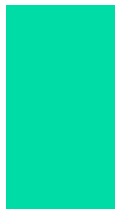
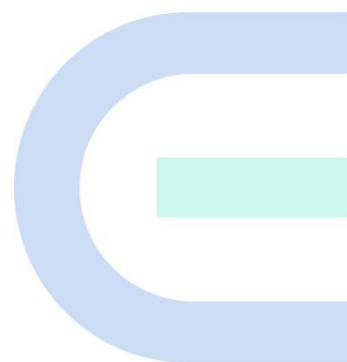


Reyee Mesh Routers

Web-based Configuration Guide ReyeeOS 1.303



Copyright

Copyright © 2024 Ruijie Networks

All rights are reserved in this document and this statement.

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



and other Ruijie networks logos are trademarks of Ruijie Networks.

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

Disclaimer

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

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

Preface

Technical Support

- The official website of Ruijie Reyee: <https://www.ruijienetworks.com/products/reyee>
- Technical Support Website: <https://www.ruijienetworks.com/support>
- Case Portal: <https://www.ruijienetworks.com/support/caseportal>
- Community: <https://community.ruijienetworks.com>
- Technical Support Email: service_rj@ruijienetworks.com

Conventions

1. GUI Symbols

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

2. Signs

The signs used in this document are described as follows:

Danger

An alert that calls attention to safety operation instructions that if not understood or followed when operating the device can result in physical injury.

Warning

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

Caution

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

Note

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

 **Specification**

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

3. Note

This manual introduces the features of the product and offers guidance on configuration and testing.

Contents

Preface	1
1 Fast Internet Access.....	1
1.1 Connecting to the Router.....	1
1.2 Logging in	1
1.3 Internet Access Mode	3
1.4 Primary Router Mode.....	3
1.4.1 Getting Started.....	3
1.4.2 Configuration Steps	4
1.4.3 Verification and Testing.....	6
1.4.4 Forgetting the PPPoE Account	7
1.5 Secondary Router Mode.....	9
1.5.1 Getting Started.....	9
1.5.2 Configuration Steps	9
1.5.3 Verification and Testing.....	16
1.6 Mesh Pairing.....	16
1.6.1 Performing Mesh Pairing through the Mesh Button	16
1.6.2 Configuring Mesh Pairing on the Management Page	17
1.6.3 Managing Secondary Router	18
1.6.4 Enabling Reyee Mesh.....	20
1.6.5 Troubleshooting	20
2 Wi-Fi Network Settings.....	22
2.1 Changing the SSID and Password.....	22
2.2 Hiding the SSID	22

2.2.1 Overview	22
2.2.2 Getting Started.....	22
2.2.3 Configuration Steps	23
2.3 Enabling Band Steering	24
2.4 Adding a Wi-Fi Network	24
2.4.1 Overview	24
2.4.2 Configuration Steps	25
2.4.3 Verification and Testing.....	27
2.5 Configuring the Wi-Fi Blocklist or Allowlist	28
2.5.1 Overview	28
2.5.2 Configuration Steps	28
2.6 Optimizing the Wi-Fi Network	29
2.6.1 Overview	29
2.6.2 Getting Started.....	30
2.6.3 Configuration Steps	30
2.7 Configuring the Healthy Mode	33
3 Networks Settings	35
3.1 Configuring Internet Connection Type.....	35
3.2 Changing the Address of a LAN Port	36
3.3 Changing the MAC Address	37
3.4 Changing the MTU.....	38
3.5 Configuring IPv6 Address	39
3.5.1 Configuring the IPv6 Address of the WAN Port.....	39
3.5.2 Configuring the IPv6 Address of the LAN Port	40

3.6 Enabling Parental Control.....	42
3.6.1 Setting the Internet Block Periods	43
3.6.2 Disabling Parental Control.....	45
3.7 Configuring XPress.....	46
3.8 Configuring Port Mapping.....	47
3.8.1 Overview	47
3.8.2 Getting Started.....	48
3.8.3 Configuration Steps	48
3.8.4 Verification and Testing.....	49
3.8.5 Solution to a Test Failure	49
3.8.6 DMZ Configuration Steps	49
3.9 Configuring DHCP Server.....	50
3.9.1 Overview	50
3.9.2 Configuration Steps	50
3.10 Configuring DNS.....	52
3.11 Configuring DHCP Option.....	53
3.12 Configuring DDNS	53
3.12.1 Overview	53
3.12.2 Getting Started.....	53
3.12.3 Configuration Steps	54
3.13 Configuring APR Binding.....	54
3.13.1 Overview	54
3.13.2 Configuration Steps	54
3.14 Connecting to IPTV.....	55

3.14.1 Getting Started	55
3.14.2 IPTV Configuration Steps (VLAN Type)	55
3.14.3 IPTV Configuration Steps (IGMP Type).....	56
3.15 Configuring WIFI/IGMP.....	57
3.15.1 Overview	57
3.15.2 Configuration Steps	57
3.16 Enabling Hardware Acceleration	58
3.17 Configuring Reyee Mesh 3.0	59
3.17.1 Configuration Steps	59
3.18 Configuring AP Networking.....	63
3.19 Enabling CWMP.....	64
3.20 Enabling Smart Flow Control.....	65
3.21 Enabling Port-Based Flow Control	67
3.22 Performing Advanced Network Settings.....	67
3.23 Configuring UPnP	68
3.23.1 Overview	68
3.23.2 Configuration Steps	68
3.24 Configuring Connectivity detection	69
3.25 Enabling Wi-Fi Switch.....	70
3.26 Configuring PPTP VPN.....	71
3.26.1 Overview	71
3.26.2 Configuring PPTP Server	71
3.26.3 Configuring PPTP Client.....	73
3.27 Configuring OpenVPN	74

3.27.1 Overview	74
3.27.2 Configuring OpenVPN (Server Mode)	74
3.27.3 Configuring OpenVPN (Client Mode)	78
4 Configuring the Repeater Mode	80
4.1 Access Point	80
4.2 Wireless Repeater	81
4.3 WISP	83
5 System Settings	85
5.1 Switching to PC View.....	85
5.2 Configuring the Login Password.....	85
5.3 Remote Access.....	86
5.4 Restoring Factory Settings	87
5.5 Configuring System Time	87
5.6 Configuring Scheduled Reboot.....	88
5.6.1 Getting Started.....	88
5.6.2 Configuration Steps	88
5.7 Performing Online Upgrade and Displaying the System Version	89
5.8 Turning On/Off the Indicator	90
5.9 Switching System Language	91
5.10 Enabling Alerts.....	91
5.11 Diagnosing Network Problems	93
5.12 Network Diagnosis Tools.....	94
5.13 Configuring Config Backup and Import	96
5.14 Configuring Session Timeout Duration.....	97

1 Fast Internet Access

1.1 Connecting to the Router

You can open the management page and complete Internet access configuration only after connecting a PC to the router. You can connect a PC to the router in either of the following ways.

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

1.2 Logging in

After a PC connects to a router in the initial state, the configuration wizard page pops up. If the configuration page does not pop up, 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 1-1 Default Configuration

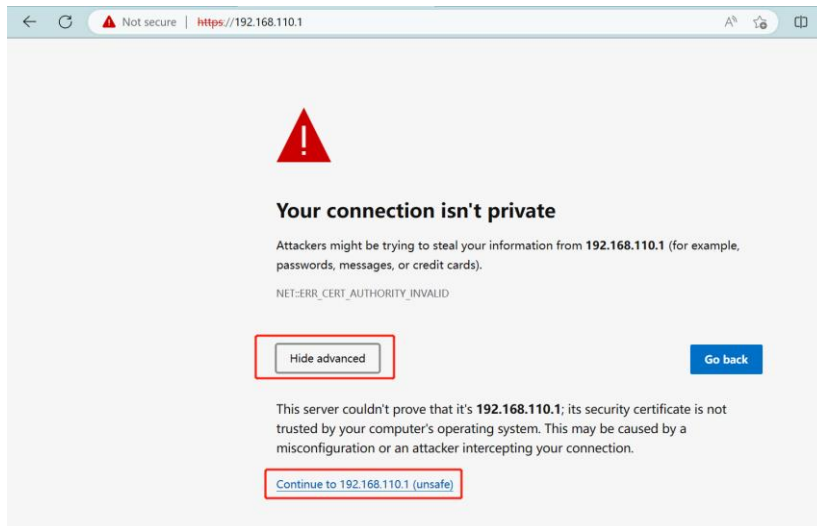
Item	Default Value
Device IP address (http or https)	192.168.110.1
Username/Password	No username and password are required at your first login and you can configure the router directly.

Enter the IP address of the router (default: 192.168.110.1) or <https://192.168.110.1> in the address bar of your browser, and press Enter. The login page is displayed.

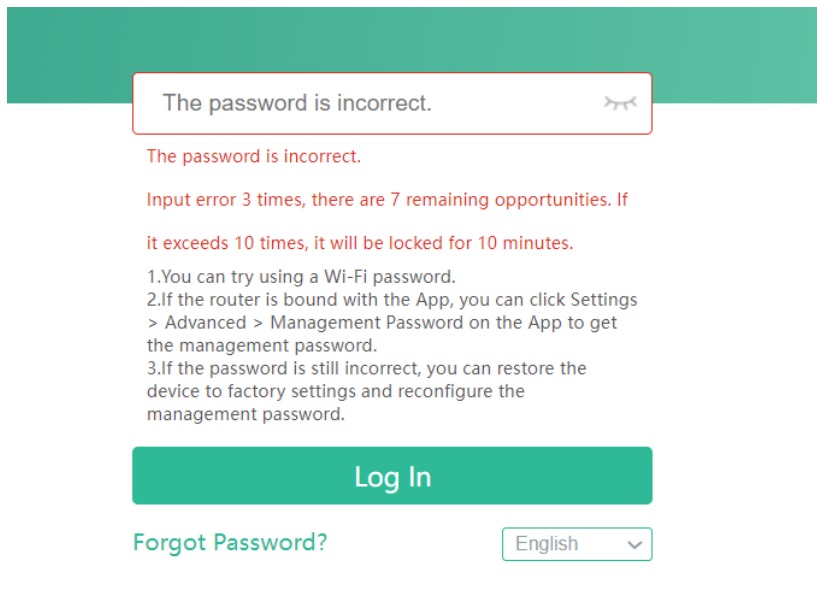
- Supported browsers: Google Chrome, and Internet Explorer 9 to 11. If an unsupported browser is used, you may encounter various errors or problems such as garbled text or formatting errors.

 Note

If you enter <https://192.168.110.1> in the address bar of your browser, and press Enter, the following page will be displayed. Click **Advanced > Continue to 192.168.110.1(unsafe)** to open the login page.



If you forget your password and enter the incorrect password to log in, you will need to wait for 10 minutes after each 10 unsuccessful attempts.



If you forget the IP address or password, hold down the **Reset** button for more than 10 seconds to restore factory settings. After restoration, you can use the default IP address and password to log in.

⚠ Caution

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 you choose to retain the configuration while restoring the device to its factory settings, the device will be reset to its default configurations while retaining the network settings, Wi-Fi parameters, and time zone configuration.

If the router in the 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 one minute later.

1.3 Internet Access Mode

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

Primary Router Mode: This mode is suitable for network creation. The router connects to the Internet through 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 PPPoE mode, Dynamic Host Configuration Protocol (DHCP) mode, and static IP address mode.

Secondary Router Mode: On an available network, the router can be connected to the primary router through either wired or wireless connection to expand the Wi-Fi coverage and increase the number of LAN ports and wireless access devices.

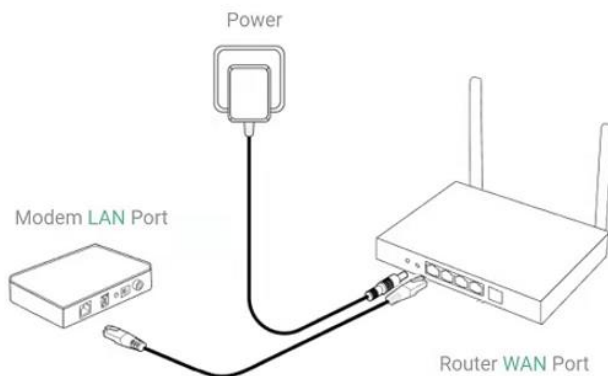
Note

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

1.4 Primary Router Mode

1.4.1 Getting Started

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



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

Figure out whether the Internet connection type is PPPoE, DHCP mode, or static IP address mode.

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

1.4.2 Configuration Steps

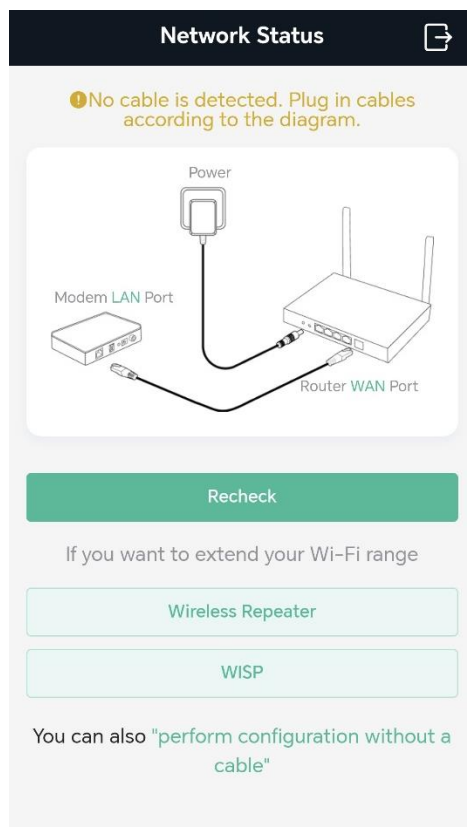
1. Configuring the Internet Connection Type

Click **Start Setup** and select the Internet connection type confirmed by the carrier.

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


⚠ Caution

- 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 change the configuration of the primary router by mistake. You can differentiate routers by checking the router model and Wi-Fi information on the home page.
- If the Ethernet cable is unplugged, you are prompted to connect the Ethernet cable first. Click **perform configuration without a cable** below to configure and connect the Ethernet cable.



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

Internet

DHCP Recommended 

Internet:

Dynamically Assigned IP Address

IP
172.17.96.147

Subnet Mask
255.255.254.0

Gateway
172.17.96.1

DNS Server
172.30.44.20 192.168.5.28

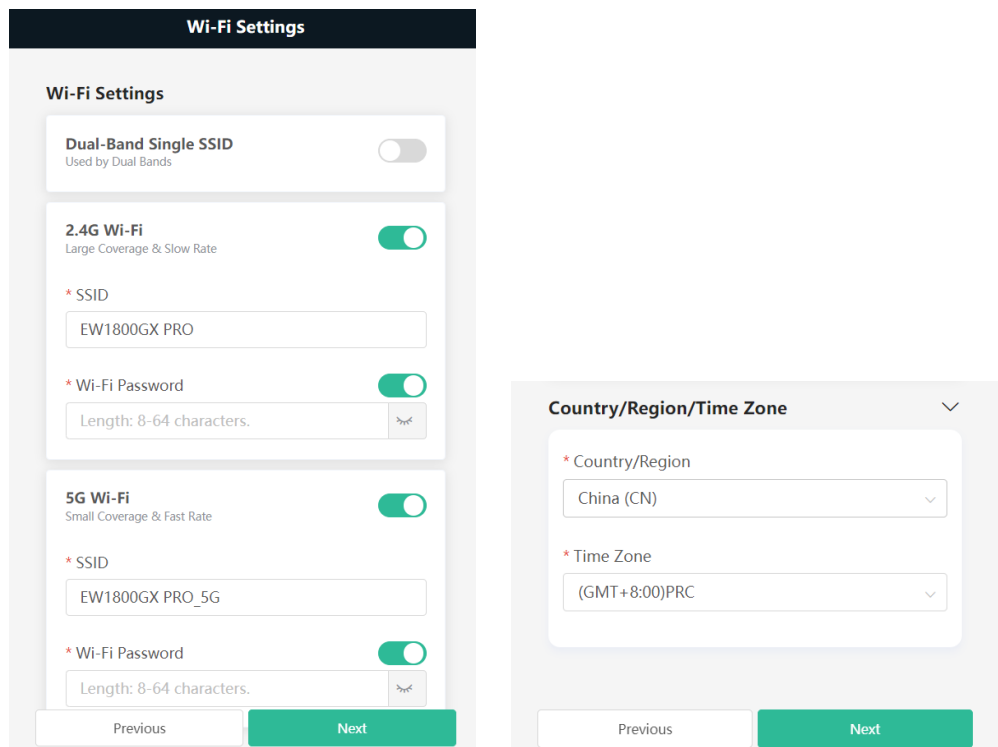
2. Configuring a Wi-Fi Network

- (1) **Dual-Band Single SSID:** After this function is enabled, the 2.4G SSID will be consistent with the 5G SSID and the 5G band will be preferred. The 2.4G signal is strong but easily interfered by various wireless signals. The 5G band boasts fast speed, low latency and less interference. The dual-band integration is abled by default. You are advised to disable this function. After configuring a 5G SSID, you can get a better Internet experience by accessing the 5G band in an unobstructed location near the device. You can also enable **Dual-Band Single SSID** in the meanwhile. The 5G-capable client will access 5G radio preferentially after the function is enabled. For details, see [2.3 Enabling Band Steering](#).

Note

- The terms “2.4G” and “5G” mentioned in this document only refer to the channels with the frequency of 2.4GHz and 5GHz, and have nothing to do with the 5G (fifth generation) Mobile Communication Technology.
-
- (2) **Setting the SSID and Wi-Fi password:** The device has no Wi-Fi password by default, indicating that the Wi-Fi network is an open network. You are advised to configure a complex password to enhance 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 but cannot contain special characters such as single quotation marks ('), double quotation marks ("), or spaces. The SSID (5G) is the name of the 5G radio. If the dual-band integration is enabled, set only one SSID.

- (3) **Setting the country or region:** The Wi-Fi channel may vary from country to country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.
- (4) **Setting time zone:** Set the system time. The network time server is enabled by default to provide the time service. You are advised to select the actual time zone.
- (5) Click **Next**. The Wi-Fi network will be restarted. You need to enter the new Wi-Fi password to connect to the new Wi-Fi network.



1.4.3 Verification and Testing

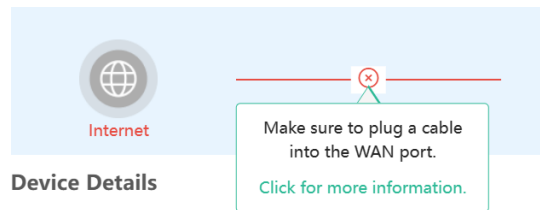
You can access the Internet after connecting to the Wi-Fi network. Log in to the management page (the default address is 192.168.110.1). The main page shows the Internet connection status and real-time upstream and downstream traffic data.

-
- Note**
 - The mobile phone view of the configuration may not be fully displayed on the vertical screen. You can view the complete network diagram on the horizontal screen.
-



Note


If the homepage shows that there is no Internet connection, please ensure that the WAN port is properly connected to the network cable. If the connection is established and you are still experiencing connectivity problems, you may click on **Click for more information** to access the **Network Check** page to perform a thorough diagnosis of your network.



1.4.4 Forgetting the PPPoE Account

- Obtain the username and password from the old device.
 - a Click from the old device
 - b Connect the old and new routers to a power supply and start them.
 - c Connect the WAN port of the new router to the modem.
 - d Connect one end of a cable to the WAN port of the old router and connect the other end to the LAN port of the new router.
 - e click **Obtain Account and Password**. The new router automatically fetches the PPPoE account of the old router.

Internet

DHCP Recommended 

Internet:

PPPoE ▼

*** Username**

Enter the broadband account provided by ISP.

