Ruijie Reyee RG-EW300T 4G Wi-Fi Router

ReyeeOS 1.420[390][380] Configuration Guide

Document Version: V1.0
Date: July 15, 2026
Copyright © 2026 Ruijie Networks

Copyright

Copyright © 2026 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 names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

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

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

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Technical Support

- Ruijie Reyee website: https://reyee.ruijie.com
- Online support center: https://reyee.ruijie.com/en-global/support
- Case portal: https://www.ruijie.com/support/caseportal
- Community: https://community.ruijie.com
- Email support: service_rj@ruijie.com
- Live chat: https://reyee.ruijie.com/en-global/rita

Conventions

1. GUI Symbols

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

1 Change Description 1

1.1 ReyeeOS 1.420 1

1.1.1 Hardware Change 1

1.1.2 Software Feature Change 1

1.2 ReyeeOS 1.390 1

1.2.1 Hardware Change 1

1.2.2 Software Feature Change 1

1.3 ReyeeOS 1.380 2

1.3.1 Hardware Change 2

1.3.2 Software Feature Change 2

2 Product Overview 4

2.1 Package Contents 4

2.2 LEDs 4

3 Quick Setup (As a Primary Router) 6

3.1 Internet Access Mode 6

3.2 Connect your Router 6

3.2.1 3G/4G Router Mode 6

3.2.2 Wireless Router Mode 6

3.2.3 Link Backup 7

3.3 Configuring the Router for Internet Access 7

3.3.1 Logging In to the Configuration Page 7

3.3.2 Primary Router Mode 10

3.3.3 Configuring a Wi-Fi Network 14
3.3.4 Configuring IoT Wi-Fi 15
3.3.5 Verification and Testing 16
4 Quick Setup (As a Secondary Router) 19
4.1 Getting Started 19
4.2 Internet Access Configuration 19
4.2.2 Wireless Repeater 20
4.2.3 WISP 24
4.3 Verification and Testing 28
5 Wi-Fi Network Settings 29
5.1 Changing the SSID and Password 29
5.2 Hiding the SSID 29
5.2.1 Overview 29
5.2.2 Getting Started 30
5.2.3 Configuration Steps 30
5.3 Adding a Wi-Fi Network 31
5.3.1 Overview 31
5.3.2 Configuration Steps 31
5.3.3 Verification and Testing 34
5.4 Configuring the Wi-Fi Blocklist or Allowlist 35
5.4.1 Overview 35
5.4.2 Configuration Steps 35
5.5 Optimizing the Wi-Fi Network 37
5.5.1 Overview 37

5.5.2 Getting Started 37
5.5.3 Configuration Steps 38
5.6 Configuring XPress 40
5.7 Configuring Wi-Fi/IGMP 41
5.7.1 Overview 41
5.7.2 Configuration Steps 41
5.8 Configuring the Health Mode 42
6 Networks Settings 43
6.1 Displaying SIM Card Information 43
6.2 Managing the SIM Card 43
6.2.1 Configuring Network Access for a SIM Card 43
6.2.2 Displaying the SIM Card List 45
6.3 Managing the PIN 45
6.4 Managing SMS 47
6.4.1 Creating an SMS Message 47
6.4.2 Displaying the Inbox 48
6.4.3 Displaying the Outbox 48
6.4.4 Displaying the Drafts Box 49
6.5 Configuring Internet Connection Type 49
6.6 Changing the MAC Address 50
6.7 Changing the MTU 51
6.8 Changing the Address of a LAN Port 52
6.9 Configuring IPv6 Address 53
6.9.1 Configuring the IPv6 Address of the WAN Port 53

6.9.2 Click Save.Configuring the IPv6 Address of the LAN Port 54
6.9.3 Viewing DHCPv6 Clients 55
6.10 Enabling Parental Control 55
6.10.1 Setting the Internet Block Periods 56
6.10.2 Disabling Parental Control 57
6.11 Configuring Port Mapping 58
6.11.1 Overview 58
6.11.2 Getting Started 58
6.11.3 Configuration Steps 58
6.11.4 Verification and Testing 59
6.11.5 Solution to a Test Failure 59
6.11.6 DMZ Configuration Steps 60
6.12 Configuring DHCP Server 60
6.12.1 Overview 60
6.12.2 Configuration Steps 60
6.13 Configuring DHCP Option 62
6.14 Configuring DNS 63
6.15 Configuring DDNS 63
6.15.1 Overview 63
6.15.2 Getting Started 63
6.15.3 Configuration Steps 63
6.16 Configuring ARP Binding 64
6.16.1 Overview 64
6.16.2 Configuration Steps 64

