi 4 (802.11n)	2.4 GHz: 300 Mbps	2.4 GHz: 2×2	8

1.2 LED

1.2.1 EW300 PRO System LED

Status	Description
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.

1.2.2 EW300N System LED

Description	Status
The router is starting up.	Blinking green
The router is connected to the Internet.	Solid green
The router is not connected to the Internet.	Solid red
The router is resetting.	Blinking green
The router is upgrading.	Blinking green
The router is rebooting.	Blinking green

1.2.3 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)	● The router is initialized. ● The router does not access the Internet.
	Fast blinking (on for 62.5 ms, off for 62.5 ms)	● The router is restored to factory settings. ● The router restarts. ● The router is initialized. ● The firmware is upgraded.
Wi-Fi LED	Solid on	Reyee mesh router is sunning normally.
	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.

1.2.4 EW1200G PRO

LED	Status	Description
System Status LED	Off	The router is not powered on.
	Solid on	The router is running normally.

LED	Status	Description
	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.

1.2.5 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.

1.2.6 M18 and M32

LED	Status	Description
Reyee Mesh Indicator	Blinking white	The device is being paired

LED	Status	Description
	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 (Reyee 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.

1.2.7 EW3000GX PRO

LED	Color/Status		Description
Reyee Mesh Indicator	Solid on		Mesh pairing succeeds.
	Off		Mesh pairing is not performed or 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.
	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.

1.2.8 EW1300G

LED	Color/Status	Description
Reyee Mesh Indicator	Solid on	Mesh pairing succeeds.
	Off	Mesh pairing is not performed or mesh network is disconnected.

LED	Color/Status		Description
	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.
	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.

1.2.9 EW300T

LED	Status	Description
System status LED	Off	The router is not powered on.
	Solid on	The router is running normally.
	Fast blinking (on for 62.5 ms, off for 62.5 ms)	● The router is restored to factory settings. ● The router restarts. ● The router is initialized. ● The firmware is upgraded.
Wi-Fi LED	Solid on	The Wi-Fi service is enabled.
	Off	The Wi-Fi service is disabled.
Internet LED	Solid on	The router is connected to the Internet.
	Off	The router is not connected to the Internet.
4G status LED	LED1 solid on	The 4G signal strength is low.
	LED2 solid on	The 4G signal strength is medium.
	LED3 solid on	The 4G signal strength is high.
	All LEDs off	There is no 4G signal.

1.3 Button

1.3.1 EW300 PRO and EW300N

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.

1.3.2 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.

1.3.3 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.

1.3.4 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.

1.3.5 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.

1.3.6 EW1300G

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.

1.3.7 EW300T

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

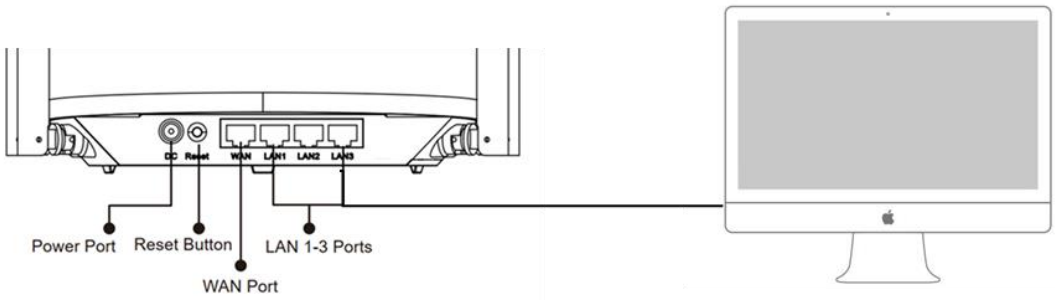
2 Reyee Login

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-s***XXXX* (*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
Password	See the label on the bottom of the router: Rexxxxxx (xxxxxx is a random number).

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.

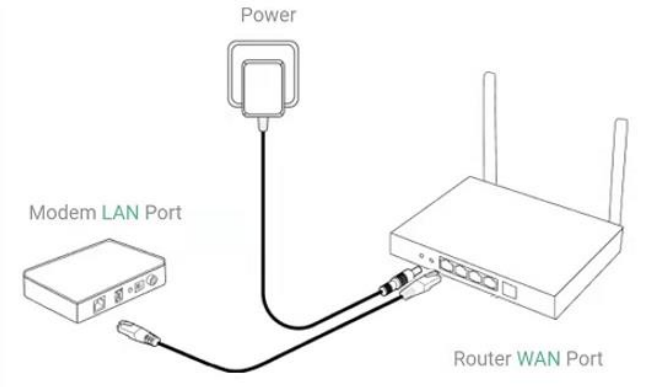
Instruction

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 Wireless Router Mode

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

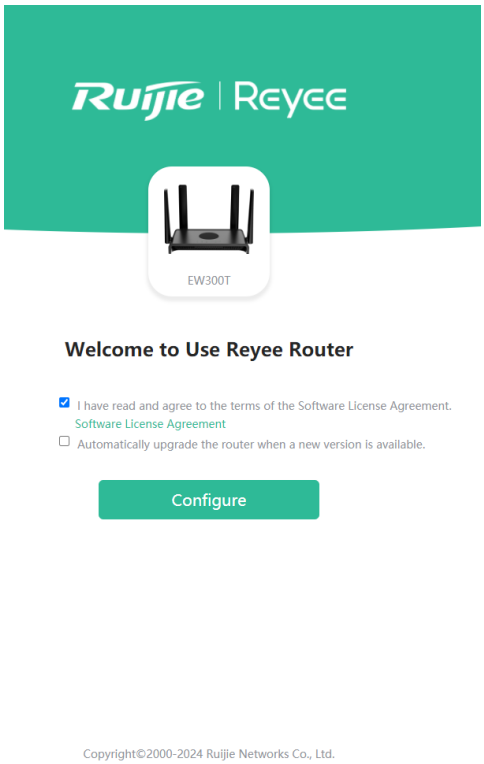
1. Configuring an Internet Connection Mode

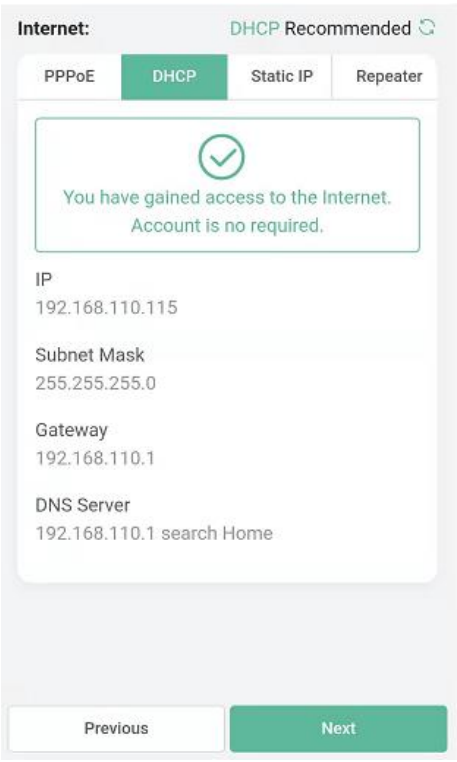
Click **Configure** and select the Internet connection mode confirmed by the carrier.

- **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.

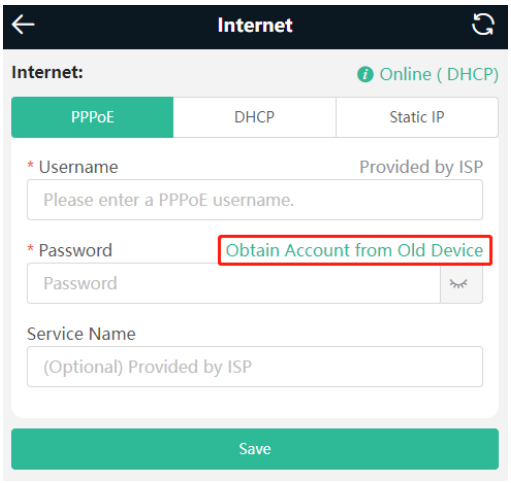


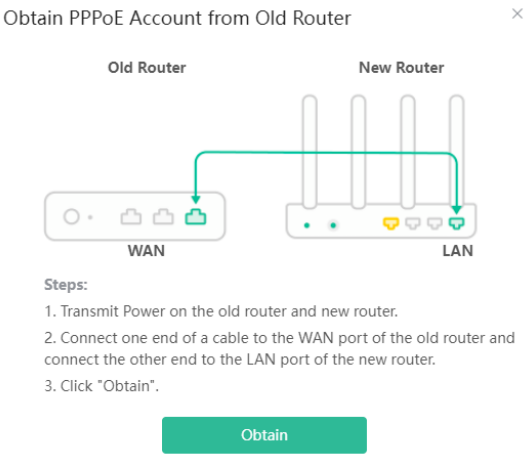


2. Forgetting the PPPoE Account

(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.





3.2.3 3G/4G Router Mode

Note

This function is only supported on the RG-EW300T.

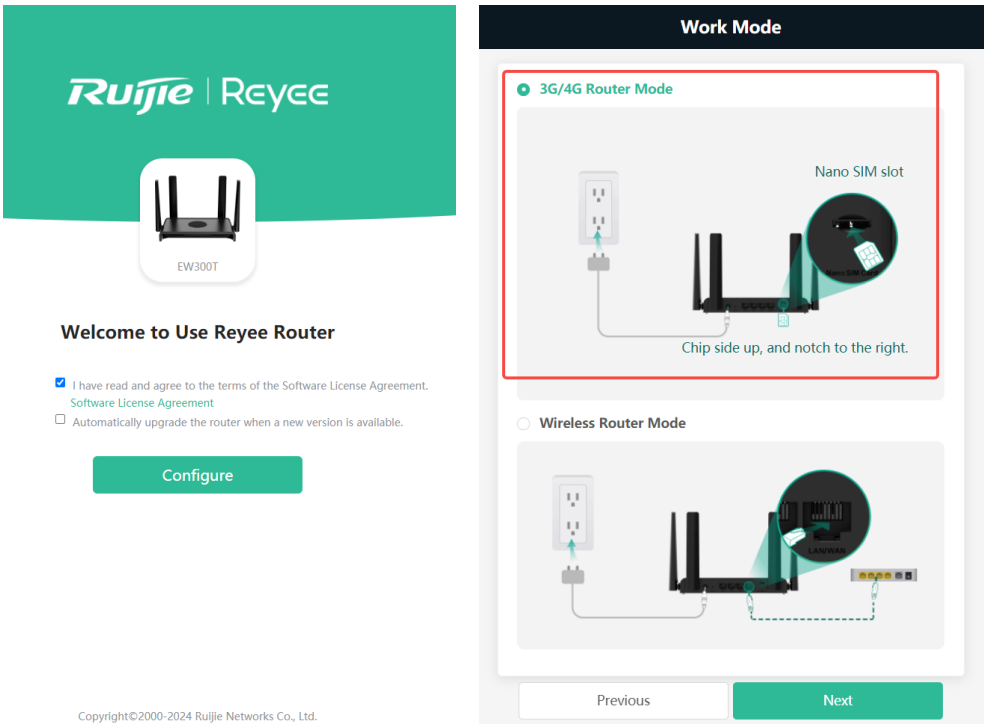
1. Getting Started

(1) Contact your ISP to obtain basic information about the SIM card for Internet access, including the APN, username, password, and authentication type.

(2) Insert a valid SIM card into the SIM card slot of the router and power on the router.

2. Configuration Steps

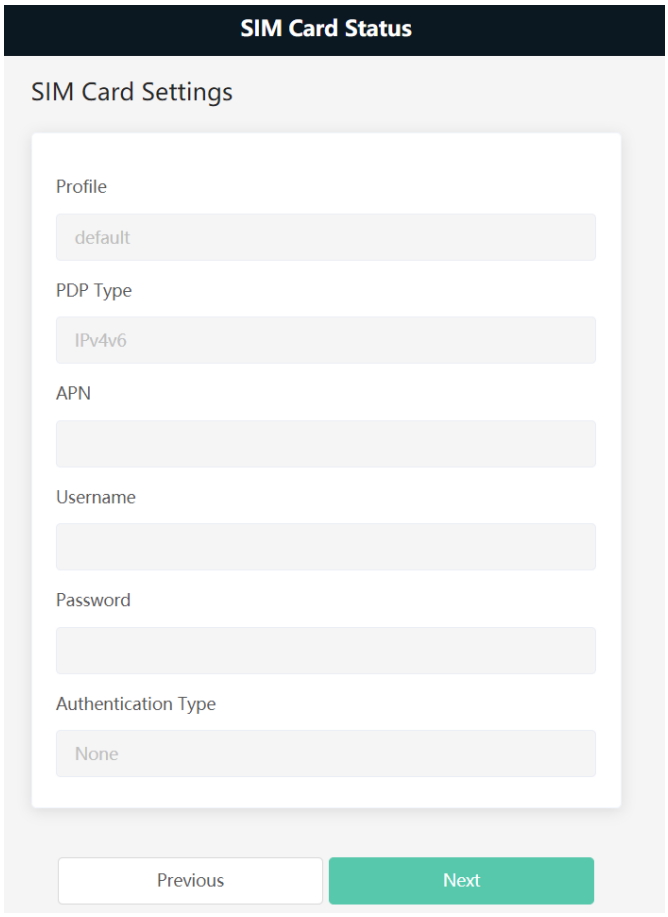
(1) Click **Configure** to go to the configuration page. On the page that opens, select **3G/4G Router Mode,** and click **Next**.



(2) Configure SIM card parameters: Generally, the system automatically populates the basic SIM card information. When an SIM card is available, you can access the Internet through the router. If the SIM card cannot be identified by the router, you need to enter values in the **Profile, DPD Type, APN, Username, Password,** and **Authentication Type** fields to enable the router to connect to the Internet. Keep the default settings unless otherwise specified, and click **Next**.

Caution

If the SIM card requires a PIN, enter the PIN on the configuration page. Otherwise, Internet access will fail.



3.2.4 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.

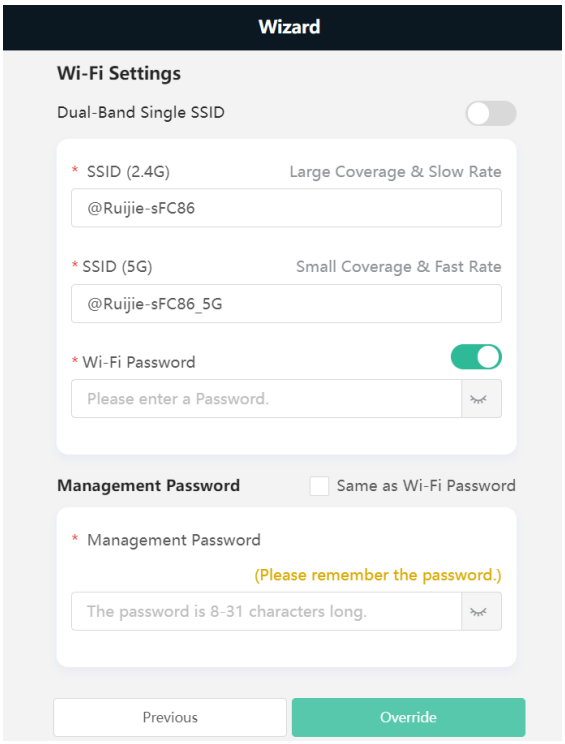
Caution

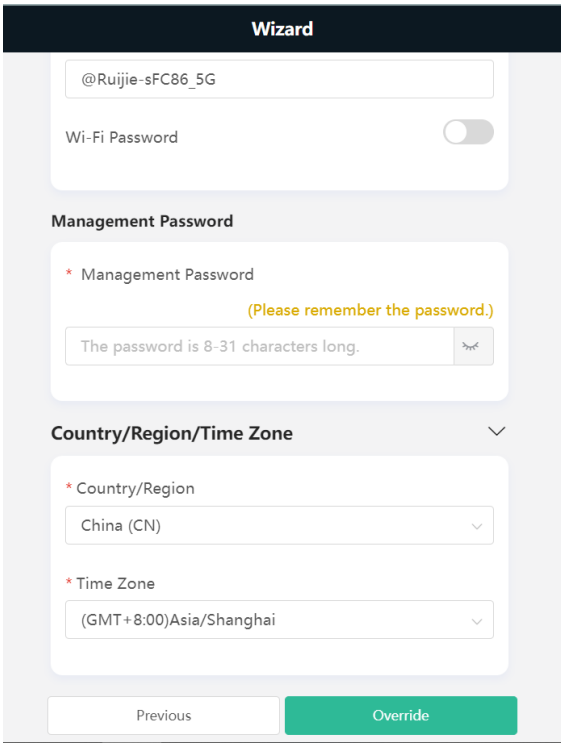
Only RG-M18, RG-M32, RG-EW1800GX PRO, RG-EW3000GX PRO and RG-EW3200GX PRO support Wi-Fi 6.

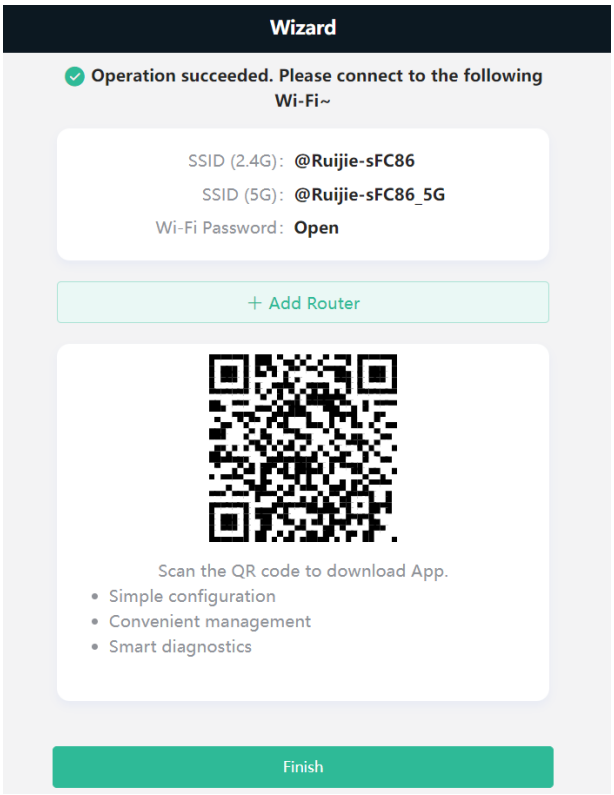
(4) Setting the country or region: A Wi-Fi channel may vary according to the country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.

(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.

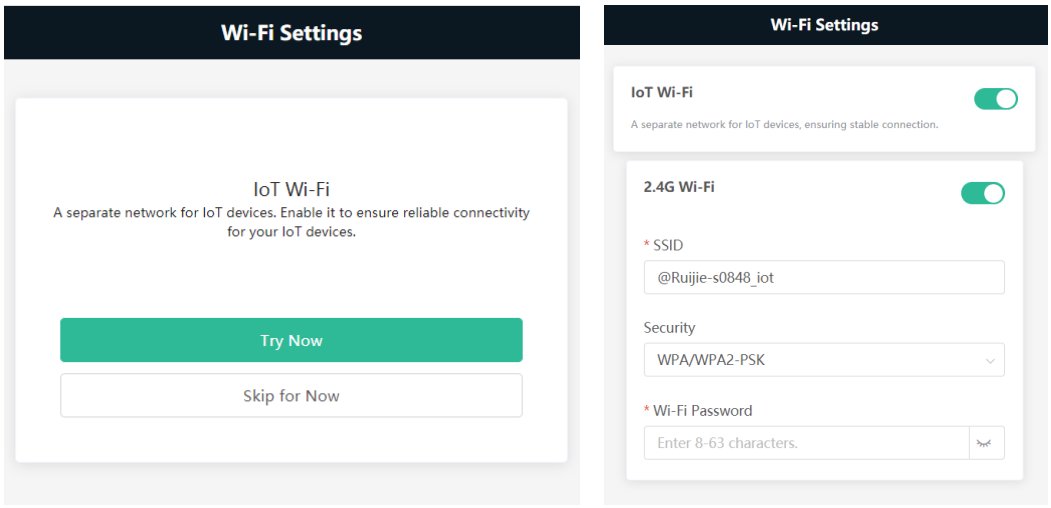






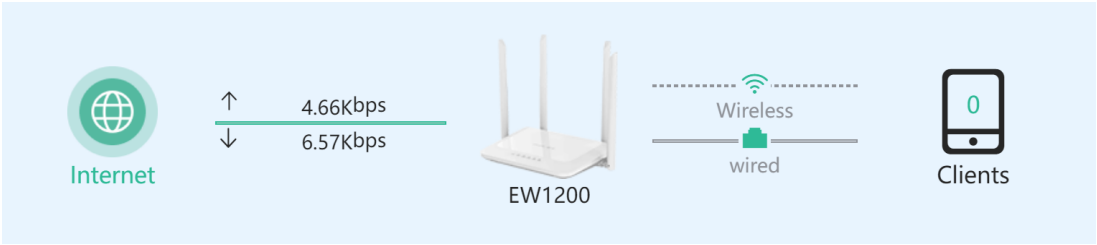
3.2.5 Configuring IoT Wi-Fi

If IoT devices exist on the network, click **Try Now** to create a separate Wi-Fi network for IoT devices to ensure reliability of network connection. For details about Wi-Fi configuration, see 3.2.4 Configuring a Wi-Fi Network.



3.2.6 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.



3.3 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.

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.

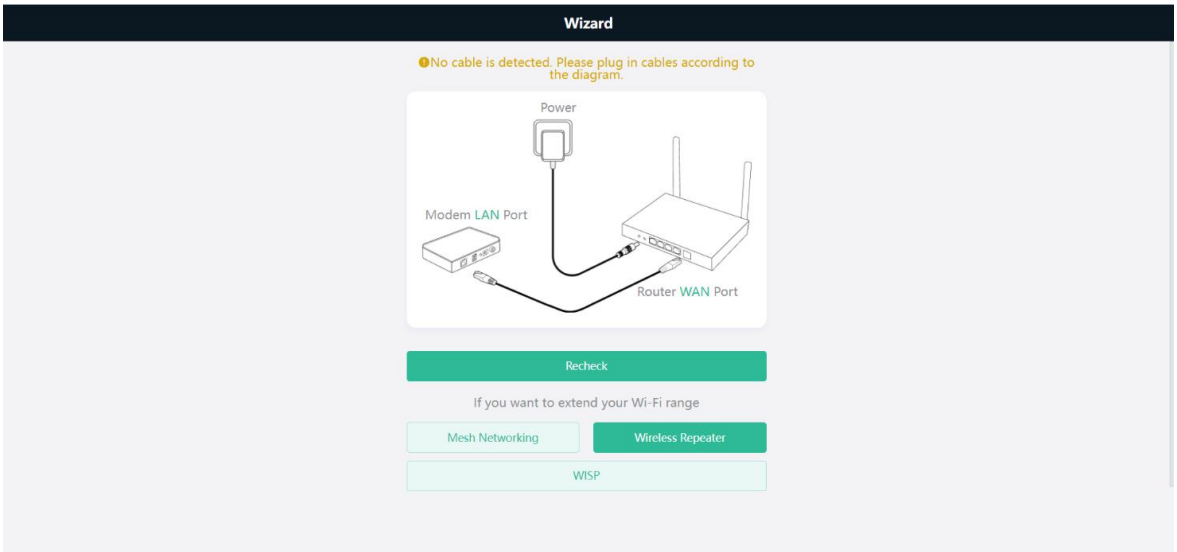
Caution

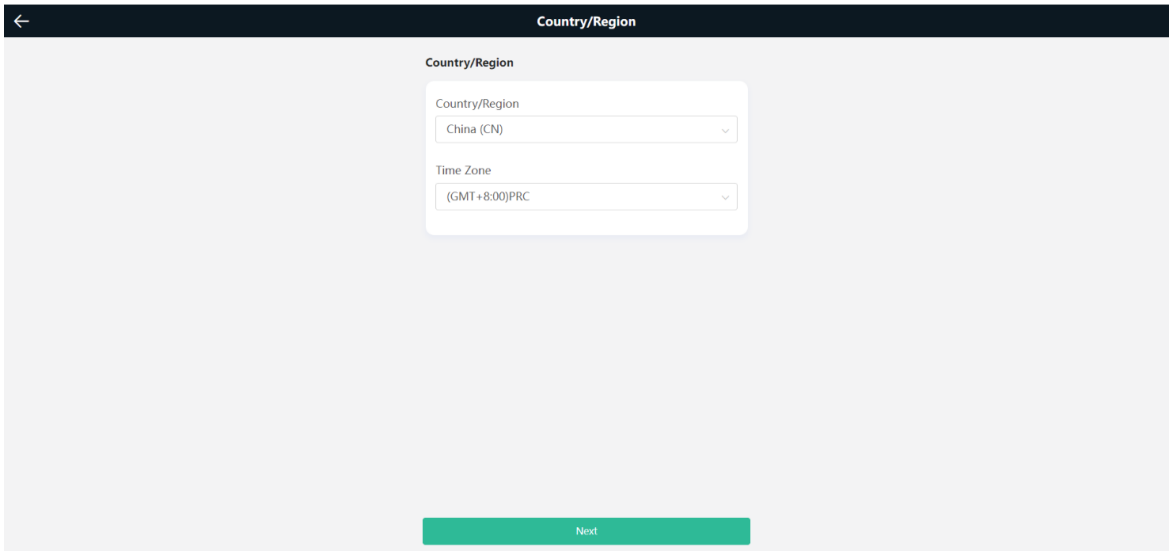
No Ethernet cable is required in the wireless repeater mode. The wireless network stability can be affected by many factors. Therefore, the wired connection is recommended.

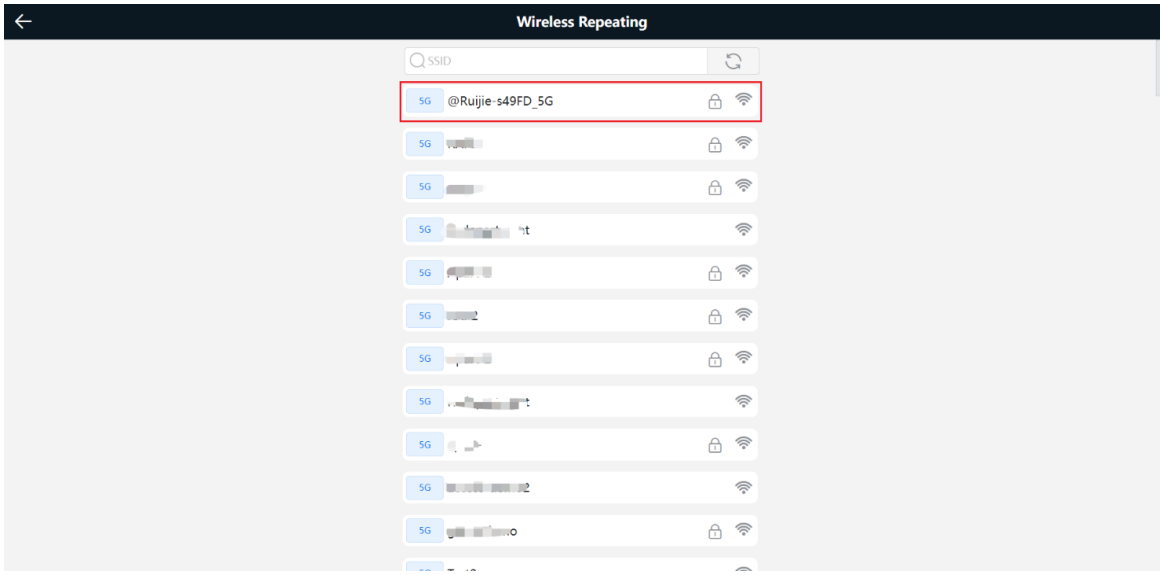
3. Wireless Connection by Web configuration

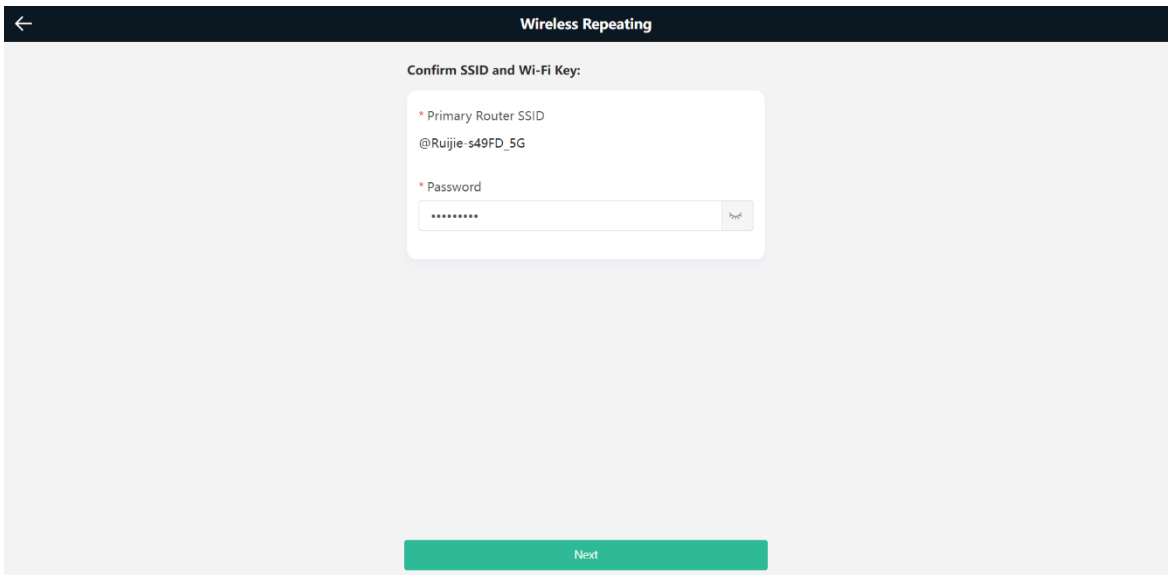
4. Wireless Repeater Mode

(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.

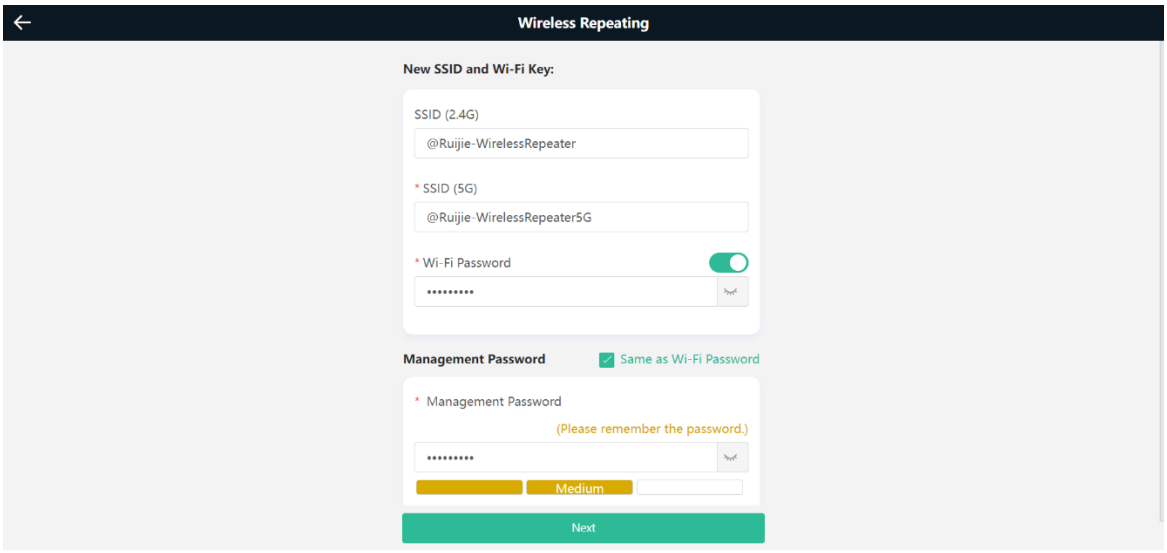


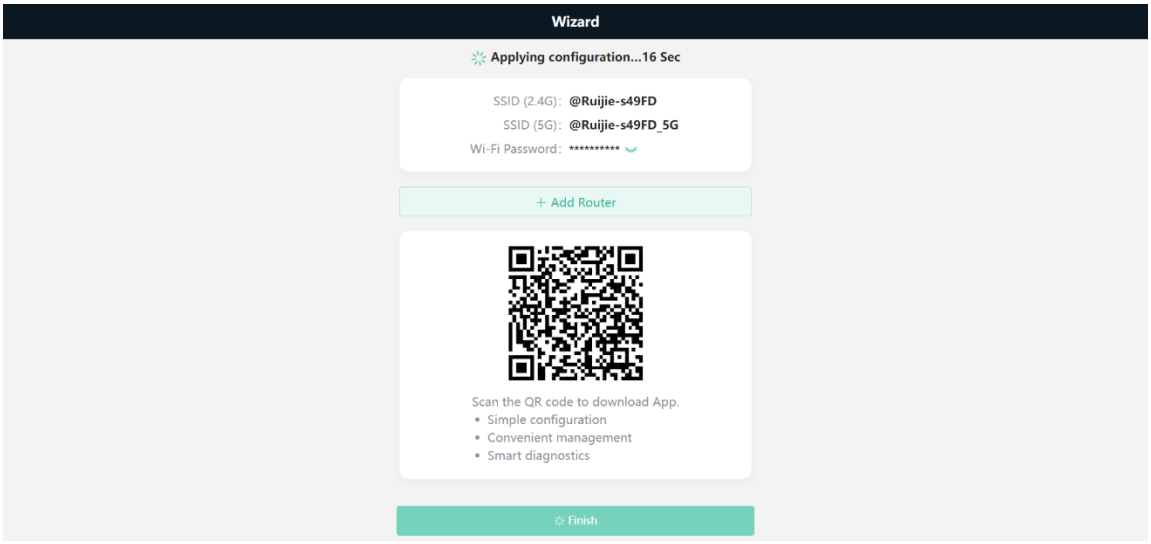


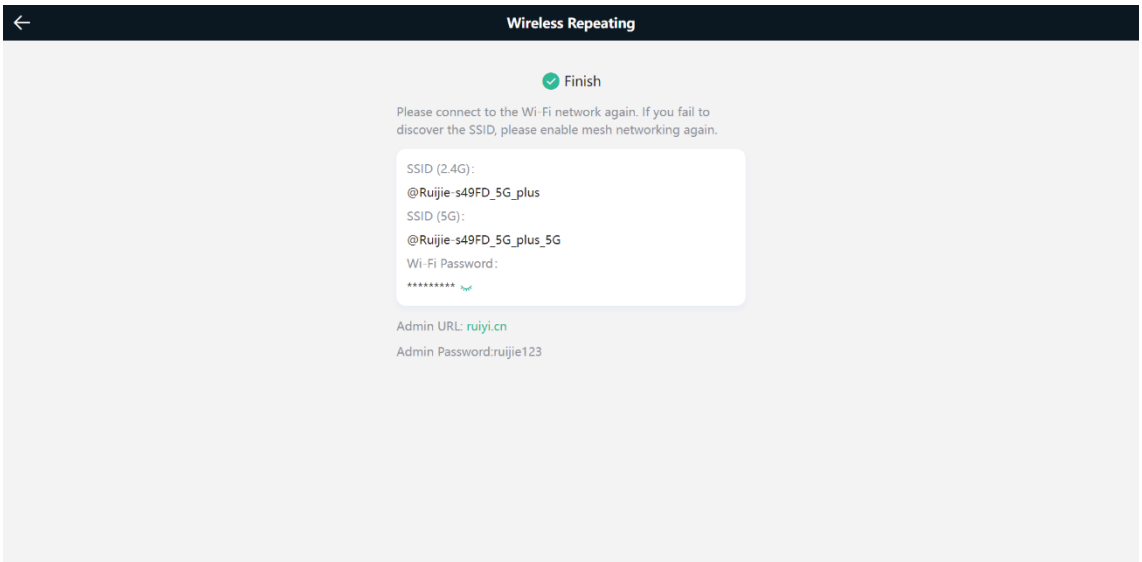




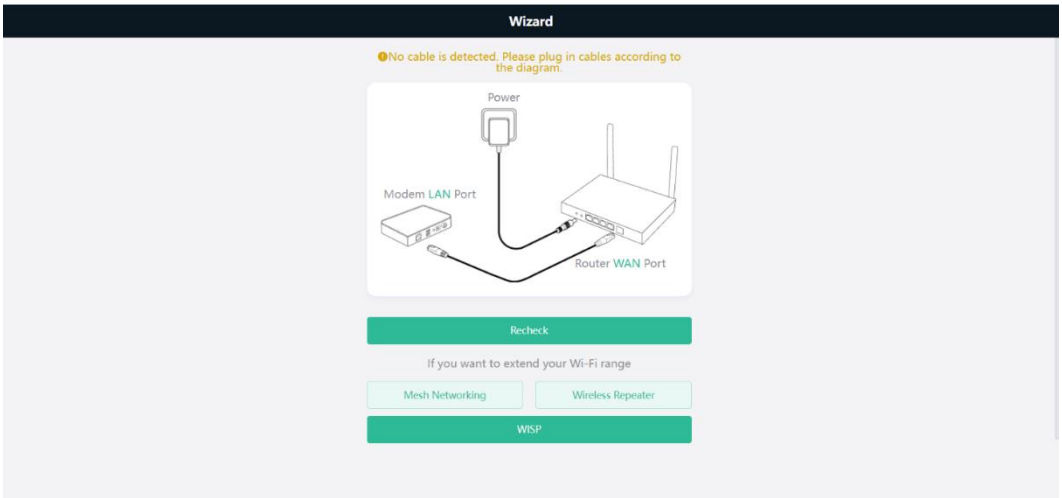
(2) Set the SSID and password and save the settings. Then settings of the Wi-Fi network are reset.