*** Password**

Enter the broadband password provided by 👁

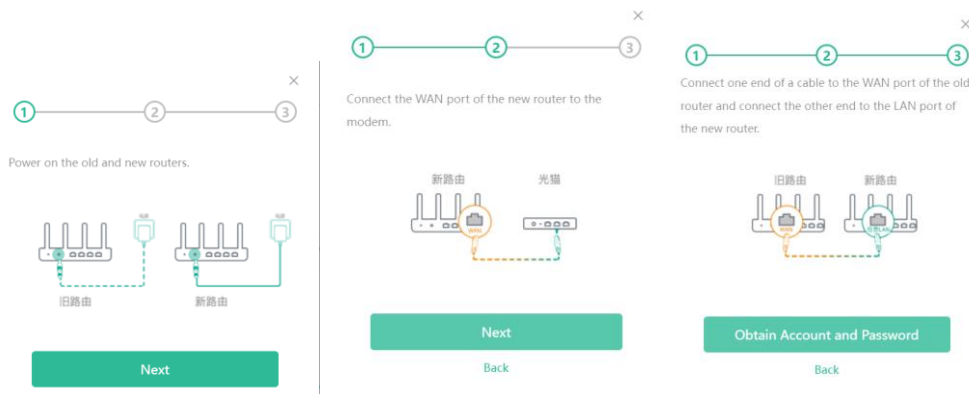
Service Name

(Optional) Provided by ISP

? **Forgot Username and Password?**
Obtain the username and password [from the old device.](#)

Previous

Next



1.5 Secondary Router Mode

1.5.1 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. If an Ethernet cable is available, you are advised to connect the secondary router to the primary router through the wired connection.
- If no Ethernet cable is available, place the secondary router in a place where it can scan at least two-bar Wi-Fi signal of the primary router.

1.5.2 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

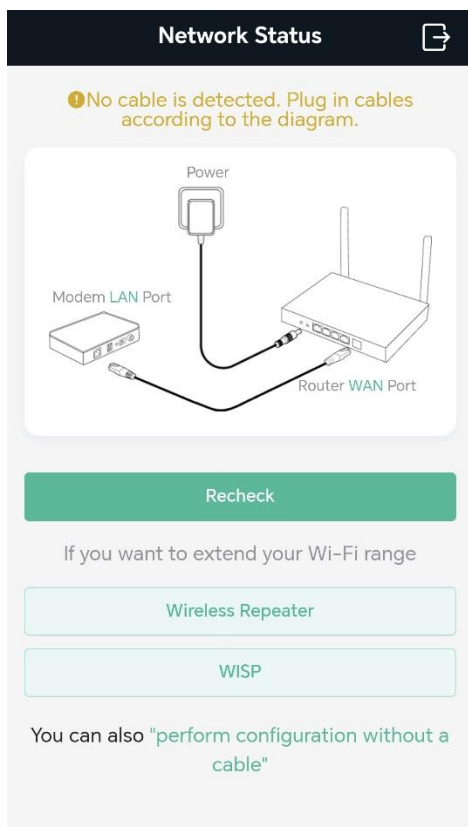
Make sure that the secondary router is in the factory default state. If the secondary router has been configured, please first restore it to factory default settings by pressing and holding the reset hole for 10 seconds, and then repeat Step 2.

2. Wireless Connection

Connect the router to a power supply and click **Start Setup** without connecting an Ethernet cable.

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.



- Wireless Repeater

- (1) Select Wireless Repeater.

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

- In wireless repeater mode, only Wi-Fi signals are extended and the DHCP function is disabled. The 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 WAN cable is plugged in, the device automatically switches to the wired repeater mode.

The image shows two side-by-side screenshots of a web-based configuration interface. The left screenshot, titled 'Scan', displays a search bar for 'SSID Filtering' and a list of 15 detected Wi-Fi networks. Each entry includes a '5G' signal strength indicator, the SSID name, and a 'High' signal quality indicator. The right screenshot, titled 'Enter Password', shows the 'Enter the Wi-Fi password' step. It features a 'Primary Router SSID' field with a dropdown menu, a '* Password' field with a text input and a visibility toggle, and 'Previous' and 'Next' navigation buttons at the bottom.

Signal	SSID	Quality
5G	RuiJie-ChengDu	High
5G	RuiJie-ChengDu	High
5G	RuiJie-ChengDu	High
5G	HUAWEI_H112_8915_5G	High
5G	RuiJie-ChengDu	High
5G	RuiJie-ChengDu	High
5G	RuiJie-ChengDu	High
5G	RuiJie-ChengDu	High
5G	RuiJie-ChengDu	High
5G	RuiJie-ChengDu	High
5G	RuiJie-ChengDu	High
5G	RuiJie-ChengDu	High
5G	RuiJie-ChengDu	High
5G	RuiJie-ChengDu	High
5G	RuiJie-ChengDu	High
5G	RuiJie-ChengDu	High

(2) Click **Next**. On the **Set Wi-Fi** page that opens,

Enter the Wi-Fi SSID and password:

- o You can select **Same as Primary Router Wi-Fi**, in which Wi-Fi SSID and password will be same as the primary router Wi-Fi,
- o Select **New Wi-Fi** to set new Wi-Fi SSID and password.

Enter management password for the extender:

- o Click **Same as Wi-Fi Password** to set the Management Password same as the Wi-Fi Password.

Set Wi-Fi

Local Router Wi-Fi

Same as Primary Router Wi-Fi New Wi-Fi

* SSID (2.4G)
RuiJie-ChengDu

* SSID (5G)
RuiJie-ChengDu

Wi-Fi Password
ChengDu@rj

Management Password Same as Wi-Fi Password

* Management Password (Remember the password.)
ChengDu@rj

High

Previous Next

- (3) Choose the **Country/Region** and **Time Zone**. You are advised to choose the correct country or region, as well as the appropriate time zone.

Set Country/Region Code

Country/Region/Time Zone

* Country/Region
China (CN)

* Time Zone
(GMT+8:00)PRC

Previous Next

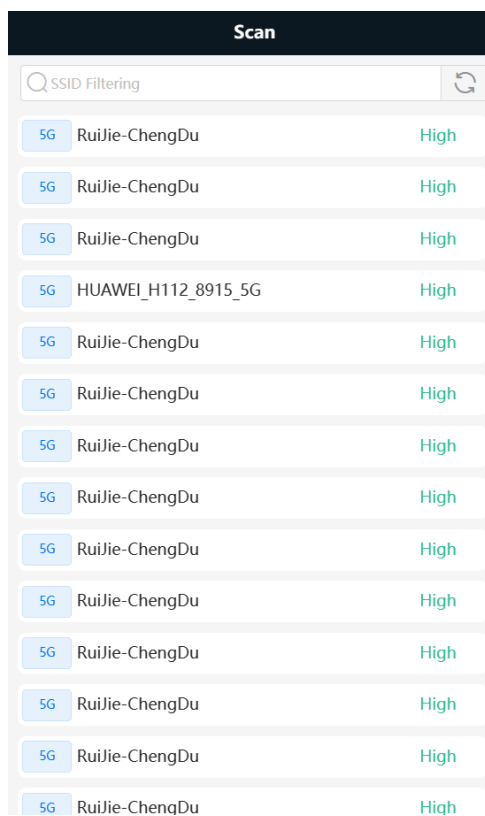
- **WISP:**

In this mode, the device enables multiple users to share Internet connection from WISP. The LAN port devices share the same IP from WISP through Wireless port. While connecting to WISP, the Wireless port works as a WAN port. The Ethernet port acts as a LAN port

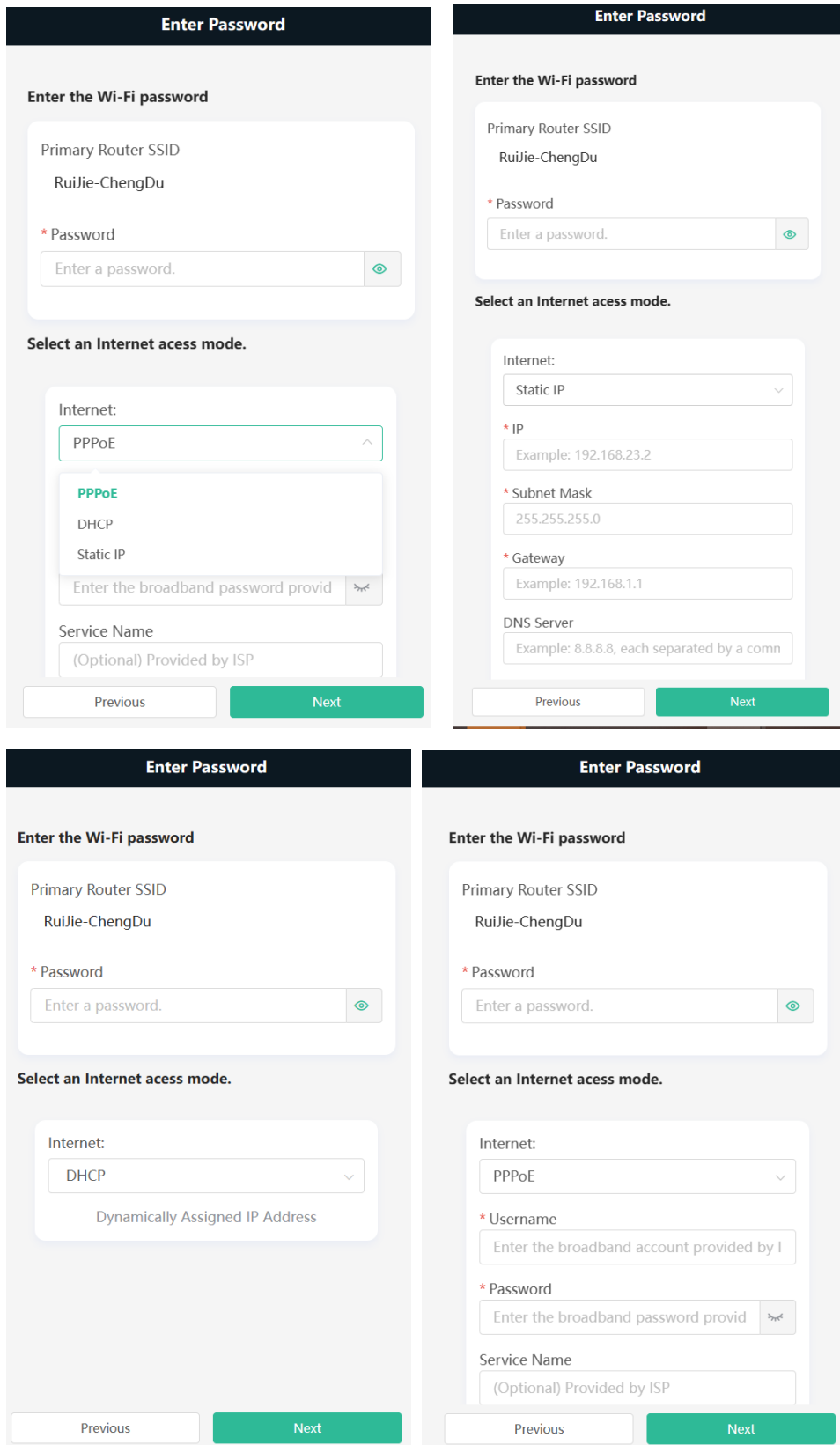
Note

In the WISP mode, the device still supports routing and DHCP. The clients connected to the primary router are assigned IP addresses by the primary router; the clients connected to the secondary router are assigned IP addresses by the secondary router.

- (1) Click **WISP**. Select the Wi-Fi of the primary router.



- (2) Enter the password of the primary router Wi-Fi.
 - o Select DHCP and the extender will automatically obtain an IP address.
 - o If the primary router cannot assign IP addresses, select **Static IP**.
 - o In the PPPoE mode, a username, a password, and possibly a service name are needed.



- (3) Click **Next**. On the **Set Wi-Fi** page that opens,
 - Enter the Wi-Fi SSID and password and management password for the extender.
 - o You can select **Same as Primary Router Wi-Fi**, in which Wi-Fi SSID and password will be same as the

primary router Wi-Fi,

- o Select **New Wi-Fi** to set new Wi-Fi SSID and password.

Enter management password for the extender:

- o Click **Same as Wi-Fi Password** to set the Management Password same as the Wi-Fi Password.

Set Wi-Fi

Local Router Wi-Fi

Same as Primary Router Wi-Fi New Wi-Fi

* SSID (2.4G)
RuiJie-ChengDu

* SSID (5G)
RuiJie-ChengDu

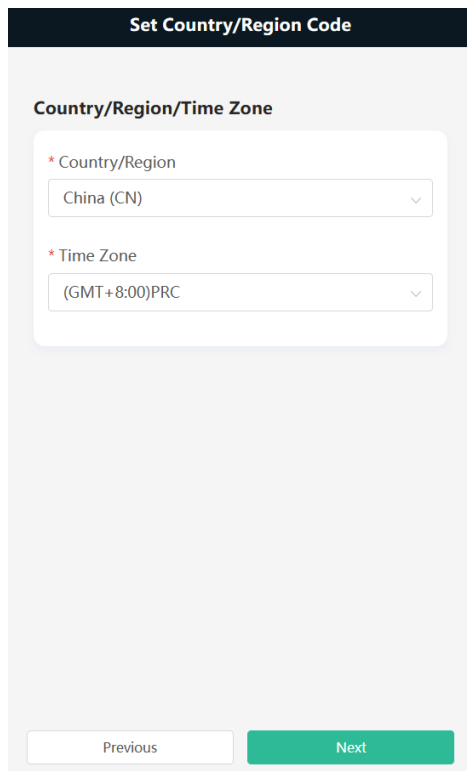
Wi-Fi Password
ChengDu@rj

Management Password Same as Wi-Fi Password

* Management Password (Remember the password.)
Length: 8-64 characters.

Previous Next

- (4) Choose the **Country/Region** and **Time Zone**. You are advised to choose the correct country or region, as well as the appropriate time zone.



Set Country/Region Code

Country/Region/Time Zone

* Country/Region
China (CN) ▾

* Time Zone
(GMT+8:00)PRC ▾

Previous Next

(5) Click **Next** to complete the configuration.

1.5.3 Verification and Testing

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

1.6 Mesh Pairing

To extend the Wi-Fi coverage, the routers can be connected to the primary router through either wired or wireless connection to build a wireless network that supports seamless roaming. You can press the **Mesh** button to automatically search for new routers around and perform automatic pairing, or log in to the router management page to select a new router for pairing. After the mesh pairing, the secondary router will synchronize the Wi-Fi settings (SSID and password) of the primary router, and the original Wi-Fi (SSID) will disappear. Up to 6 (1+5) routers are supported.

Note

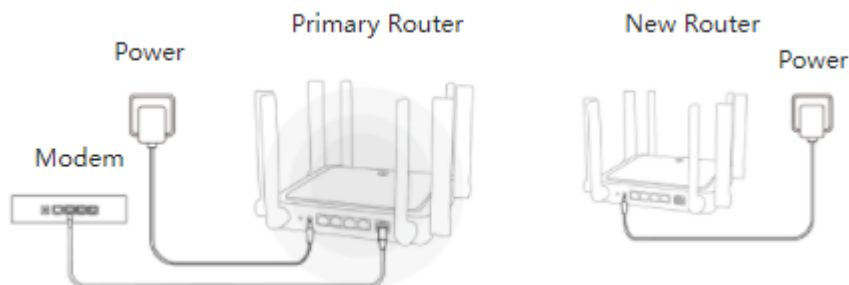
This feature is not supported on the RG-EW300 PRO router.

1.6.1 Performing Mesh Pairing through the Mesh Button

- (1) Make the primary router connect to the Internet.
- (2) Place the new router 2 meters (around 6.5ft) away from the primary router and power on the new router. The system LED of the new router starts to blink slowly.

Note

After the new router is powered on, the SYS LED of M18 and M32 turns orange.



- (3) Press the Reyee Mesh button on the primary router.

The Reyee Mesh indicator on the primary router will blink slowly, indicating that the primary router is searching nearby routers for pairing. The Reyee Mesh indicator on the secondary router will also blink slowly, indicating the secondary router is being paired with the primary router. In about 2 minutes, the Reyee Mesh indicators on both routers will be steady on, indicating Mesh pairing is complete.

Note

During Mesh pairing through the Mesh button, the Reyee Mesh indicator of M18 and M32 sequentially illuminate in four cells.

- (4) Place the secondary router in an area where the Wi-Fi signal is weak or nonexistent, and power it on again. Wait for 3 to 5 minutes until the Reyee Mesh indicator on the secondary router turns solid on. The original SSID of the secondary router (@Ruijie-sXXXX) will disappear and both routers will broadcast the same SSID, indicating that Mesh networking succeeds.

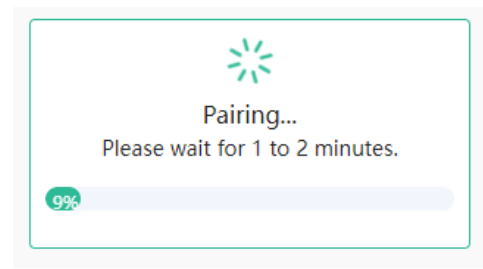
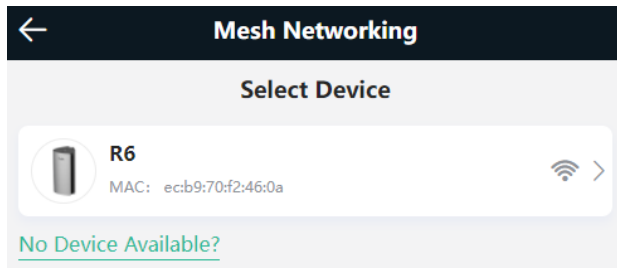
1.6.2 Configuring Mesh Pairing on the Management Page

Mobile Phone View: Choose **Home** > **+Add Mesh Router** > **next**.

PC View: Choose **Home** > **+Add Mesh Router** > **next** > **next**.

You can set up a wireless network that supports seamless roaming by mesh networking.

1. For quick pairing, please place the new router about 2 meters away from the primary router and connect the new router to the power supply. After pairing, place the new router where the Wi-Fi coverage is needed.
2. The system LED of the new router starts to blink. Wait for 2 to 3 minutes until the LED turns solid on.
3. After the new router is started, click **next** for the primary router to search for devices that can be paired. It takes one or two minutes to select the target device and perform the pairing.



4. After the Mesh pairing, place the new router where you want to have Wi-Fi coverage and then power on the router.


⚠ Caution

- Make sure that the new router is around the primary router and there are not too many obstacles between them.
- If there are 3 or more routers, repeat the above steps. Up to 6 (1+5) routers are supported.



1.6.3 Managing Secondary Router

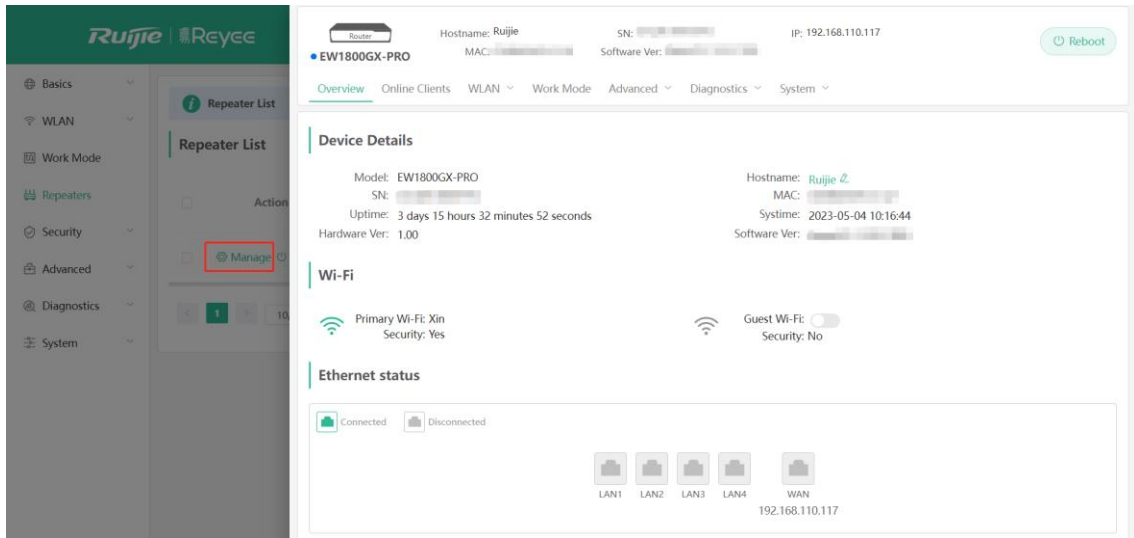
Mobile Phone View: Choose **More** > **Switch to PC view** > **More** >  **Repeaters**.

PC View: Choose **More** >  **Repeaters** or click the secondary router in the networking diagram on the home page.