6.17 Connecting to IPTV 64
6.17.1 Getting Started 65
6.17.2 IPTV Configuration Steps (VLAN Type) 65
6.17.3 IPTV Configuration Steps (IGMP Type) 66
6.18 Configuring Reyee Mesh 3.0 66
6.18.1 Configuration Steps 66
6.19 Configuring AP Networking 70
6.20 Enabling Smart Flow Control 70
6.21 Setting Blocking Schedules 72
6.21.1 Setting a Blocking Schedule 72
6.21.2 Removing a Blocking Schedule 73
6.22 Enabling Port-Based Flow Control 73
6.23 Configuring UPnP 74
6.23.1 Overview 74
6.23.2 Configuration Steps 74
6.24 Enabling Wi-Fi Switch 74
7 Configuring the Repeater Mode 75
7.1 Access Point 75
7.2 Wireless Repeater 76
7.3 WISP 77
8 System Settings 79
8.1 Switching to PC View 79
8.2 Configuring the Login Password 79
8.3 Remote Access 80

8.4 Restoring Factory Settings 81
8.5 Configuring System Time 81
8.6 Configuring Scheduled Reboot 82
8.6.1 Getting Started 82
8.6.2 Configuration Steps 82
8.7 Performing Online Upgrade and Displaying the System Version 83
8.8 Performing Local Upgrade 84
8.9 Turning On/Off the Indicator 84
8.10 Switching System Language 85
8.11 Diagnosing Network Problems 86
8.12 Network Diagnosis Tools 86
8.12.1 Ping 86
8.12.2 Traceroute 87
8.12.3 DNS Lookup 88
8.12.4 HTTP/HTTPS Detection 88
8.12.5 Packet Capture Tool 90
8.13 Configuring Config Backup and Import 91
8.14 Configuring Session Timeout Duration 91
8.15 Configuring the Compatibility Mode 92
8.16 Configuring Cloud Service 93
8.16.1 Overview 93
8.16.2 Configuration Steps 93
8.16.3 Unbinding Cloud Service 94
8.17 Switching to Accessibility Mode 94

8.18 Connectivity Detection 95

9 Expert Mode 97

10 FAQs 98

10.1 How Do I Restore the Router to Factory Settings? 98

10.2 What Should I Do If I Forgot the Password? 98

10.3 What Should I Do If the System LED Keeps Flashing After the Router is Powered On? 98

11 Appendix 98

11.1 User Ports 98

11.2 User Privacy Log 99

1 Change Description

This chapter describes the major changes in software and hardware of different versions and related documentation. For details about hardware changes, see the release notes published with software versions.

1.1 ReyeeOS 1.420

1.1.1 Hardware Change

The following table lists the applicable hardware models of this version.

Model	Hardware Version
RG-EW300T	1.xx

1.1.2 Software Feature Change

This version introduces the following new features compared to ReyeeOS 1.390.

1. New Feature — Connectivity Detection

ReyeeOS 1.420 supports the **Connectivity Detection** feature. For details, see 8.18 Connectivity Detection.

2. New Feature — HTTP/HTTPS Detection

ReyeeOS 1.420 supports the **HTTP/HTTPS Detection** feature. For details, see 8.12.4 HTTP/HTTPS Detection.

3. Changed Feature — Disable Reset

ReyeeOS 1.420 supports the **Disable Reset** feature. For details, see 8.4 Restoring Factory Settings.

1.2 ReyeeOS 1.390

1.2.1 Hardware Change

The following table lists the applicable hardware models of this version.

Model	Hardware Version
RG-EW300T	1.xx

1.2.2 Software Feature Change

1. New Feature —Accessibility Mode

ReyeeOS 1.390 supports accessibility mode. For details, see 8.17 Switching to Accessibility Mode.

1.3 ReyeeOS 1.380

1.3.1 Hardware Change

The following table lists the applicable hardware models of this version.

Model	Hardware Version
RG-EW300T	1.xx

1.3.2 Software Feature Change

1. New Feature — Compatibility Mode

ReyeeOS 1.380 supports compatibility mode. For details, see 8.15 Configuring the Compatibility Mode.

2. New Feature — Cloud Service

This version supports the cloud service feature. For details, see 8.16 Configuring Cloud Service.

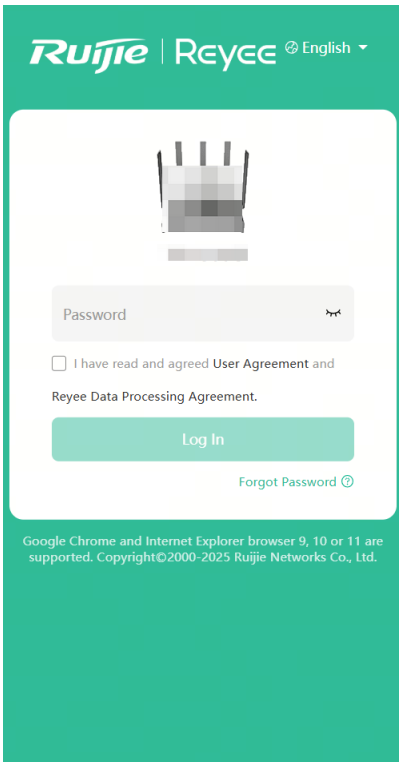
3. Changed Feature — Deployment Configuration