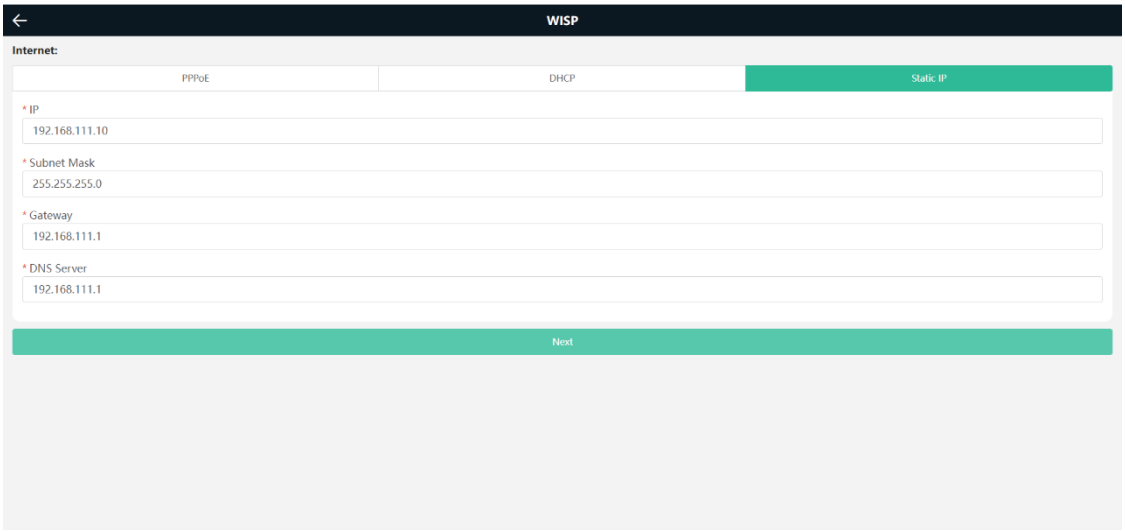


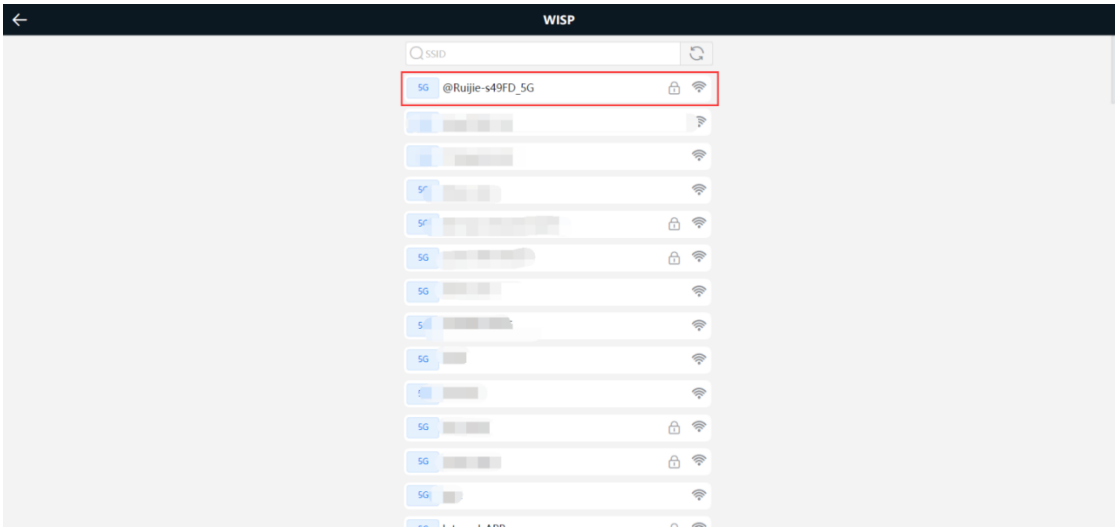
In wireless repeater mode, only Wi-Fi signals are extended and the DHCP function is disabled. IP addresses of all clients connected to the primary and secondary routers are assigned by the primary router. If the device connects to the primary router in wireless repeater mode, the WAN port of the device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

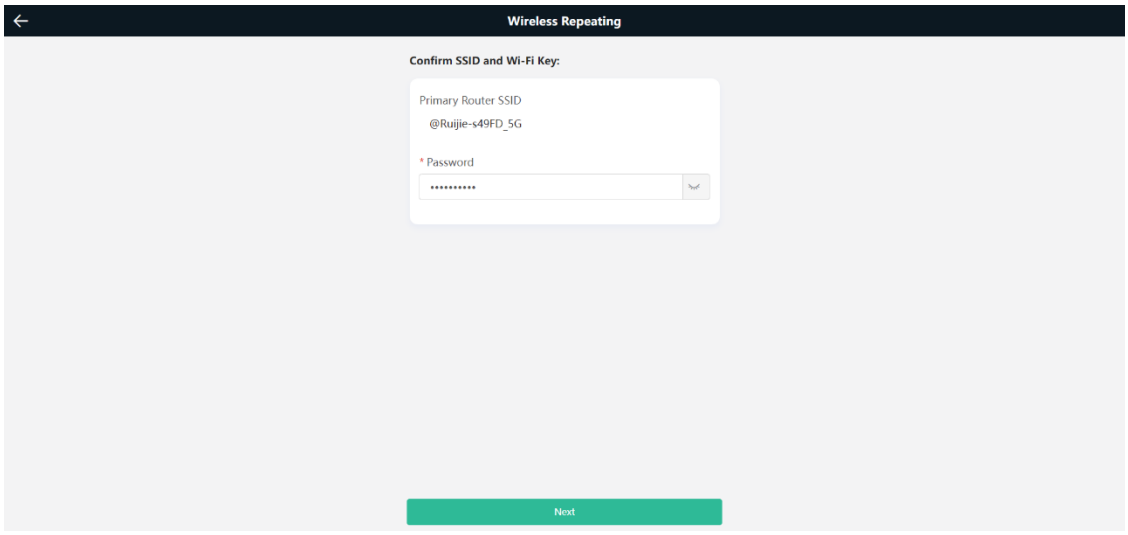


5. Wireless ISP Mode

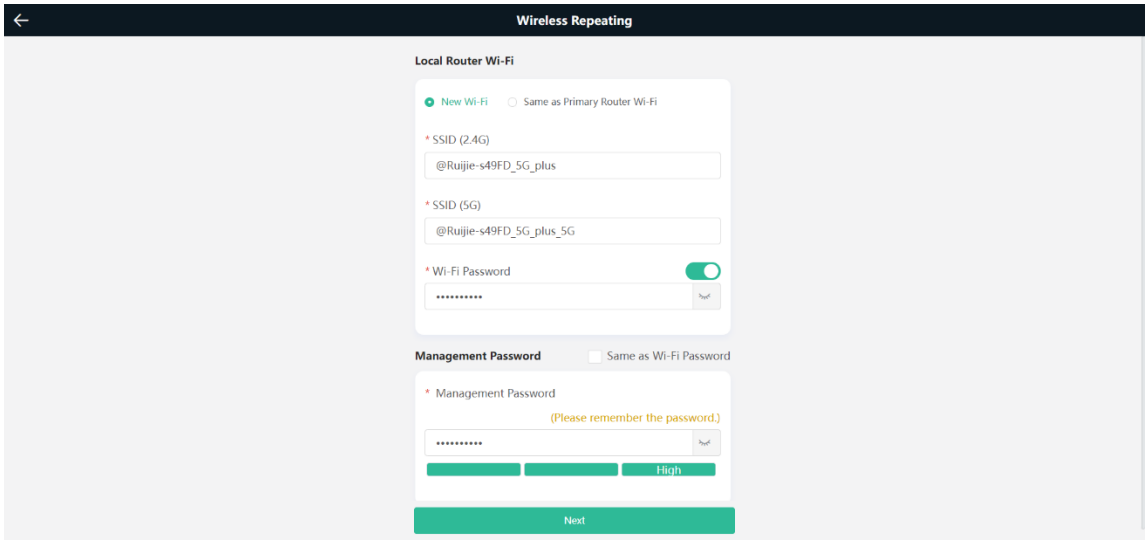
(1) Click **WISP**. On the displayed network setup page, click **Next** to automatically obtain an IP address. If the primary router cannot deliver an IP address, select **Static IP**. Select the SSID of the primary router and enter the Wi-Fi password to connect to the primary router.

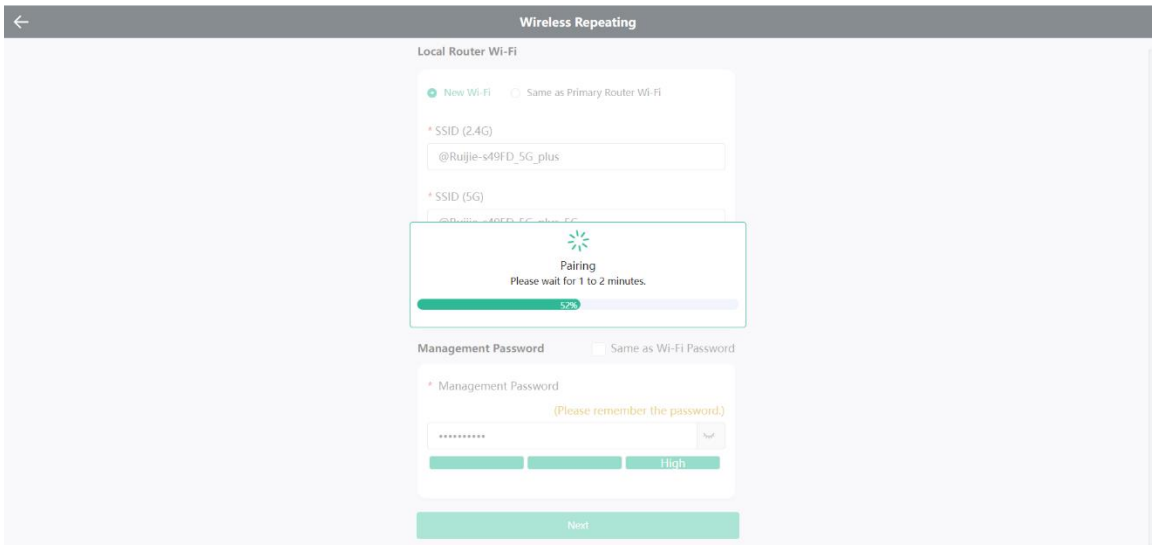


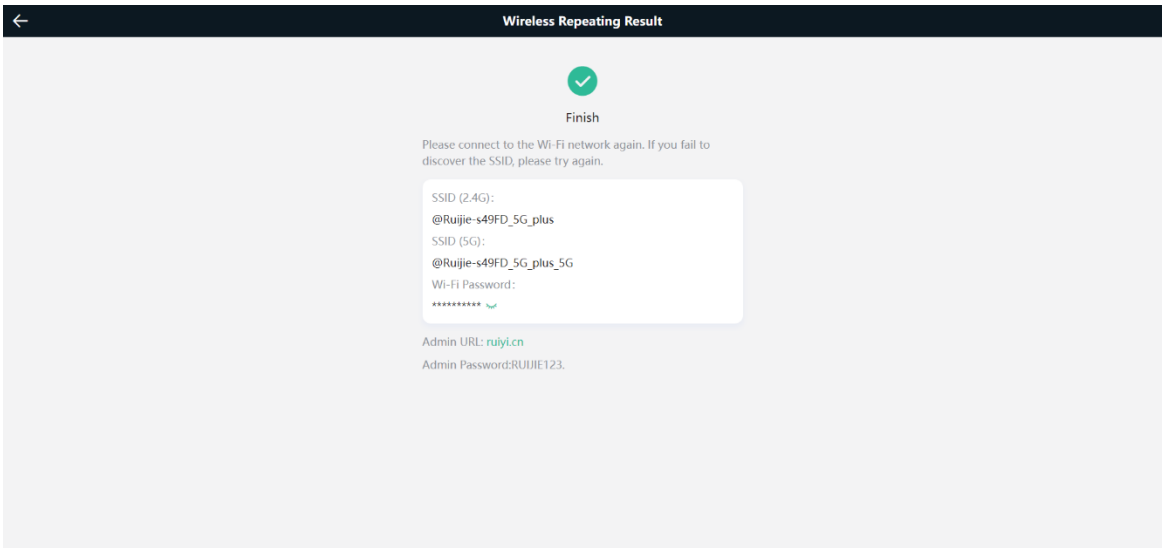




(2) Set the SSID and password and save the settings. Then settings of the Wi-Fi network are reset.



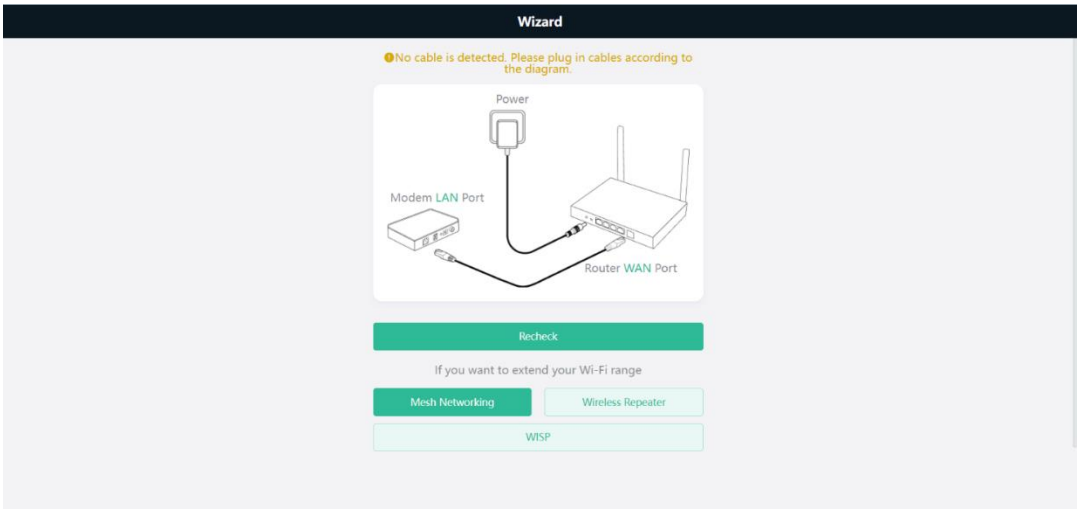


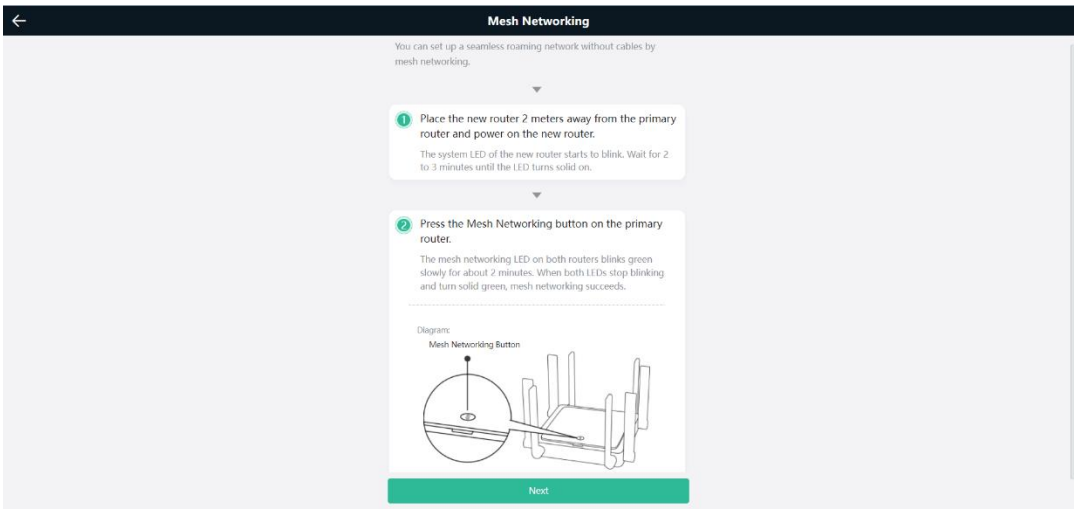


In wireless ISP mode, the device still supports routing and DHCP functions, IP addresses of clients connected to the primary router are assigned by the primary router and the IP addresses of clients connected to the secondary router are assigned by the secondary router. When the device connects to the Internet in wireless connection mode, the wired WAN port becomes the LAN port and is used by clients.

6. Mesh Networking

(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 router.

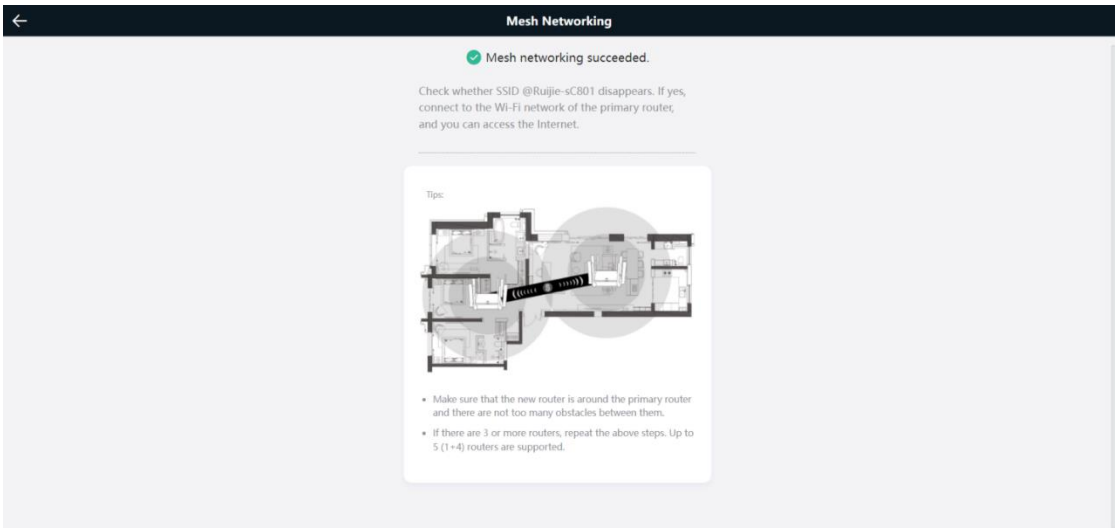




Caution

The RG-EW1200G PRO and RG-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.



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

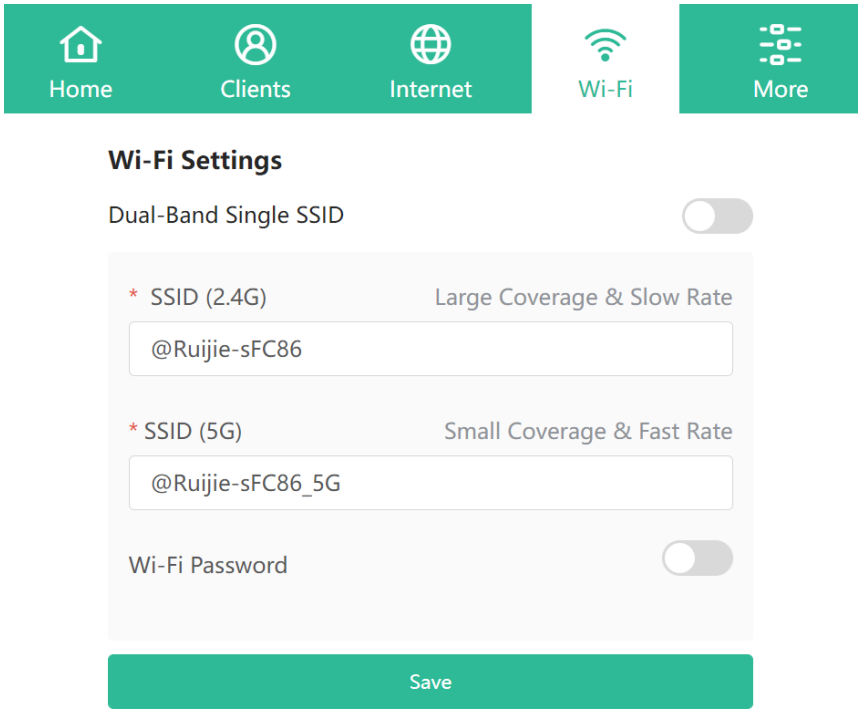
4.1 Changing the SSID and Password

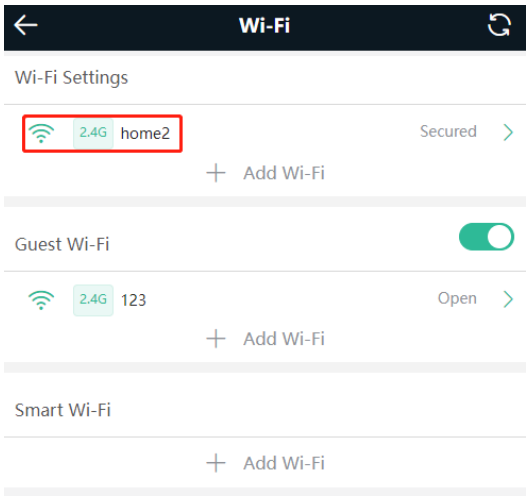
PC view: Choose **Wi-Fi** > **Wi-Fi Settings**.

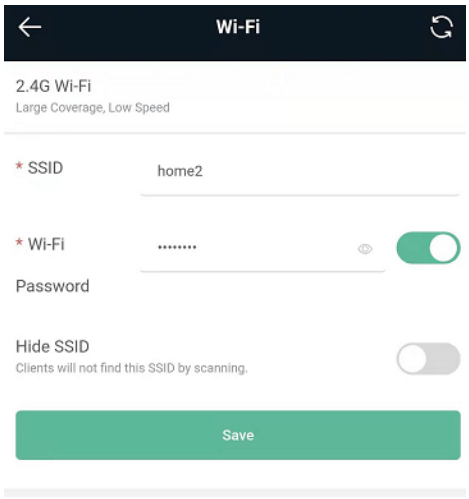
Mobile Phone: Choose **Wi-Fi** > **Wi-Fi Settings**. Click the target Wi-Fi network, change the SSID and password of the Wi-Fi network, and click **Save**.

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.







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.

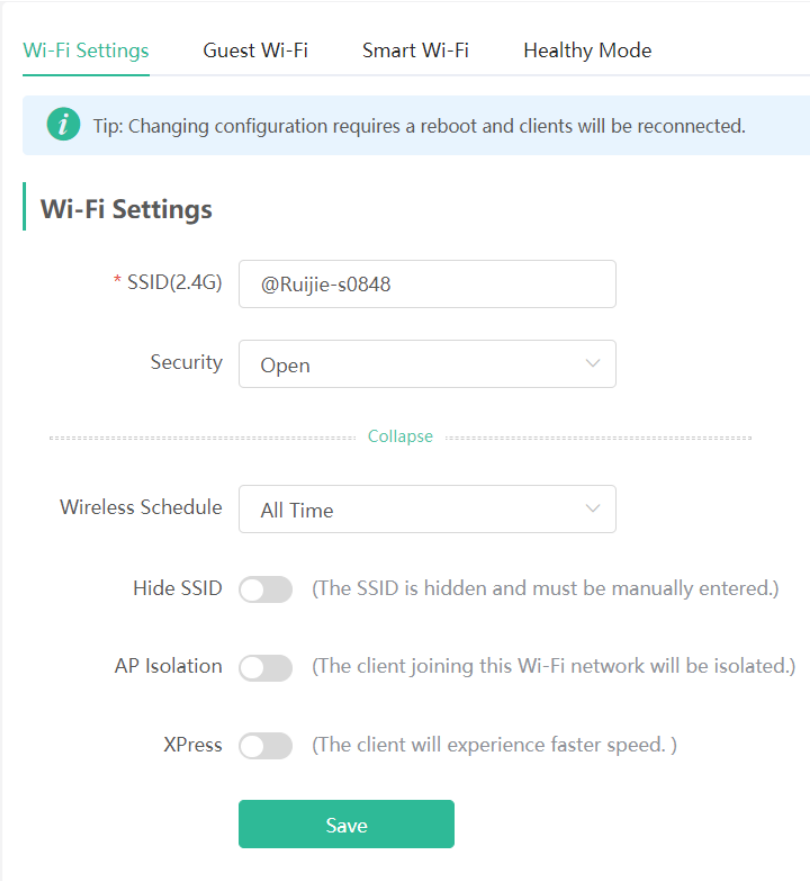
4.2.3 Configuration Steps

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.



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.

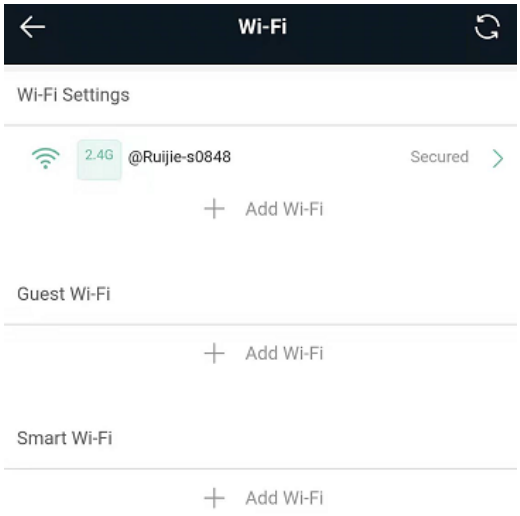
  The guest Wi-Fi network can be disabled as scheduled. You can configure the guest Wi-Fi network to be disabled 1 hour later. When the time expires, the guest Wi-Fi network is disabled.
- **Smart Wi-Fi**: The smart Wi-Fi network is disabled by default. Smart clients can connect to the smart Wi-Fi network for a long time. The smart Wi-Fi network cannot be disabled as scheduled.

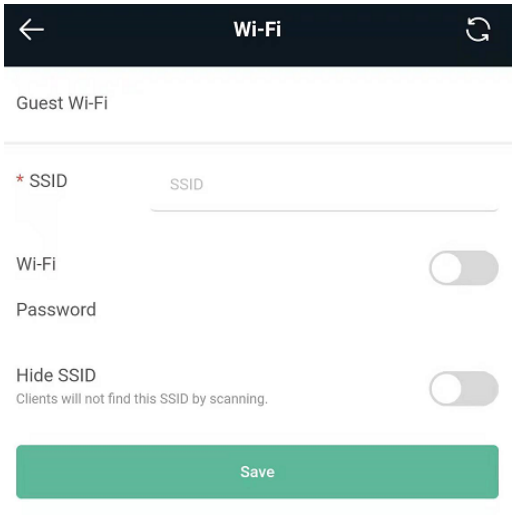
4.3.2 Configuration Steps

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 Blocklist or Allowlist

4.4.1 Overview

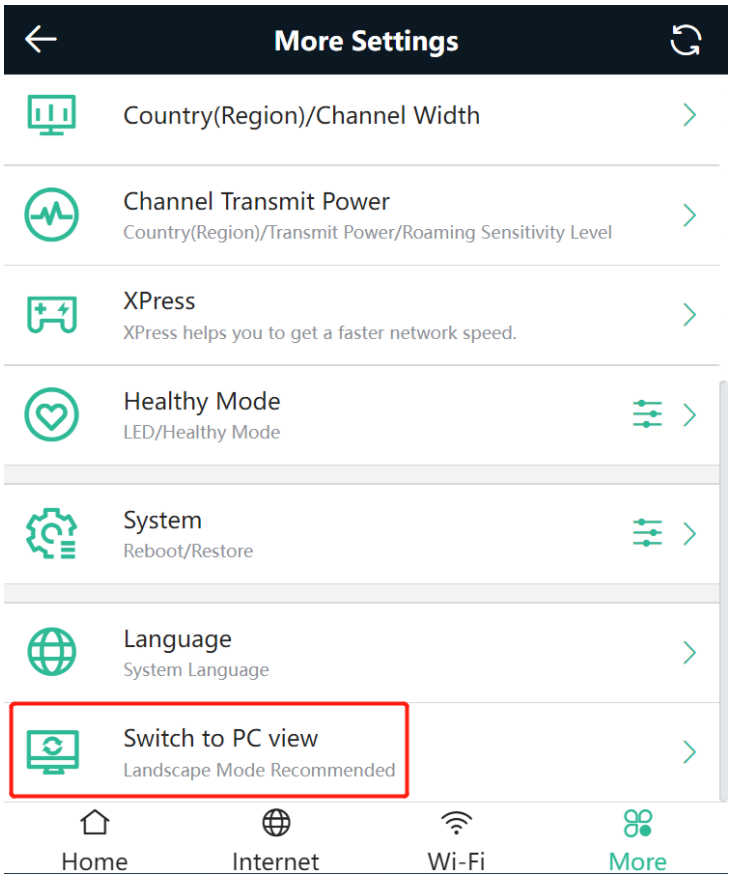
Wi-Fi blocklist: Clients in the Wi-Fi blocklist are prevented from accessing the Internet. Clients that are not added to the Wi-Fi blocklist are free to access the Internet.

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

4.4.2 Configuration Steps

Mobile phone view: Choose More > Switch to PC view > More > Wireless > Blocklist/Allowlist.

PC view: Choose More > Wireless > Blocklist/Allowlist.

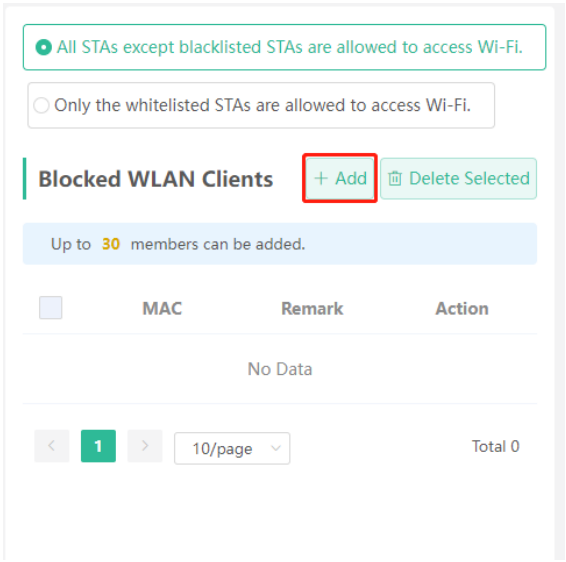


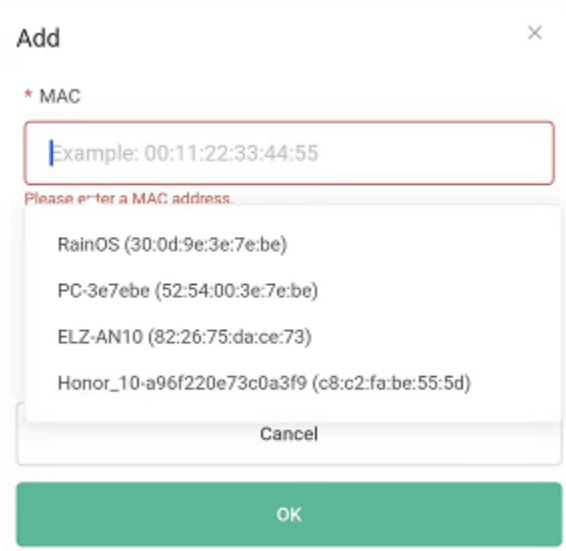
(1) Select the blocklist mode and click **Add**. The default mode is blocklist.