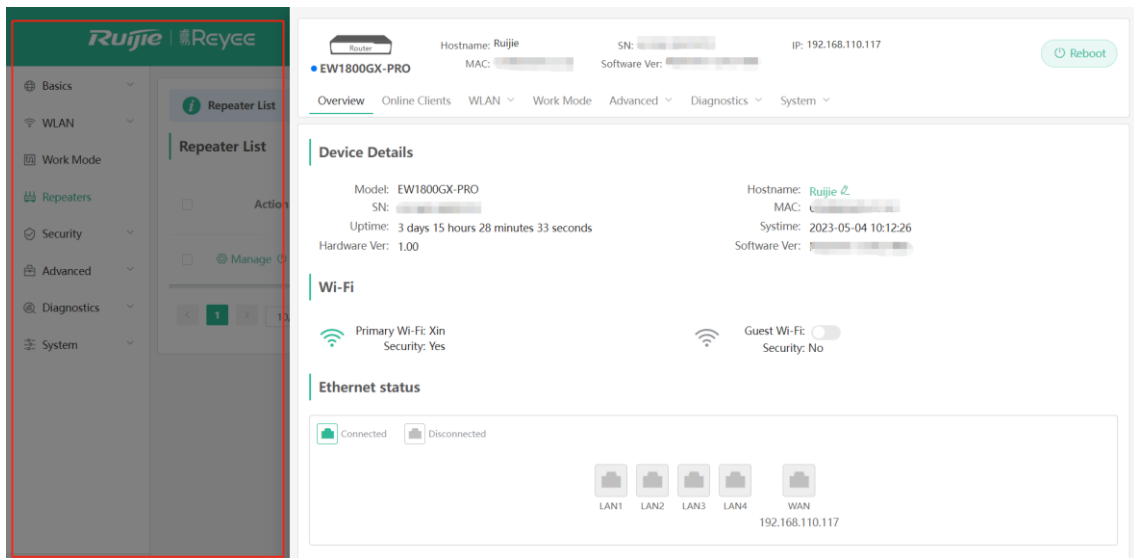
⚠ Caution

- To ensure the effect of seamless roaming, the Wi-Fi configuration of the secondary router must be consistent with that of the primary router and cannot be modified independently.

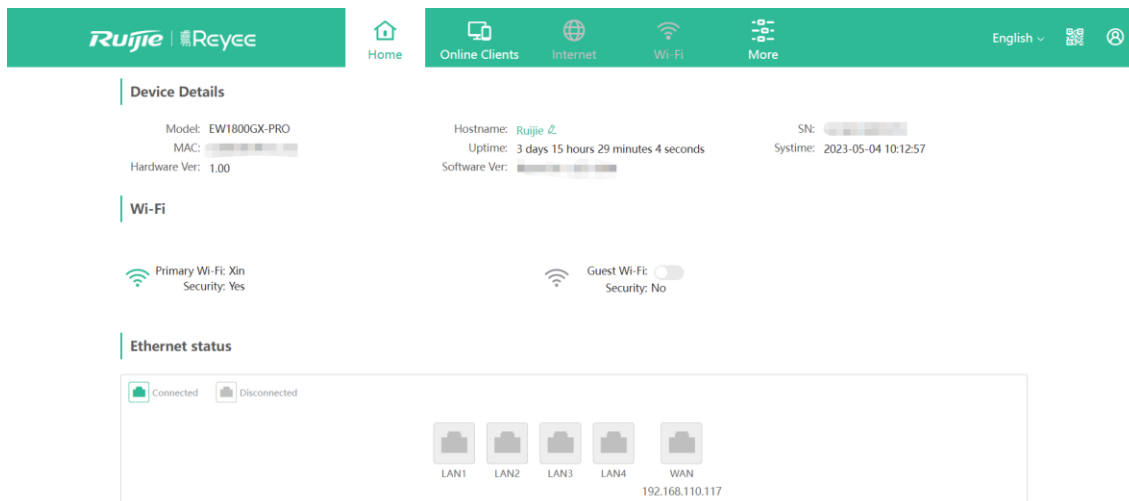
Click **Manage**, and the secondary router management page will pop up. You can make detailed settings for the secondary router.



Click on the gray area on the right to close the page.

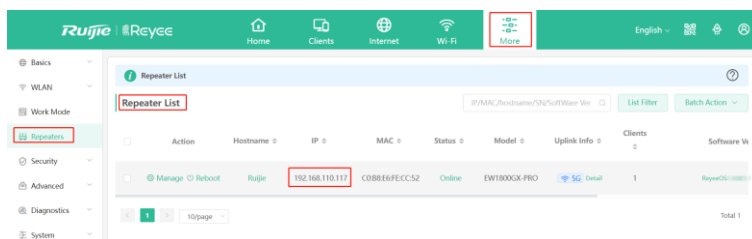


To log in to the web management system of the secondary router directly, you need to know its IP address. Connect your mobile phone or computer to the Wi-Fi network broadcast by the router. Enter the IP address of the secondary router in the address bar of the browser to access the web management system.



Note

Choose **More > Repeaters** to view the IP address of the secondary router in the Repeater List of the primary router.



1.6.4 Enabling Reyeec Mesh

Mobile Phone View: Choose **More > Switch to PC view > More > Advanced > Reyeec Mesh**.

PC View: Choose **More > Advanced > Reyeec Mesh**.

Reyeec Mesh is enabled on the device by default. You are advised to enable the function.

After Reyeec Mesh is enabled, and the secondary router is connected, press the Reyeec Mesh button on the primary router, and the secondary router will automatically join the network.

Note

- After Reyeec Mesh is enabled, press the Reyeec Mesh button on the primary router, and the secondary router will automatically join the network when connected to the primary router.
- After Reyeec Mesh is disabled, the bridged slave router will still be connected.

1.6.5 Troubleshooting

- Please make sure that the new router is powered on and around the primary router.
- Please make sure that the new router is around the primary router and there are not too many obstacles between them.
- Please make sure that the new router supports mesh networking.

- Press the **Reset** button for at least 10 seconds. Try again after the system LED blinks fast.
- Please make sure that Reyee Mesh is enabled on the primary router. (This function is enabled by default.)
- Change the channel on the 5GHz band of the primary router to a non-DFS channel, such as Channel 36.

2 Wi-Fi Network Settings

2.1 Changing the SSID and Password

On mobile phone: Choose **Wi-Fi** > **Wi-Fi Settings**.

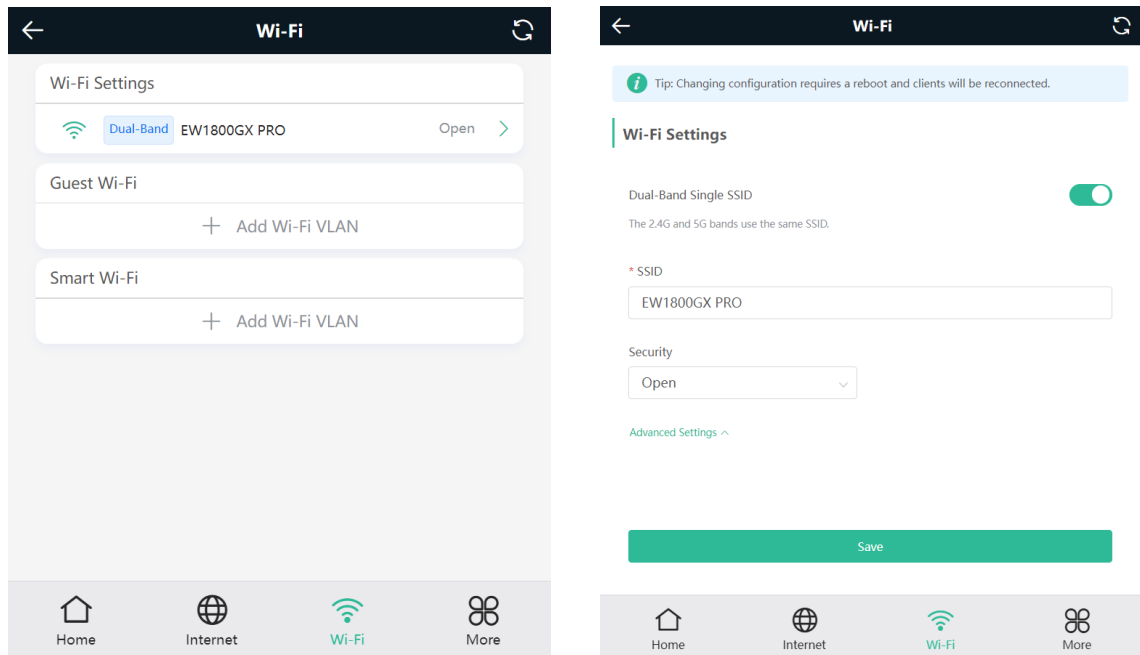
Click the target Wi-Fi network.

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

Change the SSID and password of the Wi-Fi network, and click **Save**.

Caution

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



2.2 Hiding the SSID

2.2.1 Overview

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

2.2.2 Getting Started

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

2.2.3 Configuration Steps

On mobile phone: Choose **Wi-Fi > Wi-Fi Settings**.

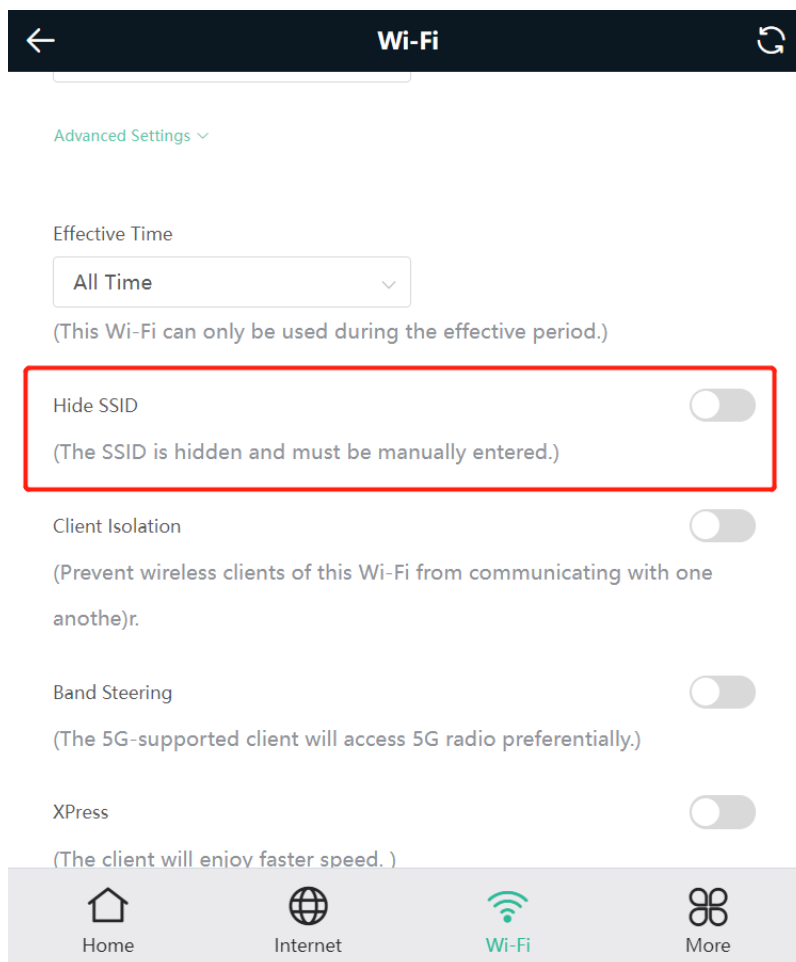
Click the target Wi-Fi network.

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


Turn on **Hide SSID** and click **Save**.

Caution

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.



Note

Users need to manually enter the SSID and password each time they connect to a hidden Wi-Fi network. Take an Android-based device 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** from the **Security** dropdown list, enter the password, and click **Connect**.

2.3 Enabling Band Steering

Caution

Before enabling the band steering, you must enable the dual-band integration. Because the client can automatically choose to steer to either band only when the 2.4G and 5G bands use the same SSID.

Note

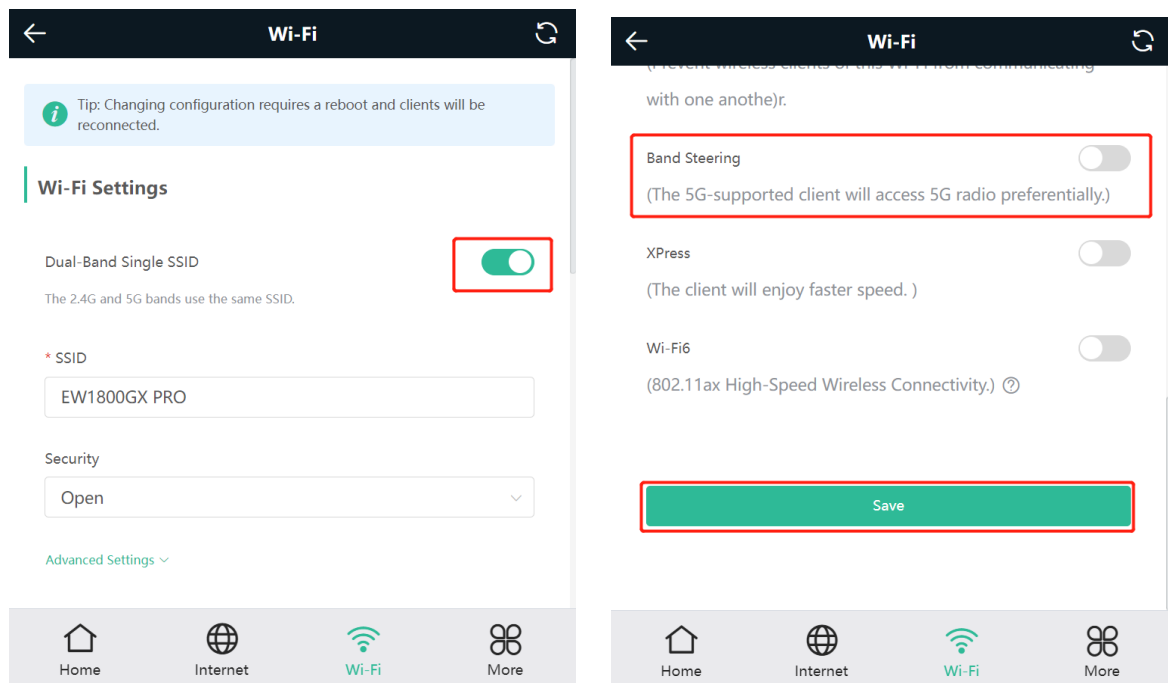
The RG-EW300-PRO router does not support the 5G band.

On mobile phone: Choose **Wi-Fi > Wi-Fi Settings**.

Click the target Wi-Fi network.

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

Click **Band Steering**. The 5G-capable client will access 5G radio preferentially after this function is enabled.



2.4 Adding a Wi-Fi Network

2.4.1 Overview

The router supports three types of Wi-Fi networks: primary Wi-Fi network, guest Wi-Fi network, and smart Wi-Fi network, and only one Wi-Fi network can be configured for each type.

- **Primary Wi-Fi:** The primary Wi-Fi network is listed in the first line of the page and is enabled by default.
- **Guest Wi-Fi:** This 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 via Wi-Fi, but cannot access each other, improving security.

The guest Wi-Fi network can be turned off as scheduled. You can configure to turn off the guest Wi-Fi network one hour later. When the time expires, the guest network is off.

You can set rate limits for the guest Wi-Fi network, and any device connected to the guest Wi-Fi network will have its Internet speed limited accordingly.

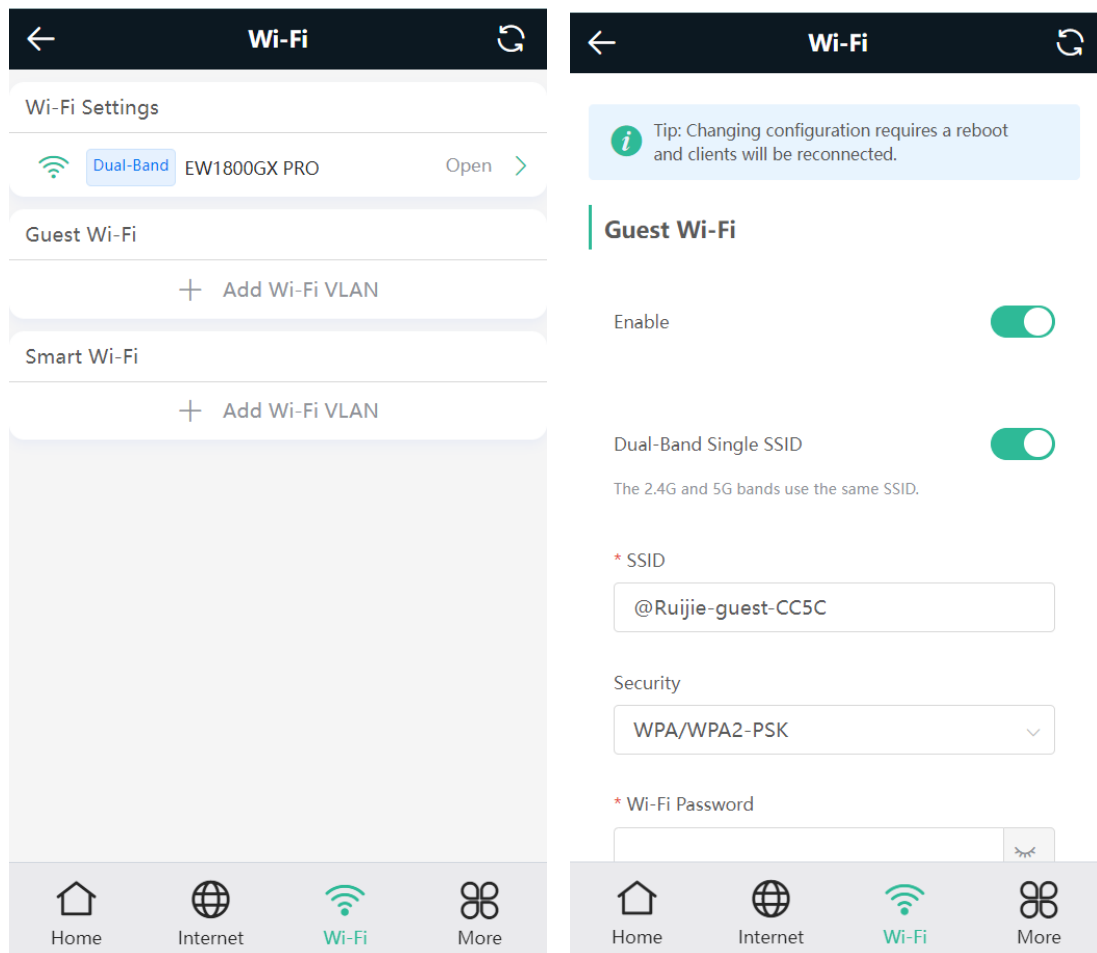
- **Smart Wi-Fi:** The smart Wi-Fi network is disabled by default. Smart clients can connect to the smart Wi-Fi network for long. You can set an effective time for the smart Wi-Fi network which will only be enabled during the set effective time.

2.4.2 Configuration Steps

On mobile phone: Choose **Wi-Fi > Wi-Fi Settings**.

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

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



- **Effective Time:** Options include Weekdays, Weekends, All Time and Custom. When Custom is selected, you can select a custom effective time. This Wi-Fi can only be used during the effective period
- **Client Isolation/Guest Isolation:** This feature is supported by **Wi-Fi Settings**, **Guest Wi-Fi** and **Smart Wi-Fi**.

You can enable **Client Isolation** in **Wi-Fi Settings** and **Smart Wi-Fi** to prevent wireless clients of this Wi-Fi from communicating with each other.

You can enable **Guest Isolation** in **Guest Wi-Fi** to enable wireless clients on the Guest Wi-Fi to access the Internet, and to prevent them from accessing the intranet and from communicating with each other.

Advanced Settings ▾

Effective Time ▾

Effective Time ▾ (This Wi-Fi can only be used during the effective period.)

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

Guest Isolation (Prohibit local access.)

- **Speed Limit:** You can set a rate limit for the Guest Wi-Fi.

You can enable **Speed Limit**, and set the **Maximum Up Rate** and **Maximum Down Rate**.

Guest Wi-Fi

Enable

Dual-Band Single SSID
The 2.4G and 5G bands use the same SSID.