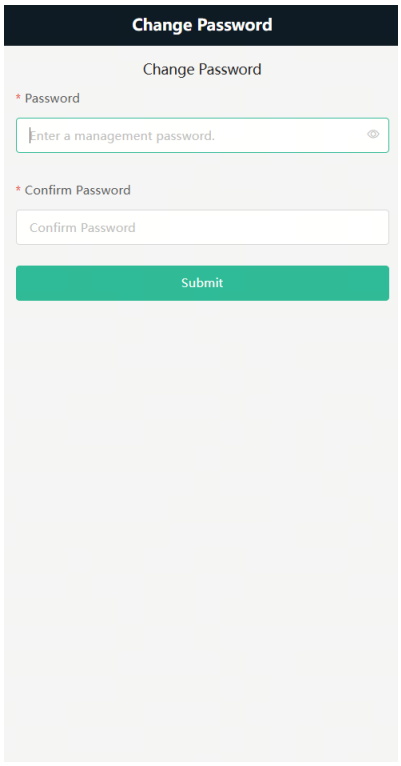
After the first login, you need to enter the default device password and reset the password before entering the deployment configuration process. For details, see 3.3.2 Primary Router Mode and 4 Quick Setup (As a Secondary Router)

⚠ Caution

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.

.


Ruijie | Reyee
English
Password
I have read and agreed User Agreement and
Reyee Data Processing Agreement.
Log In
Forgot Password
Google Chrome and Internet Explorer browser 9, 10 or 11 are supported. Copyright©2000-2025 Ruijie Networks Co., Ltd.


Change Password
Change Password
* Password
Enter a management password.
* Confirm Password
Confirm Password
Submit

2 Product Overview

2.1 Package Contents

Router x1, Power adapter x1, Ethernet cable x1, Quick Installation Guide x1, and Warranty card x1



2.2 LEDs

LED	Status	Description
System status LED	Off	The router is not powered on.
	Solid on	The router is running normally.
	Fast blinking (on for 62.5 ms, off for 62.5 ms)	● The router is restored to factory settings. ● The router restarts. ● The router is initialized. ● The firmware is upgraded.
Wi-Fi LED	Solid on	The Wi-Fi service is enabled.
	Off	The Wi-Fi service is disabled.
Internet LED	Solid on	The router is connected to the Internet.
	Off	The router is not connected to the Internet.

LED	Status	Description
4G status LED	LED1 solid on	The 4G signal strength is low.
	LED2 solid on	The 4G signal strength is medium.
	LED3 solid on	The 4G signal strength is high.
	All LEDs off	There is no 4G signal.

3 Quick Setup (As a Primary Router)

3.1 Internet Access Mode

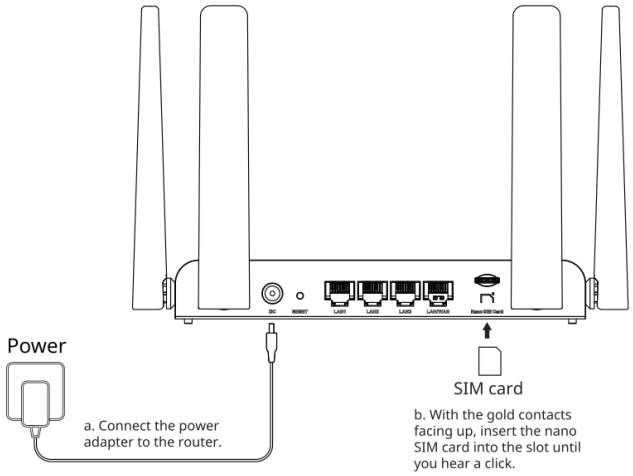
The router supports two Internet access modes: primary router mode and secondary router mode.

- **Primary Router Mode**: This mode is suitable for network creation. The router connects to the Internet through wired connection, and can manage extenders. You are advised to select the device with the best performance as the primary router. The router supports three work modes:
  - **3G/4G Router Mode**: When a SIM card is inserted into the SIM card slot of the router, the 3G/4G network is used for Internet access by default.
  - **Wireless Router Mode**: The router can be connected to an optical network terminal (ONT), and you can use the network service provided by the Internet service provider (ISP) for Internet access. The primary router can work in PPPoE mode, Dynamic Host Configuration Protocol (DHCP) mode, and static IP address mode.
  - **Link Backup**: In this mode, a nano SIM card is inserted into the router and it is connected to a modem. When the primary link fails, the system automatically switches traffic to the secondary link.
- **Secondary Router Mode**: On an available network, the router can be connected to the primary router through wireless connection to expand the Wi-Fi coverage and increase the number of LAN ports and wireless access devices. For details, see 4 Quick Setup (As a Secondary Router).