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

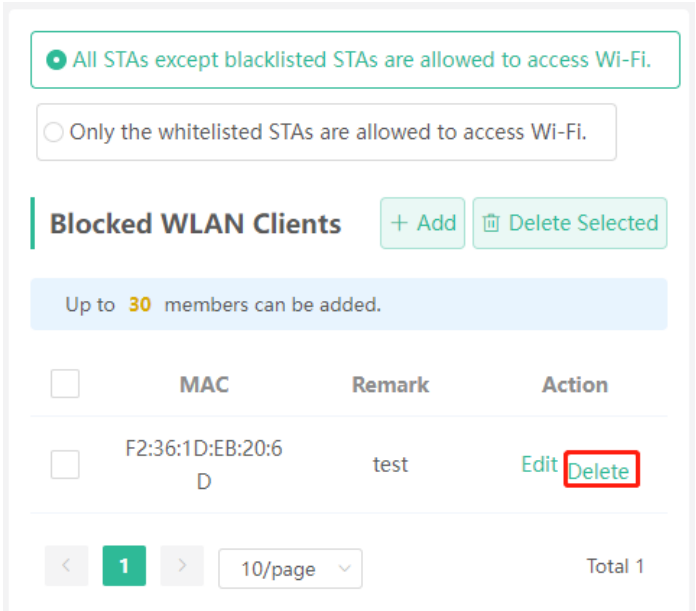
Note

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





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



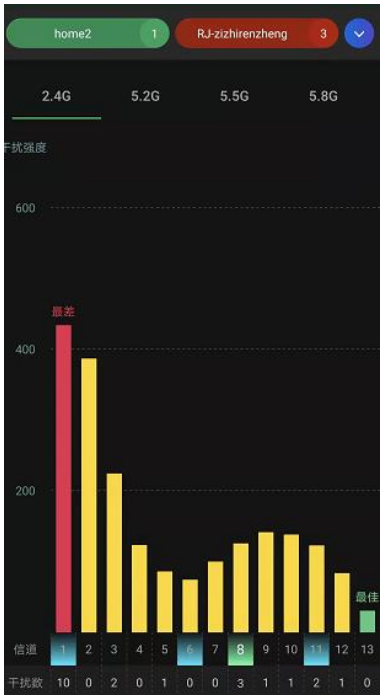
4.5 Optimizing the Wi-Fi Network

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.

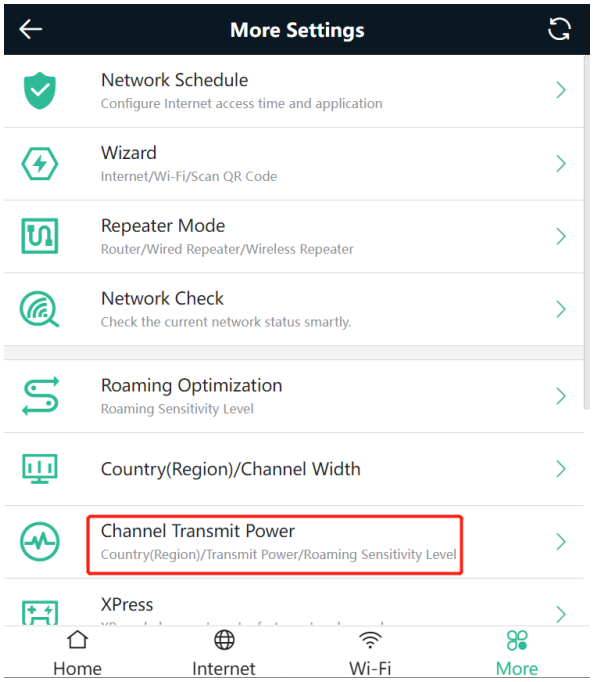
  Select the best channel identified by Wi-Fi Moho or other Wi-Fi scanning app. Click **Save** to make the configuration take effect immediately. Excess clients connected to a channel may result in stronger wireless interference.

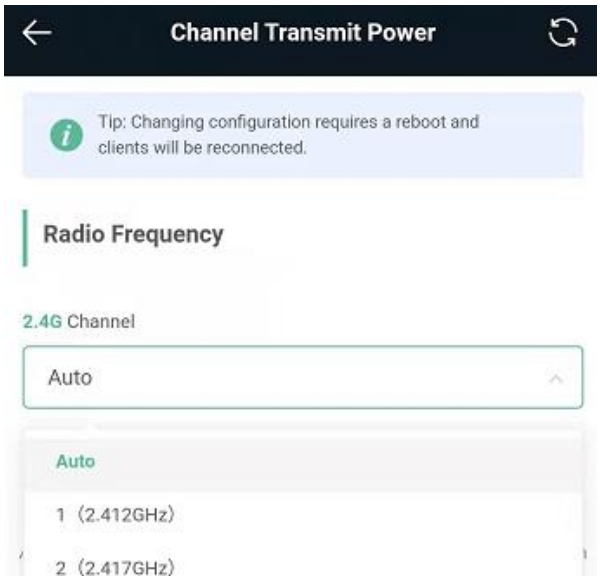
  Instruction

  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

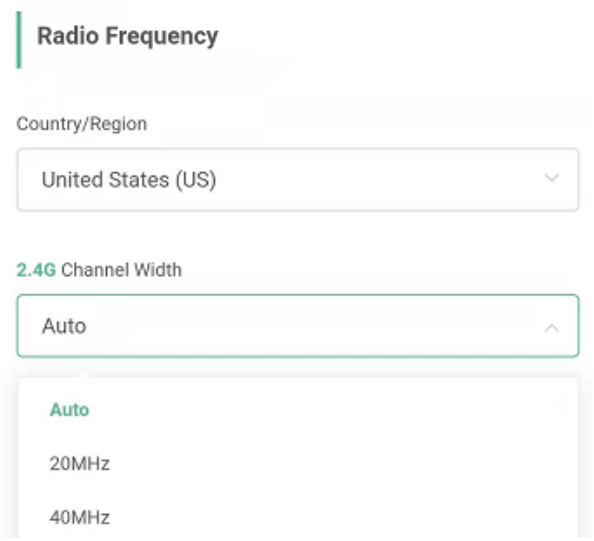
  Mobile phone view: Choose More> Country(Region)/Channel Width.

  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.



- Optimizing the transmit power

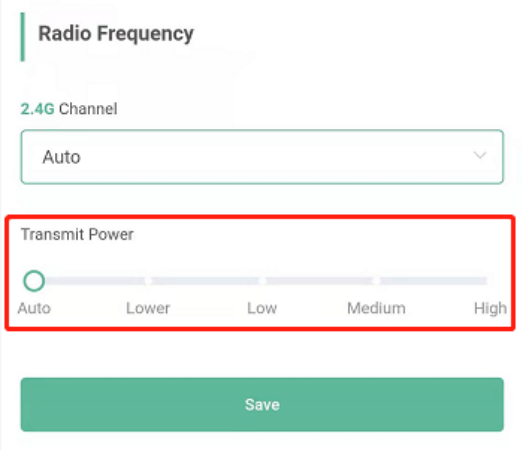
  Mobile phone view: Choose **More** > **Channel Transmit Power**.

  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.



- (Optional) Configuring the roaming sensitivity

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

  PC view: Choose More > Wireless > Radio Frequency.

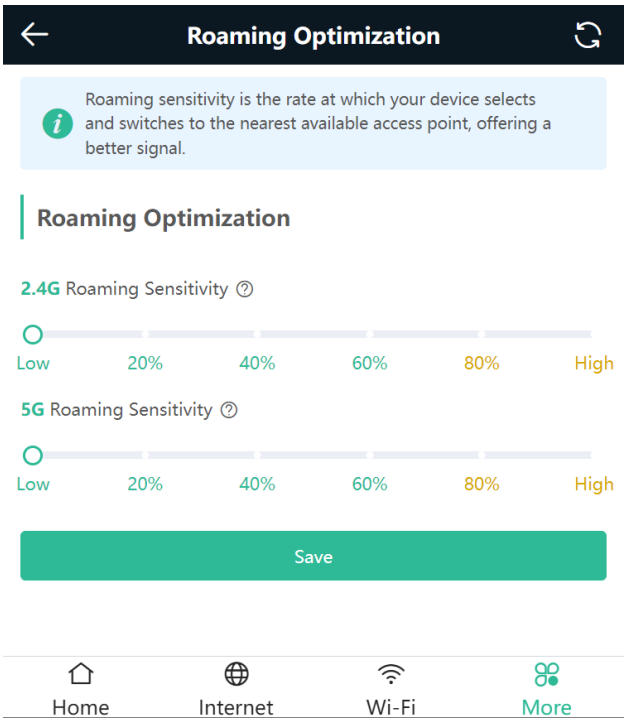
  Clients such as mobile phones support the roaming function but the sensitivity level may be not high. The roaming sensitivity enables the device to proactively disconnect a client from the Wi-Fi network when the client is far away, forcing the client to re-select the nearest signal and thus improving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

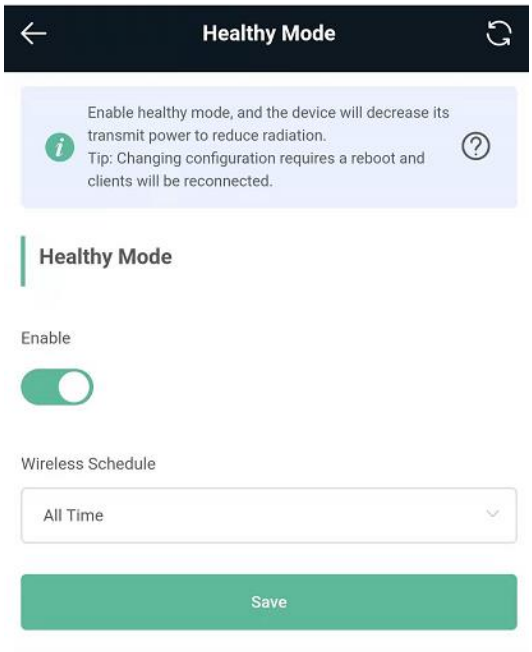
PC view: Choose More > Wireless > Wi-Fi > Healthy Mode.

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.

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.

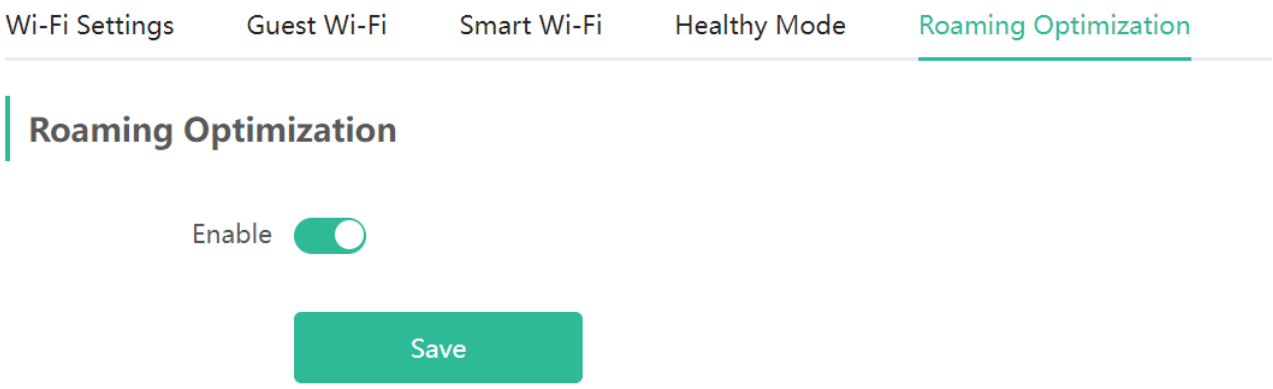


4.7 Enabling Roaming Optimization

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.



5 Reyee Networks Settings

5.1 Displaying SIM Card Information

Note

This function is only supported on the RG-EW300T router in **3G/4G Router Mode**, and is not supported on other models.

When the router works in **3G/4G Router Mode**, you can view the SIM card information on the device management page.

5.2 Managing the SIM Card

Note

This function is only supported on the RG-EW300T router in **3G/4G Router Mode**, and is not supported on other models.

5.2.1 Configuring Network Access for a SIM Card

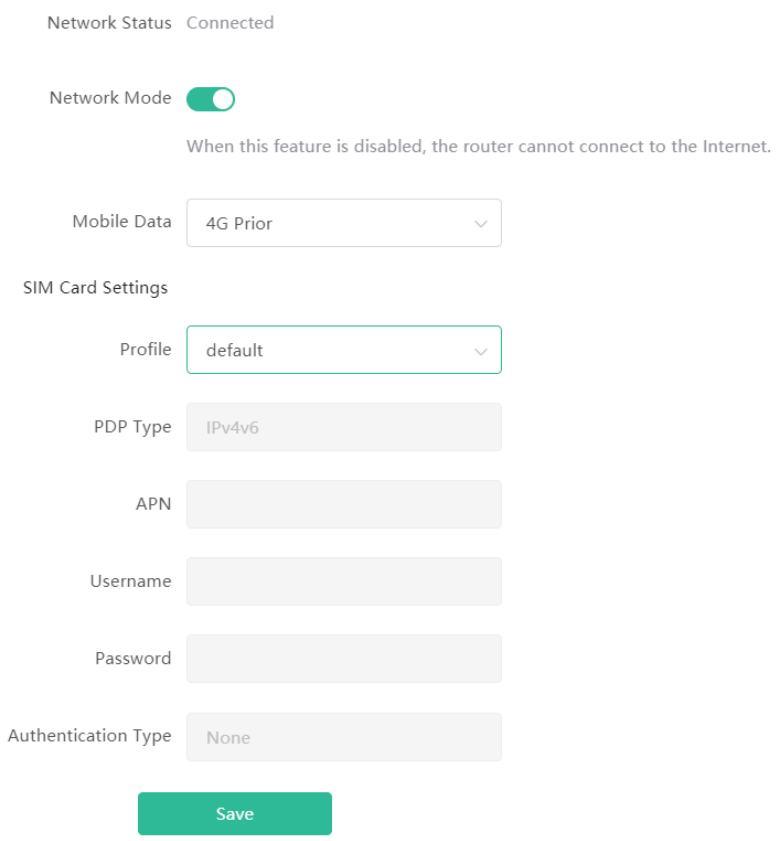
Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Basics** > **Network Access > Network Access**.

PC View: Choose **More** > **Basics** > **Network Access > Network Access**.

You can view the network connection status, and configure the network mode, mobile data type, and SIM card settings. To ensure successful access to the mobile network, contact your ISP to obtain SIM card information.

Caution

When **Network Mode** is disabled, the router cannot access the network.



- **Mobile Data**

  Mobile data refers to the mobile data service, which is data connection service provided through a mobile network (such as 3G, 4G, and 4G networks). You can maintain Internet connection in places where Wi-Fi is unavailable.

- **Profile**

  A profile is used to store parameters required for connecting to a mobile network, such as the APN, username, and password. After a profile is selected, the APN, username, password, and other parameters are automatically populated.

- **PDP Type**

  The PDP type indicates the protocol type used to establish data connection on a mobile network. On 3G and 4G networks, common PDP types include IPv4 and IPv6, indicating that IPv4 and IPv6 protocols are used for data transmission, respectively.

- **APN**
  - APN, short for Access Point Name, is the access point name that needs to be configured for the router to connect to a mobile network.
  - APN specifies the network accessed by the router when it connects to a mobile network. Different operators or ISPs may have different APNs.

- **Username and Password**
  - The username and password are used for authentication when the router connects to the mobile network.
  - The username and password are used for verifying the identity of the router by the ISP in order to obtain network access permissions.

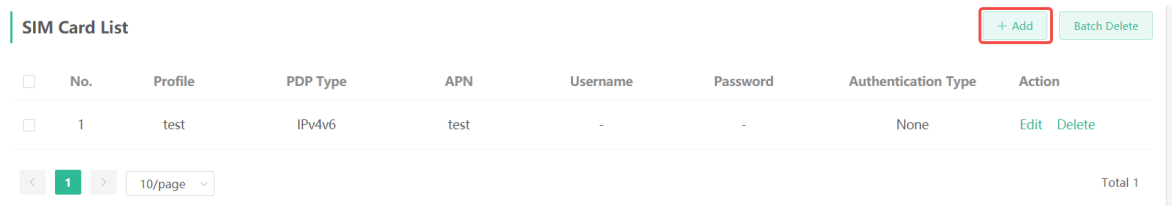
- **Authentication Type**
  - An authentication type refers to the authentication mode used when the router connects to the mobile network. Common authentication modes include Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP).
  - These authentication modes are used to ensure secure communication between the router and the mobile network and to prevent unauthorized access.

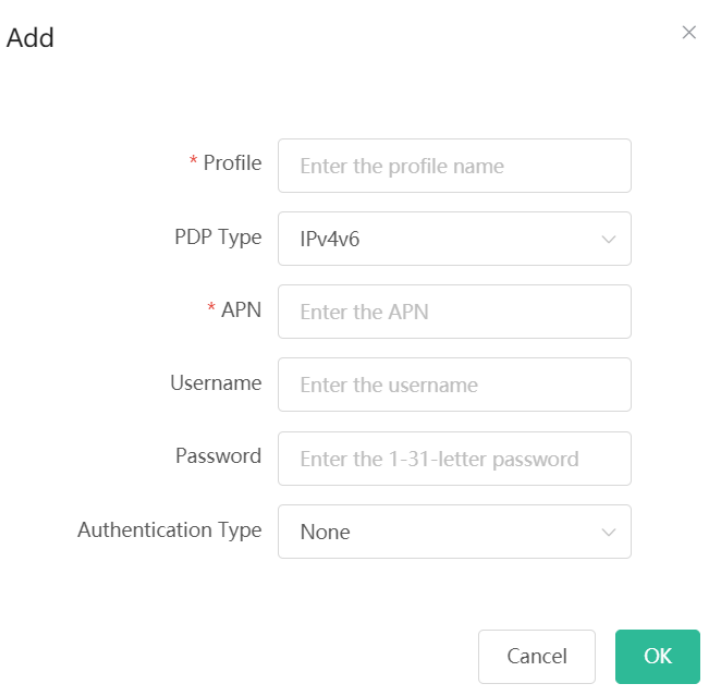
5.2.2 Displaying the SIM Card List

Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Basics** > **Network Access > SIM Card List**.

PC View: Choose **More** > **Basics** > **Network Access > SIM Card List**.

Click **Add** to create an SIM profile. Select the protocol type for establishing a data connection, and configure **APN**, **Username**, **Password**, and **Authentication Type**. For parameter descriptions, see 5.2.1 Configuring Network Access for a SIM Card.





5.3 Managing the PIN

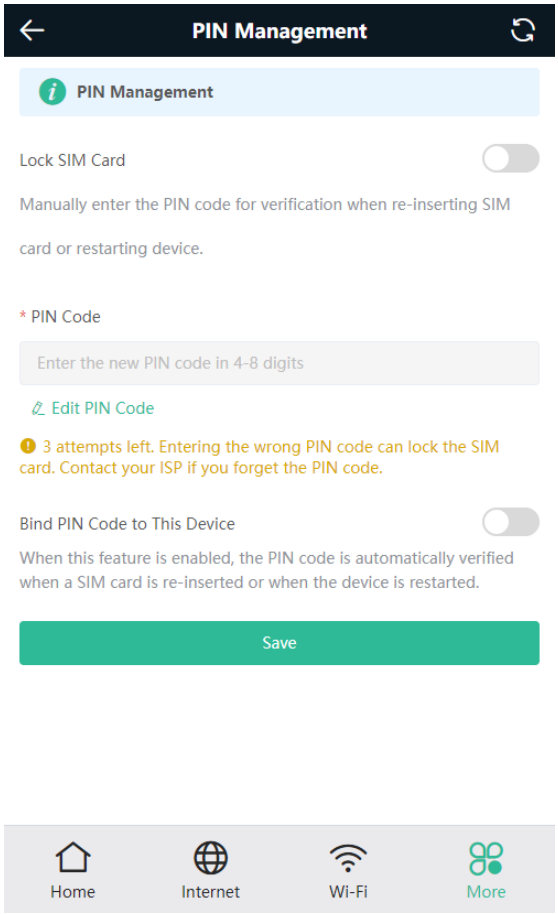
Note

This function is only supported on the RG-EW300T router in **3G/4G Router Mode**, and is not supported on other models.

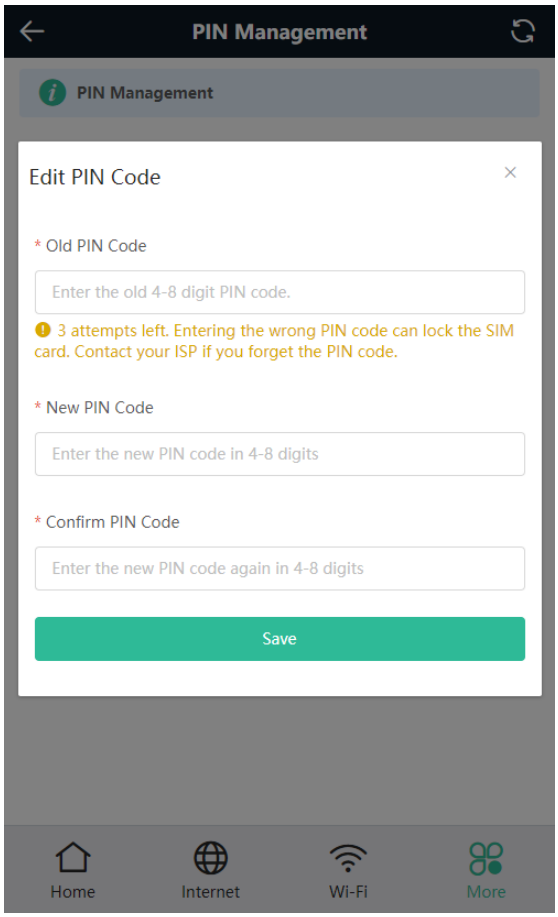
Mobile Phone View: Choose **More > PIN Management.**

PC View: Choose **More** > **Basics** > **PIN Management**.

PIN is a simple and effective security measure that protects the SIM card and user communication privacy, ensuring that only authorized users can use the communication services provided by the SIM card.



- **Lock SIM Card**: After this function is enabled, you need to manually enter the PIN for authentication every time the router is restarted or the SIM card is reinserted.
- Set a PIN: Click **Edit PIN Code** to set a PIN for the SIM card.



Caution

You have three attempts to enter the PIN. If the PIN is incorrect, the SIM card will be locked. Ensure that you obtain the correct PIN from the ISP before entering it.

- **Bind PIN Code to This Device**: After this function is enabled, you do not need to manually enter the PIN as the system automatically verifies the PIN every time the router is restarted or the SIM card is reinserted.

Note

If both **Lock SIM Card** and **Bind PIN Code to This Device** are enabled, **Lock SIM Card** takes effect.

5.4 Managing SMS

Note

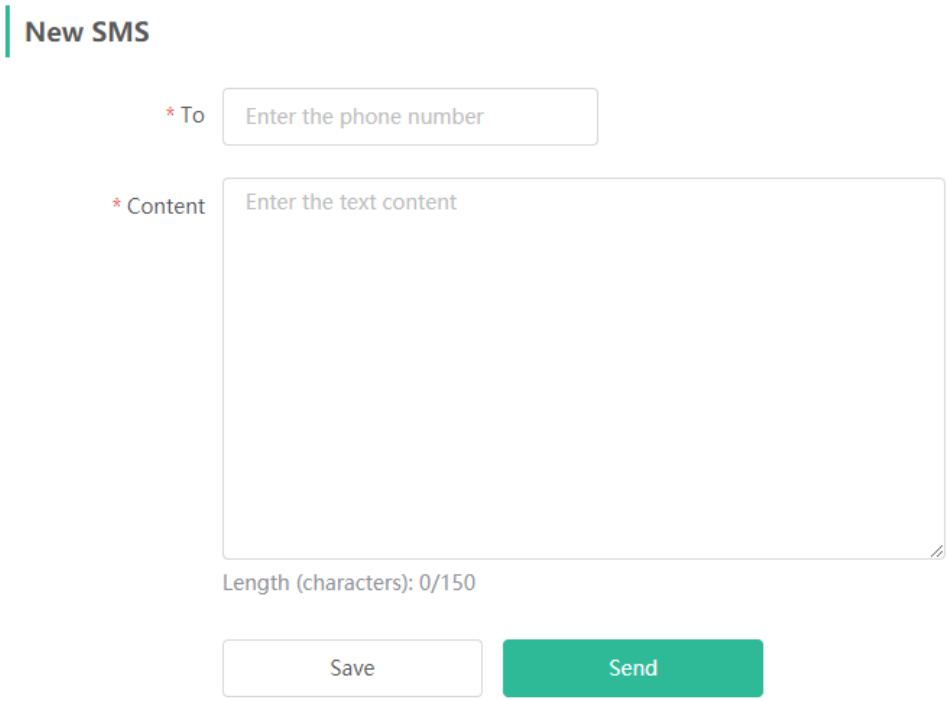
This function is only supported on the RG-EW300T router in **3G/4G Router Mode**, and is not supported on other models.

5.4.1 Creating an SMS Message

Mobile Phone View: Choose **More > SMS** > **New SMS.**

PC View: Choose **More** > **SMS** > **New SMS**.

You can create an SMS message by entering the recipient's phone number and SMS content. Click **Save** to save the message to the draft box. Click **Send** to send the message to the recipient.

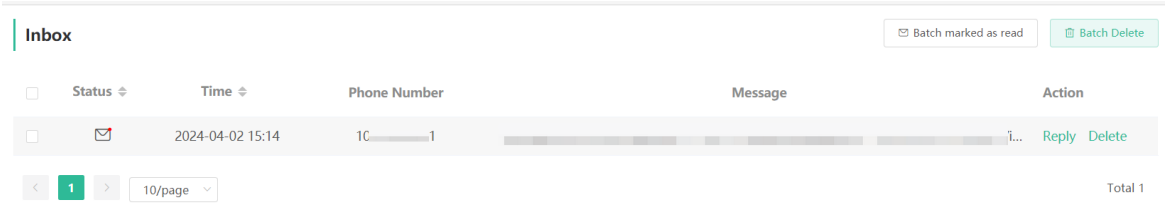


5.4.2 Displaying the Inbox

Mobile Phone View: Choose **More** > **SMS** > **Inbox**.

PC View: Choose **More** > **SMS** > **Inbox**.

The **Inbox** list displays the details of the inbox, including the read status, reception time, sender's phone number, and message summary. Click **Reply** in the **Action** column to reply to the message, or click **Delete** in the **Action** column to delete the message.

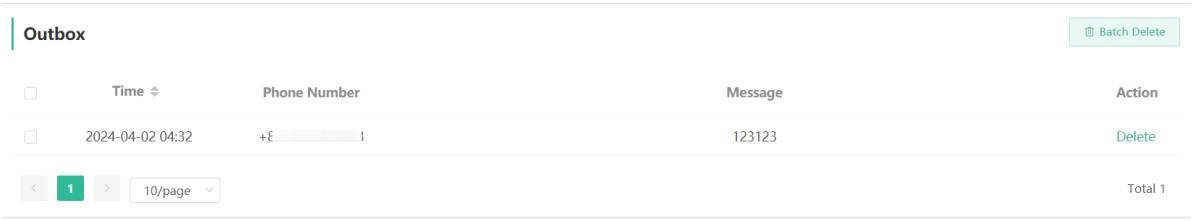


5.4.3 Displaying the Outbox

Mobile Phone View: **More** > **SMS** > **Outbox**.

PC View: Choose **More** > **SMS** > **Outbox**.

The **Outbox** list displays the details of the outbox, including the sending time, recipient's phone number, and message summary. Click **Delete** in the **Action** column to delete the message.

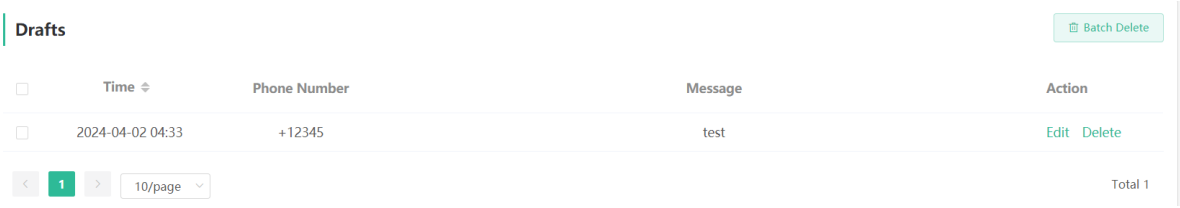


5.4.4 Displaying the Drafts Box

Mobile Phone View: Choose **More** > **SMS** > **Drafts**.

PC View: Choose **More** > **SMS** > **Drafts**.

The **Drafts** list displays the detailed information of the drafts box, including the storage time, recipient's phone number, and message summary. Click **Edit** in the **Action** column to edit the draft, or click **Delete** in the **Action** column to delete the draft.

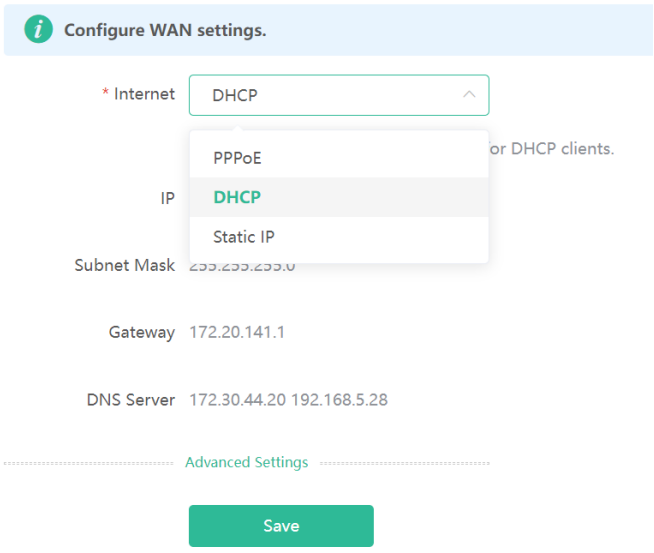


5.5 Configuring Internet Connection Type

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 Primary Router Mode.



5.6 Changing the Address of a LAN Port

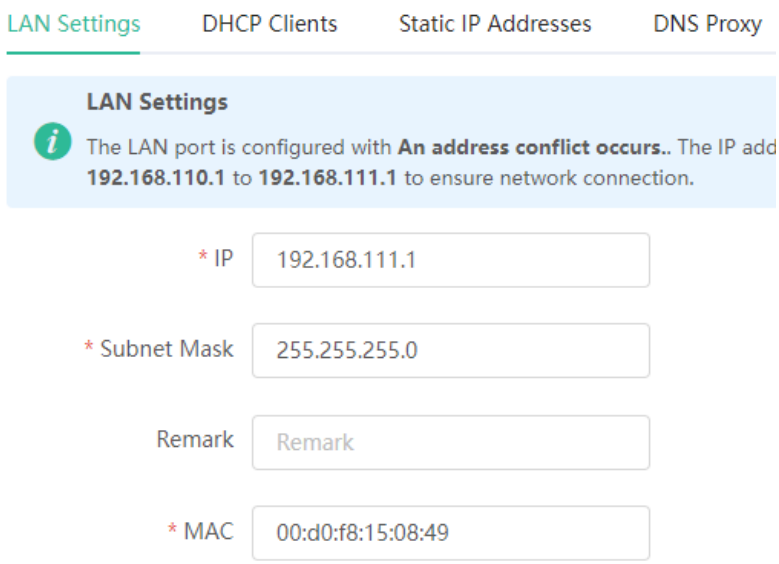
Mobile phone view: Choose **More** > **Switch to PC view** > **More** > **Basics** > **LAN**.

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.



5.7 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.

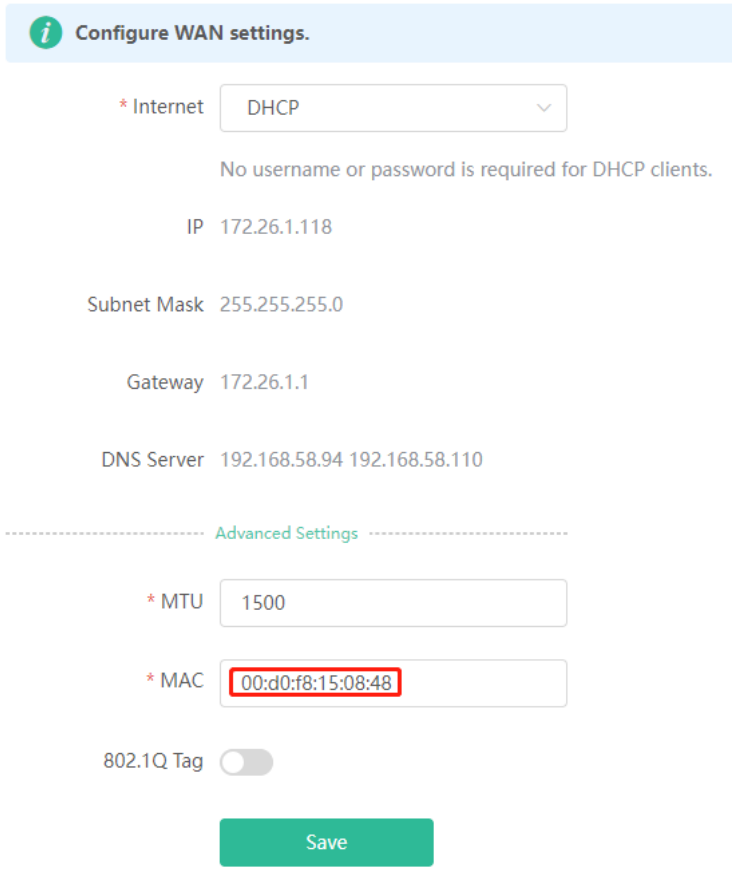
Enter the MAC address in the format of 00:11:22:33:44:55.

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



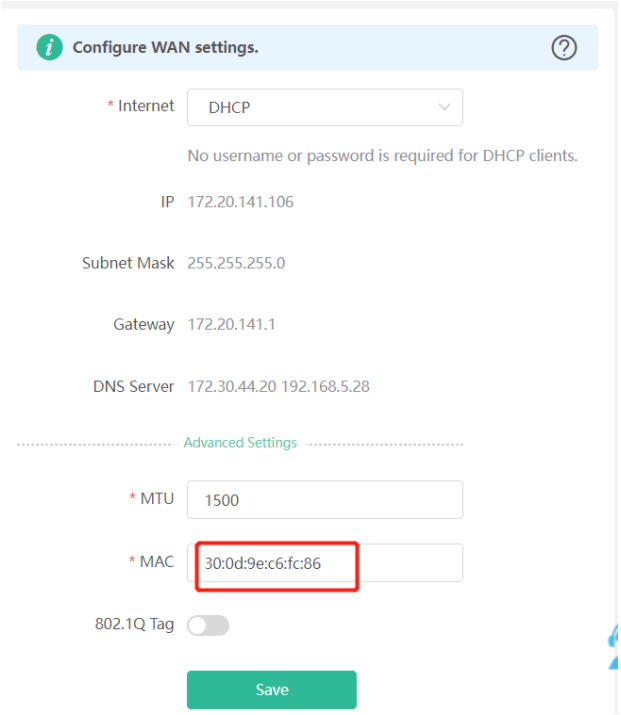
5.8 Changing the MTU

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.