* SSID

Security ▾

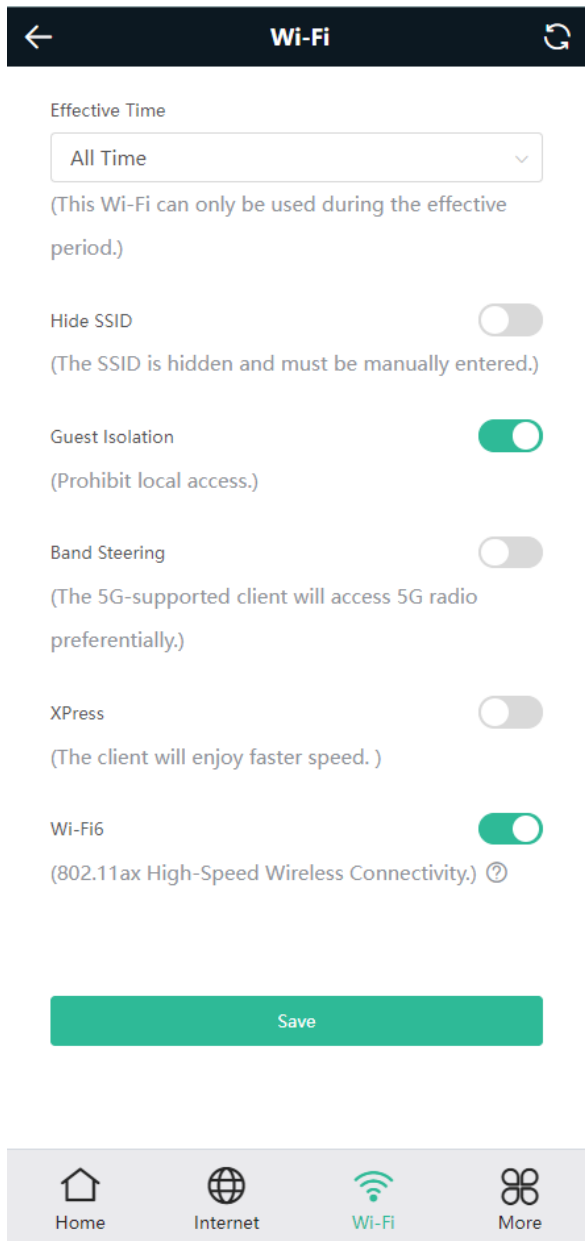
* Wi-Fi Password

Speed Limit

* Maximum Up Rate Kbps

* Maximum Down Rate kbps

- **Wi-Fi6:** You can enable Wi-Fi6 to enjoy high-speed Internet access.



2.4.3 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.



2.5 Configuring the Wi-Fi Blocklist or Allowlist

2.5.1 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.

2.5.2 Configuration Steps

Mobile Phone View: Choose **More > Switch to PC view > More >  WLAN > Blocklist/Allowlist.**

PC View: Choose **More >  WLAN > Blocklist/Allowlist.**

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

In the pop-up 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, and it 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.

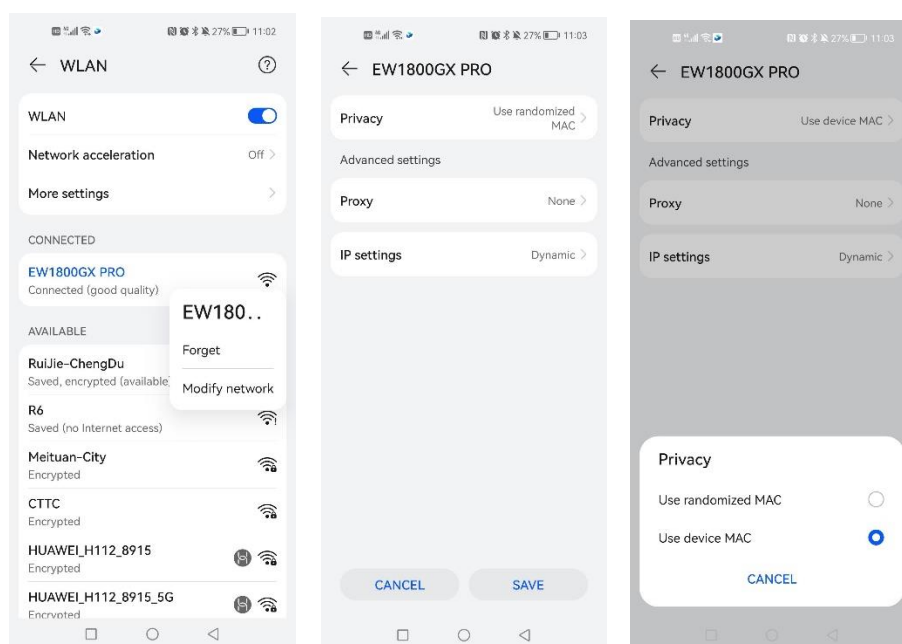
Caution

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

Note

To use this function, you must disable the randomized MAC address on the mobile device. The following example shows how to disable the randomized MAC address on an Android device.

Open the WLAN page of your device, press and hold the SSID broadcast by the router, and then choose **Modify network > Privacy > Use device MAC** to complete the configuration.



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

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

Blocked WLAN Clients + Add Batch Delete

Up to **64** members can be added.

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

Add ×

* MAC

Remark

Cancel OK

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

Blocked WLAN Clients + Add Batch Delete

Up to **64** members can be added.

<input type="checkbox"/>	MAC	Remark	Action
<input type="checkbox"/>	F2:11:34:23:56:21	test	Edit Delete

2.6 Optimizing the Wi-Fi Network

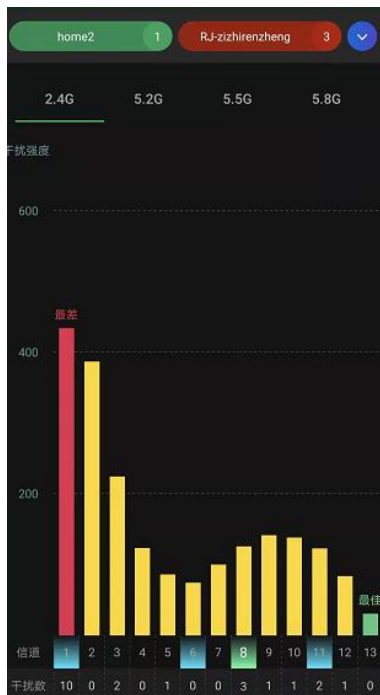
2.6.1 Overview

The device detects the surrounding wireless environment and selects the appropriate configuration upon power-on. However, network stalling caused by wireless environment changes cannot be avoided. Restarting the router is a convenient and effective method to cope with network stalling. The router supports scheduled restart. For

details, see [5.6 Configuring Scheduled Reboot](#). You can also analyze the wireless environment around the router and select appropriate parameters.

2.6.2 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.



2.6.3 Configuration Steps

- Optimizing the radio channel

Mobile Phone View: Choose **More** > **Channel Transmit Power**.

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

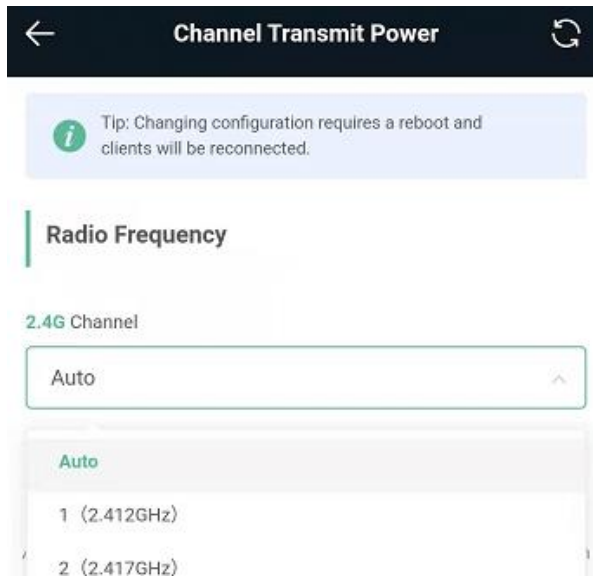
Choose the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. Excess clients connected to a channel can bring stronger wireless interference.

Note

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

Caution

The Wi-Fi network will restart after the radio channel is changed. Therefore, exercise caution when performing this operation.



- Optimizing the channel bandwidth

Mobile Phone View: Choose **More** > **Country(Region)/Channel Bandwidth**.


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

If the interference is severe, choose a lower channel bandwidth to avoid network stalling. You can select 20MHz and 40MHz bandwidths for the 2.4GHz band, or 20MHz, 40MHz, 80MHz and 160MHz for the 5GHz band. The default value is "Auto", indicating that the bandwidth will be automatically selected based on the wireless environment.

 **Note**

Only EW3000GX-PRO and EW6000GX-PRO routers support the 160MHz bandwidth for the 5GHz band.

The Wi-Fi network speed is more stable when the channel bandwidth is smaller, and a larger channel bandwidth makes the device more prone to interference. You are advised to select 20MHz bandwidth for the 2.4GHz band. After changing the channel bandwidth, click **Save** to make the configuration take effect immediately.

 **Caution**

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

← **Country(Region)/Channel Bandwidth** ↻

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

Radio Frequency

Country/Region

China (CN)
▼

2.4G Channel Bandwidth


Auto
^


Auto


20MHz


40MHz

Save


Home


Internet


Wi-Fi


More

- Optimizing the transmit power

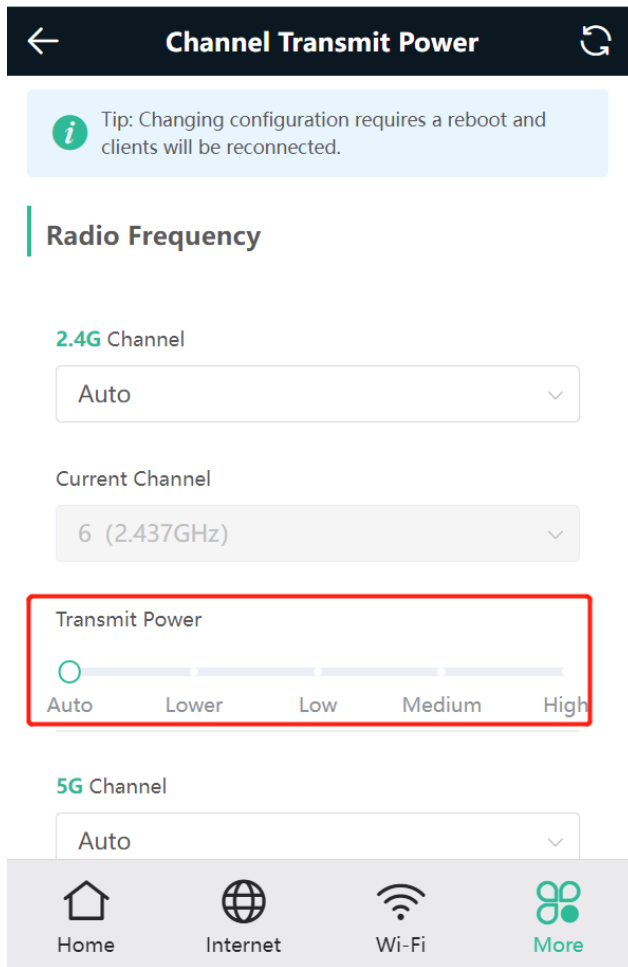
Mobile Phone View: Choose **More** > **Channel Transmit Power**.

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

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

⚠ **Caution**

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



2.7 Configuring the Healthy Mode

Mobile Phone View: Choose **More** > **Healthy Mode** > **Healthy Mode**.

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


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

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

Note

All Mesh 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 be rest assured to use them.

← **Healthy Mode** ↻

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

Healthy Mode

Enable

Effective Time

All Time ▾

Save

Home Internet Wi-Fi More

3 Networks Settings


3.1 Configuring Internet Connection Type


Mobile Phone View: Choose **Internet**.

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

The router supports three Internet connection types: PPPoE, DHCP, and static IP. For details, see [1.4 Primary Router Mode](#).

For PPPoE and DHCP Internet connection types, you can manually configure a DNS.

 **WAN**

 Online (DHCP)

* Internet

No username or password is required for DHCP clients.

DNS Type Dynamic Custom

DNS Server

IP 172.17.96.147

Subnet Mask 255.255.254.0

Gateway 172.17.96.1

[Advanced Settings](#) ▾

i WAN

i Online (DHCP)

* Internet

* Username

* Password 👁

Service Name

i Forgot Username and Password?

Obtain the username and password by [contacting the ISP](#) or [from the old device](#).

DNS Type Dynamic Custom

DNS Server

IP 172.17.96.147

Subnet Mask 255.255.254.0

Gateway 172.17.96.1

Advanced Settings ▼

Save

3.2 Changing the Address of a LAN Port

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

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

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

Caution

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

LAN Settings DHCP Clients Static IP Addresses DHCP Option DNS Proxy

LAN Settings ⓘ

* IP

* Subnet Mask

* MAC

DHCP Server

* Start

* IP Count


* Lease Time(Min)

Save


3.3 Changing the MAC Address

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

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

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

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

If you want to change the MAC address of the LAN port, choose  **Basics** > **LAN**.

Caution

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

Figure 3-1 WAN Port Settings

WAN

Online (DHCP)

* Internet

No username or password is required for DHCP clients.

DNS Type Dynamic Custom

DNS Server

IP 172.17.96.147

Subnet Mask 255.255.254.0

Gateway 172.17.96.1

Advanced Settings ^

* MTU

* MAC

802.1Q Tag

Save

3.4 Changing the MTU

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

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

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

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

WAN

Online (DHCP)

* Internet

No username or password is required for DHCP clients.

DNS Type Dynamic Custom

DNS Server

IP 172.17.96.147

Subnet Mask 255.255.254.0

Gateway 172.17.96.1

Advanced Settings ^

* MTU

* MAC

802.1Q Tag

Save

3.5 Configuring IPv6 Address

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

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

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

3.5.1 Configuring the IPv6 Address of the WAN Port

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

Enable

WAN Settings LAN Settings DHCPv6 Clients

WAN_V6

* Internet

No username or password is required for DHCP clients.

DNS Type Dynamic Custom

DNS Server

IPv6 Address

IPv6 Prefix

Gateway

NAT66

Save

3.5.2 Configuring the IPv6 Address 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 Address/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.

Enable

WAN Settings LAN Settings DHCPv6 Clients

IPv6 Assignment Auto

IPv6 Address/Prefix
Length

Advanced Settings

Subnet Prefix Name Default

Subnet Prefix Length

Subnet ID

* Lease Time(Min)

DNS Server

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

Enable


WAN Settings LAN Settings DHCPv6 Clients

DHCPv6 Clients
You can view the DHCPv6 clients information on this page.

DHCPv6 Clients

No.	Hostname	IPv6 Address	Remaining Lease Time(min)	DUID
-----	----------	--------------	---------------------------	------

3.6 Enabling Parental Control

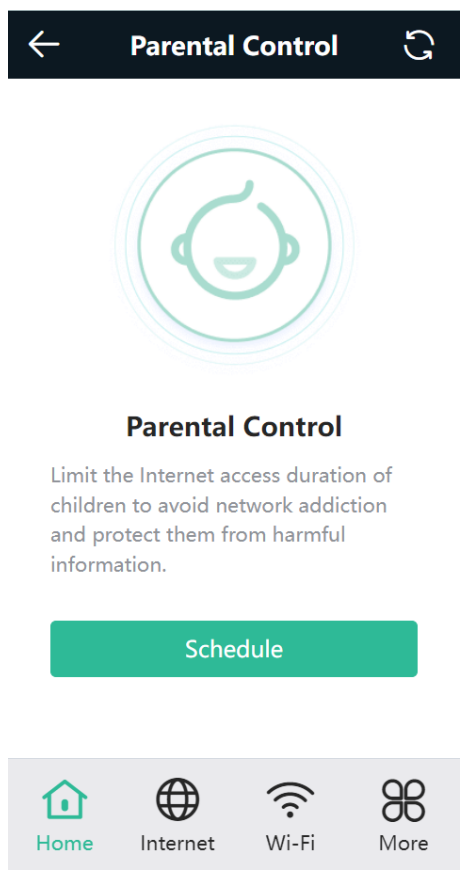
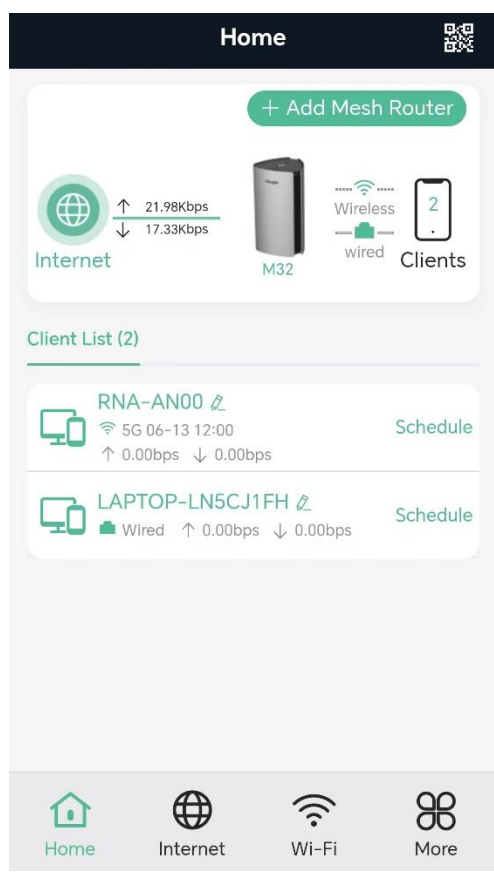
Mobile Phone View: Choose **Home** > **Schedule** or 

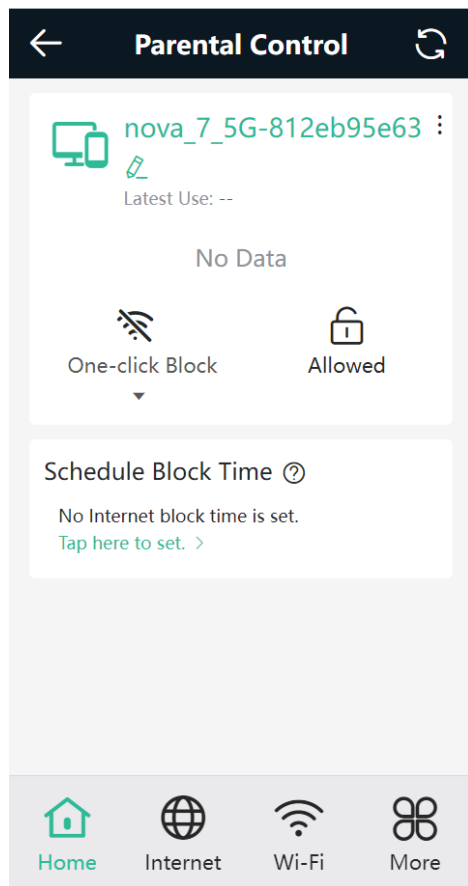
PC View: Choose **Clients** > **Blocked Time Management**.

 **Caution**

- This function is supported only in router mode.
- You can only set Internet block periods using a browser on your computer. To block apps and websites, use the client app on your mobile phone.

Select a client and tap **Schedule**. Then, you can view the Internet access details. You can also set the Internet block periods.