3.2 Connect your Router

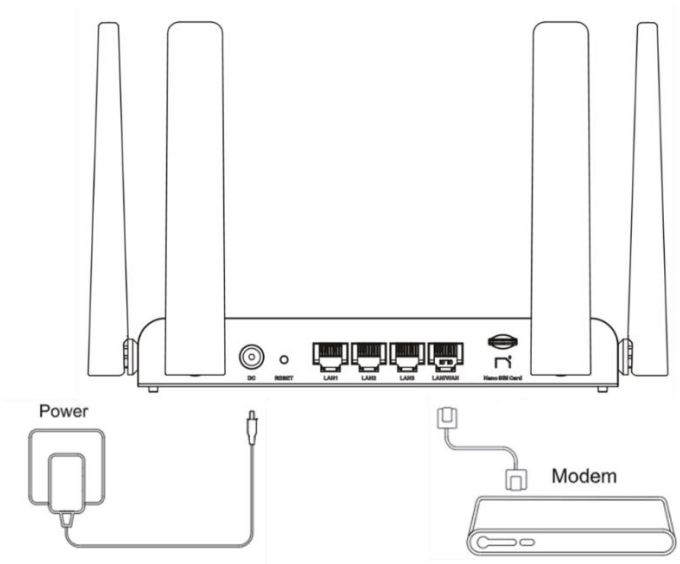
3.2.1 3G/4G Router Mode

Connect the power adapter to the router. Then, with the gold contacts facing up, insert the nano SIM card into the slot until you hear a click.



3.2.2 Wireless Router Mode

Connect the LAN port on the modem to the LAN/WAN port on the router using an Ethernet cable. Then, connect the power adapter to the router.



3.2.3 Link Backup

For details about how to insert a nano SIM card into the router and connect its LAN/WAN port to the modem, see 3.2.1 3G/4G Router Mode and 3.2.2 Wireless Router Mode.

3.3 Configuring the Router for Internet Access

3.3.1 Logging In to the Configuration Page

Caution

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.

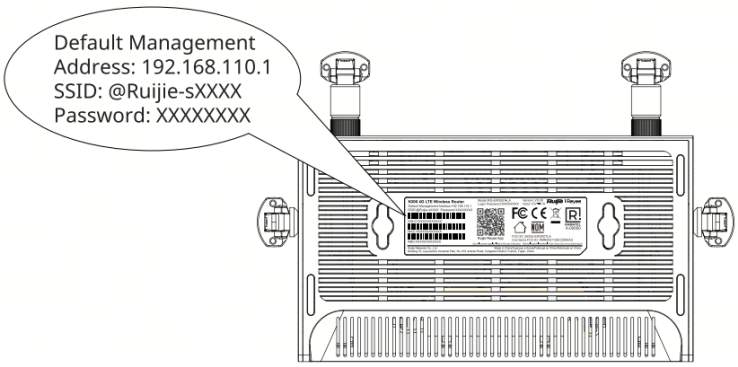
Table 3-1 Default Configuration

Item	Default Value
Device IP address (http or https)	192.168.110.1
Password	See the label on the bottom of the router.

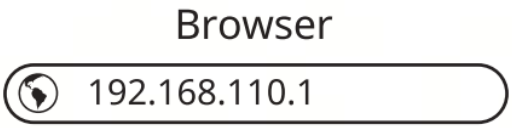
(1) You can open the management page and complete Internet access configuration only after connecting a smartphone or laptop to the router. You can connect a smartphone or laptop to the router in the following way.

- **Wireless Connection**

  Connect your smartphone or computer to the router's Wi-Fi network with the SSID: @Ruijie-s*XXXX* (*XXXX* represents the last four digits of the router's MAC address). After successful connection, you will be redirected to the setup page.



If the setup page is not displayed, open a web browser, and enter 192.168.110.1 in the address bar to access the setup page.



If you encounter any difficulties while connecting to the SSID, please scan the QR code on the back of the packaging box for further assistance.

- **Wired Connection**

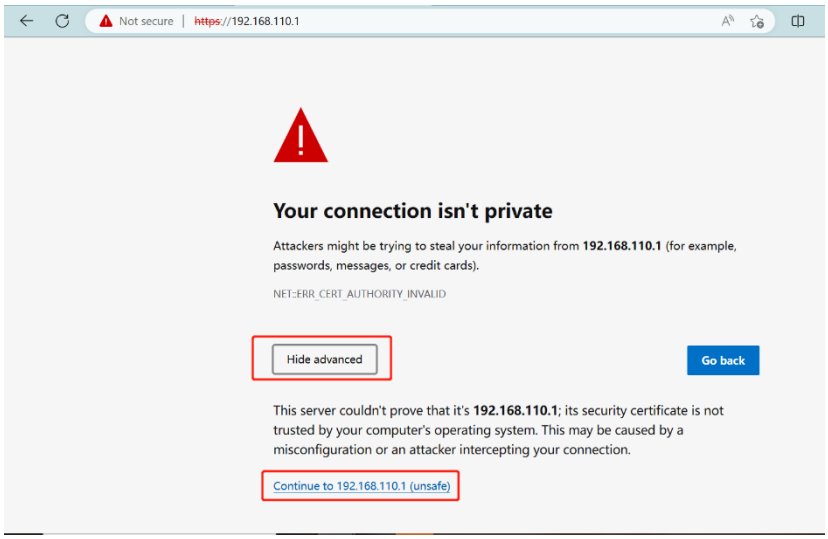
  a Connect a local area network (LAN) port of the router to the network port of the PC, and configure Obtain an IP address automatically on the PC.

  b Enter the IP address of the router (default: 192.168.110.1) in the address bar of your browser, and press **Enter**. The login page is displayed.