5.9 Configuring the Repeater Mode

Caution

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

5.9.1 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)

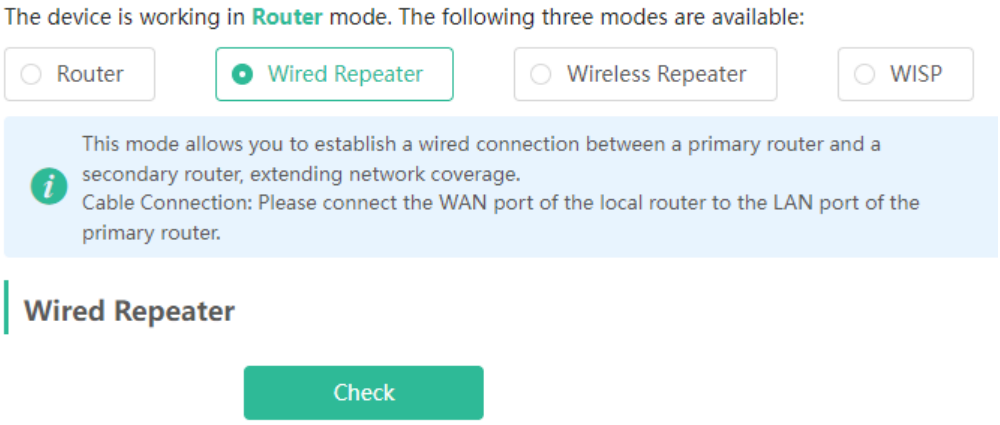
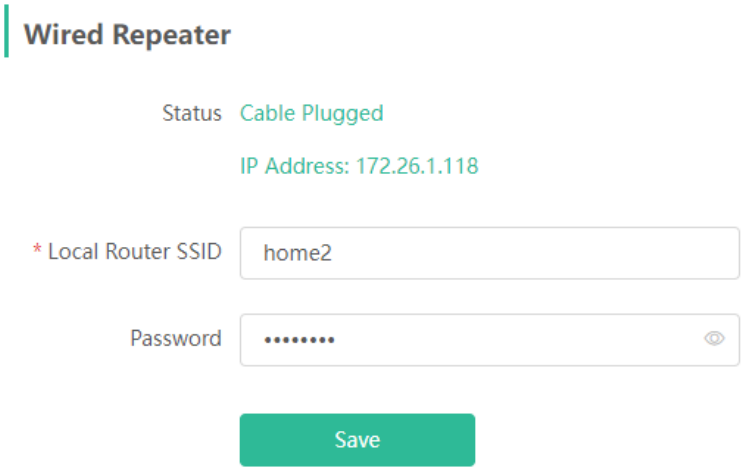


Figure 5-3 Wired Repeater Settings (2/2)



5.9.2 Wireless Repeater

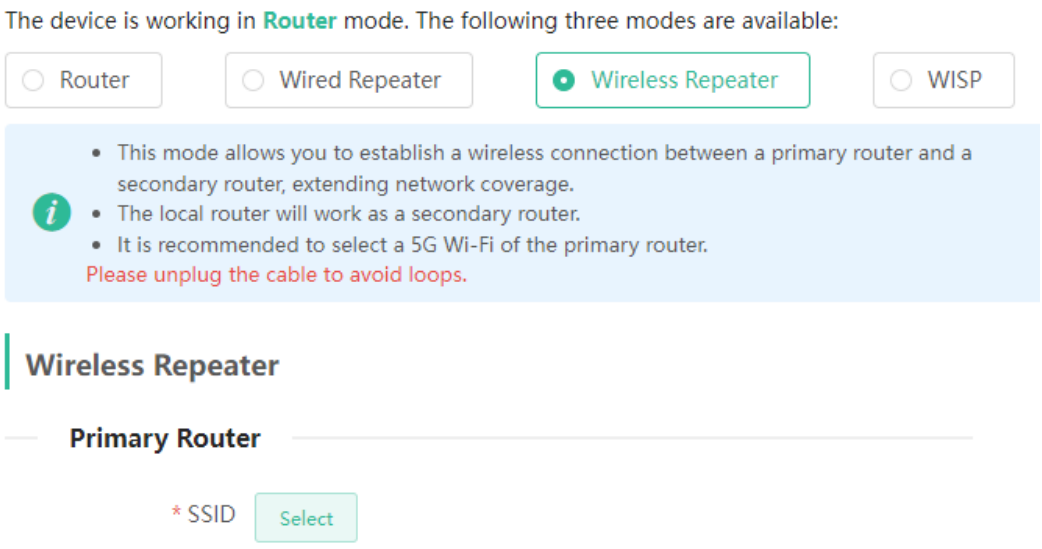
The wireless repeater mode extends the Wi-Fi coverage of the primary router.

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.



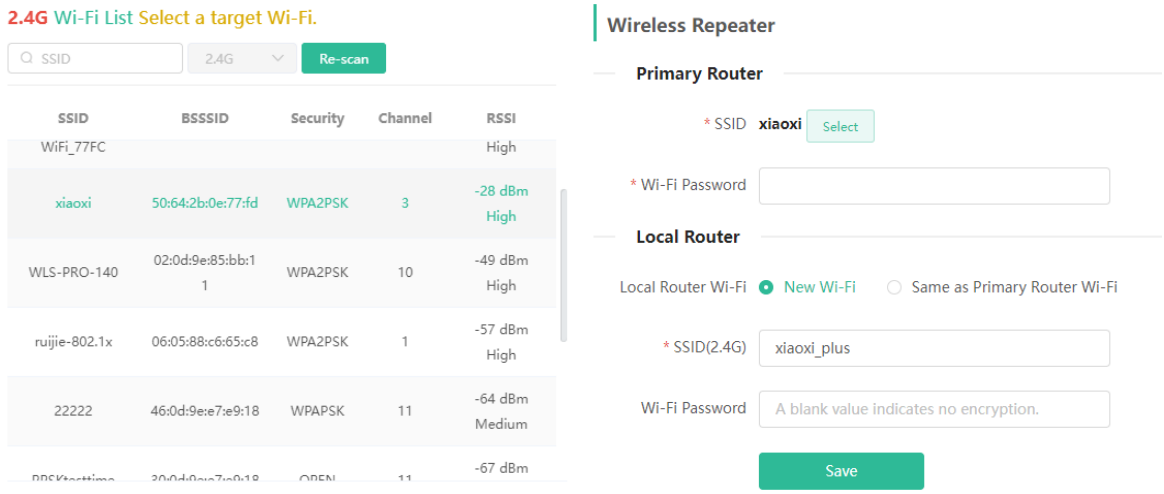
(2) Select the Wi-Fi signal of the primary router and enter its Wi-Fi password. You can configure a new Wi-Fi network or use the same Wi-Fi network as that of the primary router.

- 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

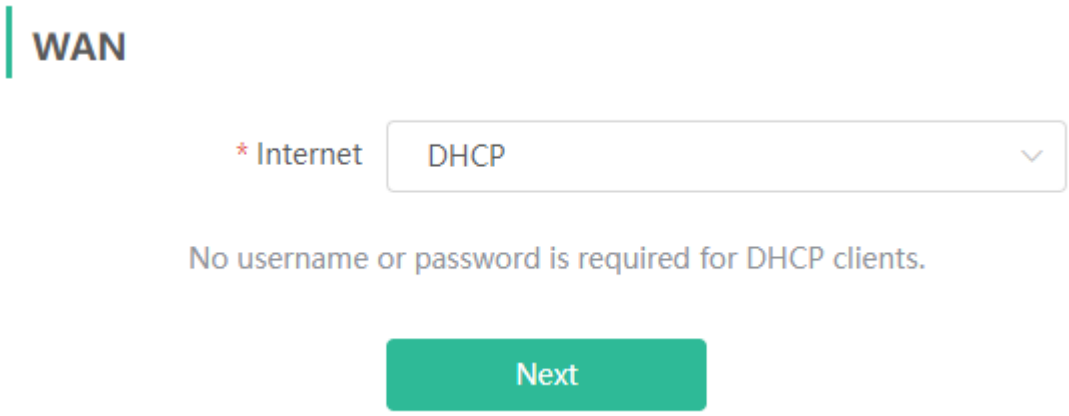


5.9.3 WISP

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**.



(2) Click **Select**, select a Wi-Fi signal, and click **Save**.

> **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.

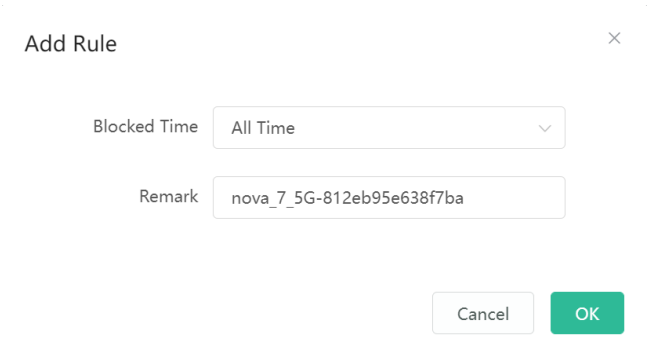
5.10 Controlling the Internet Access Time Range

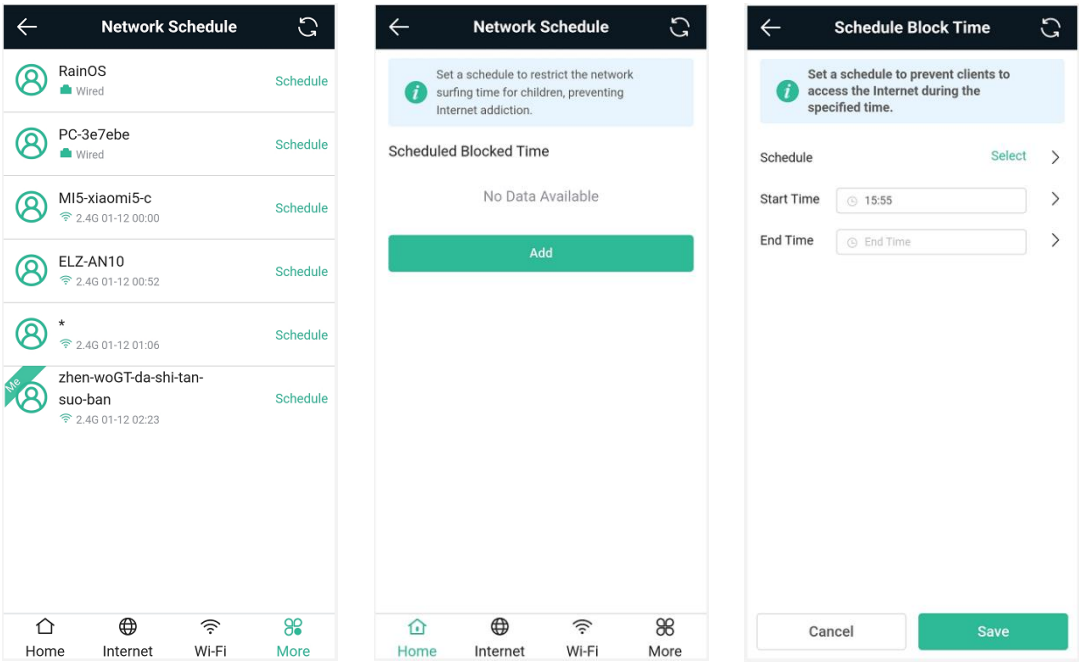
Mobile phone view: Choose **More** > **Network Schedule**. Select a client and click **Schedule**. Click **Add** and set the time range in which Internet access is blocked. In the specified time range, the client is prevented from accessing the Internet.

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.



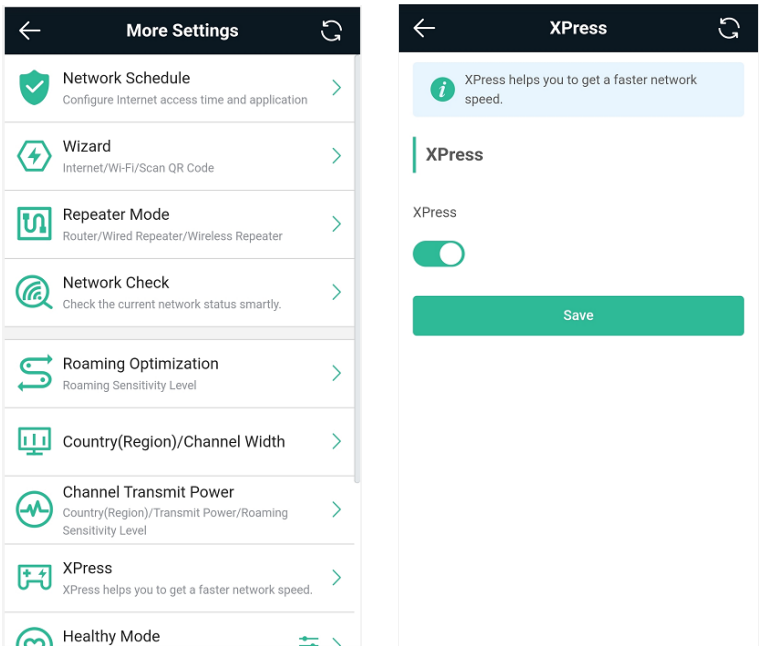


5.11 Configuring XPress

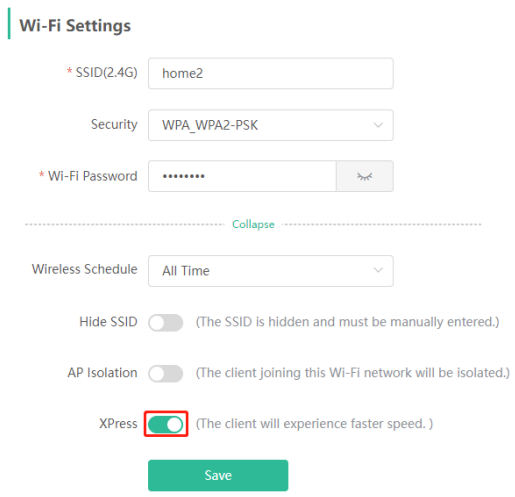
Mobile phone view: Choose **More** > **XPress**.

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.



5.12 Configuring Port Mapping

5.12.1 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.

5.12.2 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.

5.12.3 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.

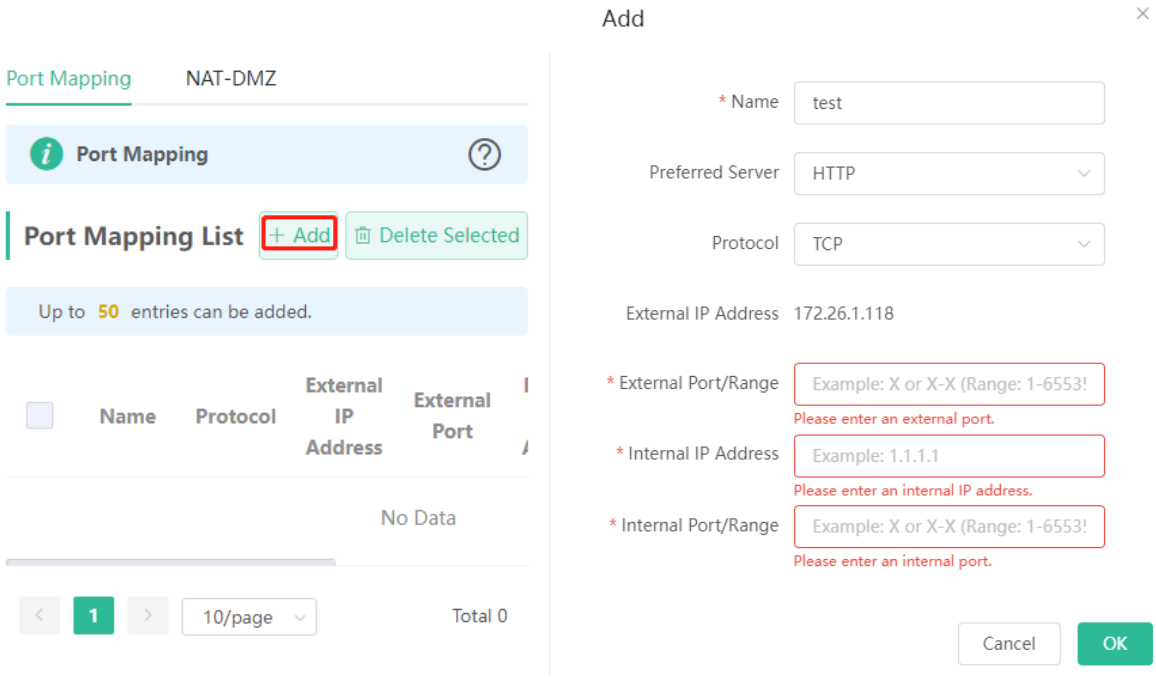
Preferred Server: Select a service to be mapped, such as HTTP or FTP. The device will automatically fill in the internal port number of the service. If the service is uncertain, you can select **Custom**.

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.



5.12.4 Verification and Testing

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

5.12.5 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.

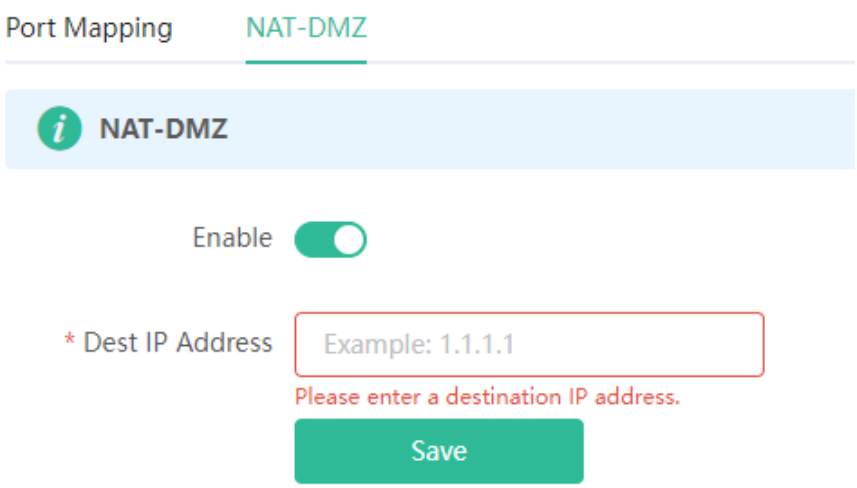
(3) Enable the DMZ service. For details, see 5.12.6 DMZ Configuration Steps. The common cause is that port configuration is incorrect or incomplete.

5.12.6 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**.



5.13 Configuring the DHCP Server

5.13.1 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.

5.13.2 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.

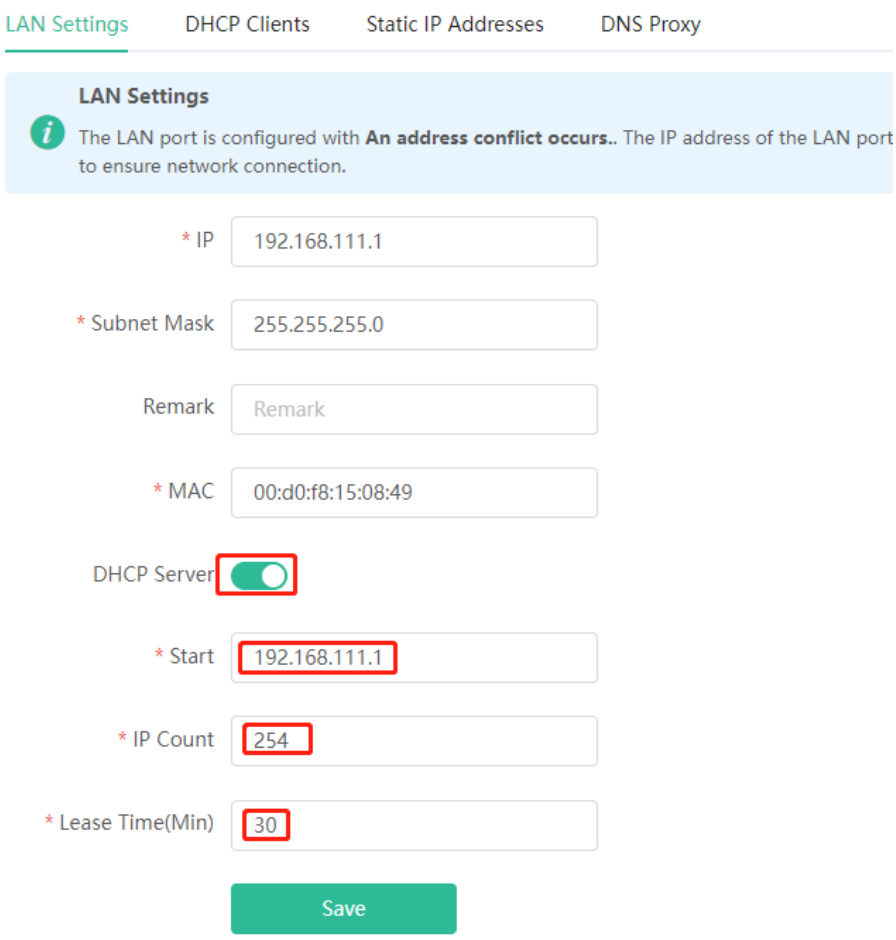
Note

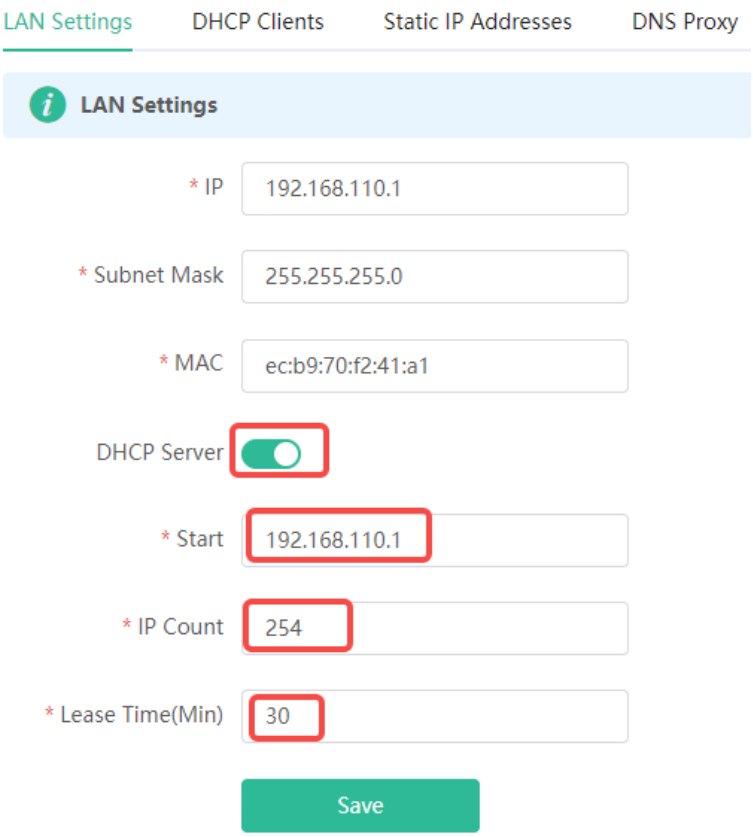
If the DHCP server function is disabled on all routers on the network, clients cannot automatically obtain IP addresses. In this case, you need to enable the DHCP server on a router or manually configure a static IP address for each client for Internet access.

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
The LAN port is configured with An address conflict occurs.. The IP address of the LAN port to ensure network connection.
* IP
192.168.111.1
* Subnet Mask
255.255.255.0
Remark
Remark
* MAC
00:d0:f8:15:08:49
DHCP Server
* Start
192.168.111.1
* IP Count
254
* Lease Time(Min)
30
Save

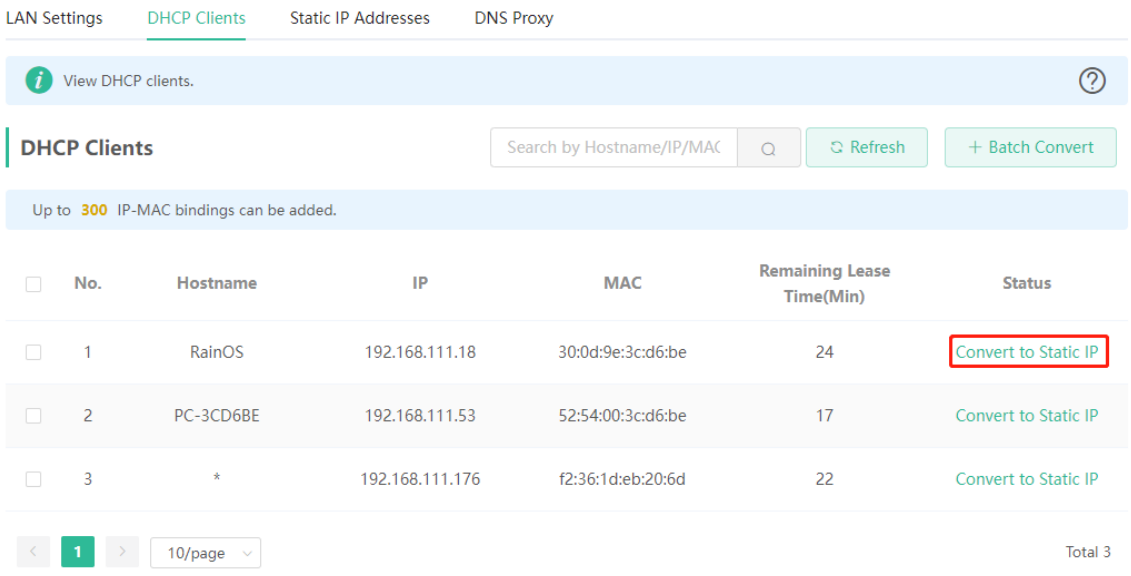


2. Displaying Online DHCP Clients

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.

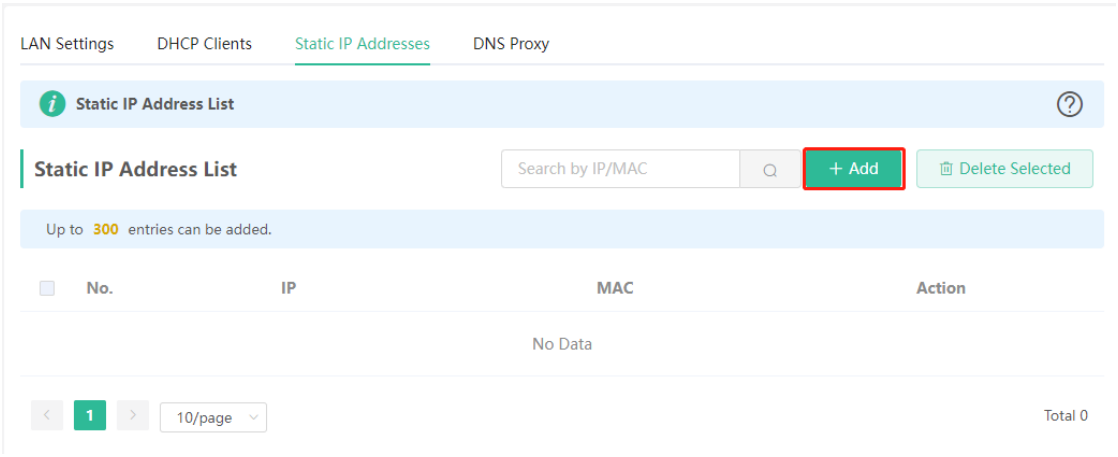


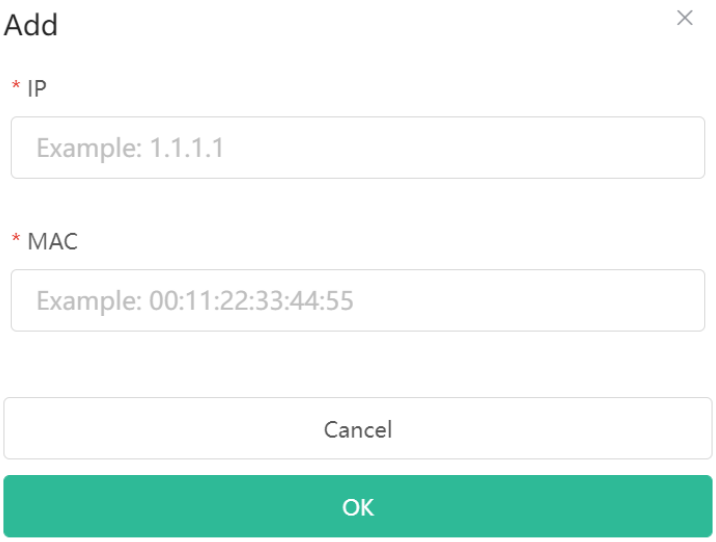
3. Displaying the DHCP Static IP Address Table

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.





5.14 Configuring DNS

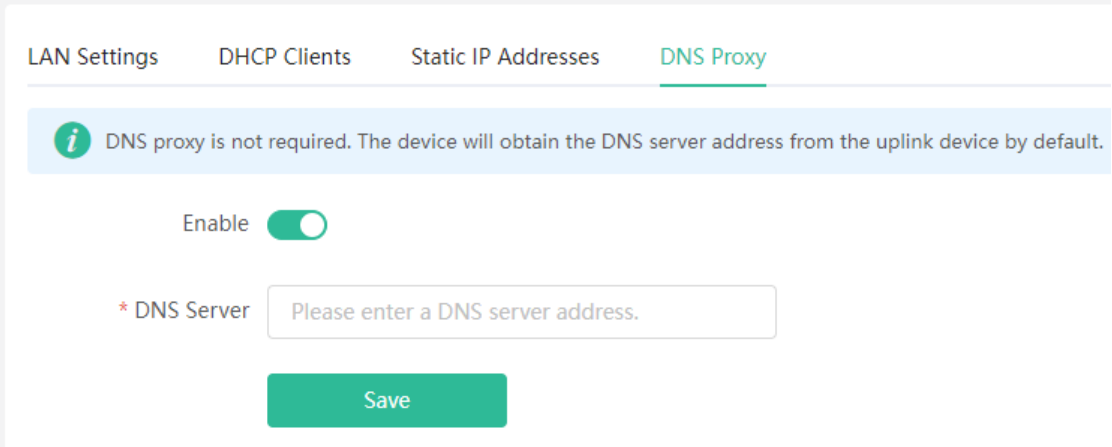
The domain name system (DNS) proxy configuration is optional. The device obtains the DNS server address from the uplink device by default.

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.



5.15 Configuring DDNS

5.15.1 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.

5.15.2 Getting Started

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

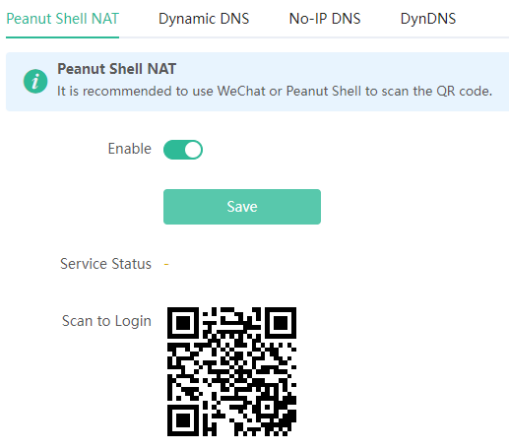
5.15.3 Configuration Steps

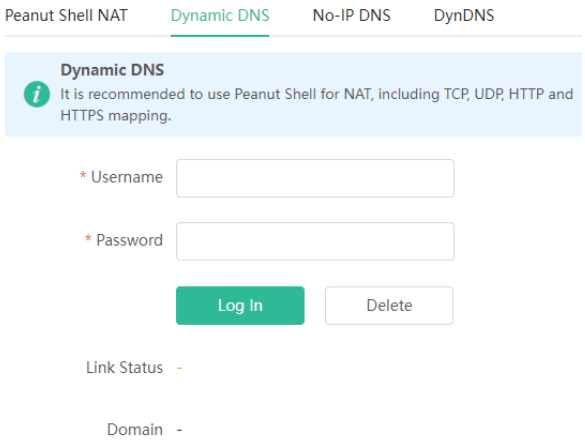
Mobile phone view: Choose More > Switch to PC view > More > Advanced > Dynamic DNS > Dynamic DNS.

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.





5.16 Configuring APR Binding and ARP Guard

5.16.1 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.

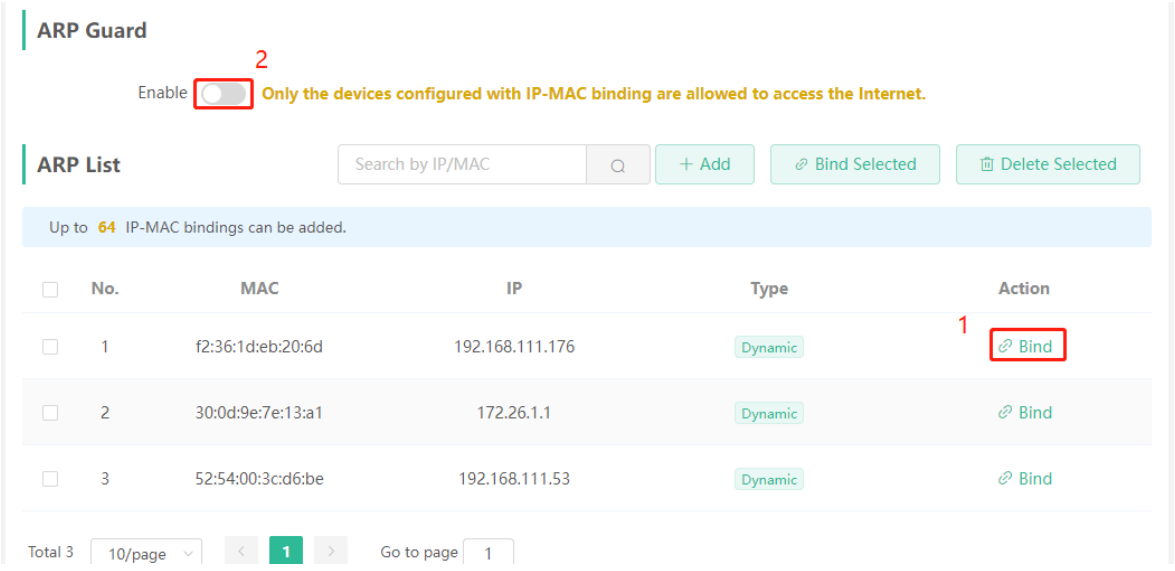
5.16.2 Configuration Steps

(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.