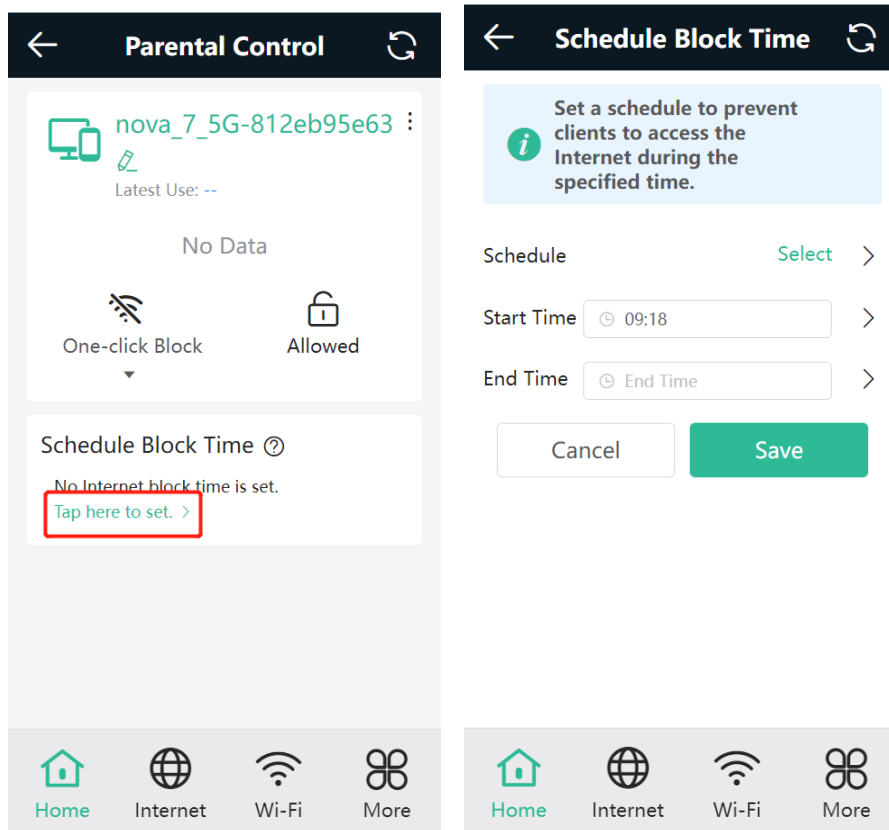


3.6.1 Setting the Internet Block Periods

1. Setting the Internet Block Rules

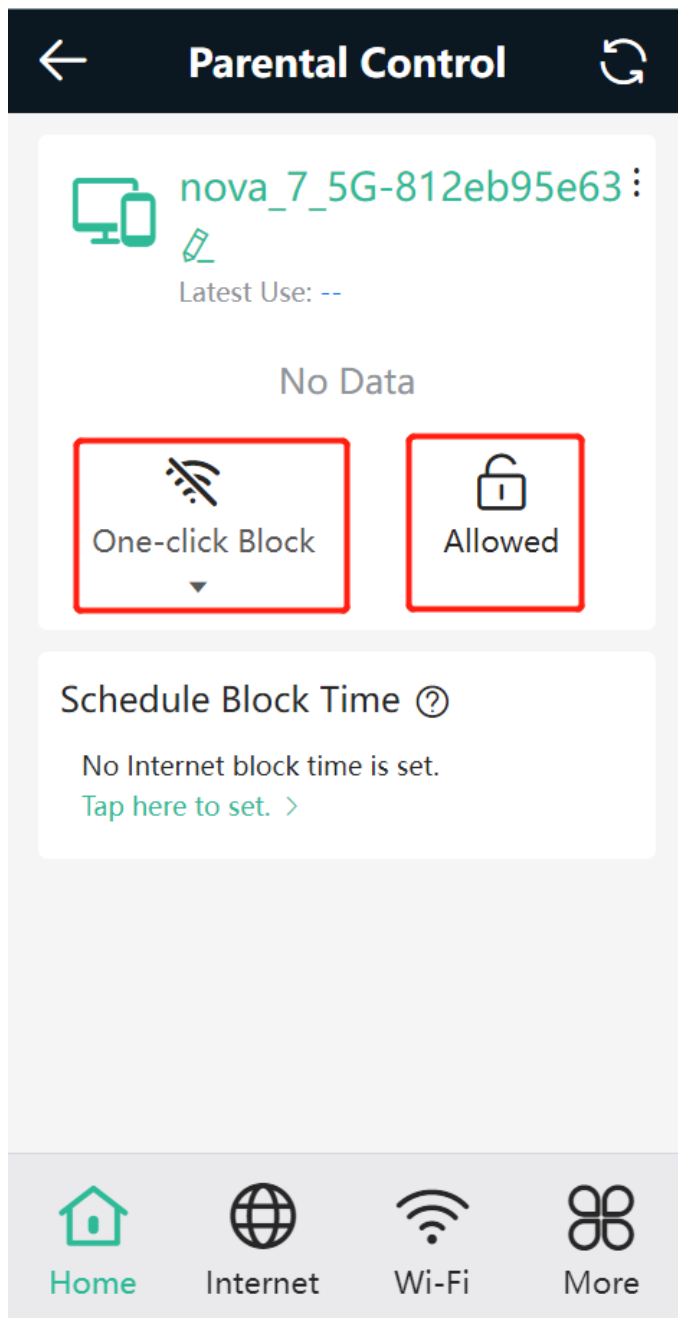
Tap **Tap here to set** to set the Internet block periods. In the block periods, the client cannot access the Internet.

You can select certain days of the week or customize the Internet block periods.



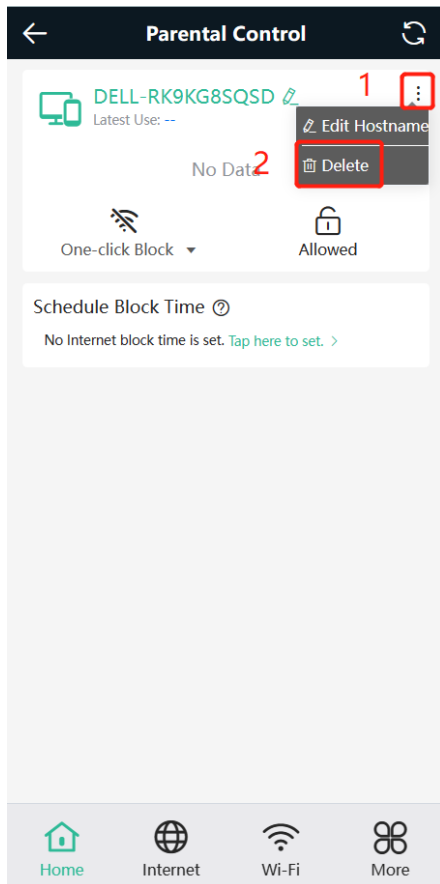
2. Blocking Internet Access Temporarily

- Tap **One-click Block** and select a period to block the client from accessing the Internet temporarily.
- Tap **Allowed** to lift all Internet access restrictions imposed on the client on the current day. The lifting operation is valid only on the current day. The restrictions will be resumed the next day.



3.6.2 Disabling Parental Control

To disable parental control, tap **Delete** in the upper right corner to lift the restrictions on the client.

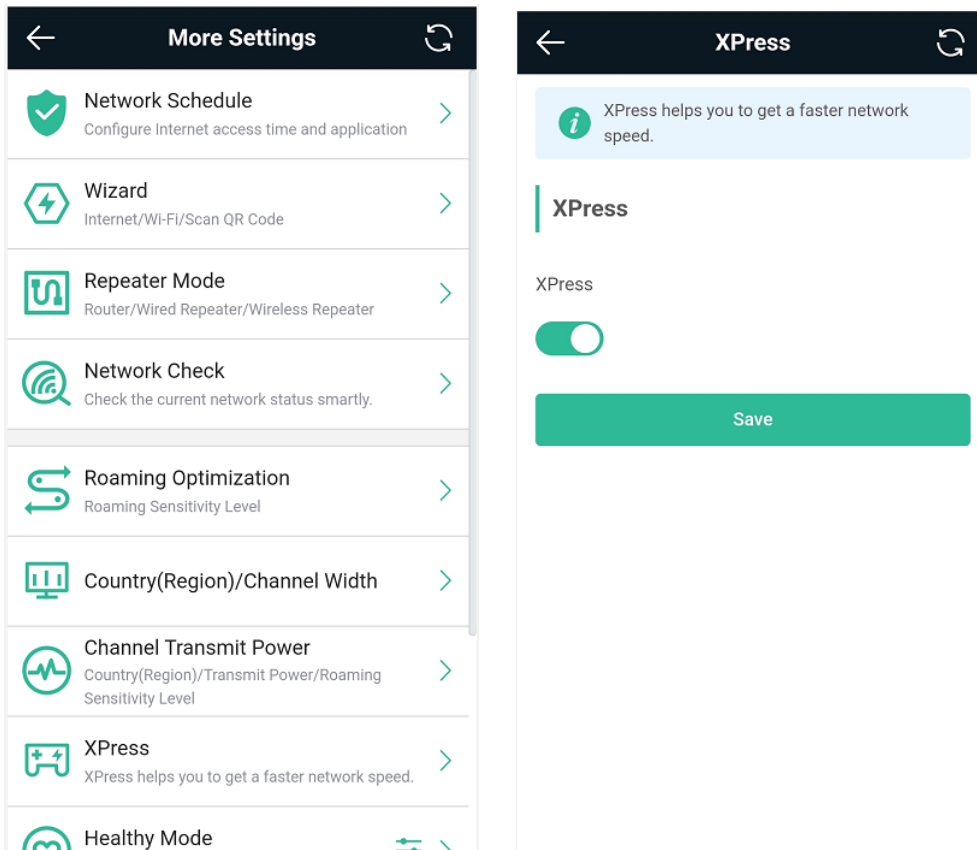


3.7 Configuring XPress

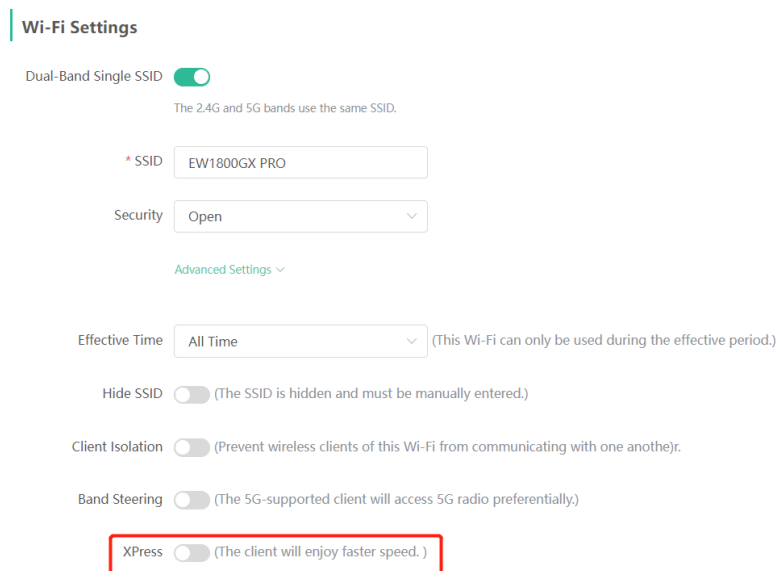
Mobile Phone View: Choose **More** > **XPress**.

PC View: Choose **More** > **WLAN** > **Wi-Fi** > **Wi-Fi Setting** > **Advanced Settings** > **XPress**.

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



In the PC view, turn on **XPress** as follows.



3.8 Configuring Port Mapping

3.8.1 Overview

- Port mapping maps the IP address of a device on the LAN to an external network in the form of a combination

of a WAN IP address and 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 in the home network for Internet access, port mapping or demilitarized zone (DMZ) needs to be configured.
- Port mapping maps the WAN port IP address of a router to an internal network host and port so that Internet users can proactively access hosts on the LAN.
- DMZ forwards all packets from the Internet to DMZ hosts to provide the Internet access service.

3.8.2 Getting Started

- Confirm the IP address of the target device in the internal network and service port ID.
- Ensure that port mapping is available in the internal network.
- Verify that your router has a public IP address. If the IP address is dynamic, changing it may cause port mapping failure. In this case, you are advised to use a dynamic domain name service (DDNS) to resolve any potential IP changes.

3.8.3 Configuration Steps

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

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

Click **Add**. In the pop-up 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 you are not sure of the service, 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 end must be consistent with that on the client end.

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 Server IP: Enter the LAN IP address used by external networks to access the device, such as the IP address of an IP camera.

Internal Port/Range: Enter the port number used by an application accessed by external networks, such as port 8080 used by the Web service.

The screenshot displays the 'Port Mapping' configuration page under 'NAT-DMZ'. The main area shows a 'Port Mapping List' with an '+ Add' button highlighted in red. Below the list, it states 'Up to 50 entries can be added.' The table has columns for Name, Protocol, External IP Address, and External Port, but it is currently empty with 'No Data' displayed. At the bottom, there are navigation controls showing page 1 of 1 and a total of 0 entries.

The 'Add' modal form on the right contains the following fields:

- * Name: [Text input field]
- Preferred Server: HTTP (dropdown menu)
- Protocol: TCP (dropdown menu)
- External IP Address: 172.17.96.147
- * External Port/Range: Example: X or X-X (Range: 1-6553!)
- * Internal Server IP: Example: 1.1.1.1
- * Internal Port/Range: 80

Buttons for 'Cancel' and 'OK' are located at the bottom right of the modal.

3.8.4 Verification and Testing

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

3.8.5 Solution to a Test Failure

- (1) Use a new external port number and perform a test again. The test often fails on the ports blocked by firewalls of some ISPs.
- (2) Enable the remote access permission on the server. The common cause is that remote access is disabled on the server by default. As a result, the internal network access is successful but the access across different network segments fails.
- (3) Enable the DMZ service. For details, see [3.8.6 DMZ Configuration Steps](#). The common cause is that port configuration is incorrect or incomplete.

3.8.6 DMZ Configuration Steps


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

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

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

Port Mapping

NAT-DMZ

 NAT-DMZEnable

* Dest IP Address

Example: 1.1.1.1

Please enter a destination IP address.

Save

3.9 Configuring DHCP Server

3.9.1 Overview

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

3.9.2 Configuration Steps

1. Configuring the DHCP Server Function

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

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

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

Caution

If the DHCP server function is disabled on all routers in the network, clients cannot automatically obtain IP addresses. 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 period. When a client keeps connected, the lease is automatically renewed. If a lease is not renewed due to the client disconnection or network instability, the IP

address will be reclaimed after the lease period expires. After the client connection is restored, the client requests an IP address again. The default lease period is 120 minutes.

LAN Settings DHCP Clients Static IP Addresses DHCP Option DNS Proxy

i LAN Settings

* IP

* Subnet Mask

* MAC

DHCP Server

* Start

* IP Count

* Lease Time(Min)

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**. Then, the client obtains the IP address each time connecting to the router.

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

i View DHCP clients. ?

DHCP Clients Search by Hostname/IP/MAC

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

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

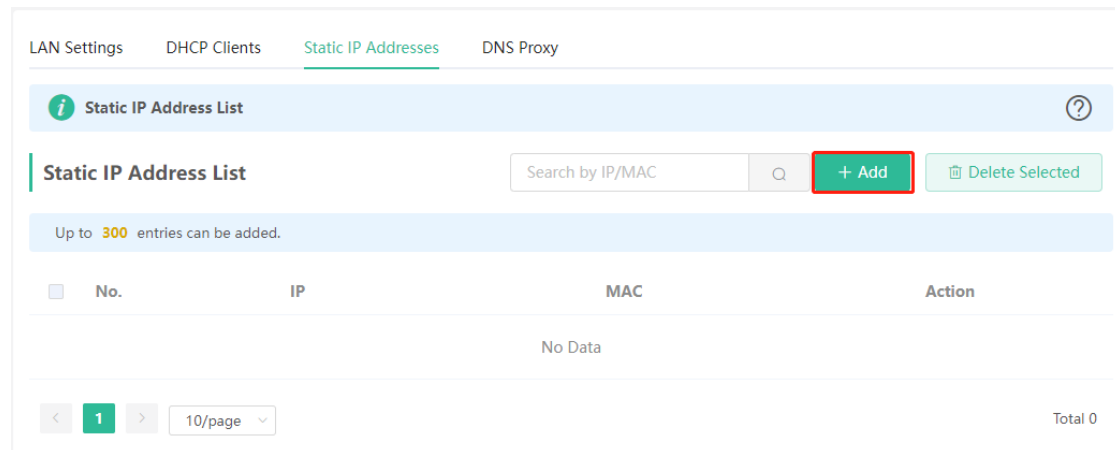
< **1** > 10/page Total 3

3. Displaying the DHCP Static IP Address Table

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

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

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



3.10 Configuring DNS

The domain name system (DNS) proxy configuration is not mandatory. The device obtains the DNS server address from the uplink device by default.


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

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

DNS Proxy: The function is disabled by default and the DNS delivered by a carrier is used. If the DNS is incorrectly configured, 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. After the DNS proxy function is enabled, you can enter the IP address of the DNS server. The available DNS service varies from region to region. You can consult the local ISP.

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

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

Enable

* DNS Server

Save

3.11 Configuring DHCP Option


Mobile Phone View: Choose **More** > **Switch to PC view** > **More** >  **Basics** > **LAN** > **DHCP Option**.

PC View: Choose **More** >  **Basics** > **LAN** > **DHCP Option**.

Enter the DNS address provided by the ISP, and click **Save**.

The DHCP Option settings are applied to all LAN ports. The **DHCP Option** configuration is optional.

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

 **DHCP Option**
DHCP option settings are applied to all LAN ports.

DNS Server

Save

3.12 Configuring DDNS

3.12.1 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 Dyn DNS, and No-IP DNS.

3.12.2 Getting Started

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


3.12.3 Configuration Steps

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

PC View: Choose **More** >  **Advanced** > **Dynamic DNS**


If you select **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.

No-IP DDNS DynDNS

 **DynDNS**

* Username [Register](#)

* Password

* Domain 

Link Status -

3.13 Configuring APR Binding


3.13.1 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.

3.13.2 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**.

Bind the MAC address and IP address on the LAN, that is, ARP binding.

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

ARP List

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

<input type="checkbox"/>	No.	MAC	IP	Type	Action
<input type="checkbox"/>	1	c0:b8:e6:f8:8d:7c	172.17.96.1	Dynamic	Bind
<input type="checkbox"/>	2	c0:25:a5:81:c1:90	172.17.96.49	Dynamic	Bind

Total 2 Go to page

3.14 Connecting to IPTV

IPTV is an Internet television service provided by ISP.

3.14.1 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 local IPTV is of the VLAN type, confirm the VLAN ID. If you are not sure of the IPTV type, contact your local ISP.

3.14.2 IPTV Configuration Steps (VLAN Type)

Mobile Phone View: Choose **More** > **IPTV**.

PC View: Choose **More** > **Basics** > **IPTV**.

Click to enable IPTV, and select the LAN port to be connected to the IPTV STB.

Click to enable VLAN, and enter the designated VLAN ID for IPTV provided by the ISP.

After the configuration, confirm that the IPTV STB is connected to the specified port properly. Take the following figure as an example, connect the IPTV STB to LAN1.

Caution

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

IPTV/VLAN

IPTV/IGMP

WIFI/IGMP

i **IPTV**
Provide Internet access and IPTV services through only one Ethernet cable.

IPTV/VLAN

IPTV

IPTV Port Connect the default or configured IPTV port .

DC	IPTV	LAN2	LAN3	LAN4	WAN

VLAN

* **IPTV VLAN ID**

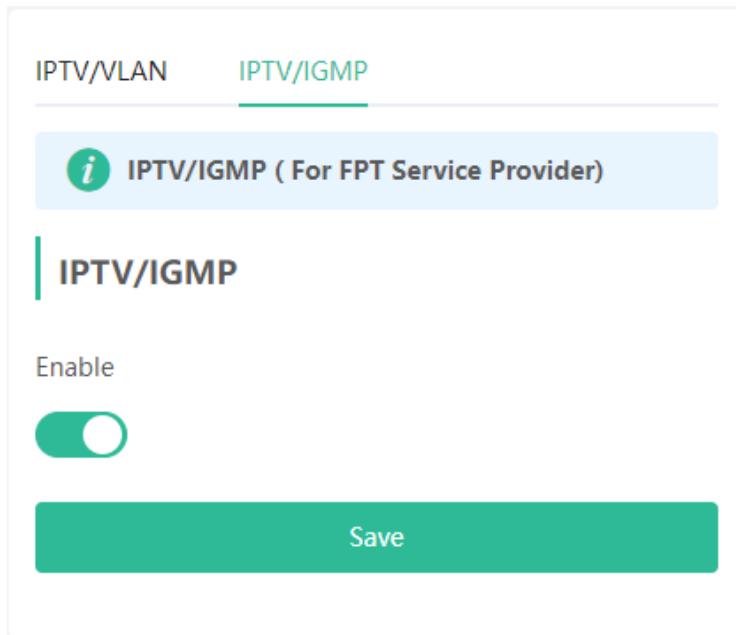
Save

3.14.3 IPTV Configuration Steps (IGMP Type)

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

PC View: Choose **More** > **Basics** > **IPTV**.

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



3.15 Configuring WIFI/IGMP

3.15.1 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.

3.15.2 Configuration Steps

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

Click M2U(5G) to enable WIFI/IGMP for 5G wireless clients.

IPTV/VLAN

IPTV/IGMP

WIFI/IGMP



WIFI/IGMP

WIFI/IGMP

M2U (2.4G) M2U (5G)

Save

3.16 Enabling Hardware Acceleration

Mobile Phone 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.