Note

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.

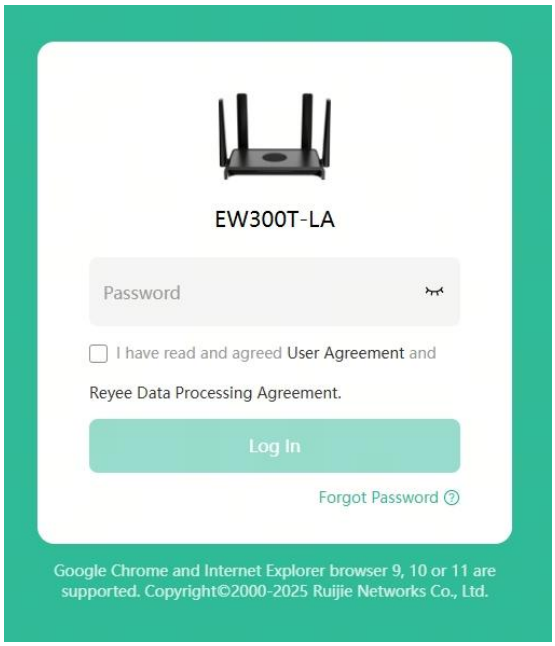
If the following page is displayed. Choose **Advanced** > **Continue to 192.168.110.1(unsafe)** to access the login page.



(2) Enter the device login password and tap **Log In** to configure the router.

Note

The default password can be found on the nameplate at the bottom of the router. To change the password, see 8.2 Configuring the Login Password



Caution

- 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.
- 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.

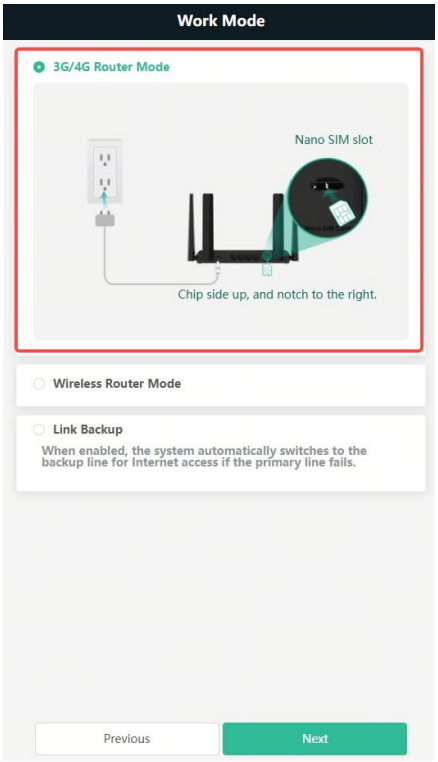
3.3.2 Primary Router Mode

1. 3G/4G Router Mode

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

(2) Insert a valid SIM card into the SIM card slot of the router and power on the router. For details, see 3.2.1 3G/4G Router Mode.

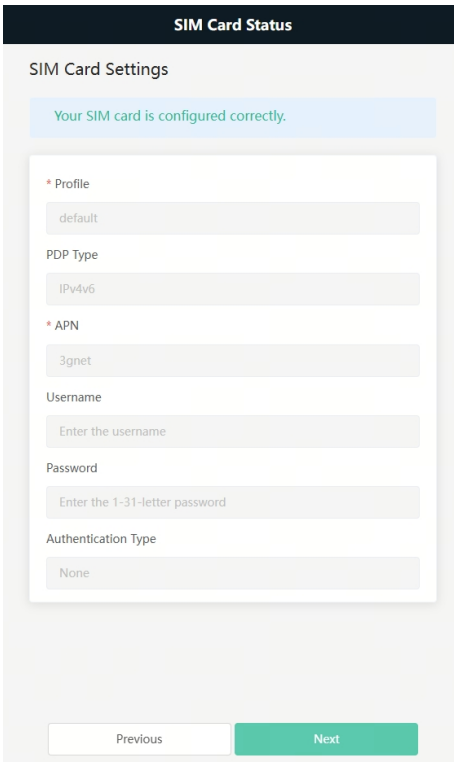
(3) On the page that opens, select **3G/4G Router Mode,** and click **Next**.