(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.

5.17 Configuring Static Routing

Note

Only RG-EW3000GX PRO supports this function.

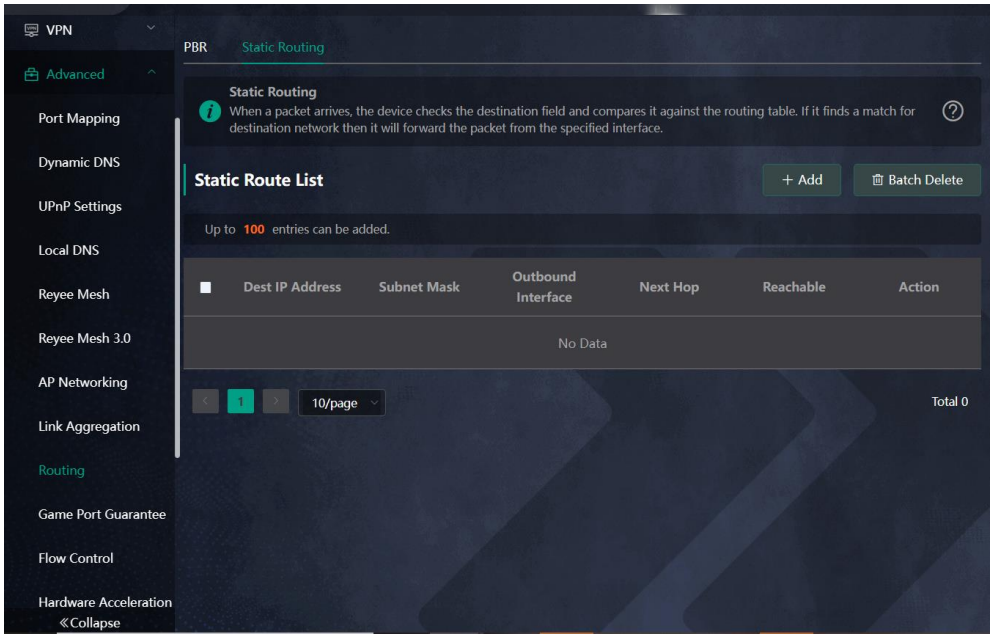
Smartphone View: Choose More > Switch to PC view > More > Advanced > Routing > Static Routing.

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.



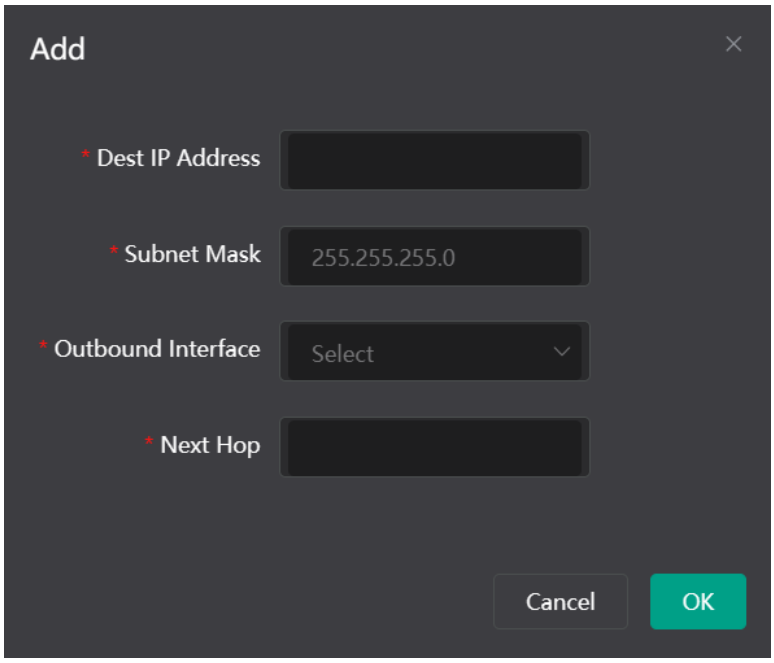
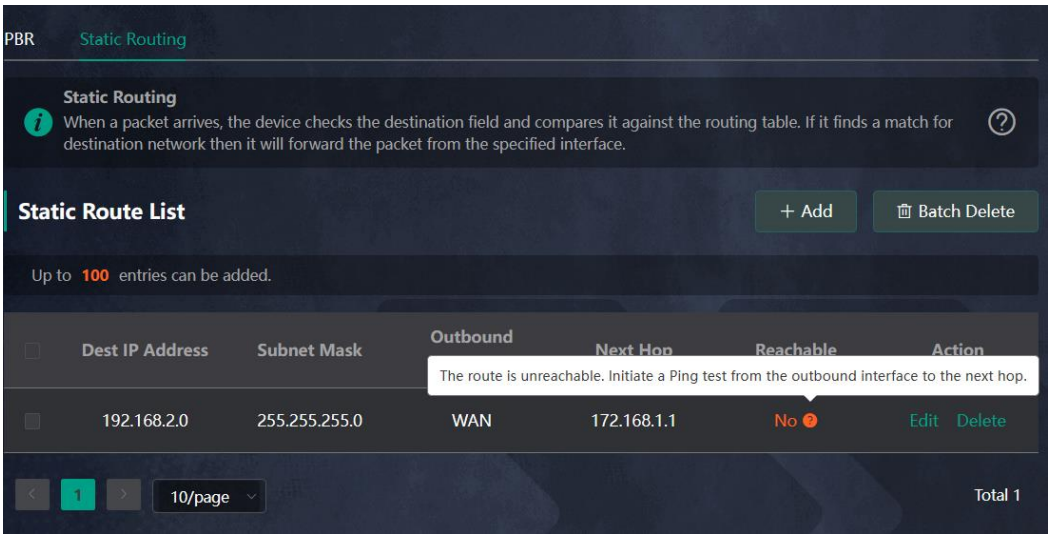


Table 5-1 Description of Static Routing Configuration

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.
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.



5.18 Policy-based Routing

Note

Only RG-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.

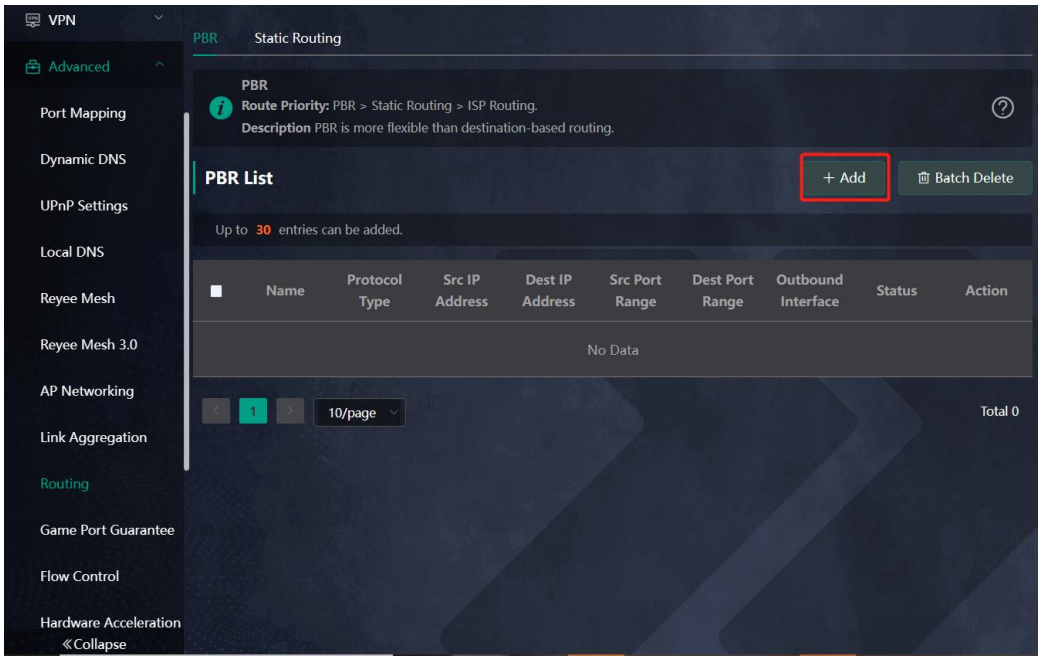
In the multi-line scenario, if a device is connected to both the Internet and the intranet through different lines, if no routing settings are made, traffic will be routed in a balanced way by default, and packets destined for the intranet may be mistakenly sent to the Internet, and vice versa, which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



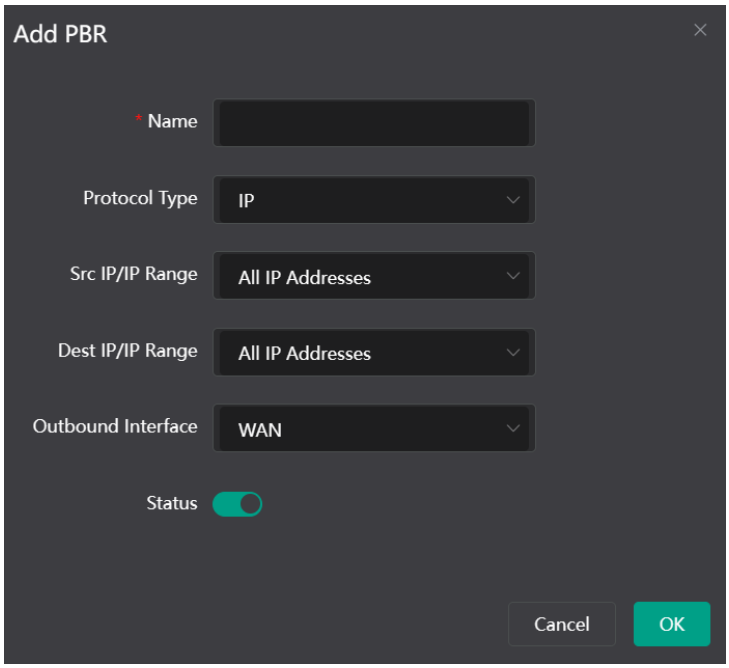


Table 5-2 Description of Policy-based Routing

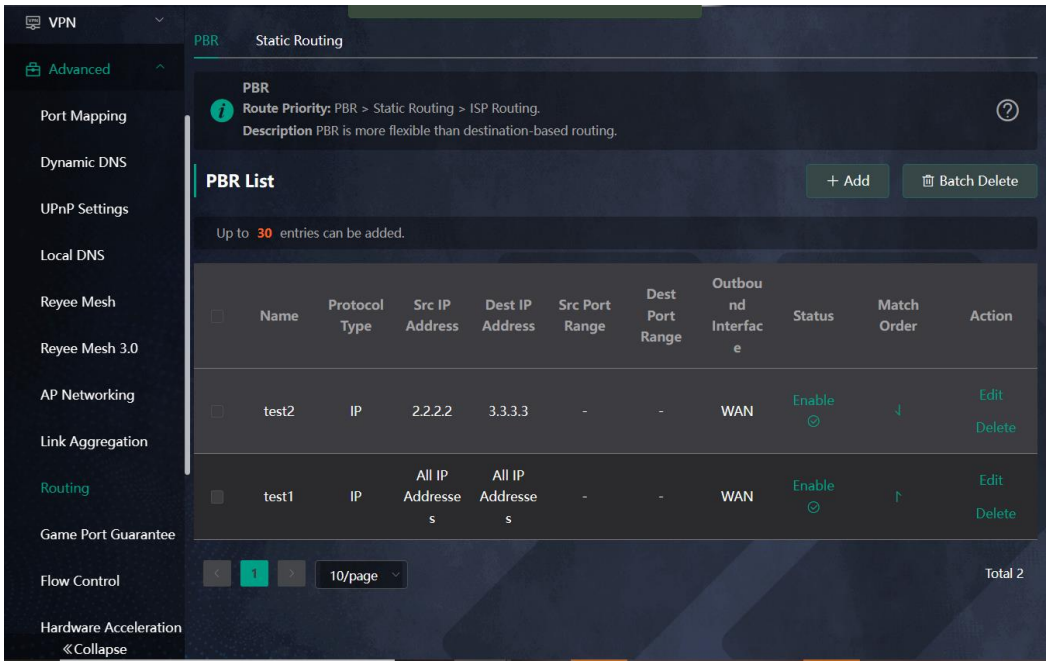
Parameter	Description
Name	The name of the PBR rule, as the identifier of the PBR route. The name must be unique.
Protocol Type	The protocol for the PBR route to take effect, which can be IP, ICMP, UDP, TCP, or a custom protocol type as needed.
Protocol Number	When the protocol type is Custom, the protocol number is required.

Parameter	Description
Src IP/IP Range	The source IP/IP range to which the PBR rule matches. By default, All IP is selected. ● All IP: Matches all source IP addresses. ● Custom: Matches source IP addresses in the specified range.
Custom Src IP	The source IP address or range is required when the matching source IP/IP range is Custom.
Dest IP/IP Range	The destination IP/IP range to which the PBR rule matches. By default, All IP is selected. ● All IP: Matches all destination IP addresses. ● Custom: Matches destination IP addresses in the specified range.
Custom Dest IP	The destination IP address or range is required when the matching destination IP/IP range is Custom.
Src Port Range	This field is displayed only when the protocol type is TCP or UDP. 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 TCP or UDP. 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 Status 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.



5.19 Connecting to IPTV

Internet Protocol Television (IPTV) is provided by ISPs.

5.19.1 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.

5.19.2 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**

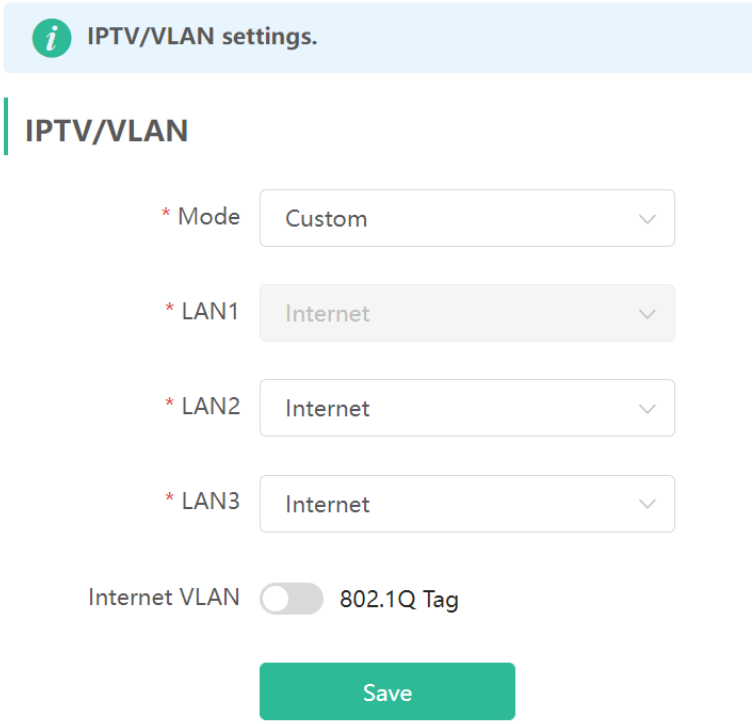
Select the local ISP mode, click the drop-down list of the target port, select **IPTV** from the drop-down list, and enter the VLAN ID provided by the ISP. For example, connect an IPTV set top box (STB) to LAN3 and set the VLAN ID to 2. The configuration is shown in the figure below.

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.

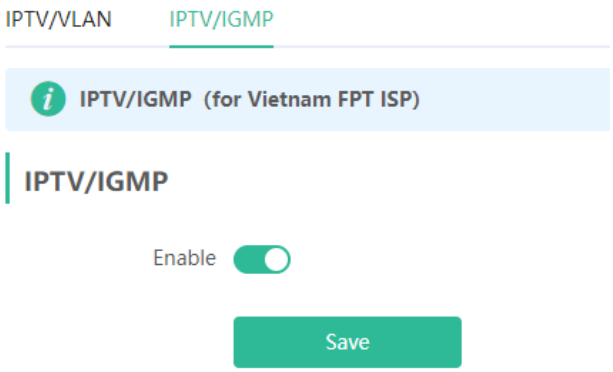


5.19.3 IPTV Configuration Steps (IGMP Type)

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.



Caution

The RG-EW1200 does not support the IGMP type.

5.20 Configuring Wi-Fi/IGMP

5.20.1 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.

5.20.2 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

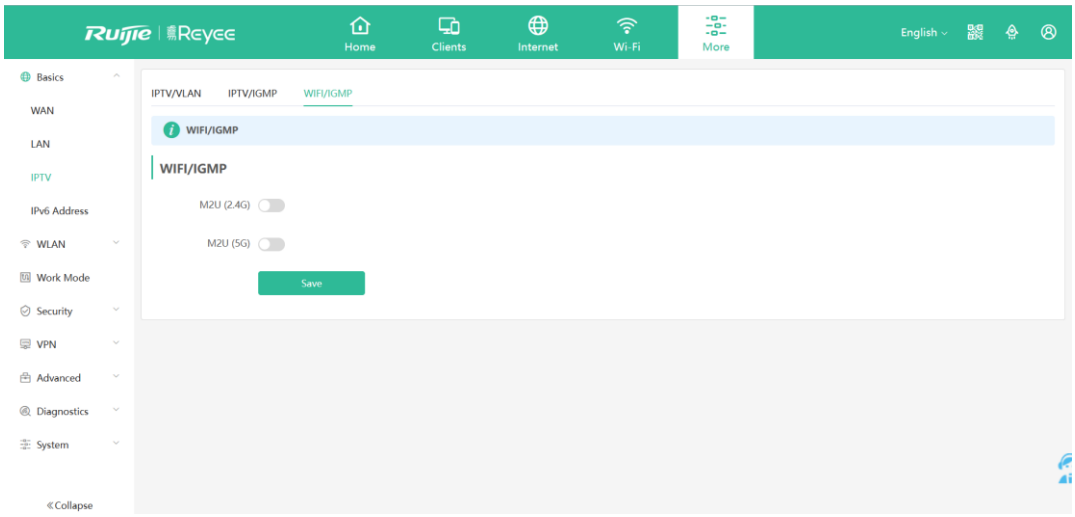
Select the method to configure RG-EW3000GX PRO:

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.



5.21 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

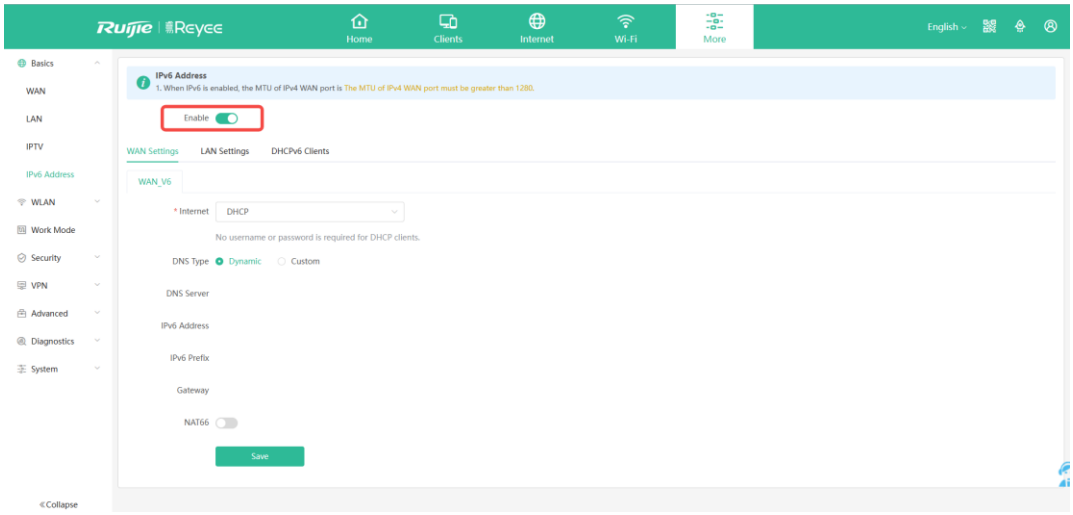
5.21.1 Configuring the IPv6 of the WAN Port

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.



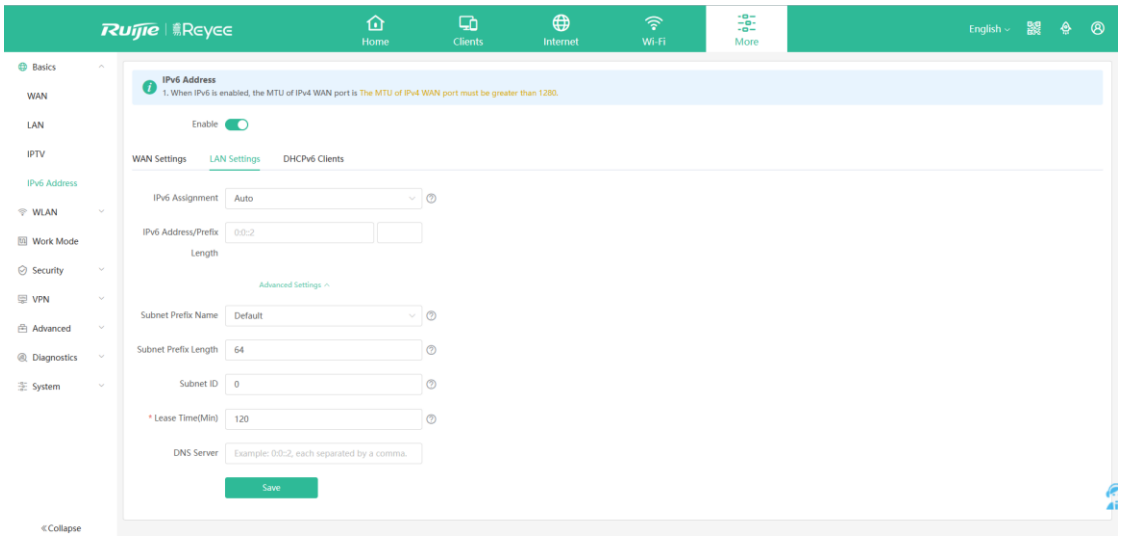
5.21.2 Configuring the IPv6 of the LAN Port

Click LAN Settings.

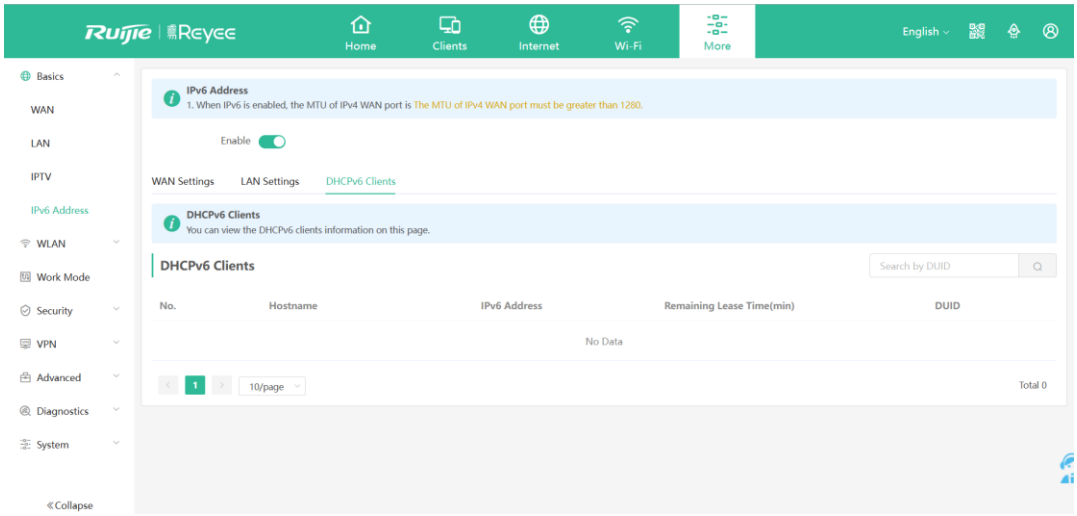
IPv6 Assignment: Choose **Auto** to use both DHCPv6 mode and SLAAC mode to allocate address. Choose **Null** to assign no address. You are advised to choose **Auto**.

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.



5.22 Enabling Smart Flow Control

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

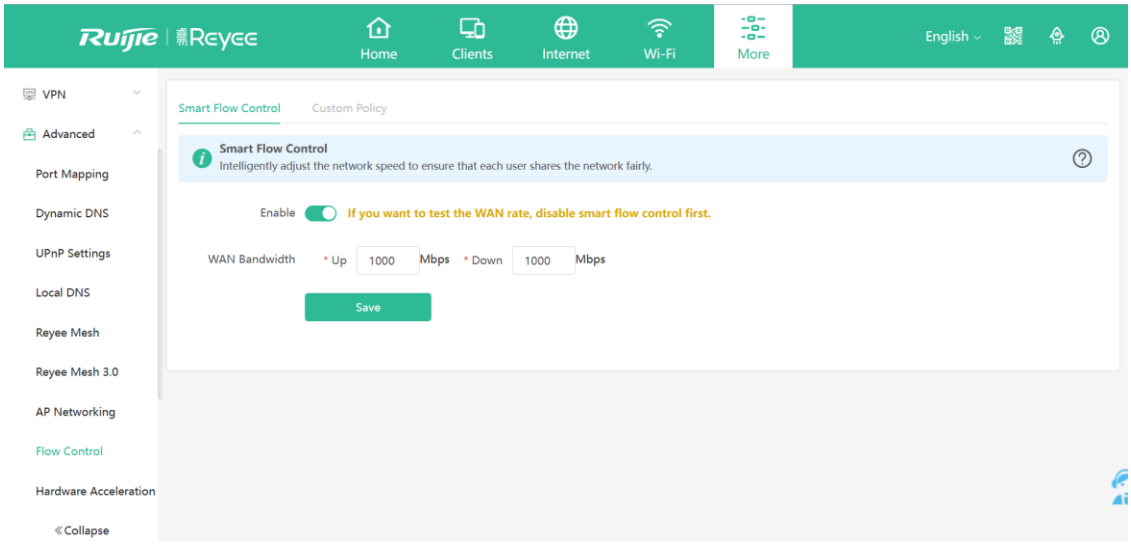
PC View: Choose More > Advanced > Flow Control > Smart Flow Control.

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.

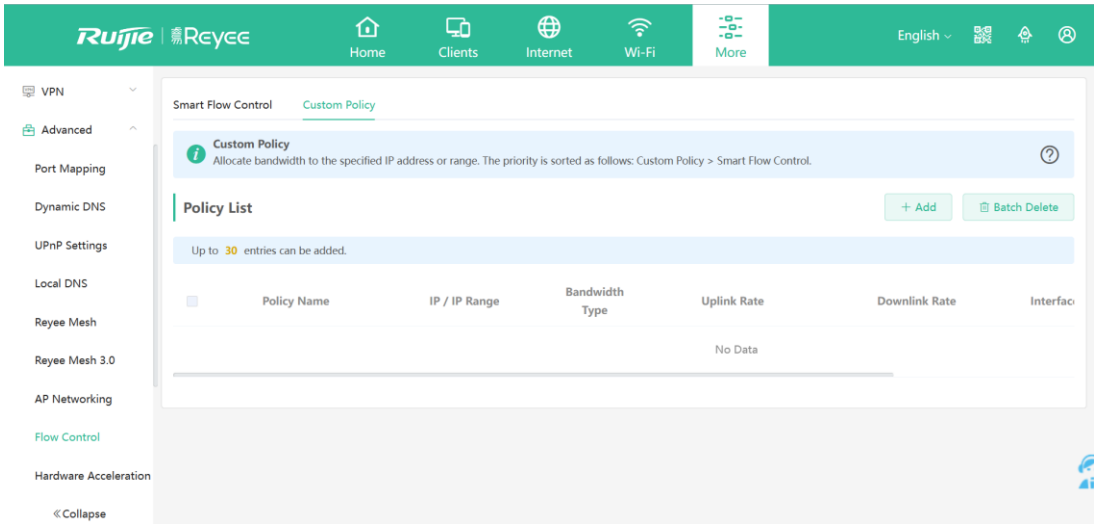
Caution

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.



5.23 Configuring Firewall

Caution

This feature is supported in router mode.

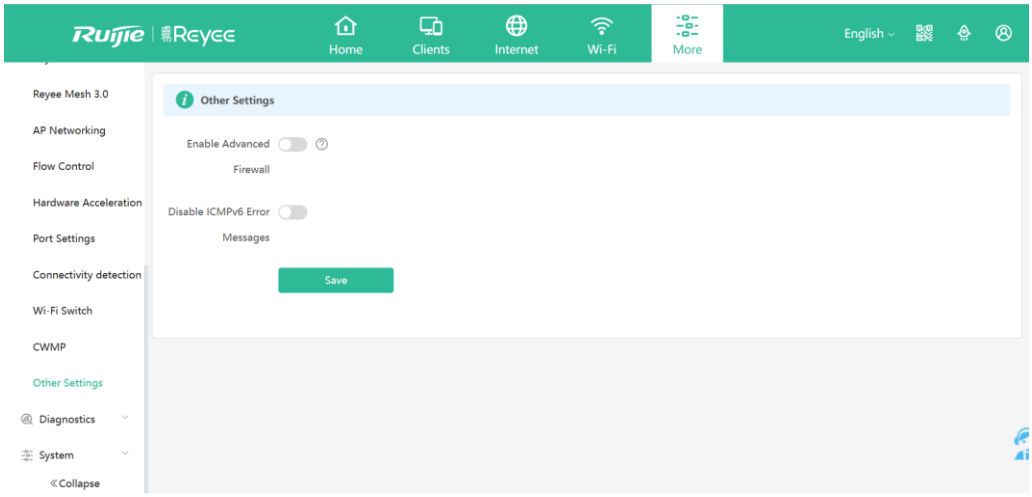
Smartphone View: Choose More > Switch to PC view > More > Advanced > Other Settings.

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.



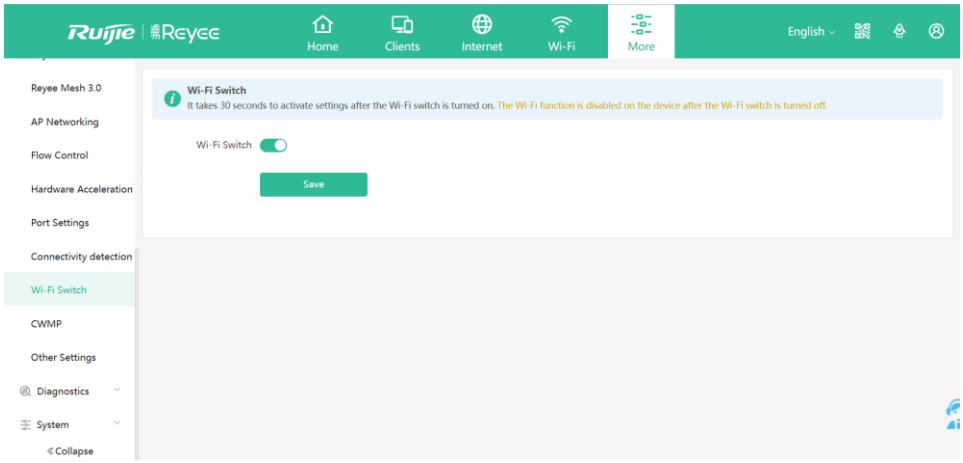
5.24 Enabling Wi-Fi Switch

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.



5.25 Configuring UPnP

5.25.1 Overview

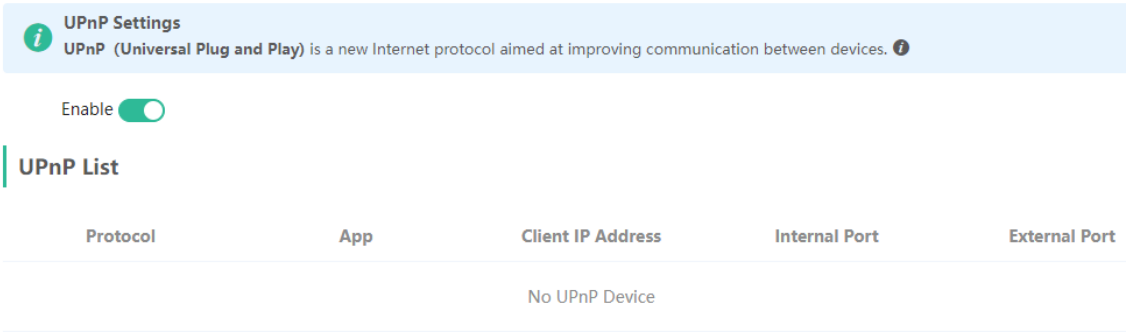
The Universal Plug and Play (UPnP) function can map the port used by a client for Internet access according to the client's request so that related applications run more fast or stably. Common applications that support UPnP include MSN Messenger, Xunlei, BT, and PPLive.

5.25.2 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.



5.26 Configuring PPTP VPN

Caution

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

5.26.1 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.

5.26.2 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**.

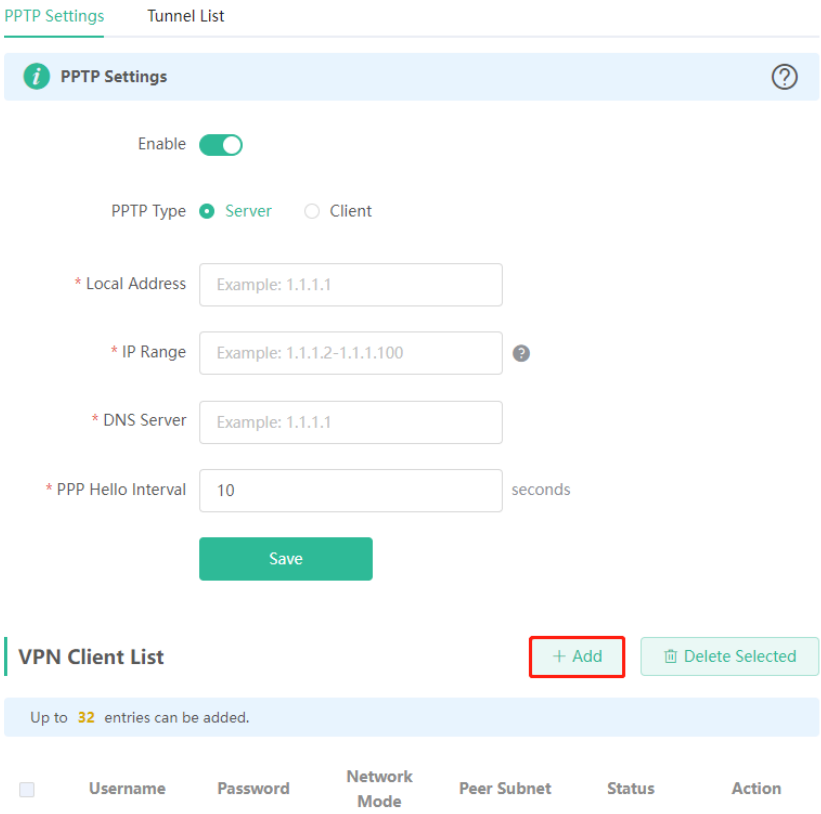
Local Address: Enter the local address. It is used as the local virtual IP address of the VPN tunnel for the client to access the server after dial-up.