Hardware Acceleration



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

Enable



Save

Caution

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

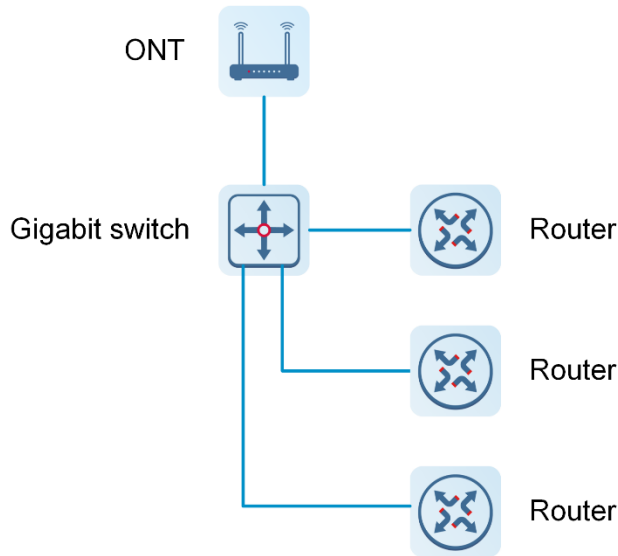
3.17 Configuring Reyee Mesh 3.0

3.17.1 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**

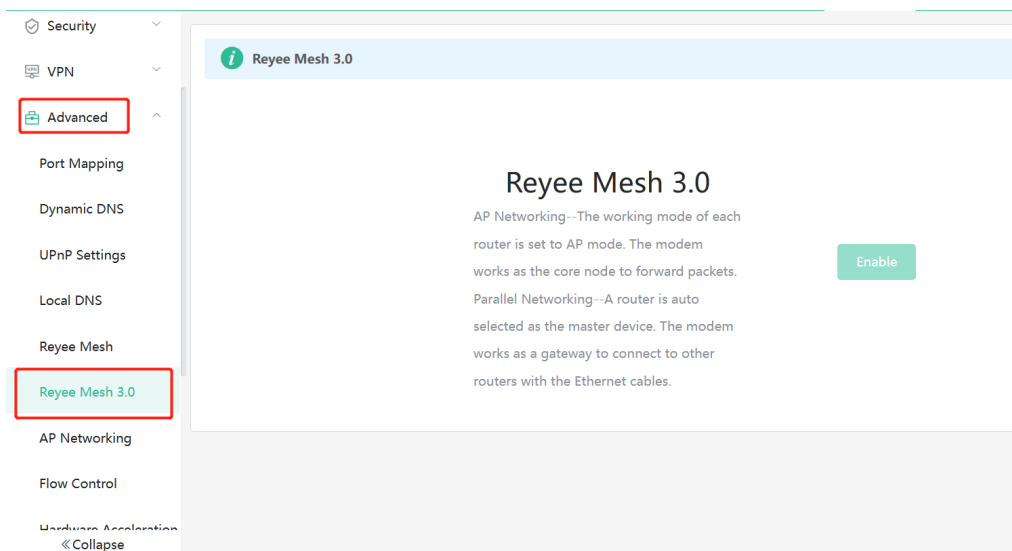
Connect the routers as indicated in the following figure:



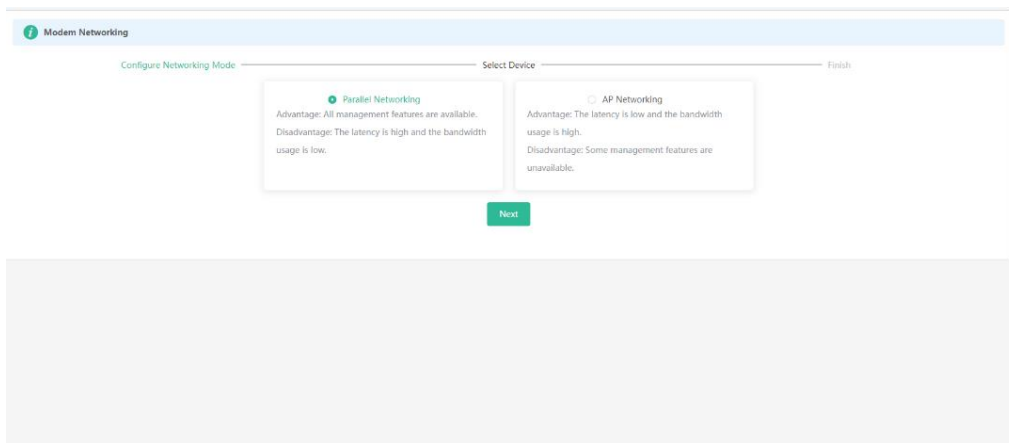
1. Parallel Networking

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.

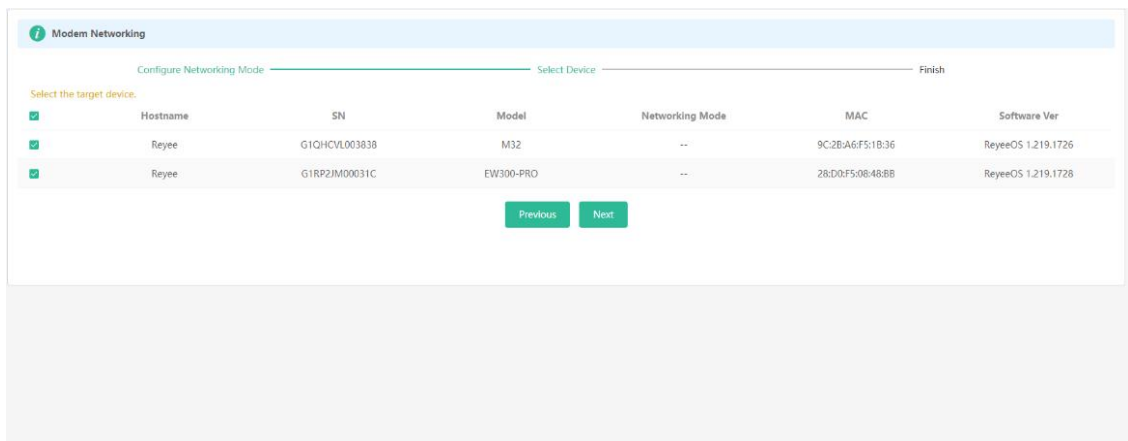
(1) Click **Enable** to enable Reyee Mesh 3.0.



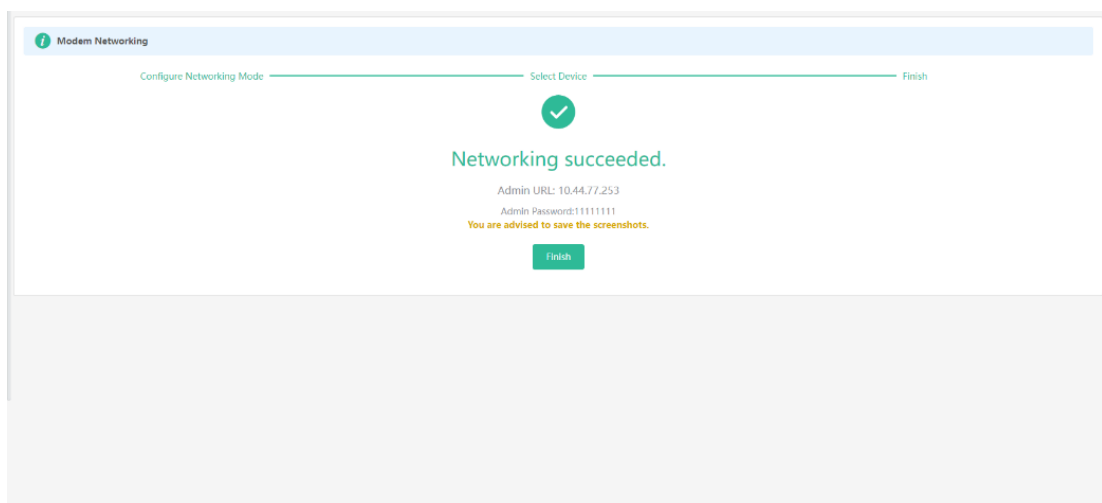
(2) Choose **Parallel Networking**, and click **Next**.



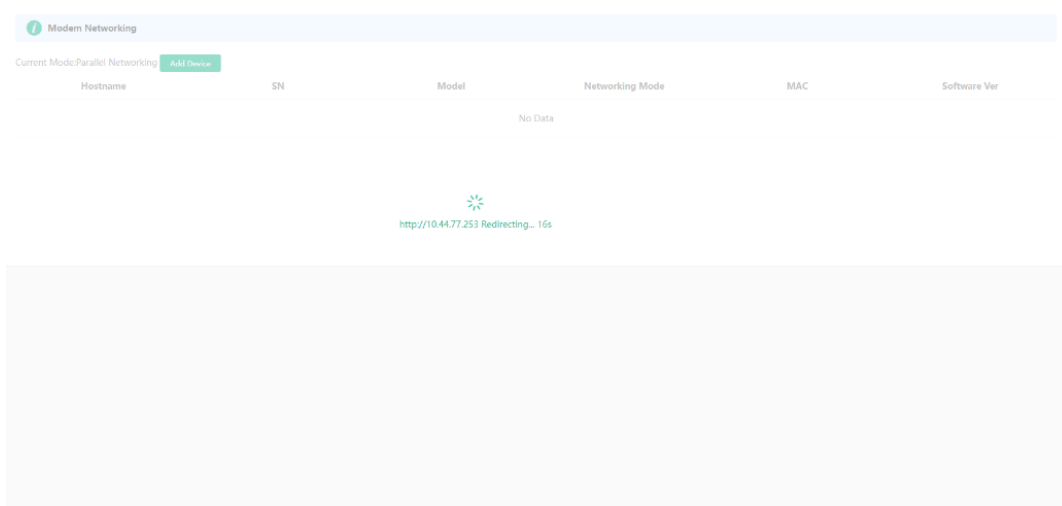
(3) Check routers for the networking.



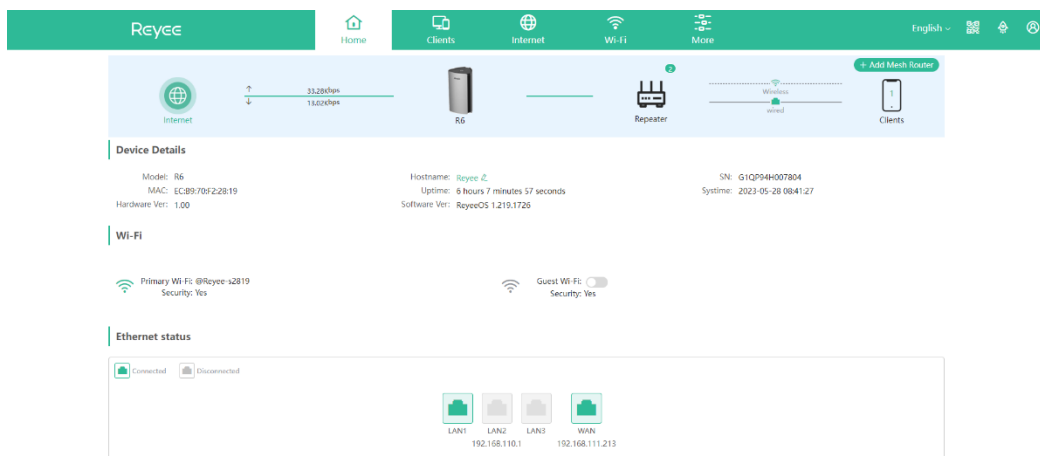
(4) Click **Next**.



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



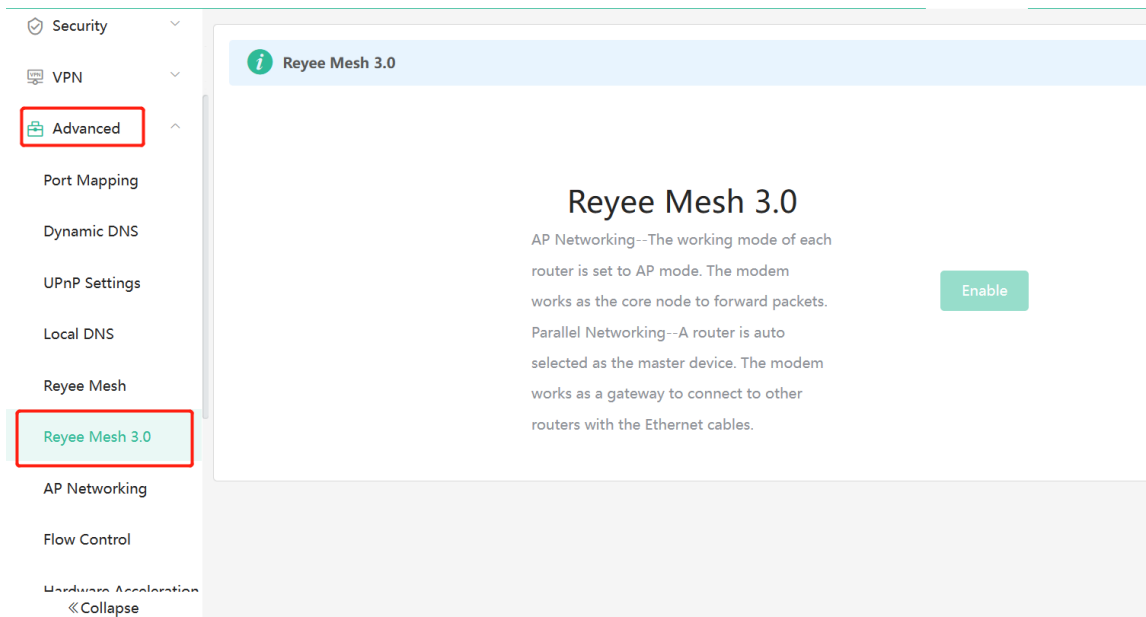
(6) On the master router page that is displayed, enter the password to log in.



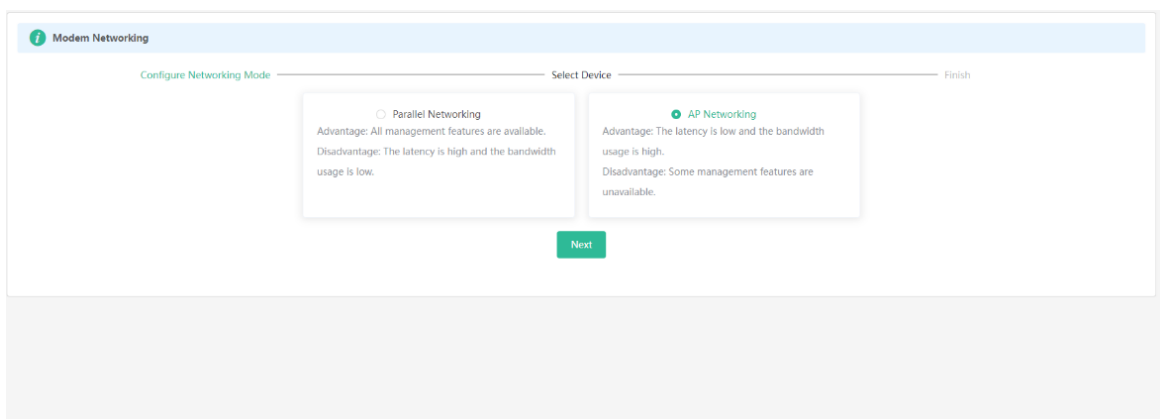
2. AP Networking

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.

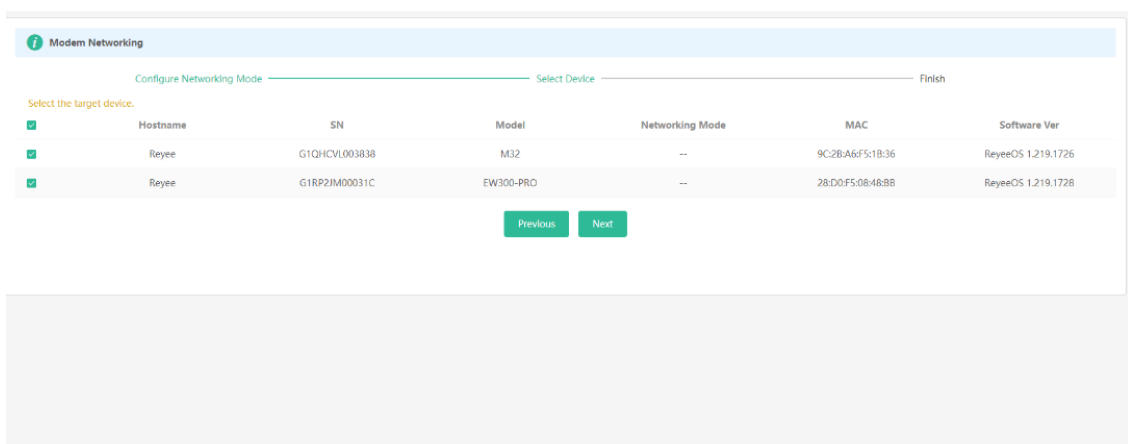
(1) Click **Enable** to enable Reyeec Mesh 3.0.



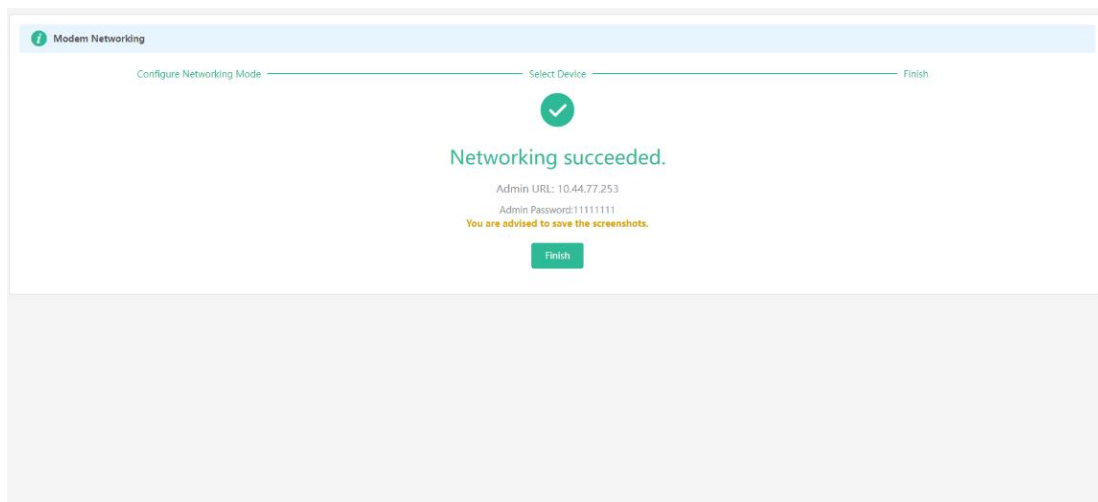
(2) Choose **AP networking**, and click **Next**.



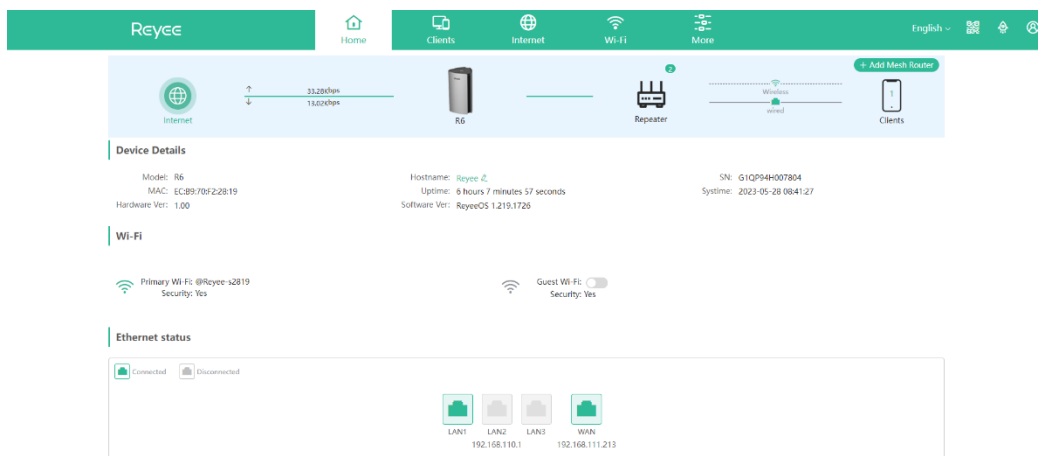
(3) Check routers for AP networking, and click **Next**.



(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.