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

Caution

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



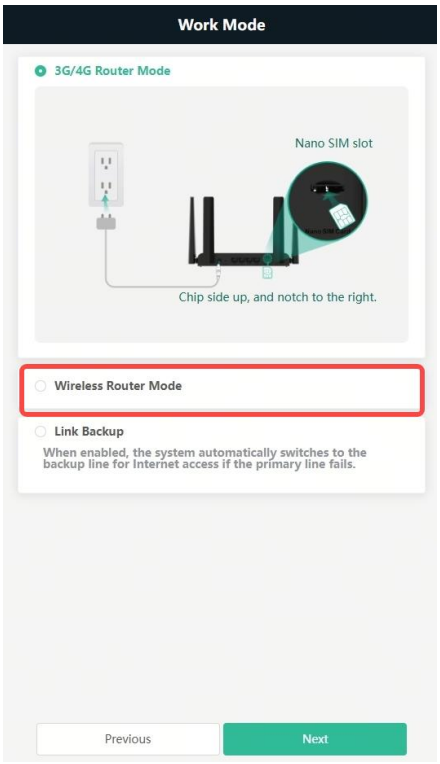
2. Wireless Router Mode

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:

The device supports the following Internet access modes, and the following configuration parameters are required:

- **DHCP**: The uplink DHCP server automatically assigns an IP address to the device, with no configuration parameters required.
- **PPPoE**: The device initiates a connection request to the ISP server via the PPPoE protocol. A broadband username and password must be obtained in advance.
- **Static IP**: The device uses a fixed IP address to connect to the Internet. You must obtain the IP address, subnet mask, gateway IP, and DNS server address in advance.

(1) On the page that opens, select **Wireless Router Mode**, and click **Next**.

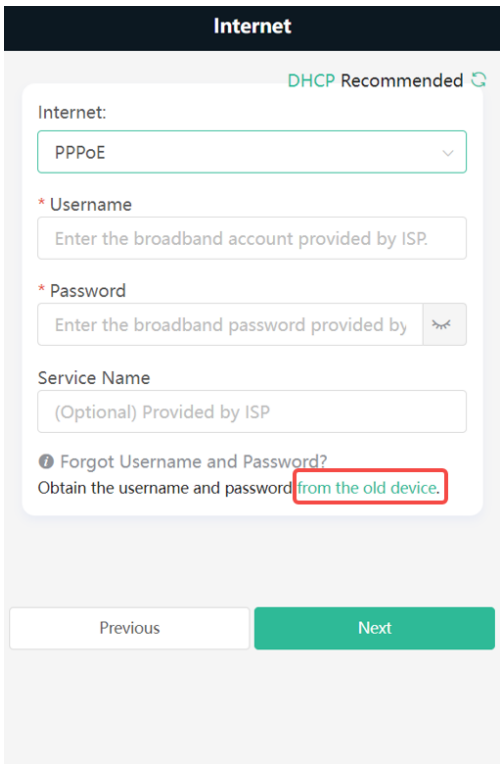


(2) Select the Internet connection type confirmed by the carrier.

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

  You can obtain the username and password from the old device.

  a Click **from the old device**.

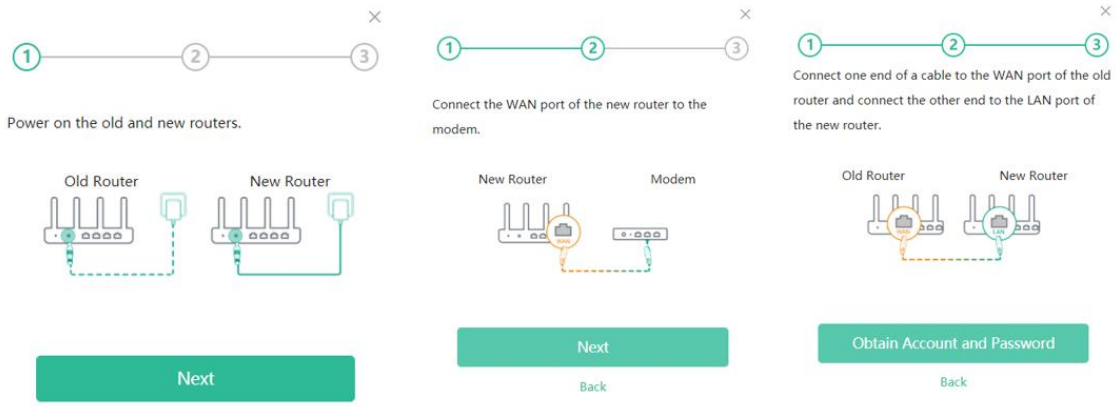


b Connect the old and new routers to a power supply and start them.

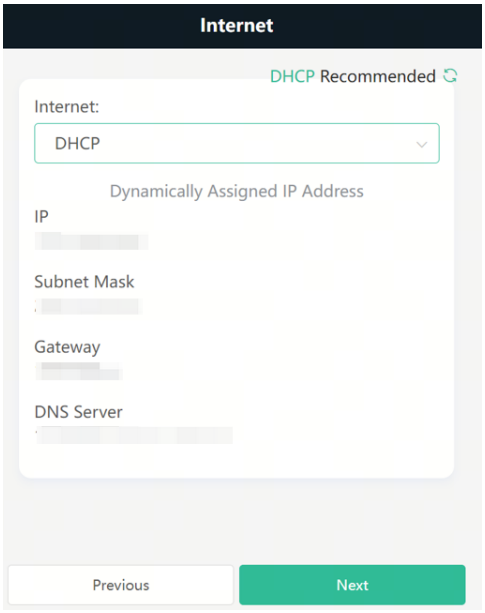
c Connect the WAN port of the new router to the modem.