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.

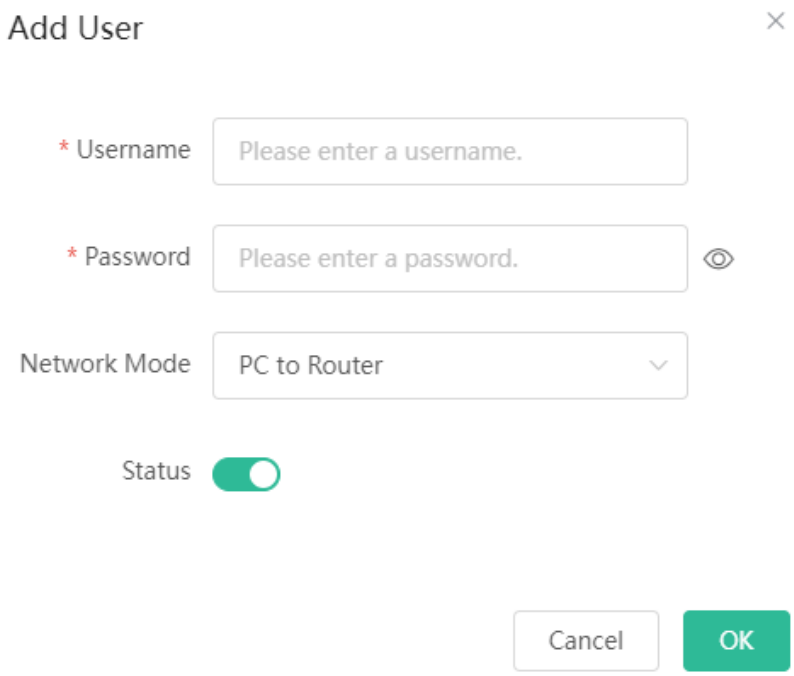


(2) Add a PPTP user.

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**.



5.26.3 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.

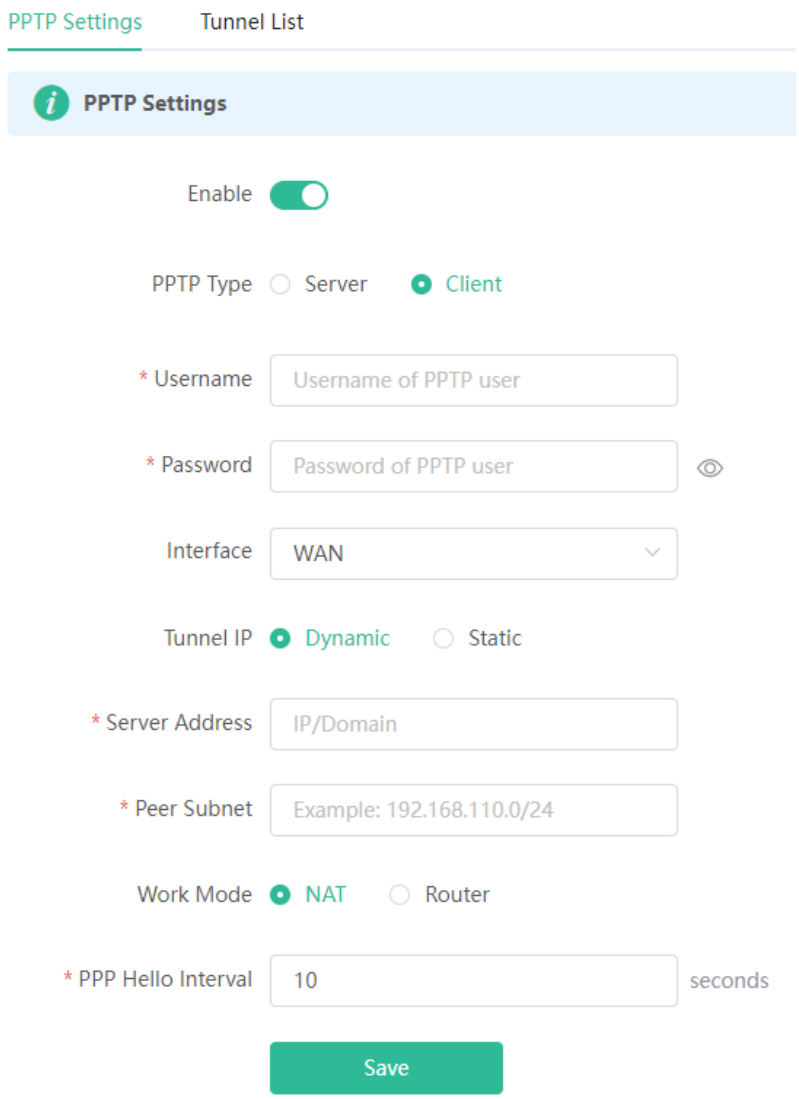
Server Address: Enter the WAN port's IP address (public IP address is required) or domain name of the server.

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.



5.27 Configuring OpenVPN

5.27.1 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.

5.27.2 Configuring OpenVPN (Server Mode)

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

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

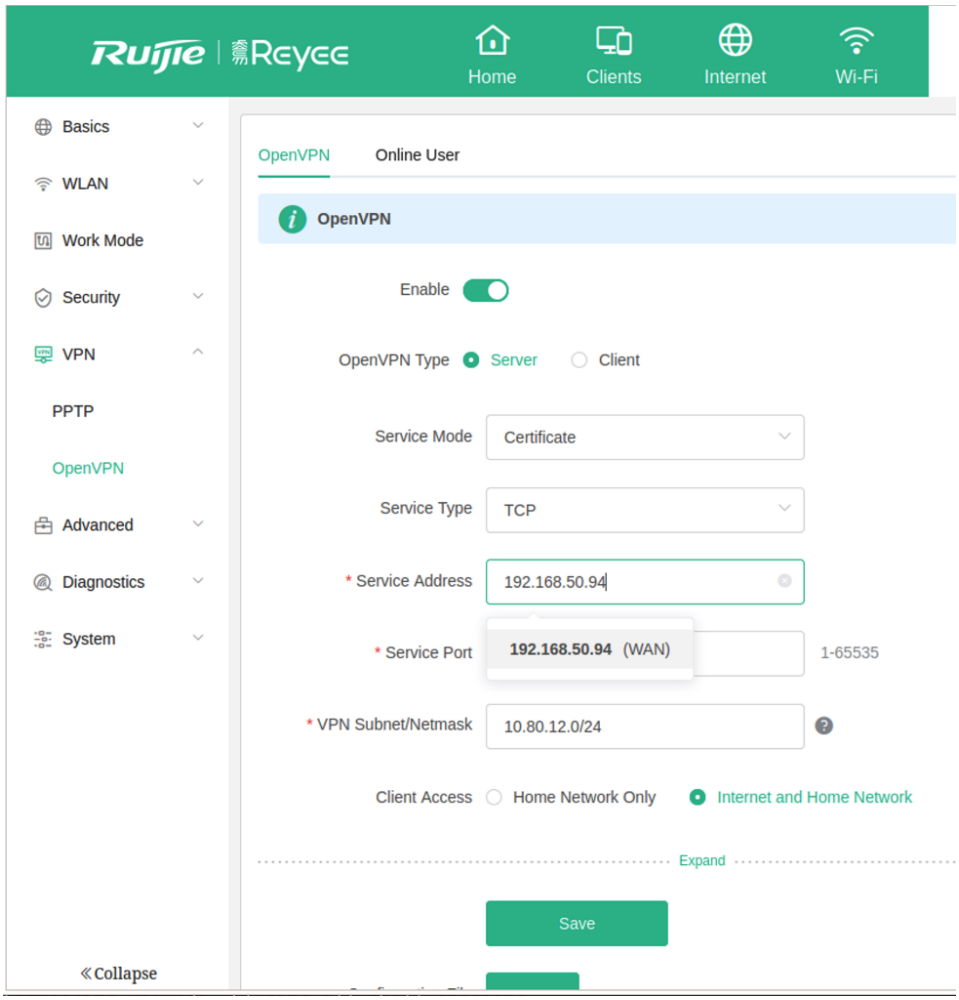
1. Configuring OpenVPN

(1) Click **Enable** to enable the OpenVPN feature.

(2) Select Server for the OpenVPN Type.

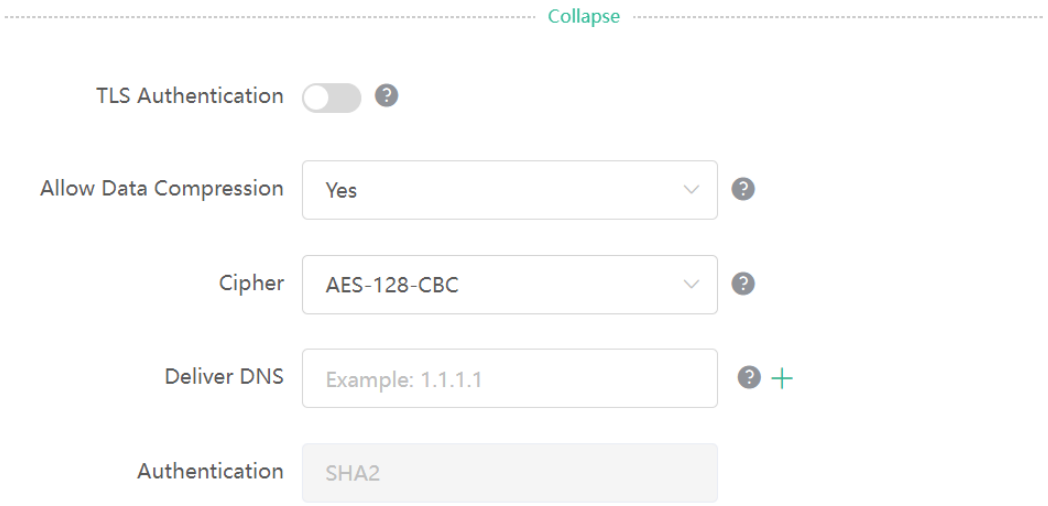
(3) Select the protocol, and enter the server address, port number and other information.

Figure 5-5 Configuring OpenVPN Server



(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.



(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

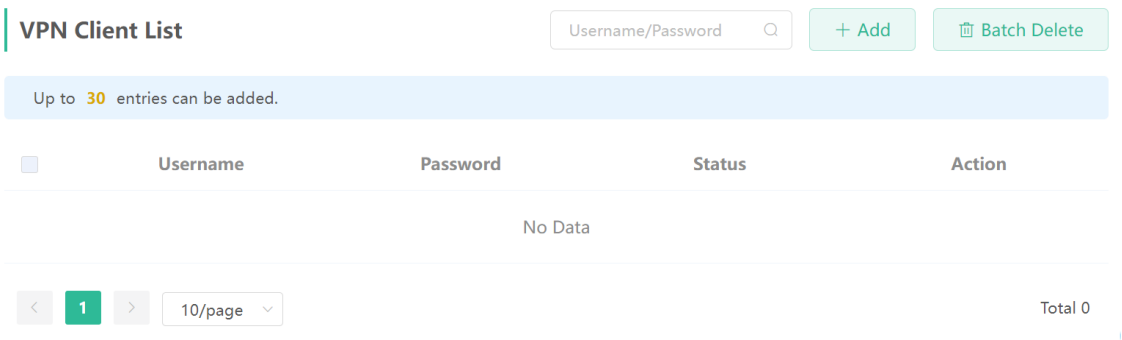
Item	Description
Server Mode	The device supports Account, Certificate and Account & Certificate authentication modes: ● Account mode: The correct account name, password, and CA certificate are required to connect to the server. The configuration is simple. ● Certificate mode: The client needs the correct CA certificate, client certificate, and pre-shared key to connect to the server. ● Account & 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.
Service Type	All communication on OpenVPN is based on a single IP port, using UDP or TCP protocols. 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.
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	The IP address pool delivered to VPN clients, in the form of a network segment. 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.
Client will access	You can choose Home Network Only or Internet and Home Network

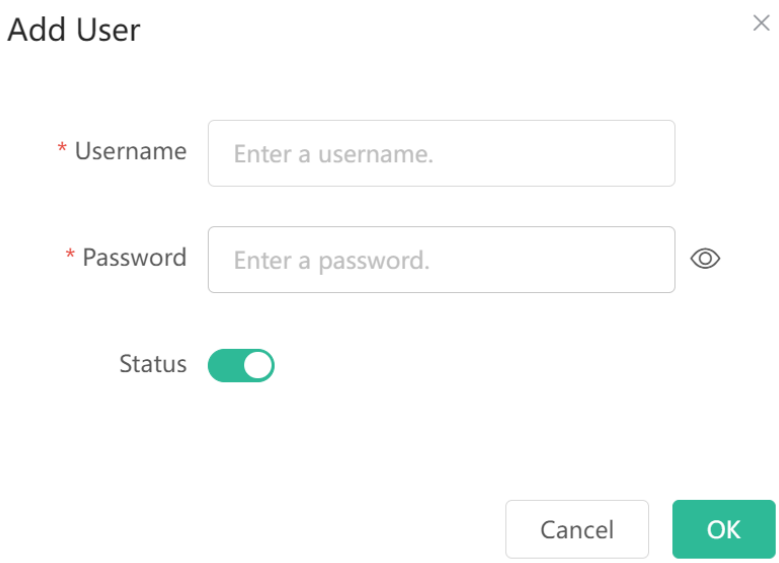
Item	Description
	● **Home Network Only**: The client can only access the LAN segment on the server. ● **Internet and Home Network**: The client can access the LAN and WAN segments on the server. In this mode, all traffic from the client will be forwarded to the server.
TLS Authentication	TLS Authentication 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.





5.27.3 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.

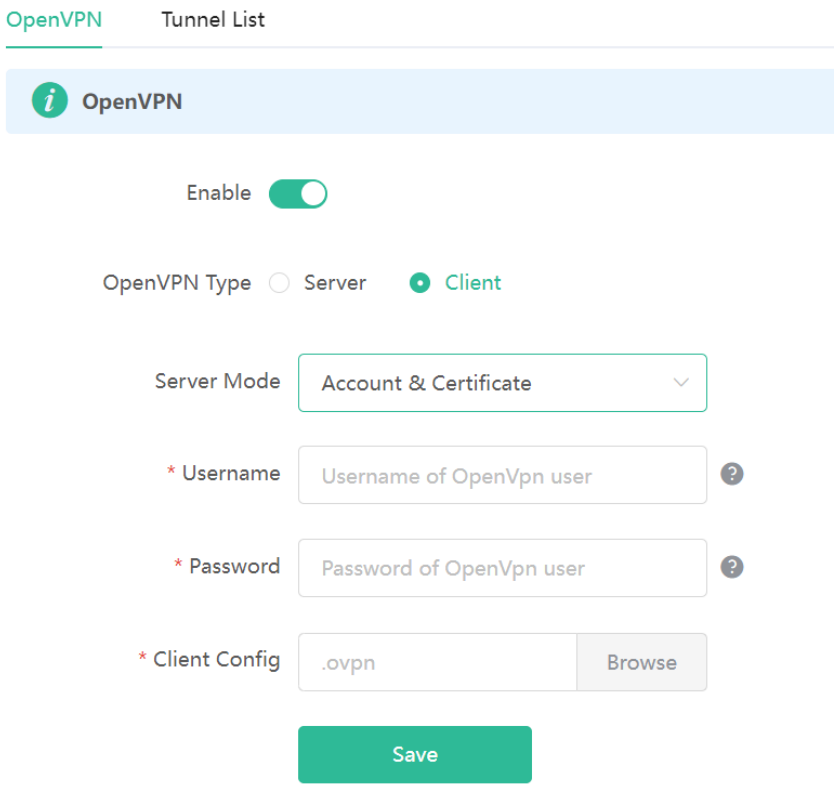


Table 5-4 Configuration Items of OpenVPN Client Web Setting Configuration Mode

Parameter	Description
Server Mode	The device supports Account, Certificate and Account & Certificate authentication modes: ● Account mode: The correct account, password, and CA certificate is required to connect to the server. The configuration is simple. ● Certificate mode: The client needs the correct CA certificate, client certificate, and pre-shared key to connect to the server. ● Account & 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.
Username and password	Enter the usersname and password configured on the server. This parameter can be left blank if the **Server Mode** is **Certificate**.
Client Config	Click **Browse** and select the client configuration file with the suffix .ovpn.

5.27.4 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)

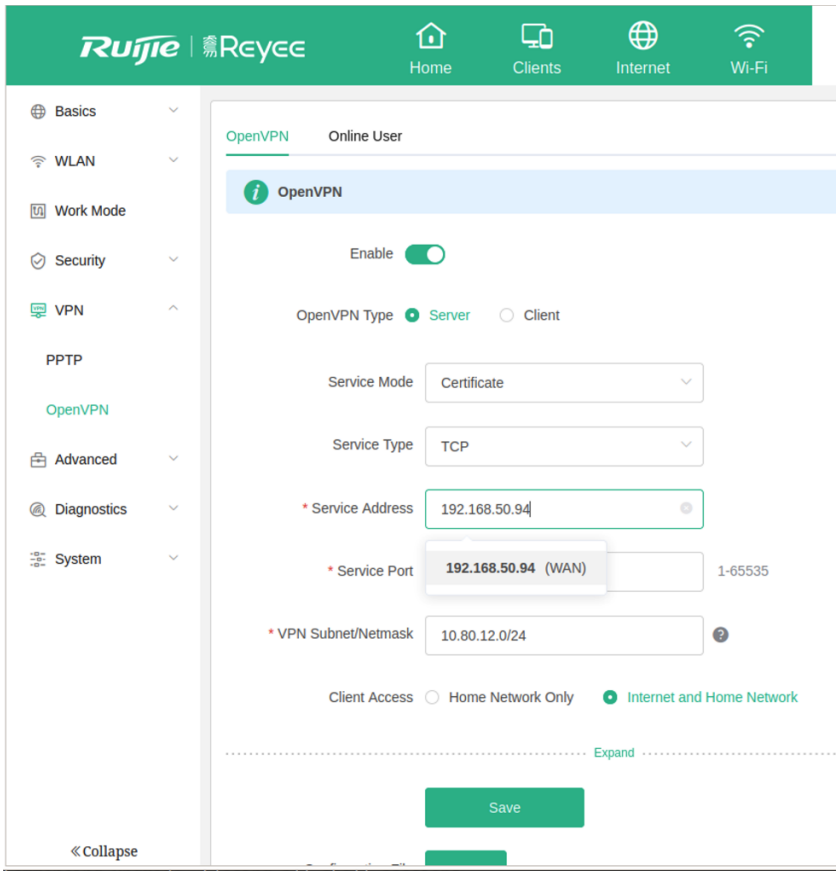
(1) Log in to the Eweb management system of the device, and choose **VPN** > **OpenVPN**. Then, flip on the toggle switch next to **Enable** to enable the OpenVPN function. On the page that is displayed, enter the IP address of the WAN port as the service address, as well as other required parameters.

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.

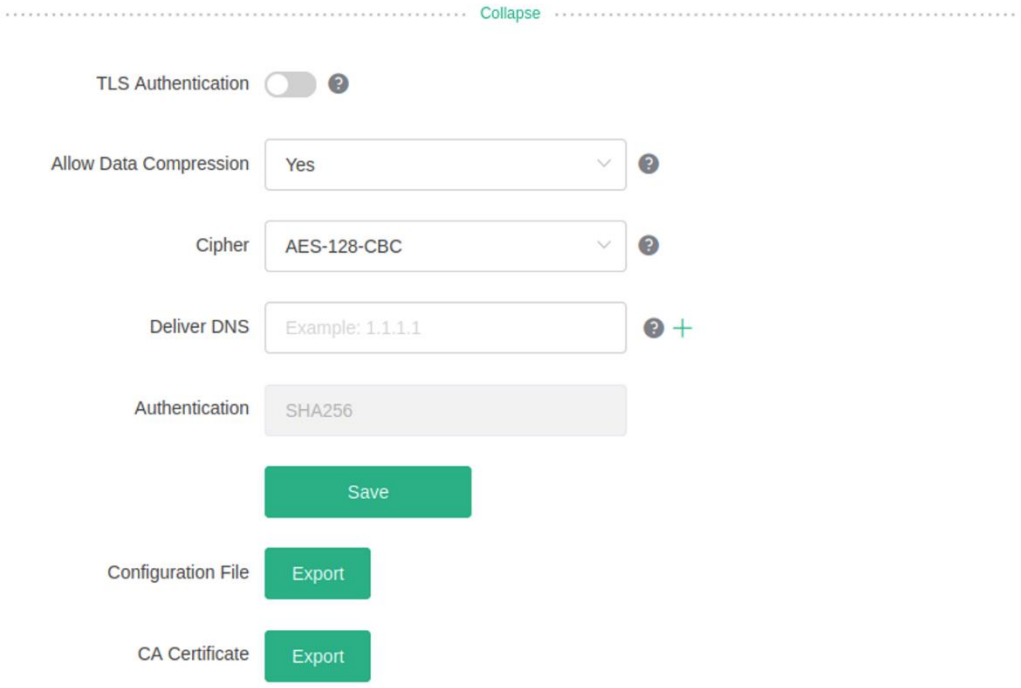


(2) Click **Save**. The OpenVPN settings are saved.

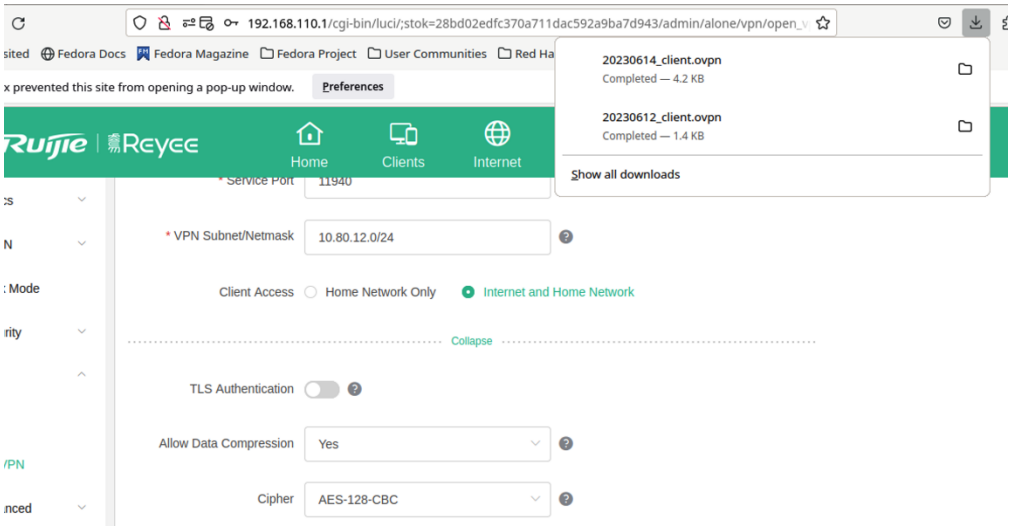
(3) The following table describes the OpenVPN server configuration.

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 **TCP**.
Service Address	The IP address of the WAN port is automatically populated.
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 **10.80.12.0/24**, 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.

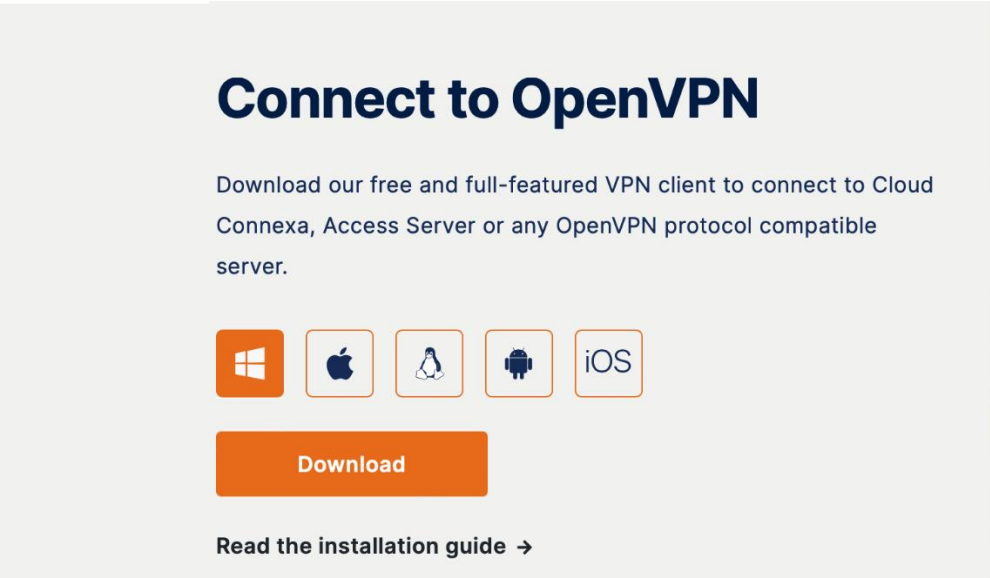


(5) Click **Export** next to **Configuration File** to export the .ovpn file which can be imported on the client side. Unless there are specific requirements, you do not need to export the CA certificate.

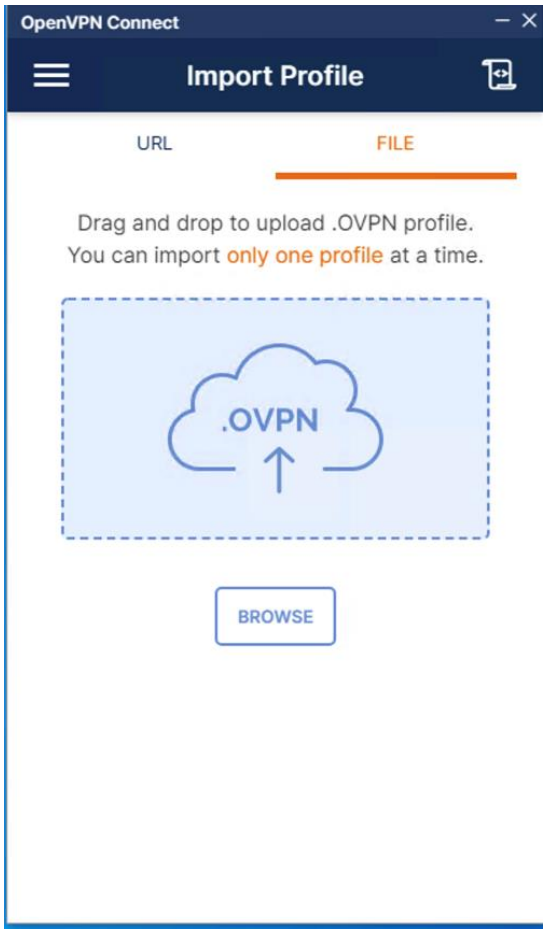


5. Configuring OpenVPN Client (Use Windows Client as an Example)

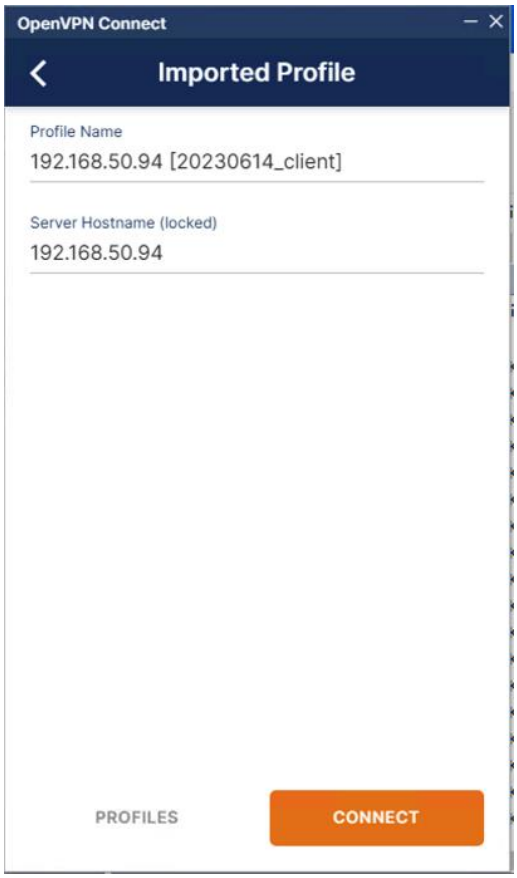
(1) Download the OpenVPN client (https://openvpn.net).



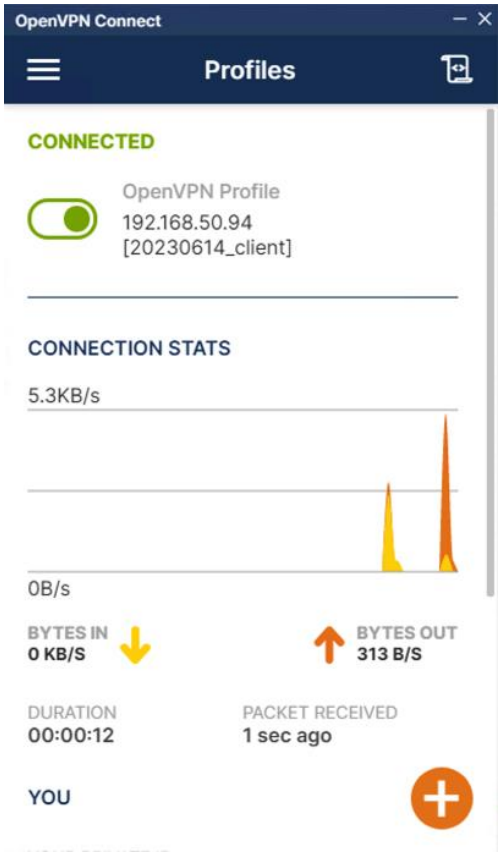
(2) Open the Windows OpenVPN client and choose the **File** tab.



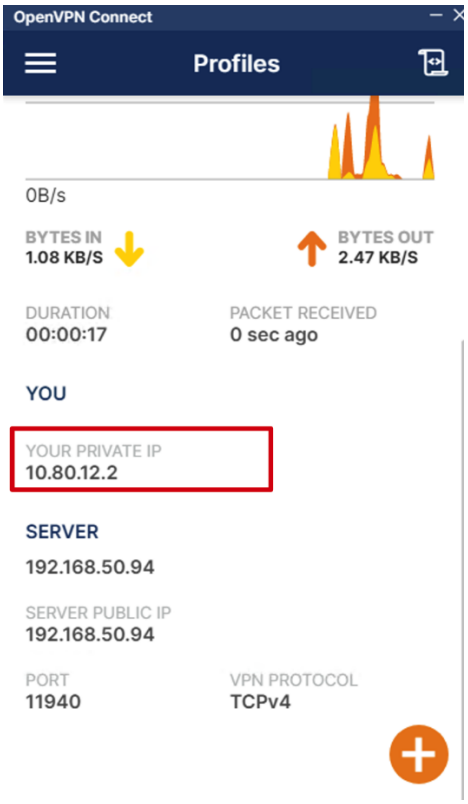
(3) Click **BROWSE** and select the .ovpn file exported from the server side.



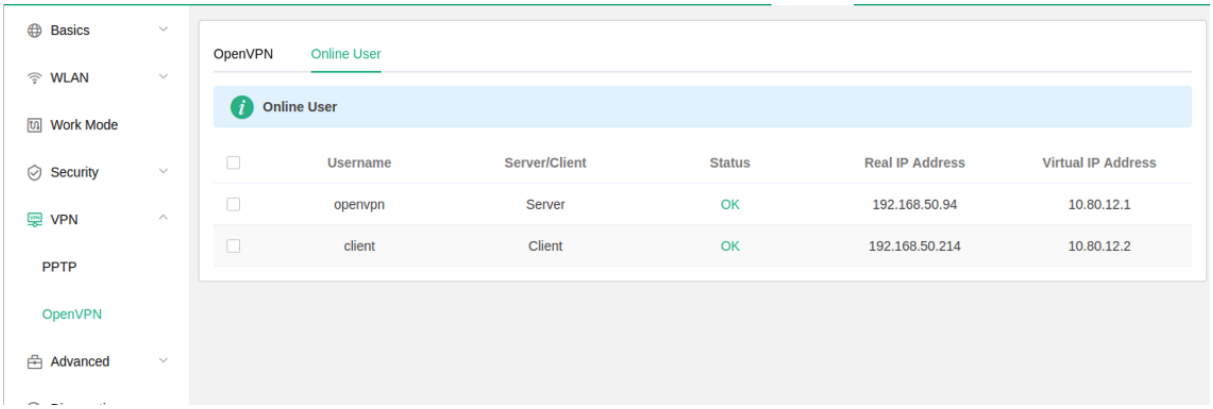
(4) Click **CONNECT** to connect to the OpenVPN server.



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.