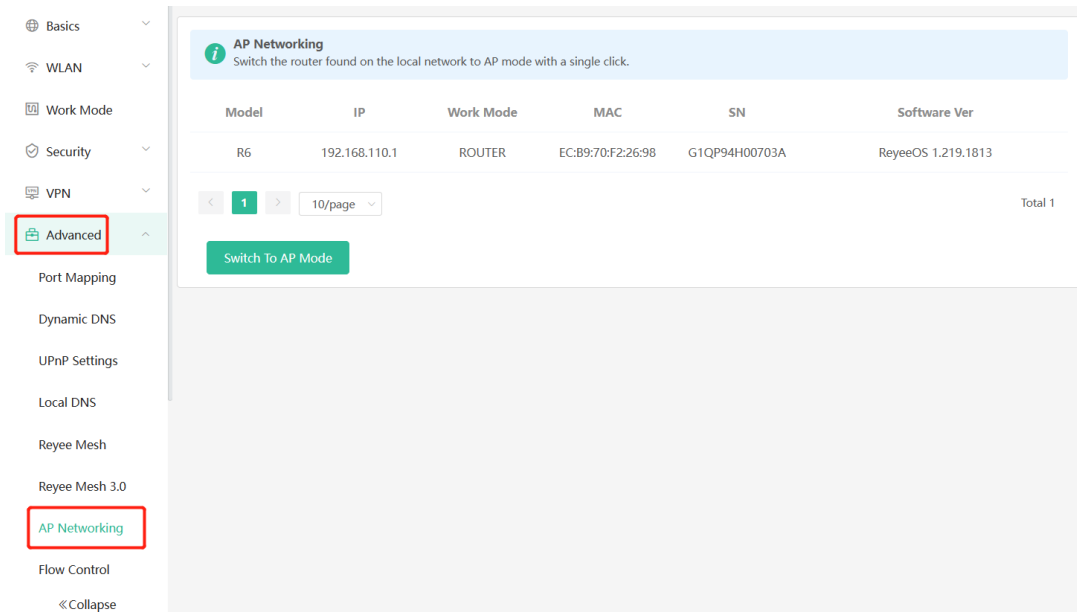


3.18 Configuring AP Networking

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

Mobile Phone 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.



3.19 Enabling CWMP

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

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

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.

2. Configuration Steps

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

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

CWMP

* Inform Interval

* ACS Address

* ACS Account

* ACS Password

STUN

* STUN Server Address

* STUN Server Port

* STUN Server Account

* STUN Server Password

3.20 Enabling Smart Flow Control

Mobile Phone 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.

Smart Flow Control Custom Policy

Smart Flow Control
Intelligently adjust the network speed to ensure that each user shares the network fairly.

Enable **If you want to test the WAN rate, disable smart flow control first.**

WAN Bandwidth * Up Mbps * Down Mbps

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.

Smart Flow Control Custom Policy

Custom Policy
Allocate bandwidth to the specified IP address or range. The priority is sorted as follows: Custom Policy > Smart Flow Control. (?)

Policy List

Up to 30 entries can be added.

<input type="checkbox"/>	Policy Name	IP / IP Range	Bandwidth Type	Uplink Rate
				No Data

Add
×

* Policy Name

* IP / IP Range

Bandwidth Type ▾

Uplink Rate * CIR * PIR ⓘ

Downlink Rate * CIR * PIR ⓘ


Status

3.21 Enabling Port-Based Flow Control

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

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

Port-based flow control can relieve the data congestion caused by ports at different speeds and improve the network speed.

 **Port Flow Control**
Port Flow Control can mitigate the data congestion caused by ports at different speeds and improve the network speed.

Enable

Save

3.22 Performing Advanced Network Settings

Mobile Phone 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.

Other Settings

Enable Advanced [?](#)
Firewall

Disable ICMPv6 Error
Messages

- Destination Unreachable
- Datagram Too Big
- Time Exceeded
- Parameter Problem

Save

3.23 Configuring UPnP

3.23.1 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 faster or more stably. Common applications that support UPnP include MSN Messenger.

3.23.2 Configuration Steps

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

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

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

 **UPnP Settings**
UPnP (Universal Plug and Play) UPnP is a new Internet protocol aimed at improving communication between devices. 

Enable

UPnP List

Protocol	App	Client IP Address	Internal Port	External Port
No UPnP Device				

3.24 Configuring Connectivity detection

Mobile Phone 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.

The screenshot shows a web-based configuration interface. On the left is a sidebar menu with the following items: VPN, Advanced (highlighted with a red box), Port Mapping, Dynamic DNS, UPnP Settings, Local DNS, Reeye Mesh, Reeye Mesh 3.0, AP Networking, Flow Control, Hardware Acceleration, Port Settings, and Connectivity detection (highlighted with a red box). Below the menu is a '« Collapse' button. The main content area is titled 'Connectivity detection' and contains the following settings:

- * Reachable Check: 120 seconds (Period)
- * Unreachable Check: 5 seconds (Period)
- * URL List:
 - http://www.amazon.com (Add)
 - http://www.google.cc (Delete)
 - http://www.yahoo.co (Delete)
 - http://wikipedia.org (Delete)
 - http://www.msn.com (Delete)

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

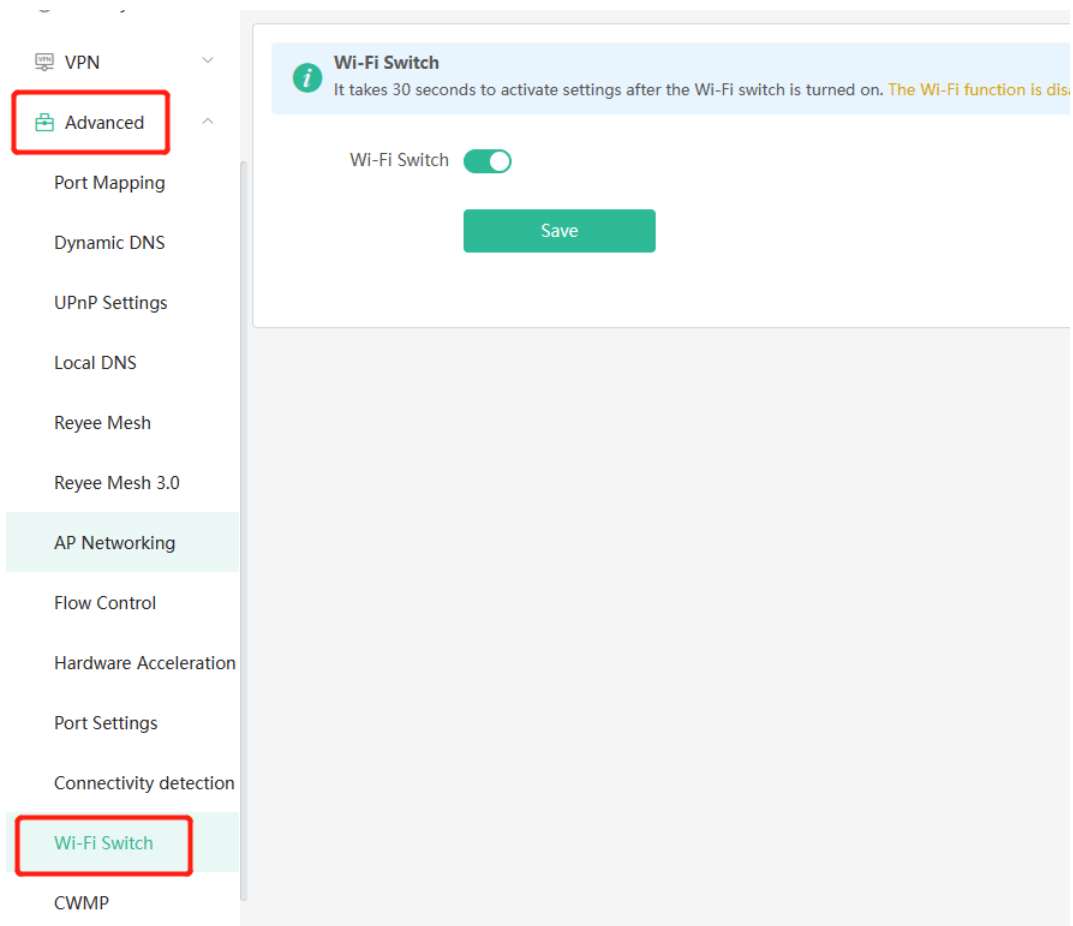
3.25 Enabling Wi-Fi Switch

Mobile Phone 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.



3.26 Configuring PPTP VPN

3.26.1 Overview

The device can support 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.

3.26.2 Configuring PPTP Server

Note

This feature is not supported on RG-EW300 PRO, RG-EW1200G PRO and RG-EW1200 routers.

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

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

1. Click **Enable** to enable the function of PPTP and select **Server**.

Local Tunnel IP: 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 dialing in.

VPN Subnet/Netmask: Enter the range of IP addresses. The IP addresses in this range will be assigned to clients.

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

MPPE: Use MPPE to encrypt PPTP tunnels. By default, encryption is not enabled on the server. Once MPPE is enabled, the Internet speed will slow down. You are advised to disable MPPE if you don't have specific security requirements.

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

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

PPTP Settings Tunnel List

i PPTP Settings

Enable

PPTP Type Server Client

* Local Tunnel IP

* VPN Subnet/Netmask ?

* DNS Server

MPPE Disable Enable

* PPP Hello Interval seconds

Save

2. Add the PPTP user.

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

Select the network mode. **PC to Router** indicates the dial-in mode from PC to router. **Router to Router** indicates the dial-in mode from router to router.

Enable **Status** and click OK.

VPN Client List Username/Password

Up to 30 entries can be added.

	Username	Password	Network Mode	Status	Action
No Data					

Add User×

* Username

* Password 👁

Network Mode ▾

Status

3.26.3 Configuring PPTP Client

Note

This feature is not supported on RG-EW300 PRO and RG-EW1200 routers.

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

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

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

Tunnel IP: It is the virtual IP address used to create the 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 that does not cause conflicts.

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

Peer Subnet: Enter the target network segment of the server, which cannot be the same as that of the client.

Work Mode: The **NAT** mode only allows the 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** and the device will send the VPN tunnel request to the WAN port.

PPTP Settings Tunnel List

PPTP Settings

Enable

PPTP Type Server Client

* Username

* Password

Interface

Tunnel IP Dynamic Static

* Server Address

* Peer Subnet

MPPE Disable Enable

Work Mode NAT Router

* PPP Hello Interval seconds

Save

3.27 Configuring OpenVPN

3.27.1 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.

3.27.2 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 3-2 Configuring OpenVPN Server

The screenshot displays the 'OpenVPN' configuration page. At the top, there are tabs for 'OpenVPN' and 'Tunnel List'. Below this is a blue header bar with an information icon and the text 'OpenVPN'. The main configuration area includes:

- An 'Enable' toggle switch that is turned on.
- 'OpenVPN Type' with radio buttons for 'Server' (selected) and 'Client'.
- 'Server Mode' dropdown menu set to 'Account'.
- 'Protocol' dropdown menu set to 'UDP'.
- '* Server Address' text input field containing 'IP/Domain'.
- '* Port ID' text input field containing '1194', with a range indicator '1-65535' to its right.
- '* VPN Subnet/Netmask' text input field containing '10.80.12.0/24', with a help icon to its right.
- 'Client will access' radio buttons for 'Lan only' (selected) and 'LAN and Internet'.

A dashed line with the word 'Expand' is positioned below these settings. Underneath, there are three green buttons: 'Export' for 'OpenVPN configuration', 'Export' for 'CA Certificate', and a larger 'Save' button at the bottom.

- (4) (Optional) Advanced settings.

Click **Expand** to perform the following advanced settings, 若无特殊需求可保持默认. If there are no special requirements, use the default settings, as shown in the following figure.

Collapse

TLS Authentication ?

Allow Data Compression ?

Cipher ?

Deliver DNS ? +

Authentication

- (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 3-1 Configuration Items of OpenVPN Server Mode

Item	Description
Server Mode	<p>The device supports Account, Certificate and Account & Certificate authentication modes:</p> <ul style="list-style-type: none"> ● 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.
Protocol	<p>All communication on OpenVPN is based on a single IP port, using UDP or TCP protocols.</p> <p>The default value is UDP. You can select TCP for higher performance. TCP protocol can be used to improve the stability of VPN channels in high latency or unstable network conditions.</p>
Server Address	The server address used for client docking, which can be a domain name.
Port ID	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 Lan Only or LAN and Internet

Item	Description
	<ul style="list-style-type: none"> ● Lan only: The client can only access the LAN segment on the server. ● LAN and Internet: 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.
OpenVPN configuration	You can click Export to export the parameter configuration tar tar file of the client connected to the server. After decompression, this file can be used to set up the OpenVPN client.
CA Certificate	Click Export to export VPN server credentials to verify the communication with clients.
TLS Authentication	TLS Authentication can enhance the security of OpenVPN. Once enabled, the client must import the TLS key. (The version of the peer OpenVPN client must be later than 2.40.)
Allow Data Compression	Once enabled, the device will compress the transmitted data to save bandwidth, but it will occupy a certain amount of CPU resources. This configuration must be consistent on the client and the server to avoid any potential connection failures.
CIPher	Encrypts the data to prevent it from being intercepted midway. The default encryption standard is AES-128-CBC. If the server is configured in auto mode, the client can be configured with any data encryption algorithm, which will be automatically matched by the server. If a specific encryption method is configured on the server, the client must be configured with the same encryption method. Otherwise, the connection between the server and the client cannot be established.
Deliver DNS	The information pushed by the server to the client's DNS. Currently only Windows clients are supported.
Authentication	The digest algorithm informed by the server to the client. The default value is SHA256.

2. Adding OpenVPN clients

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

Enable **Status** and click OK.

VPN Client List

Up to 30 entries can be added.

	Username	Password	Status	Action
No Data				

<
1
>

Total 0

Add User×


* Username

* Password 👁

Status

Cancel OK

3.27.3 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.

OpenVPN Tunnel List

i OpenVPN

Enable

OpenVPN Type Server Client

Server Mode Account & Certificate

* Username Username of OpenVpn user ?

* Password Password of OpenVpn user ?

* Client Config .ovpn Browse

Save

Table 3-2 Configuration Items of OpenVPN Client Web Setting Configuration Mode

Parameter	Description
Server Mode	The device supports Account, Certificate and Account & Certificate authentication modes: <ul style="list-style-type: none"> ● 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 username 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.

4 Configuring the Repeater Mode

4.1 Access Point

The access point mode relies on an Ethernet cable to provide reliable transmission over a more stable Wi-Fi network with less interference. You are advised to use the access point mode. Ensure that the primary router can access the Internet with DHCP server enabled. Otherwise, the configuration will fail.

Mobile Phone View: Choose **More > Switch to PC view > More > Work Mode**

PC View: **More >Work Mode**

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


Caution

Ensure that the primary router can access the Internet with DHCP server enabled. After the configuration is saved, the Wi-Fi network will be restarted, and clients need to reconnect to the Wi-Fi network.

Figure 4-1 Access Point Settings

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

Router **Access Point** Wireless Repeater WISP

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

Access Point

Check

Figure 4-2 After Clicking Check

Access Point

Status **Cable Plugged**

IP Address: 172.17.96.147

* Local Router

EW1800GX PRO

SSID(2.4G)

* Local Router SSID(5G)

EW1800GX PRO

Password

A blank value indicates no encryption.

Save

4.2 Wireless Repeater

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

Note

- The wireless repeater mode will affect the network speed and stability. You are advised to plug in an Ethernet cable and select the access point mode if an Ethernet cable is available.
- In the wireless repeater mode, unplug the WAN cable to prevent loops, which may cause network interruption.
- Obtain the SSID and Wi-Fi password of the primary router.

Mobile Phone View: Choose **More > Switch to PC view > More > Work Mode**

PC View: **More >Work Mode**

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

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

Router Access Point **Wireless Repeater** WISP



- This mode allows you to establish a wireless connection between the primary router and the local device, extending network coverage.
 - You are advised to select a 5G Wi-Fi of the primary router for better Internet experience.
- Unplug the cable to avoid loops.**

Wireless Repeater

Primary Router

* SSID

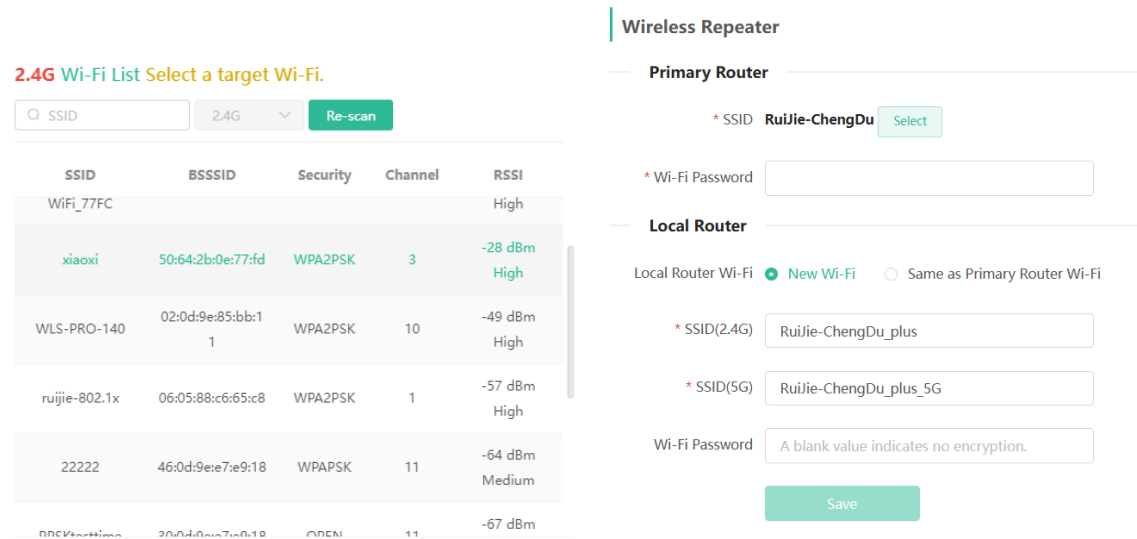
Select

- (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 have a Wi-Fi network the same as that of the primary router:
- If you select **Same as Primary Router Wi-Fi**, the Wi-Fi settings of the primary router are automatically synchronized to the current router. Generally, 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 a local SSID and password. Clients will search out a Wi-Fi signal different from the primary router Wi-Fi signal.

Caution

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 4-3 Selecting the Wi-Fi Signal of the Primary Router and Connecting to the Wi-Fi Network



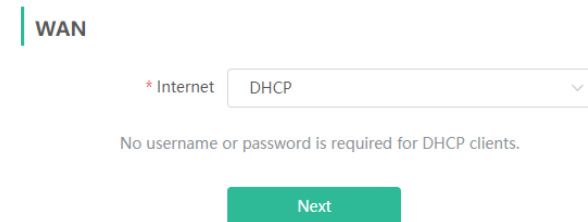
4.3 WISP

WISP allows users to establish their own WLAN for Internet access in public spaces, including coffee, hotel, airport or restaurant.

Mobile Phone View: Choose **More > Switch to PC view > More > Work Mode**

PC View: **More > Work Mode**

(1) Click **WISP** and select an Internet connection type. Click **Next**.



(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 have a Wi-Fi network the same as that of the primary router:

- o If you select **Same as Primary Router Wi-Fi**, the Wi-Fi settings of the primary router are automatically synchronized to the current router. Generally, 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.
- o If you select **New Wi-Fi**, you can set a local SSID and password. Clients will search out a Wi-Fi signal different from the primary router Wi-Fi signal.

⚠ Caution

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

Wireless Repeater

Primary Router

* SSID

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

SSID	BSSID	Security	Channel
dt680AR-2G	e2:05:46:56:59:92	OPEN	6
@@ZYQ-WIFIDOG	16:2b:a6:43:2f:89	OPEN	6
@@ZYQ-PORTAL	12:2b:a6:43:2f:89	OPEN	6
@@ZYQ-中文测试-UTF8	0e:2b:a6:43:2f:89	OPEN	6
@@ZYQ-中文测试-GBK	0a:2b:a6:43:2f:89	OPEN	6
@@ZYQ-wechat	1a:2b:a6:43:2f:89	OPEN	6

Wireless Repeater

Primary Router

* SSID **RuiJie-ChengDu**

Select an SSID for the primary router.