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.

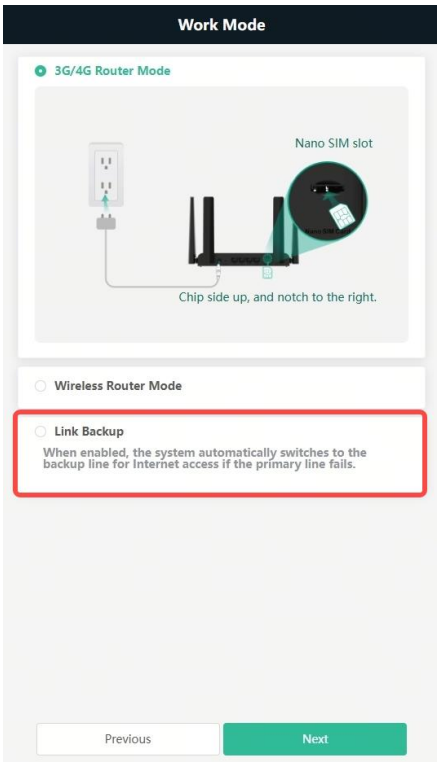


- **Static IP**: Enter the IP address, subnet mask, gateway, and DNS server, and click **Next**.



3. Link Backup Mode

(1) On the page that opens, select **Link Backup**, and click **Next**.



(2) Configure the two Internet access modes according to 1. 3G/4G Router Mode and 2. Wireless Router Mode.

3.3.3 Configuring a Wi-Fi Network

(1) Set the SSID and password,

- **2.4G Wi-Fi**: After this function is enabled, the 2.4G band will be preferred. The 2.4G signal is strong but easily interfered by various wireless signals.

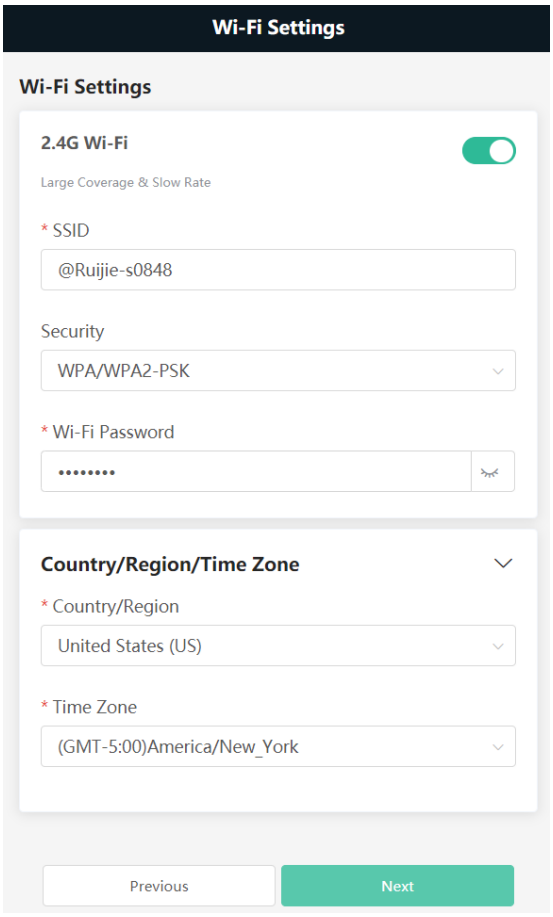
> Note
>
> The term "2.4G" mentioned in this document only refer to the channels with the frequency of 2.4GHz.

- **SSID** and **Wi-Fi Password**: Set the SSIDs and passwords of the primary device. You are advised to use the default encryption type and set strong passwords to enhance security.

> Note
>
> For security purposes, set a Wi-Fi password with at least eight characters, including numbers, letters, and special characters.

- **Country/Region**: The Wi-Fi channel may vary from country to country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.
- **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.

(2) 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.



3.3.4 Configuring IoT Wi-Fi

Note

Some smart home clients only support legacy Wi-Fi standards (IEEE 802.11b/g), which can operate only at a 20 MHz channel width. To ensure the clients can connect to the router for Internet access properly, enabling IoT Wi-Fi limits the 2.4 GHz Wi-Fi network to a 20 MHz channel width.

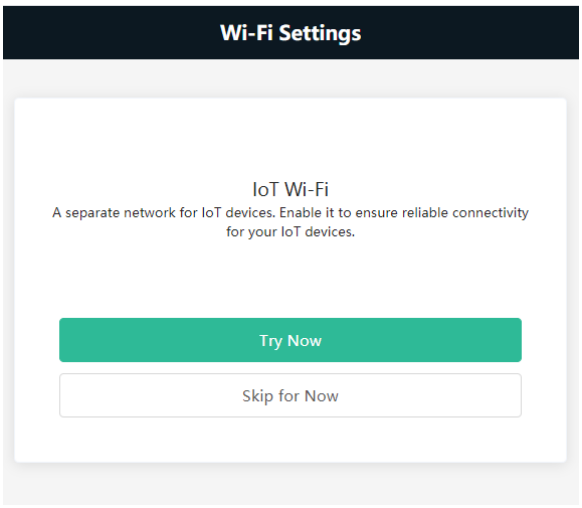
IoT Wi-Fi provides a dedicated wireless network channel for smart home clients, effectively reducing interference and improving connection stability. If multiple smart home clients exist in your home, you are advised to enable this feature.