5.28 Configuring Connectivity Detection

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

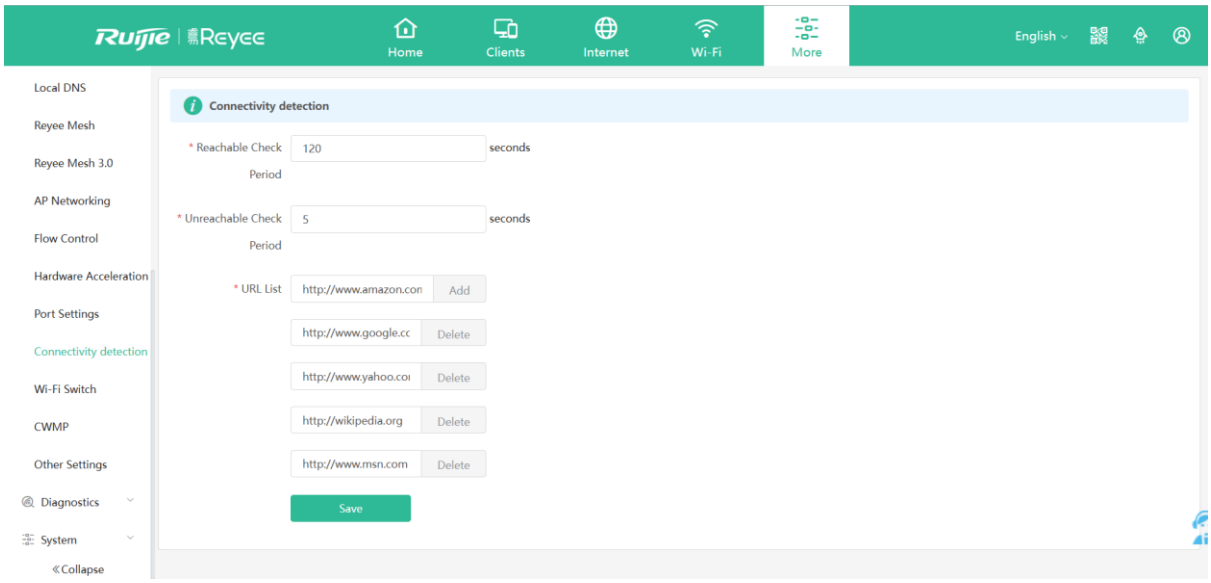
PC View: Choose **More** > **Advanced** > **Connectivity detection**.

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.



5.29 Enabling CWMP

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

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

5.29.1 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.

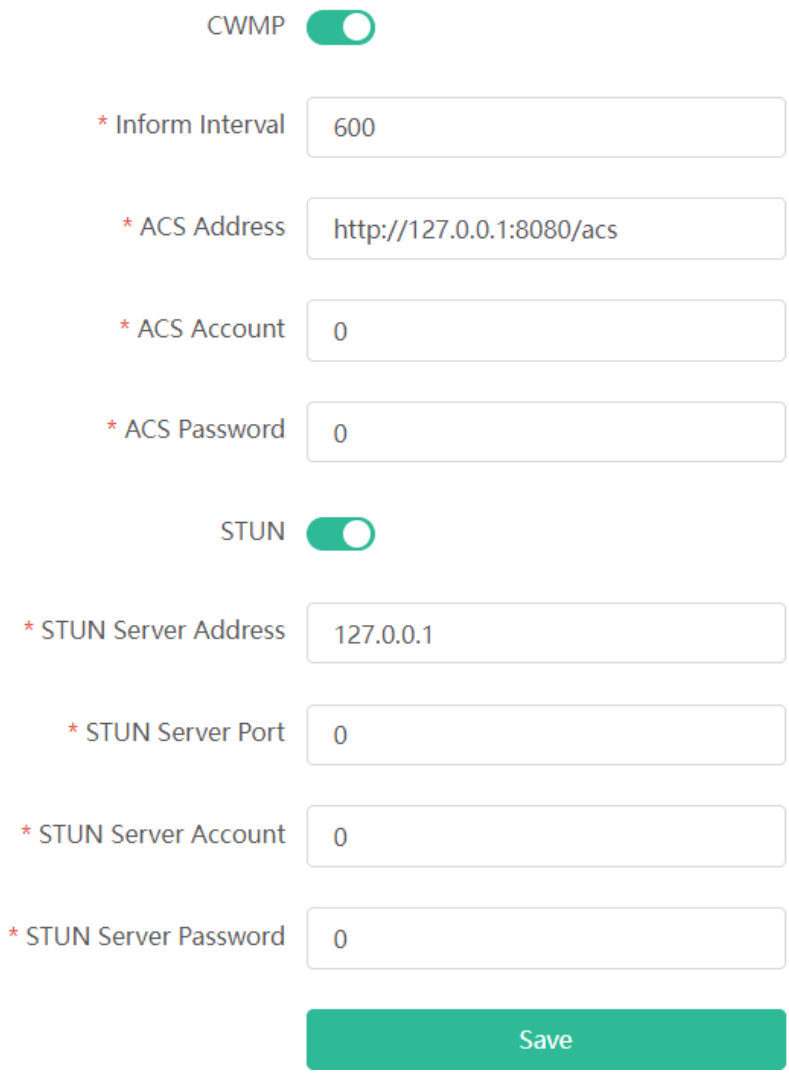
CWMP uses ACS and CPE models to manage devices. With CWMP, CPE can perform mandatory initialization and O&M actions such as service activation, function settings, file upload and download, and system detection.

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.

5.29.2 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.

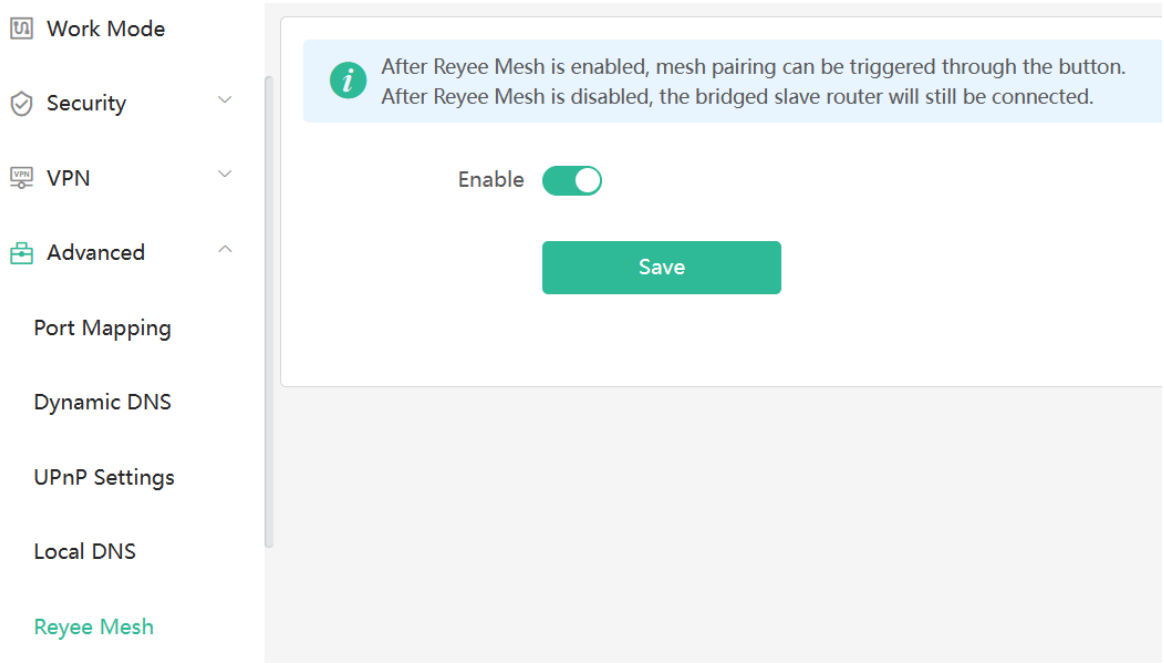


5.30 Enabling Reyee Mesh

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.



Note

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

5.31 Enabling Hardware Acceleration

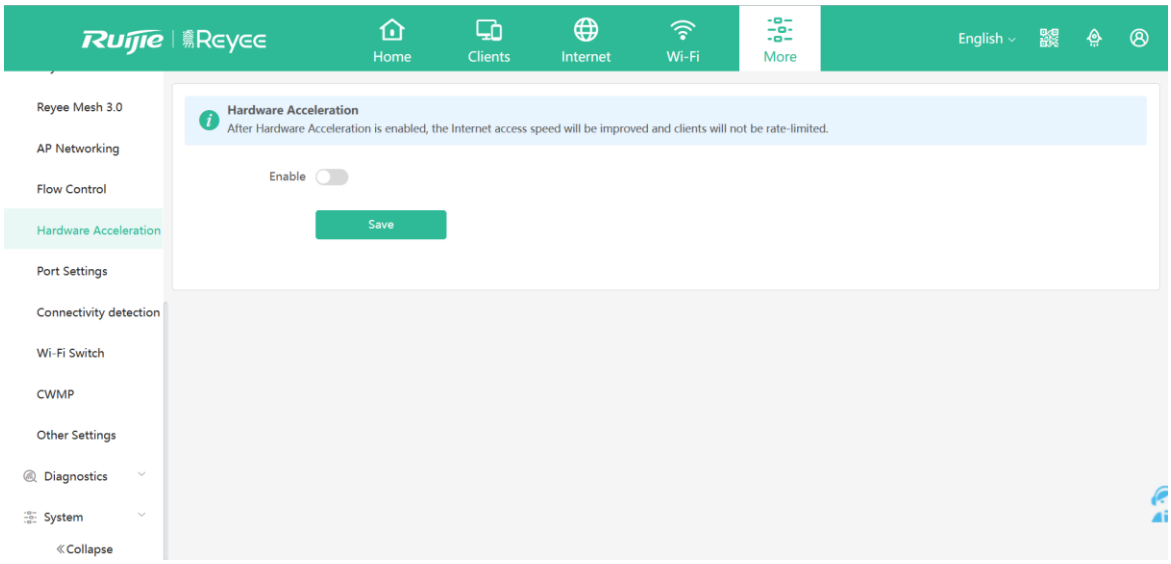
Caution

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.

5.32 Configuring Console Booster

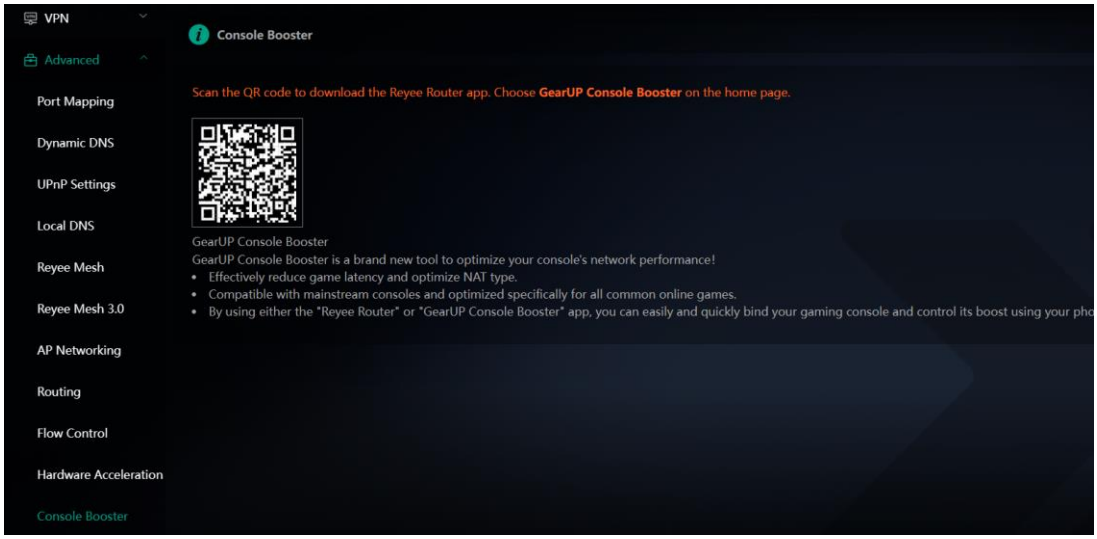
Note

Only RG-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.

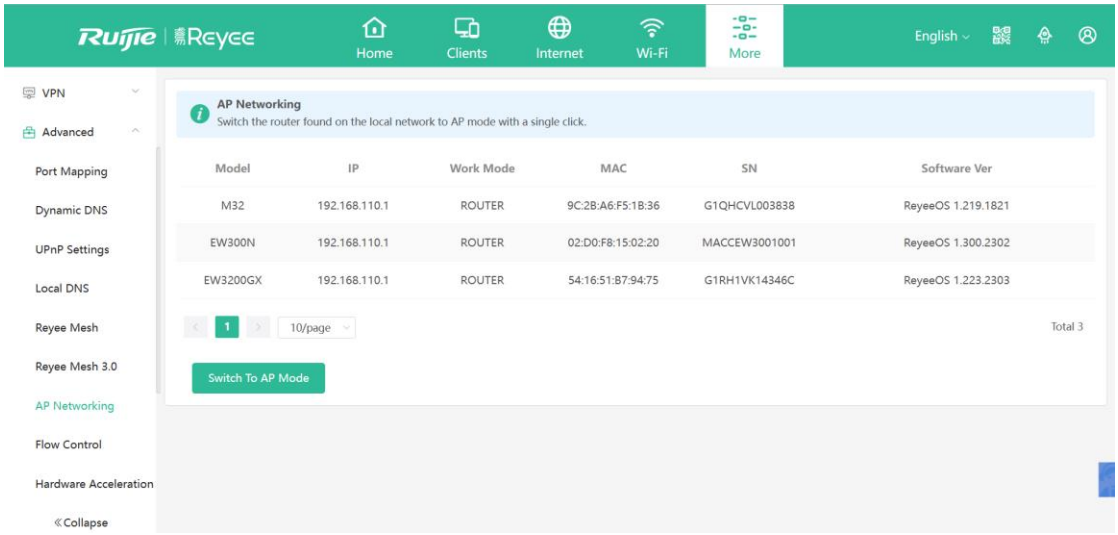


5.33 Configuring AP Networking

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.



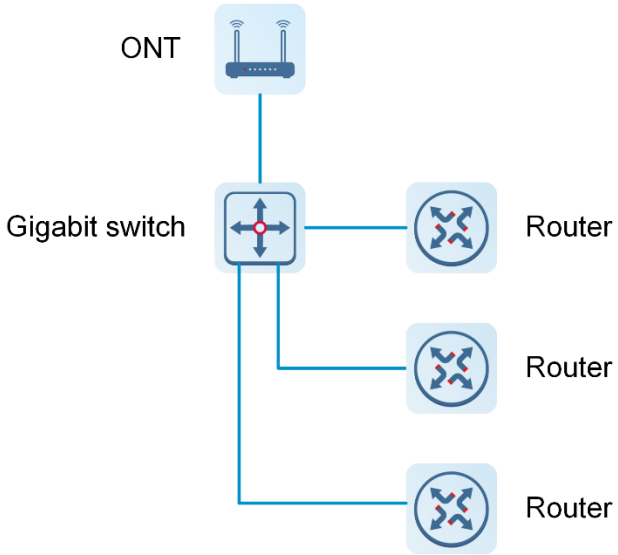
5.34 Configuring Reyee Mesh 3.0

5.34.1 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**

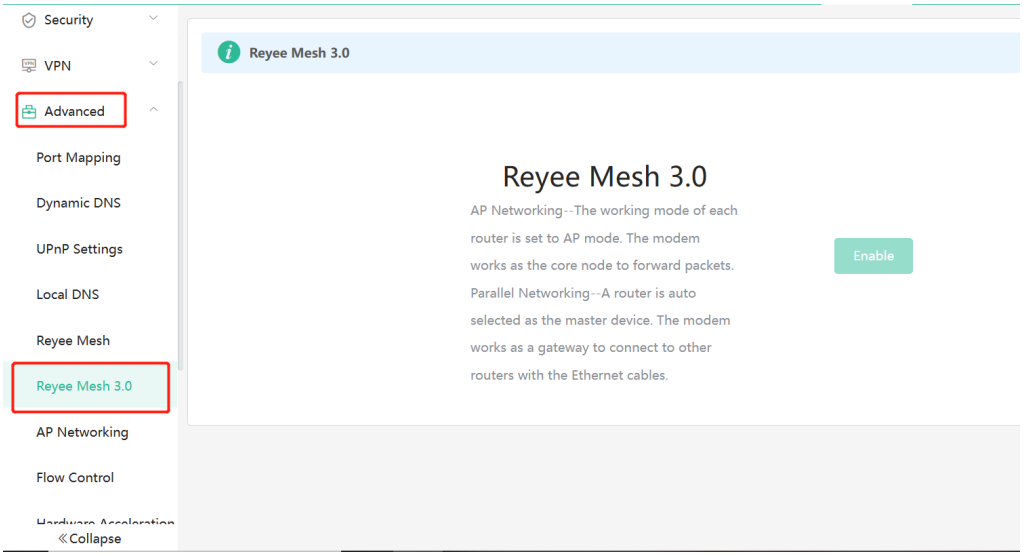
Connect the routers as indicated in the following figure:



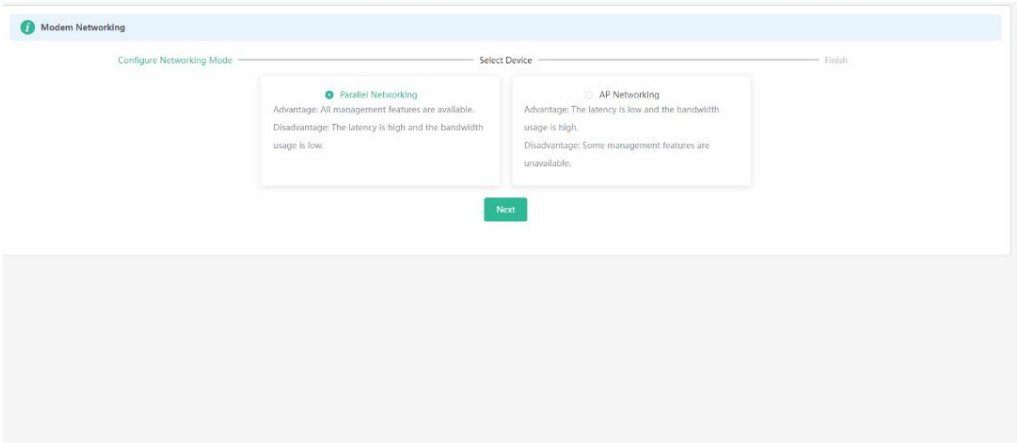
1. Parallel Networking

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.

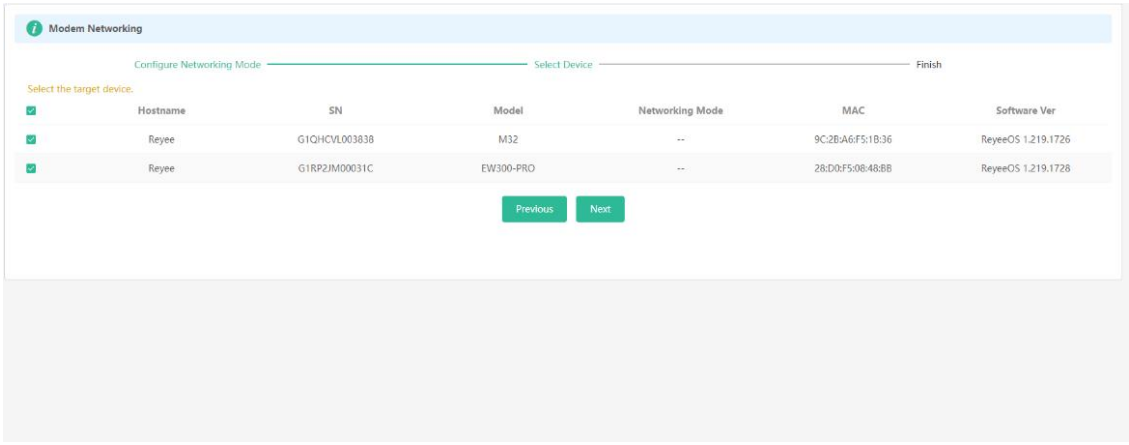
(1) Click **Enable** to enable Reyee Mesh 3.0.



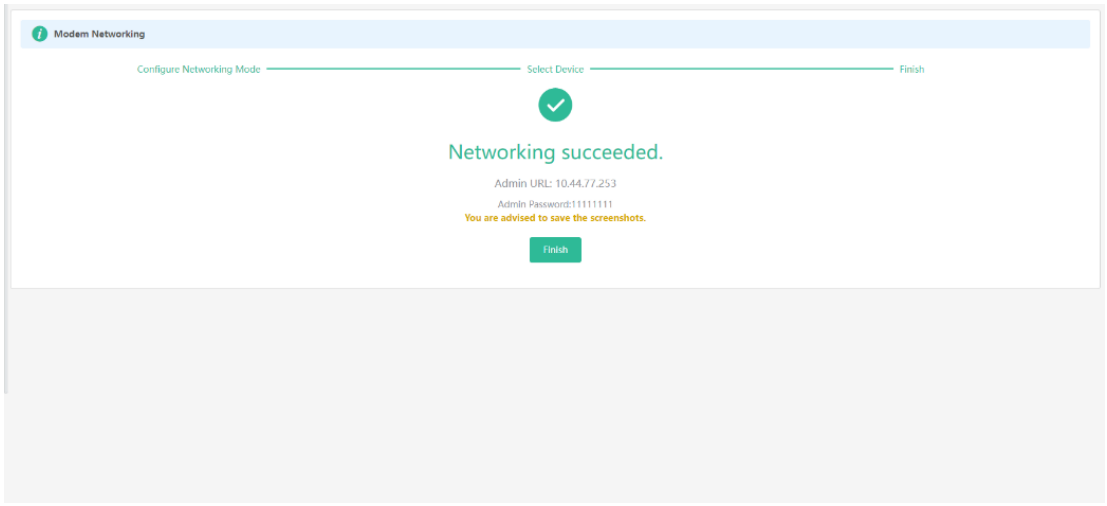
(2) Choose **Parallel Networking**, and click **Next**.



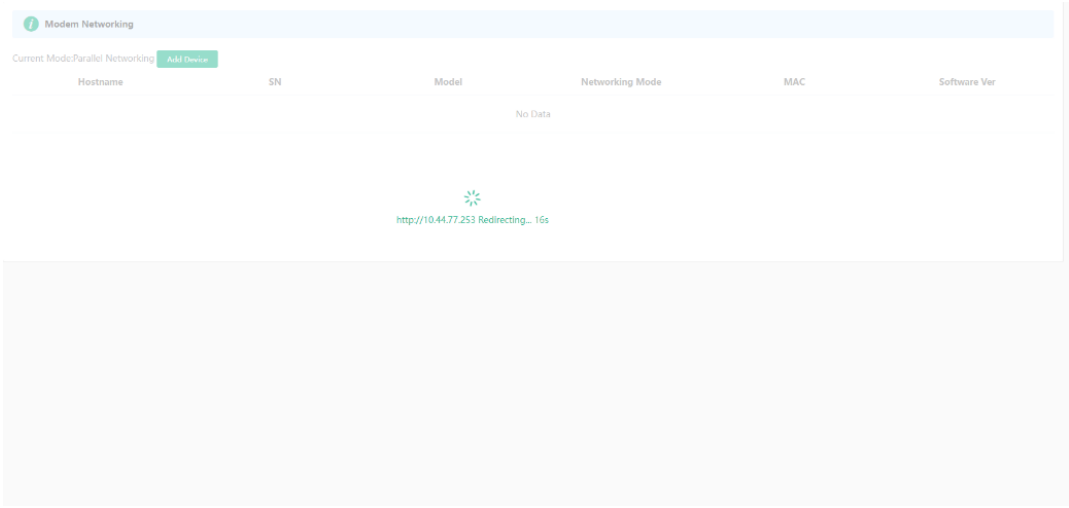
(3) Check routers for the networking.



(4) Click **Next**.



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

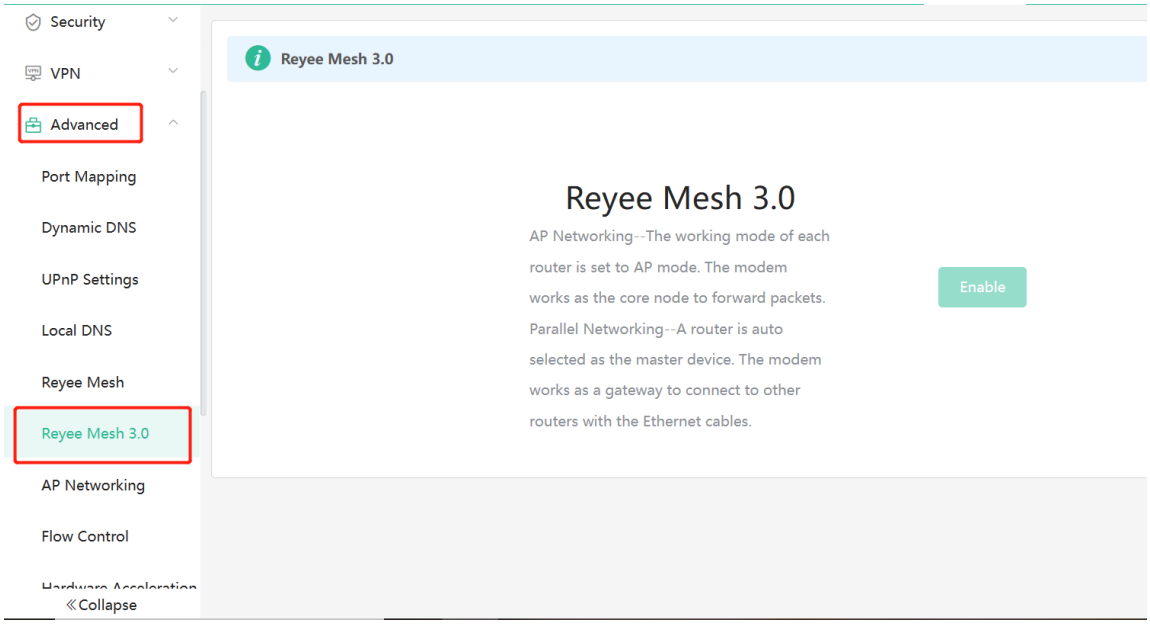


(6) On the master router page that is displayed, enter the password to log in.

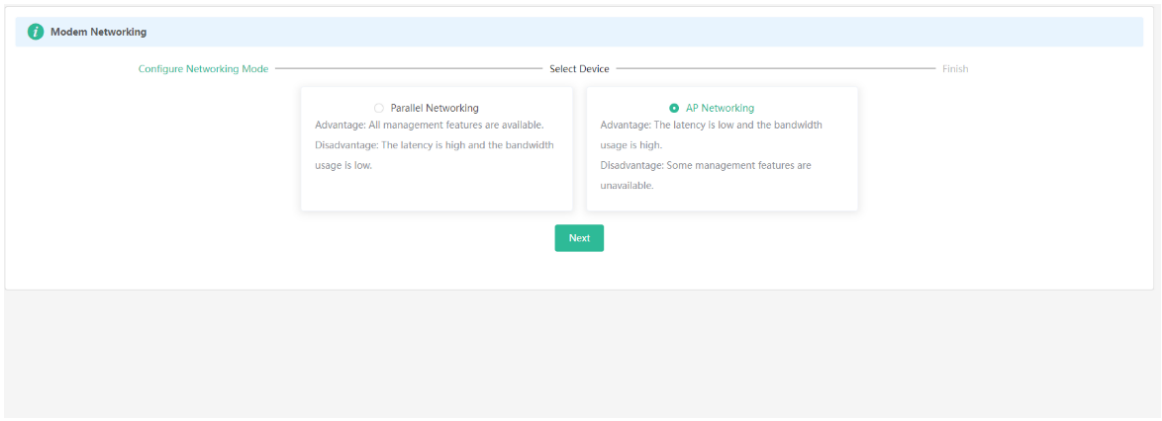
2. AP Networking

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.

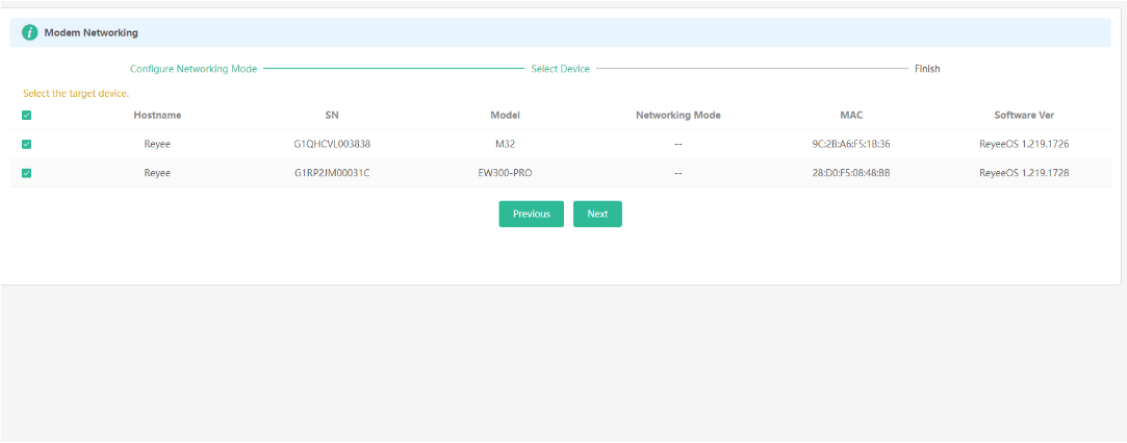
(1) Click **Enable** to enable Reyee Mesh 3.0.



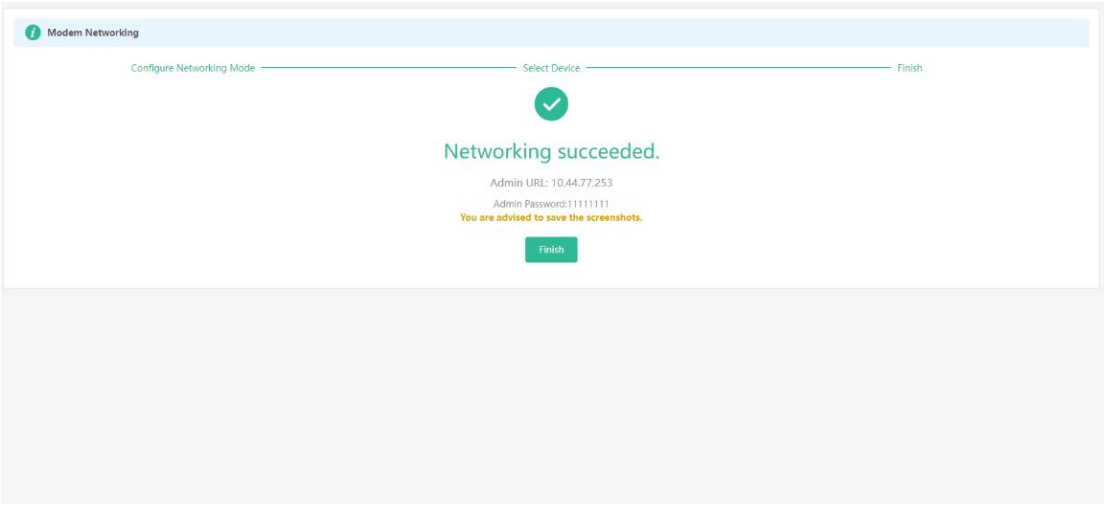
(2) Choose **AP networking**, and click **Next**.



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



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



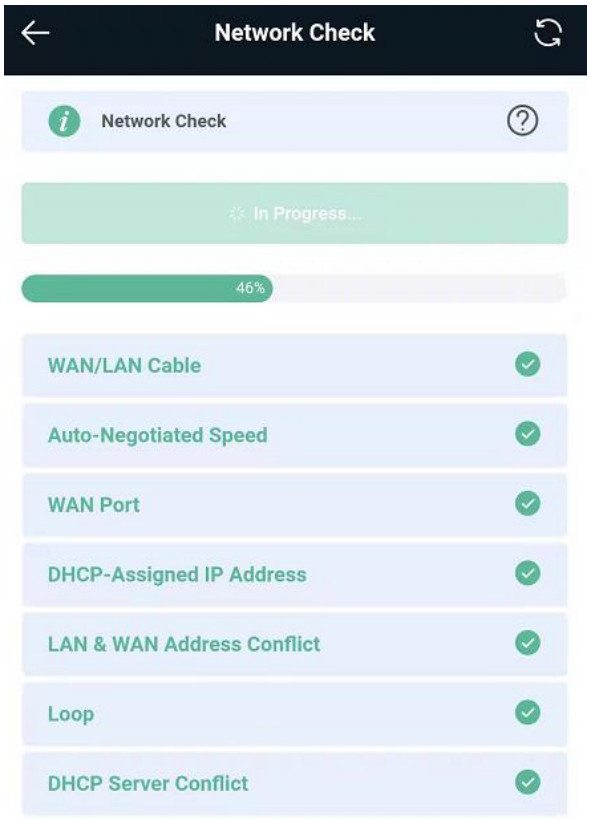
(5) On the master router page that is displayed, enter the password to log in.

5.35 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.


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

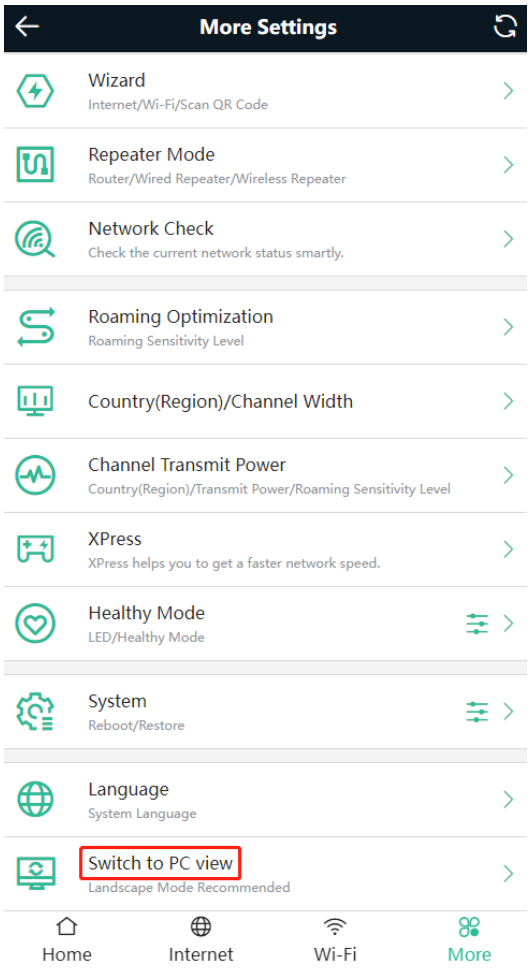
6 Reyee System Settings

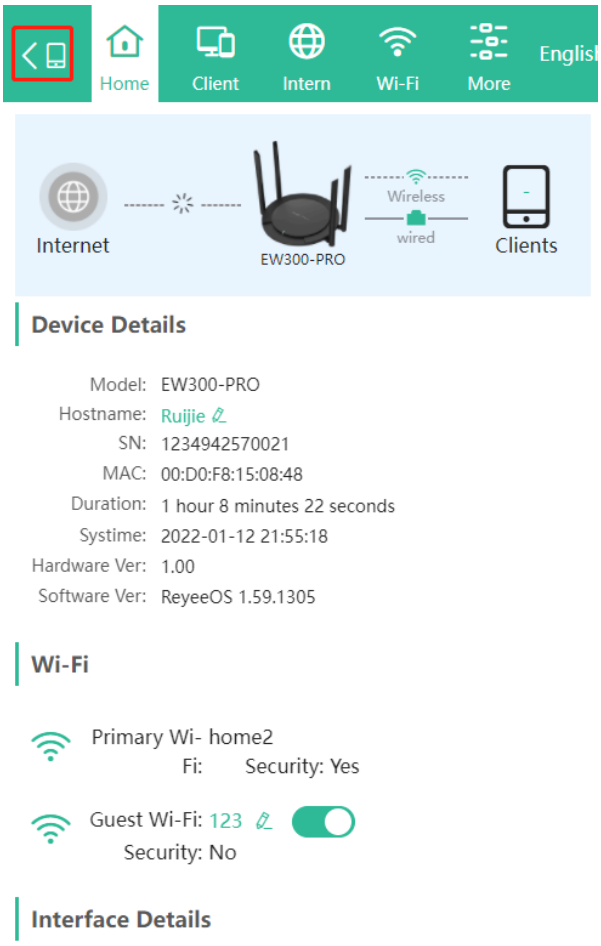
6.1 Switching to the PC View

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.