* Wi-Fi Password

Local Router

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

* SSID(2.4G)

* SSID(5G)


Wi-Fi Password

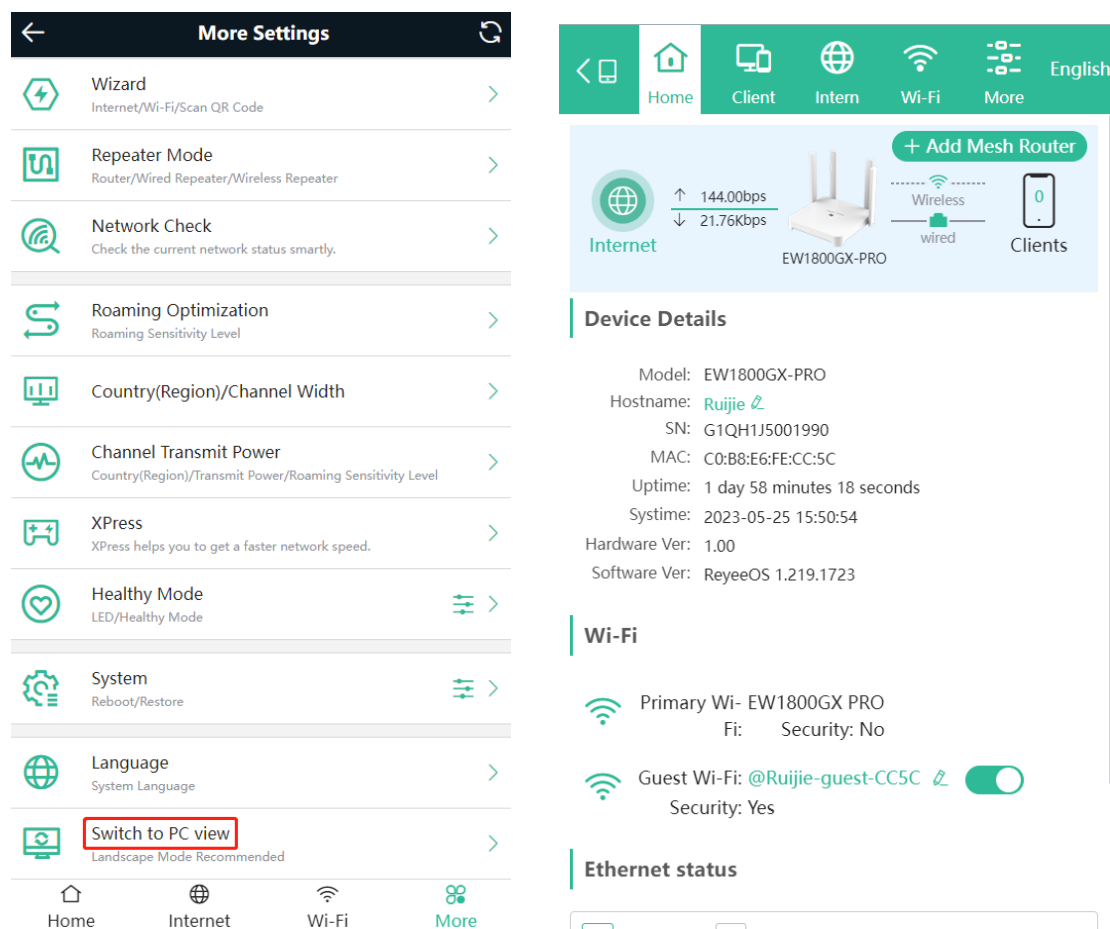
5 System Settings

5.1 Switching to 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 the mobile phone.

You can click  in the upper left corner to return to the mobile view (you can also drag the page to the narrowest position on the PC to enter the mobile view).



The screenshot displays the web-based configuration interface. On the left, the 'More Settings' menu is visible, listing various configuration options. The 'Switch to PC view' option is highlighted with a red box. On the right, the main dashboard shows network status, device details, Wi-Fi settings, and Ethernet status.

More Settings Menu:

- Wizard (Internet/Wi-Fi/Scan QR Code)
- Repeater Mode (Router/Wired Repeater/Wireless Repeater)
- Network Check (Check the current network status smartly.)
- Roaming Optimization (Roaming Sensitivity Level)
- Country(Region)/Channel Width
- Channel Transmit Power (Country(Region)/Transmit Power/Roaming Sensitivity Level)
- XPress (XPress helps you to get a faster network speed.)
- Healthy Mode (LED/Healthy Mode)
- System (Reboot/Restore)
- Language (System Language)
- Switch to PC view** (Landscape Mode Recommended)

Main Dashboard:

- Home, Client, Intern, Wi-Fi, More navigation tabs.
- Internet status: 144.00bps (upload), 21.76Kbps (download).
- Device Details for EW1800GX-PRO:
 - Model: EW1800GX-PRO
 - Hostname: Ruijie
 - SN: G1QH1J5001990
 - MAC: C0:B8:E6:FE:CC:5C
 - Uptime: 1 day 58 minutes 18 seconds
 - Systime: 2023-05-25 15:50:54
 - Hardware Ver: 1.00
 - Software Ver: ReyeOS 1.219.1723
- Wi-Fi settings:
 - Primary Wi-Fi: EW1800GX PRO (Security: No)
 - Guest Wi-Fi: @Ruijie-guest-CC5C (Security: Yes, toggle on)
- Ethernet status section.



5.2 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.

← **Password** ↻

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

* Old Password

* New Password

* Confirm Password

Save

5.3 Remote Access

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

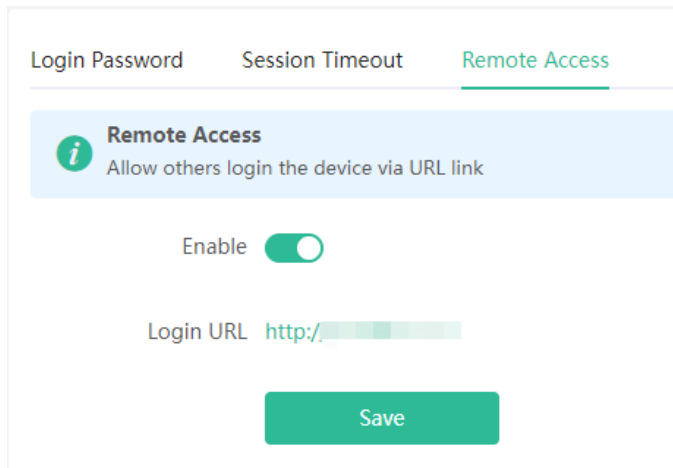
PC View: Choose **More** >  **System** > **Login** > **Remote Access**.

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

Caution

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

This function cannot be enabled if the device management password has a weak security strength, such as being purely numerical or alphabetical. See [5.2 Configuring the Login Password](#) to configure a strong and secure device management password.



5.4 Restoring Factory Settings

Mobile Phone View: Choose **More** > **System** > **Reset**.

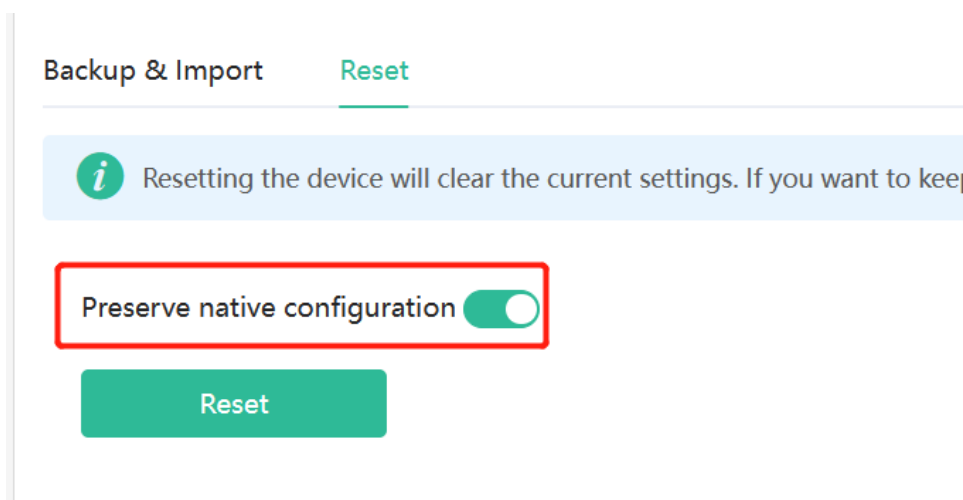
PC View: Choose **More** >  **System** > **Management** > **Reset**.

Click to enable **Preserve native configuration** to retain the network configuration, Wi-Fi settings, time zone and other configurations after the router is restored to factory settings.

Click **Reset** to restore factory settings.


Caution

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

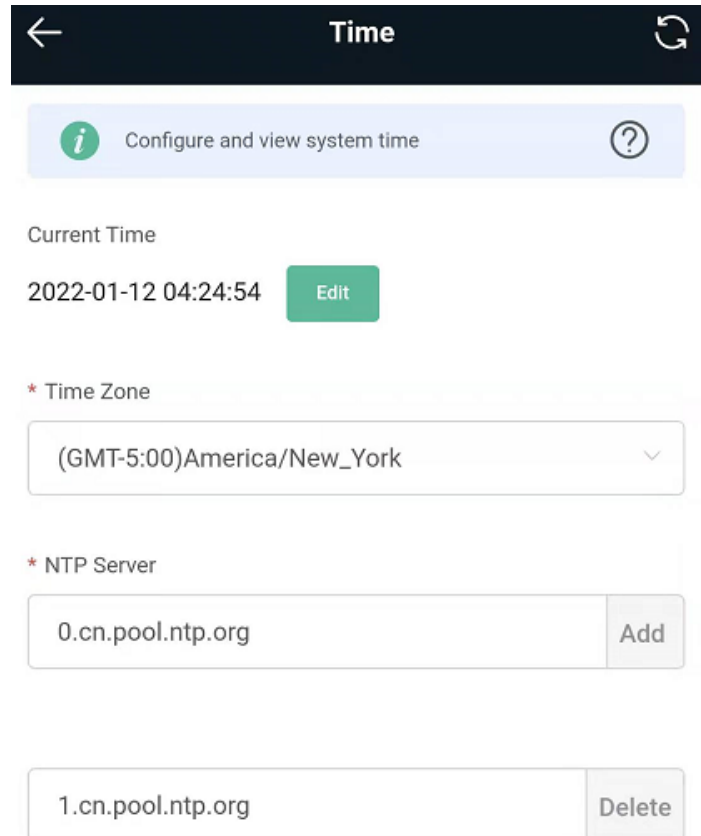


5.5 Configuring System Time

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 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.



← **Time** ↻

i Configure and view system time *?*

Current Time
2022-01-12 04:24:54 **Edit**

* Time Zone
(GMT-5:00)America/New_York

* NTP Server
0.cn.pool.ntp.org **Add**

1.cn.pool.ntp.org **Delete**

5.6 Configuring Scheduled Reboot

5.6.1 Getting Started

Confirm that the system time is accurate to avoid network interruption caused by device reboot at the wrong time. For details, see [5.5 Configuring System Time](#).

5.6.2 Configuration Steps

Mobile Phone View: Choose **More** > **System** > **Scheduled Reboot**.

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

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

← **Scheduled Reboot** ↻

Enable

Day

Mon Tue Wed Thu

Fri Sat Sun

Time

03 : 00

Save

5.7 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 there is a new version available, you can click it for an upgrade.


Caution

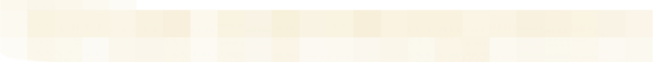
After being upgraded, the device will restart. Therefore, exercise caution when performing this operation. You are advised to set the scheduled upgrade time to an early morning time to avoid affecting Internet access.


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

← **Online Upgrade** ↻

 Online upgrade will keep the current configuration. The device will be rebooted during upgrade.

Current Version
ReyeeOS 1 





New Version
ReveeOS


Description


Tip

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

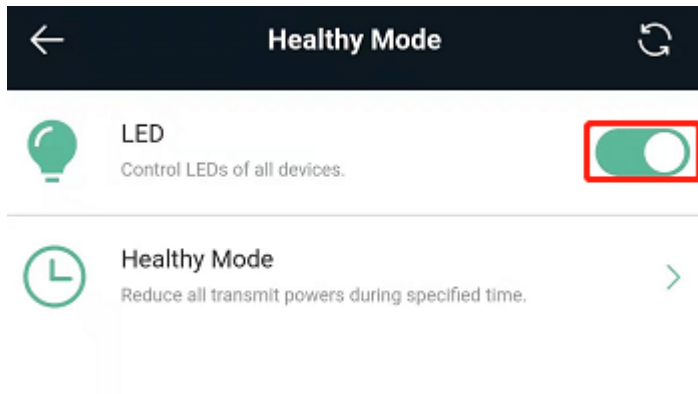
[Upgrade Now](#)

 Home  Internet  Wi-Fi  More

5.8 Turning On/Off the Indicator

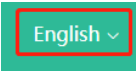
Mobile Phone View: Choose **More** > **Healthy Mode**. > **LED**

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

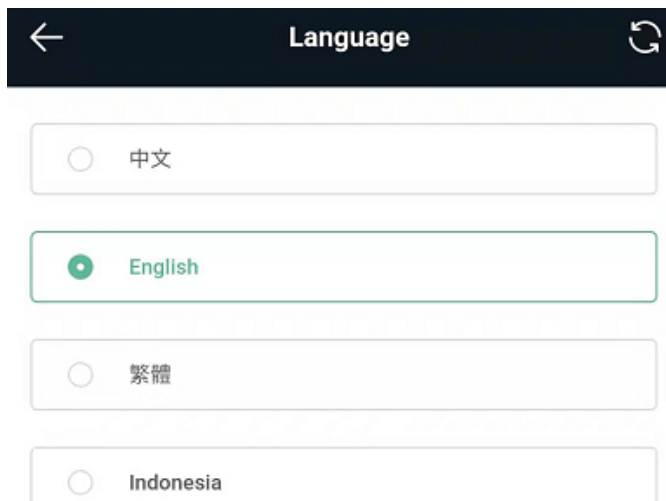


5.9 Switching System Language

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.



5.10 Enabling Alerts

Mobile Phone View: Choose **More** > **Switch to PC** > **More** >  **Diagnostics** > **Alerts**.

PC View: Choose **More** >  **Diagnostics** > **Alerts**

The device may be affected by conflicts and attacks in the network, which leads to network anomalies. Enable the **Alerts** function, and you can view the alerts for fault prevention and troubleshooting. You can also customize the followed alerts. All alerts are followed by default. The unfollowed alerts will not be detected or displayed. You are advised to follow all alerts.

i View and manage alarms.

Alert List
View Unfollowed Alert

Expand	Alerts	Suggestion	Action
No Data			

<
1
>

10/page ▾

Total 0

Click the arrow under **Expand** to view alarm details.

Click **Delete** to delete the corresponding alarm messages. You are advised to retain all alerts for review.

Click **Unfollow** and then click **OK**. The device will no longer report the corresponding alerts. After clicking **View Unfollowed Alarm**, select the alarm you want to follow again. Click **OK**, and the device will keep following the corresponding alerts.


Table 5-1 Alerts and Suggested Action

Alerts	Suggested Action
The WAN port has no link.	Please check whether a cable is plugged into the WAN port.
The port is operating at 10Mbps.	Please check the peer port settings, unplug and re-plug the cable, or replace the cable.
There is more than one DHCP server in the LAN network.	Please disable the extra DHCP server in the LAN network.
There is more than one DHCP server in the WAN network.	Please disable the extra DHCP server in the WAN network.
Address pool of DHCP server is full.	Enlarge the DHCP address pool.
WAN & LAN Address Conflict.	Please check the IP addresses of WAN and LAN ports. If the network addresses conflict (including IP address conflict), change the IP of LAN port.
The WAN IP address is already in use.	Please check the WAN IP address. If it is a static IP address, please change the IP address.
The LAN IP address is already in use.	Please check the LAN IP address. If it is a static IP address, please change the IP address.
The IP address of the downlink address is already in	Please check the IP address of the downlink device.

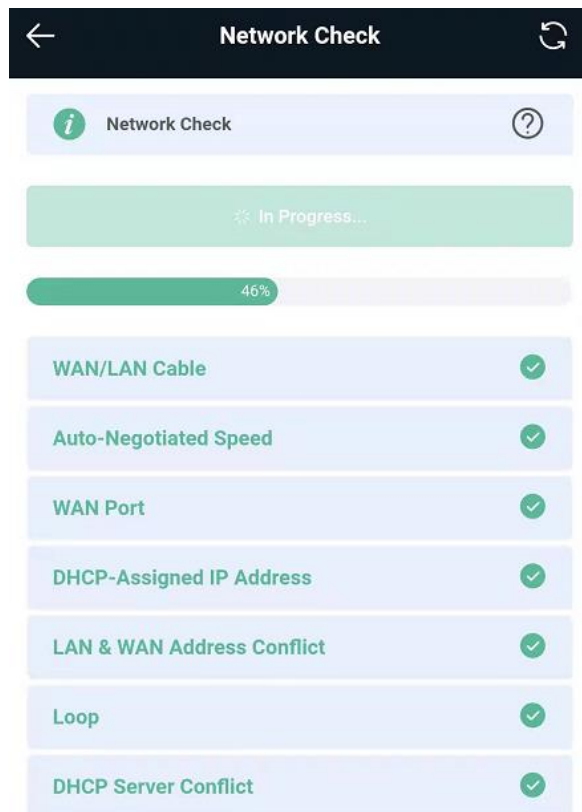
Alerts	Suggested Action
use.	If it is a static IP address, please change the IP address.
A MAC address conflict or loop error occurs.	Please troubleshoot the MAC address conflict or loop error.
No DNS server address is configured.	Please add a DNS server address, e.g., 114.114.115.115.
DNS failure	Please check the network configuration.
DNS resolution error.	Please check the network configuration.
Cloud service is not running.	Please reboot the device.
Cloud service is not enabled.	Please contact Ruijie technical support.
The device is not connected to the Ruijie Cloud server.	Please reboot the device.
Loops occur.	Please check the network environment.

5.11 Diagnosing Network Problems

Mobile Phone View: Choose **More** > **System** > **Network Check**.

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


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



5.12 Network Diagnosis Tools

1. Network Test Tool

Mobile Phone View: Choose **More** > **System** > **Network Tools**.

PC View: Choose **More** >  **Diagnostics** > **Network Tools** .

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

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

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

Network Tools

Tool Ping Traceroute DNS Lookup

* IP Address/Domain

* Ping Count

* Packet Size Bytes

Result

2. Packet Capture Tool

Note

This feature is not supported on RG-EW1200 routers.

Mobile Phone View: Choose **More** > **Switch to PC view** > **More** >  **Diagnostics** > **Packet Obtaining** .

PC View: Choose **More** >  **Diagnostics** > **Packet Obtaining**

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

Caution

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

i Packet Obtaining ?

Interface


Protocol


IP Address

File Size Limit Available Memory **153.43 M**

Packet Count Limit

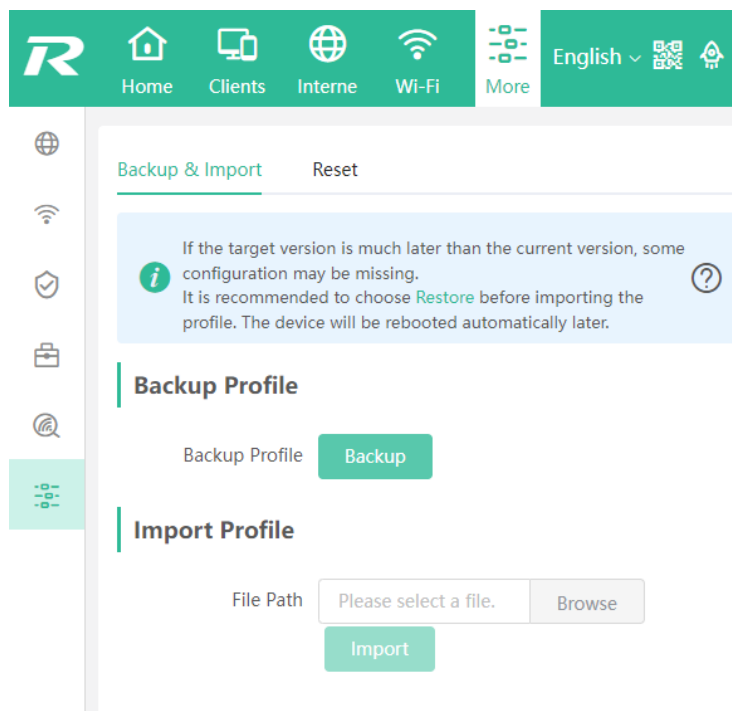
5.13 Configuring Config Backup and Import

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

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

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

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.



5.14 Configuring Session Timeout Duration

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

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

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

Login Password

Session Timeout

Remote Access

Session Timeout

* Session Timeout

seconds

Save