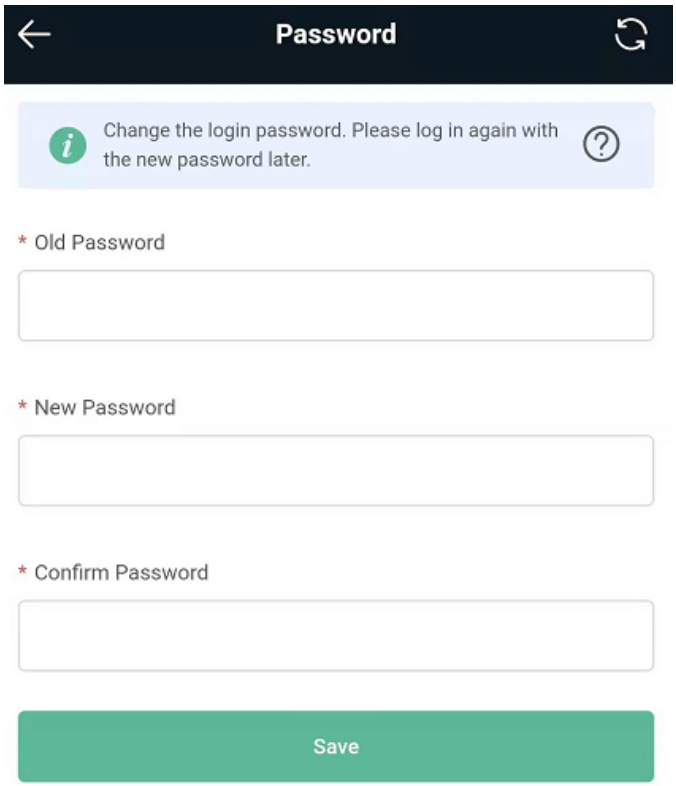


6.2 Configuring the Login Password

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.



6.3 Remote Access

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

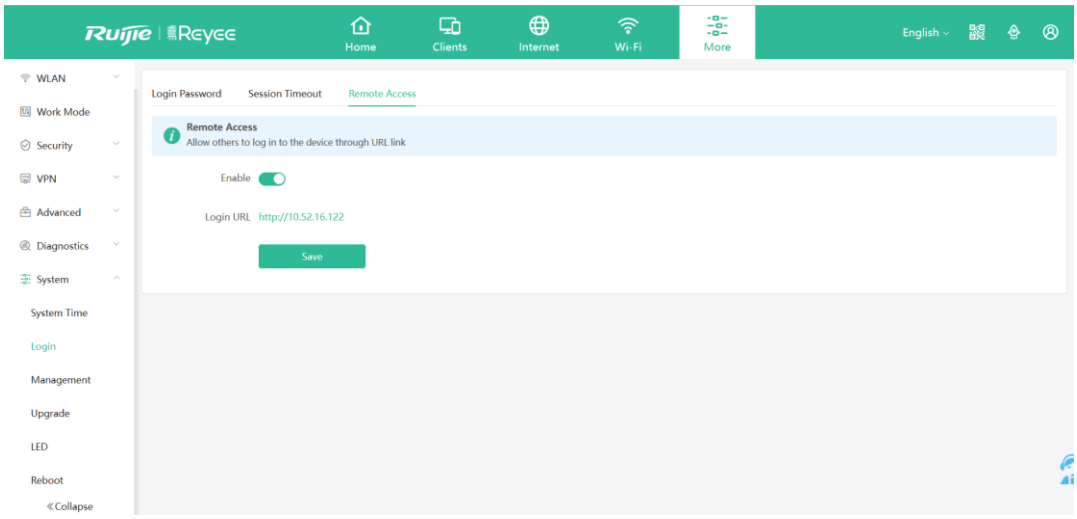
PC View: Choose **More** > **System** > **Login** > **Remote Access**.

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

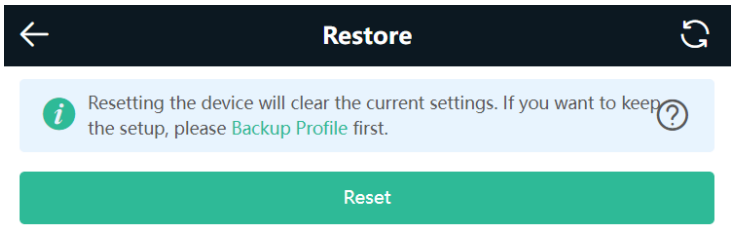
Mobile phone view: Choose **More** > **System** > **Restore**.

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.

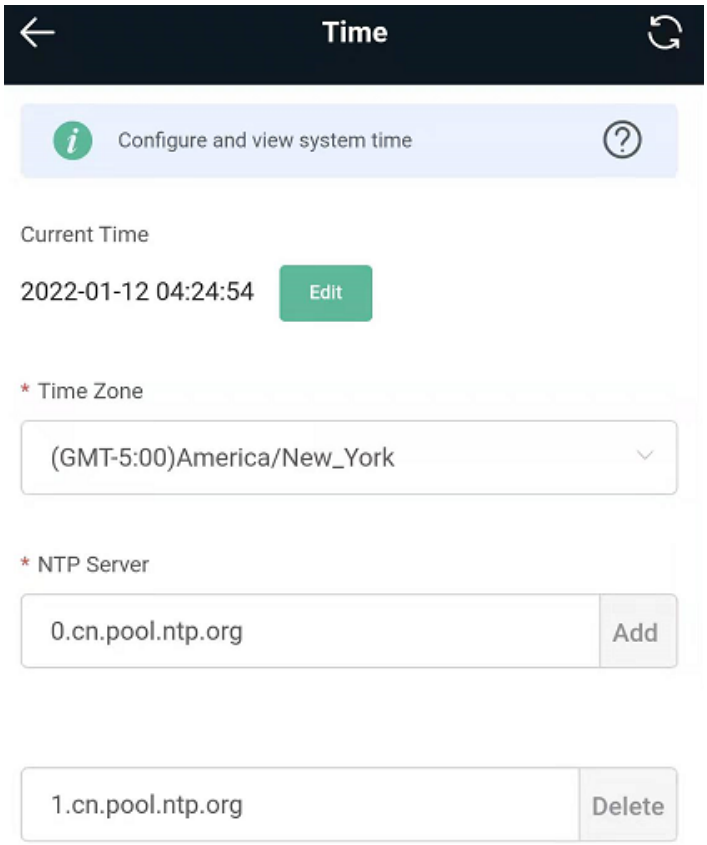


6.5 Configuring the System Time

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

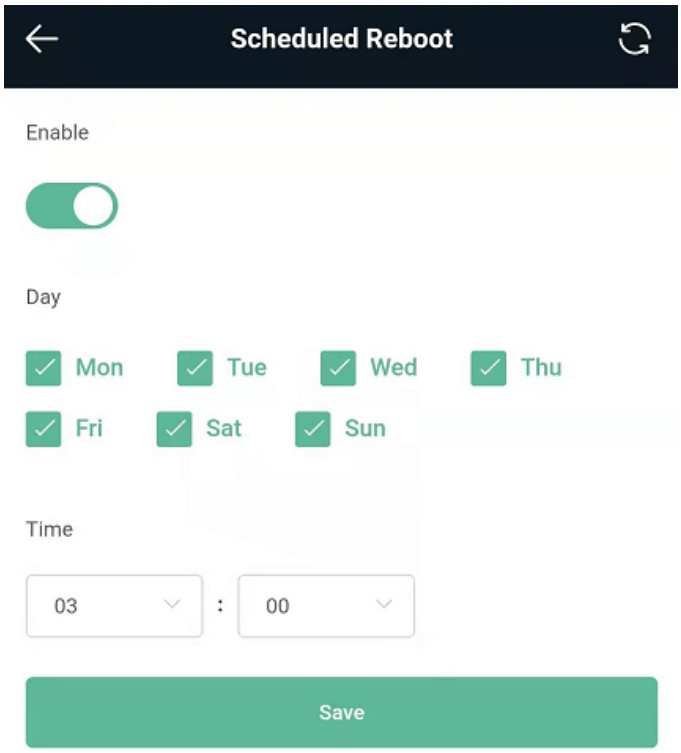
Confirm that the system time is accurate to avoid network interruption caused by device reboot at the incorrect time point. For details, see 6.5 Configuring the System Time.

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.



6.7 Performing Online Upgrade and Displaying the System Version

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

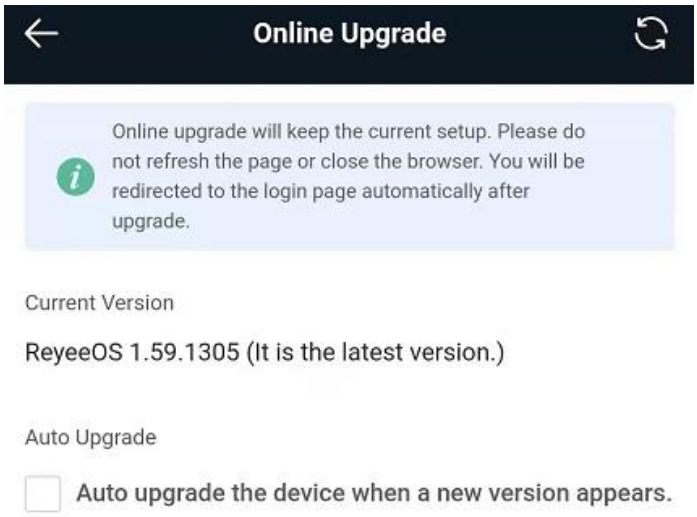
PC view: Choose More > System > Upgrade > Online Upgrade.

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.

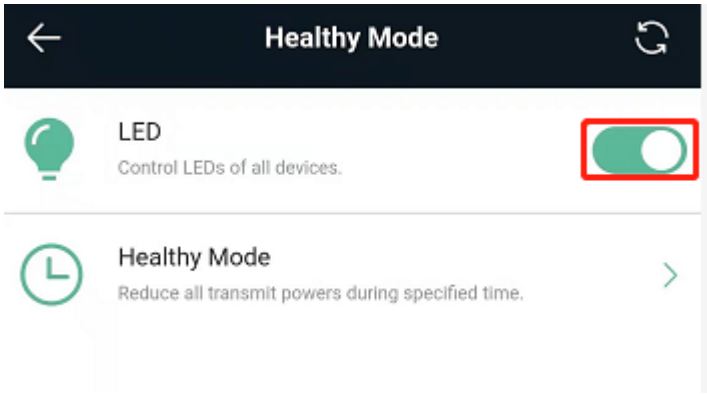
If no version upgrade is detected and online upgrade cannot be performed, check whether the DNS configuration is correctly obtained or go to **More** > **Advanced** > **Local DNS** to set the DNS server for the router.



6.8 Enabling or Disabling the LED

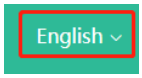
Mobile phone view: Choose **More** > **System** >**Healthy Mode**.

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



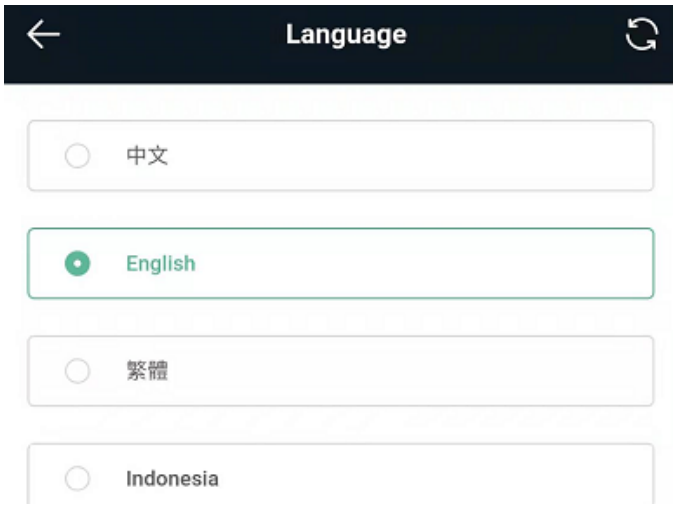
6.9 Switching the System Language

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

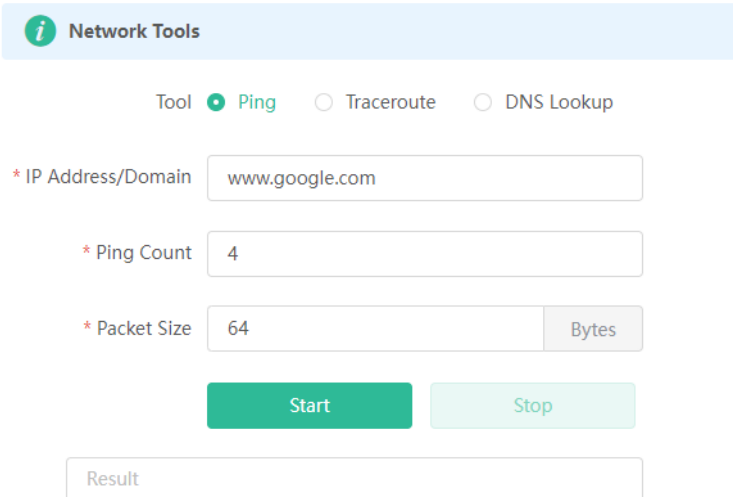
Mobile phone view: Choose **More** > **System** > **Network Tools**.

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

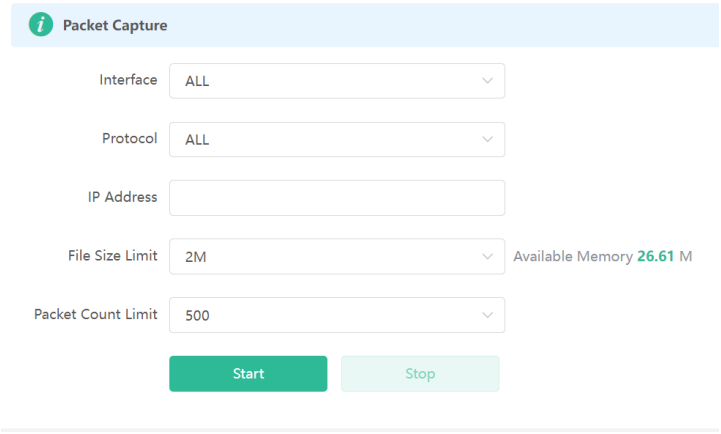
Mobile phone view: Choose More > Switch to PC view > More > Diagnostics > Packet Capture.

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.



Caution

If the preceding troubleshooting steps fail to resolve the issue, and remote assistance from technical support is needed, you can contact them to assist in enabling the developer mode. The technical support team can then perform diagnostics to identify and address the issue effectively.

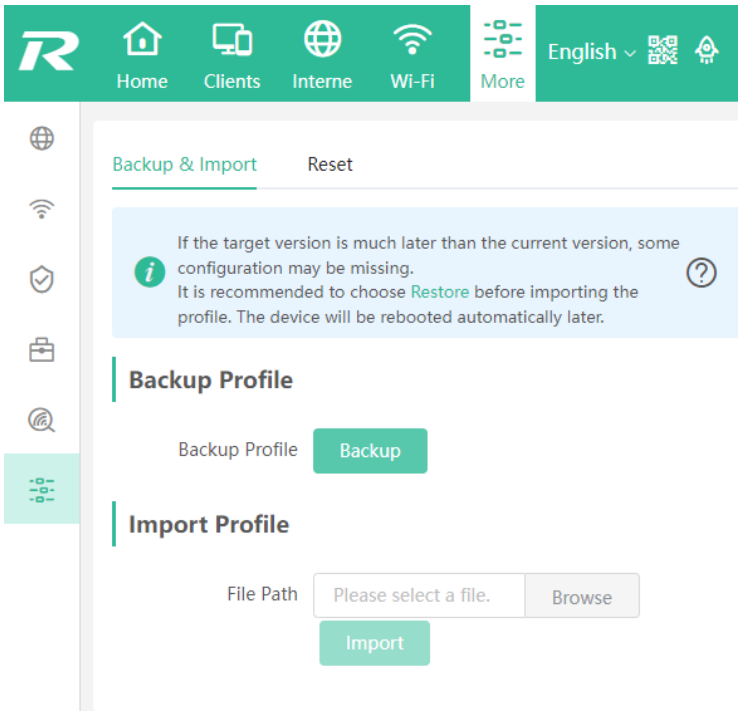
6.11 Configuring Backup and Import

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.

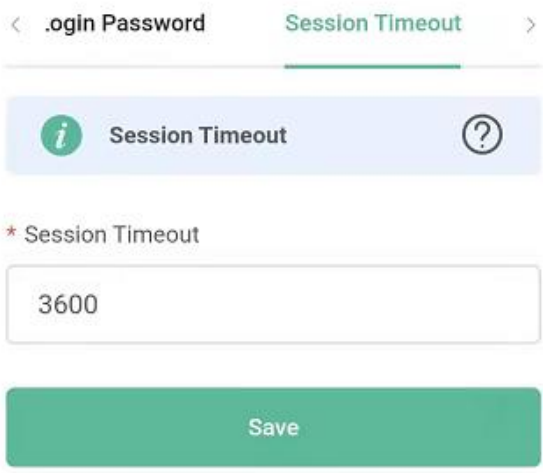


6.12 Configuring the Session Timeout

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.



7 Reyee FAQ

7.1 Reyee Password FAQ (Collection)

7.2 Reyee Wireless Repeater FAQ (Collection)

7.3 Reyee Parental Control FAQ (Collection)

7.4 Reyee Mesh FAQ (Collection)

7.5 Reyee Self-Organizing Network (SON) FAQ (Collection)

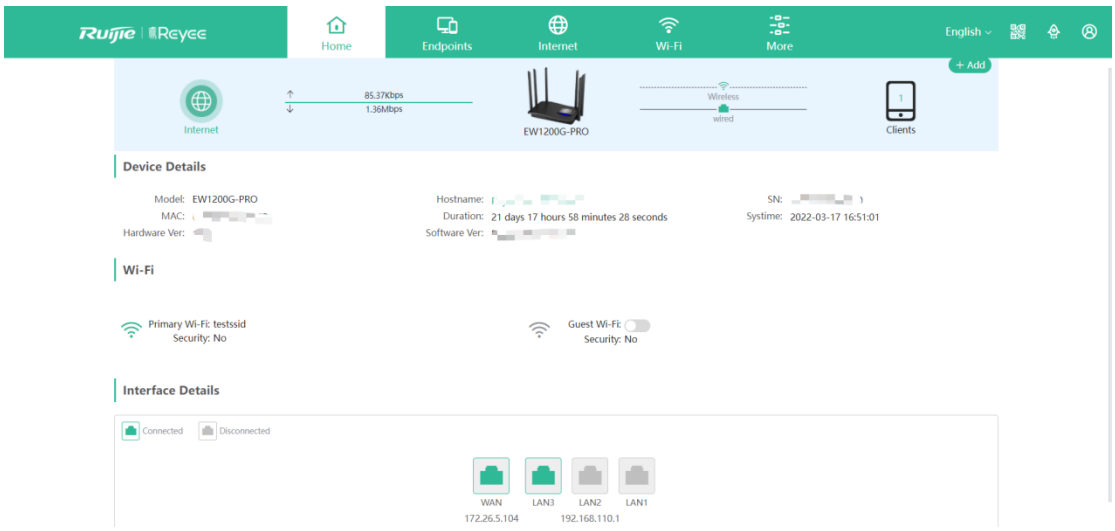
7.6 Reyee series Devices Parameters Tables

7.7 Reyee Parameter Consultation FAQ (Collection)

8 Appendix: Monitoring of Reyee Mesh Wi-Fi Routers

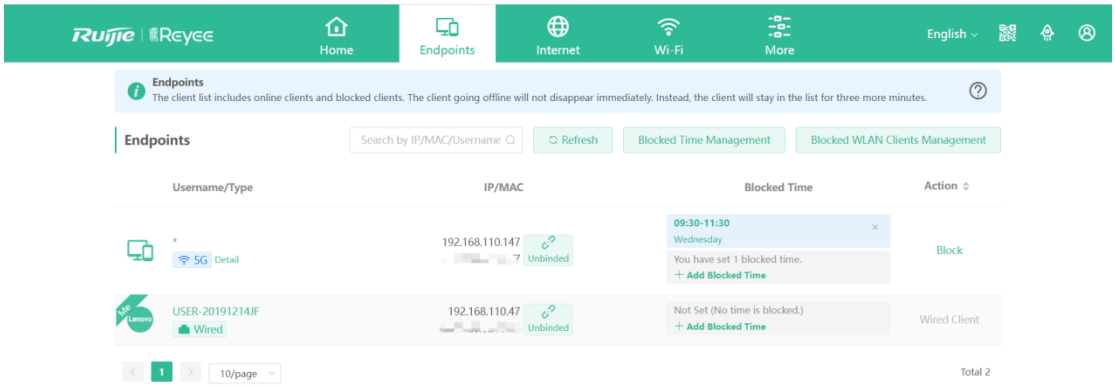
8.1 Overview

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.

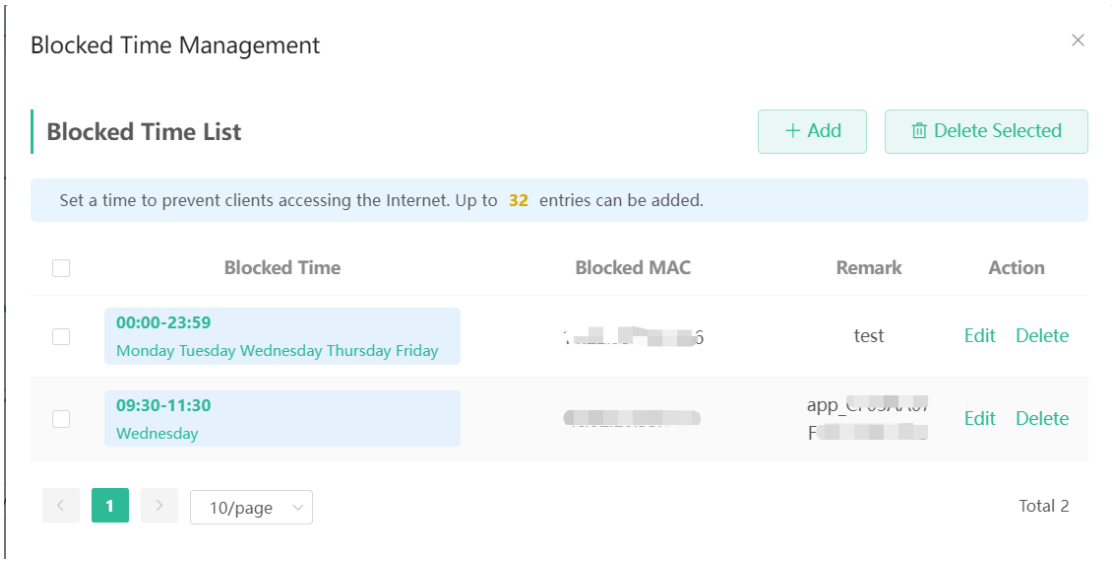


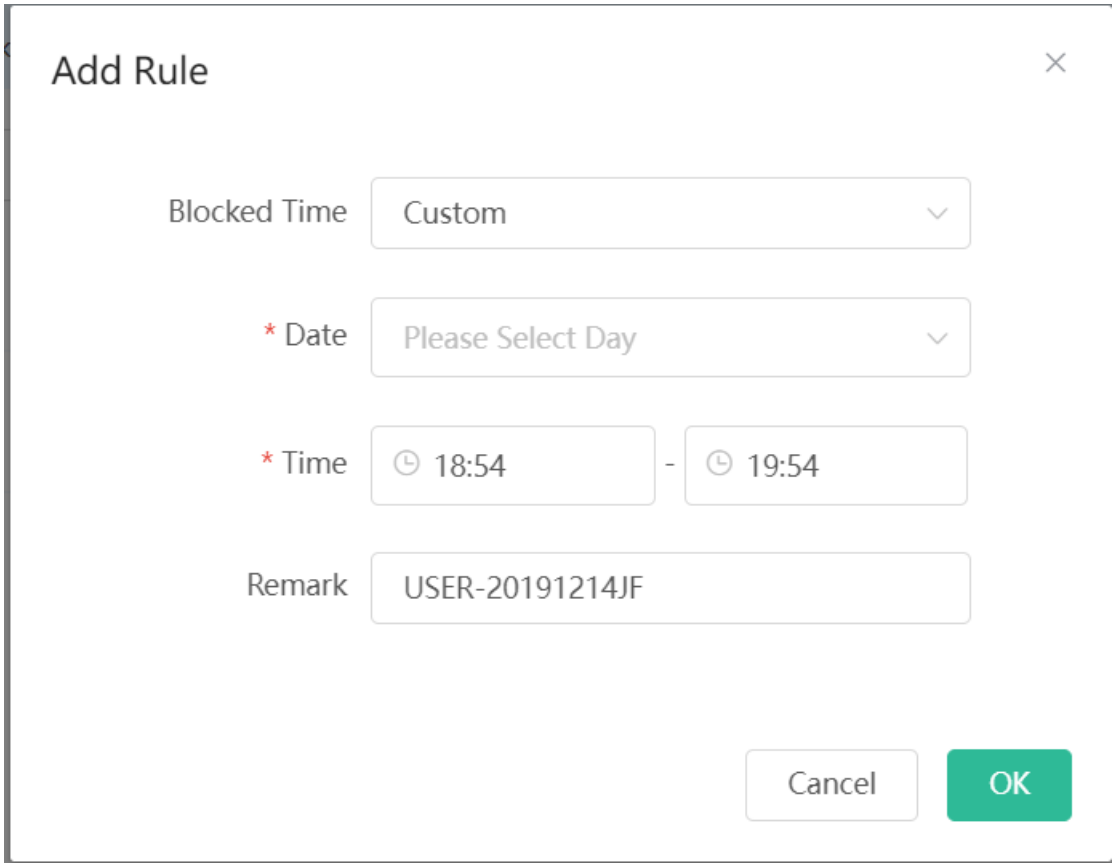
8.2 Endpoints

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.

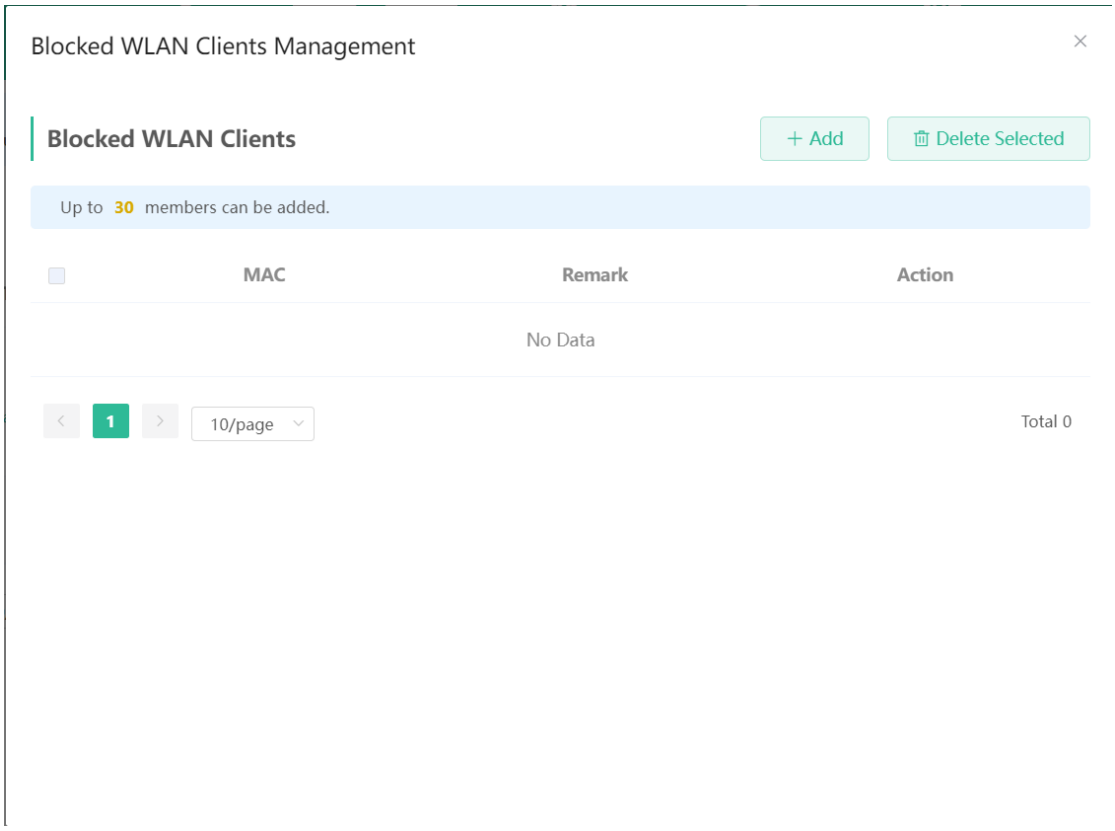


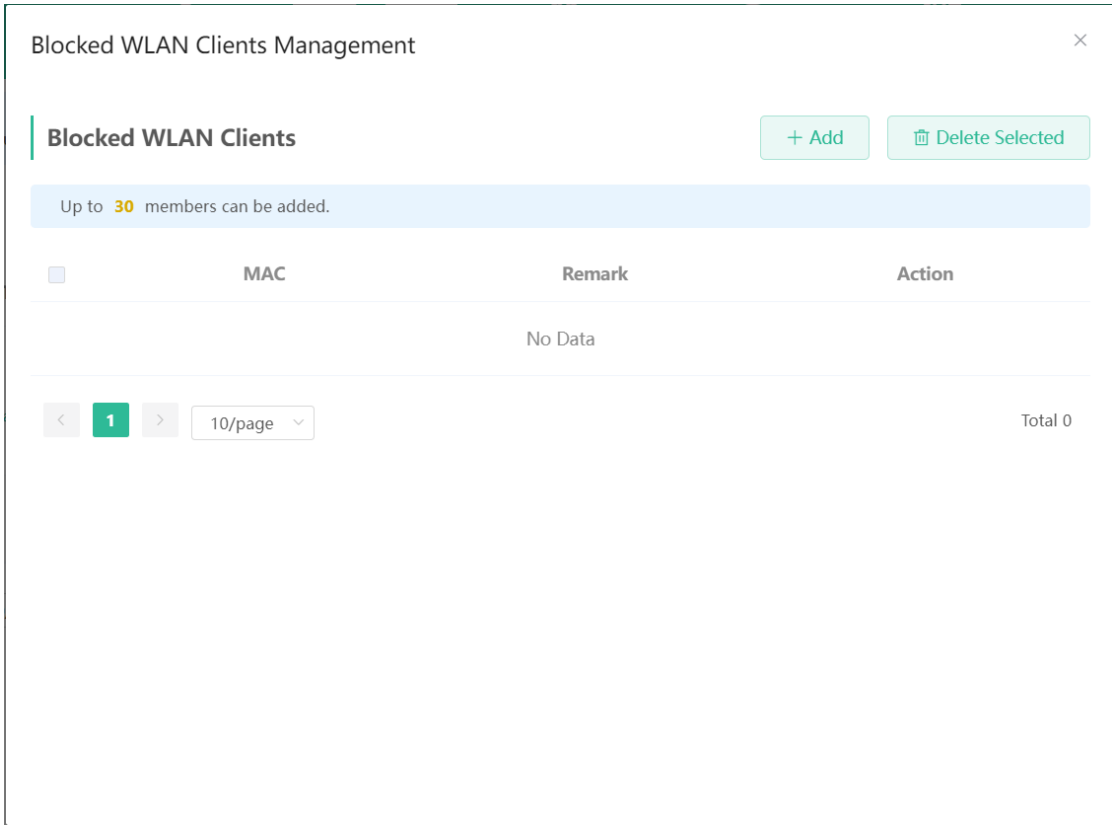
Click **Blocked Time Management** to customize the time to block users.





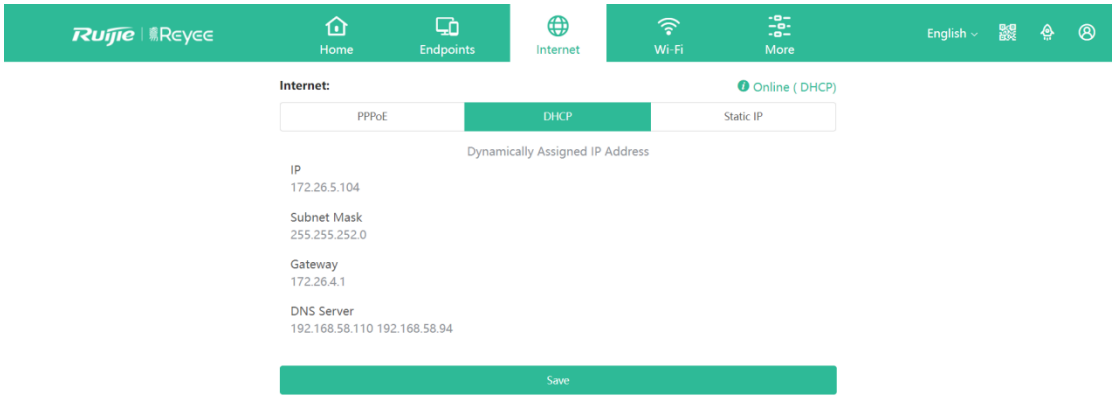
Click **Blocked WLAN Clients Management** and add the MAC address to prevent WLAN users from connecting the SSID.


Blocked WLAN Clients Management
Blocked WLAN Clients
+ Add
Delete Selected
Up to 30 members can be added.
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.
MAC
Remark
Action
No Data
1
10/page
Total 0

8.3 Internet

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



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**.