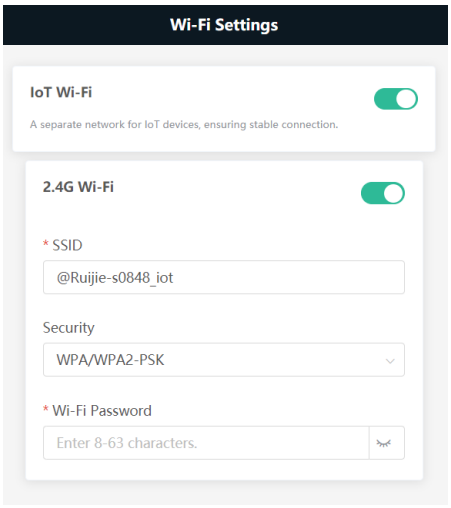
(1) Tap **Try Now** to configure the IoT Wi-Fi network.

Note

If you do not need to configure the IoT Wi-Fi network, tap **Skip for Now** to proceed to step (3) .

(2) Toggle on **IoT Wi-Fi**, configure the Wi-Fi parameters, and tap **Next**.



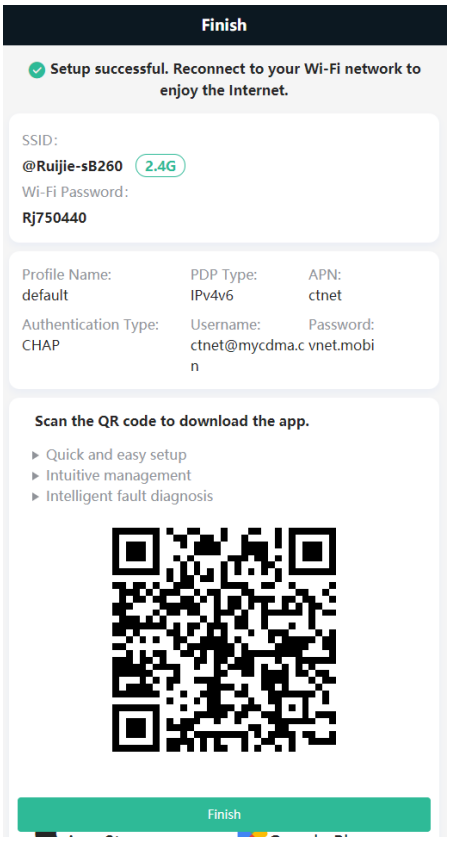


(3) After configuration is complete, the Wi-Fi networks configured on the router will automatically restart. Reconnect to a network with a new SSID using the configured password.

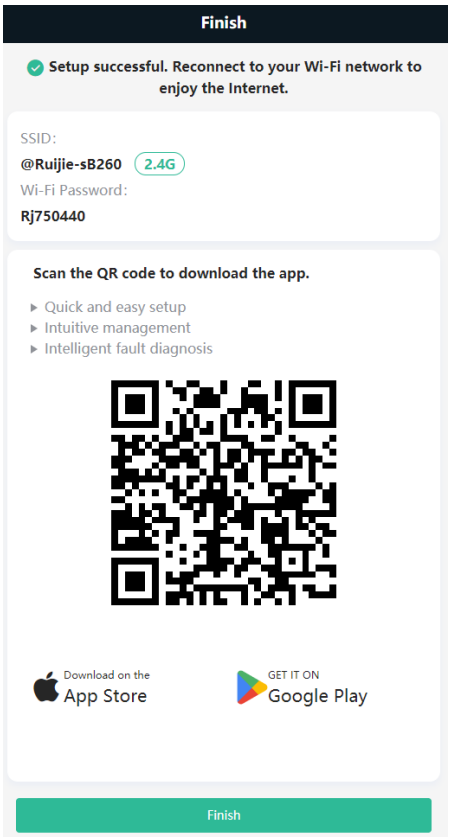
3.3.5 Verification and Testing

After network settings are complete, all Wi-Fi networks on the device will restart. You need to use the new Wi-Fi name and password to reconnect to the network.

- 3G/4G Router Mode



- Wireless Router Mode



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.

- 3G/4G Router Mode

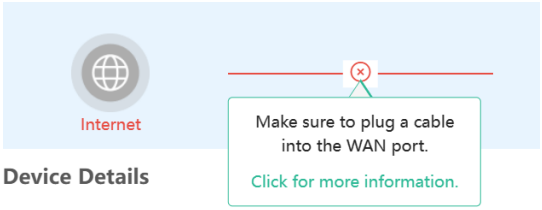


- Wireless Router Mode



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.



4 Quick Setup (As a Secondary Router)

Caution

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.

4.1 Getting Started

- Before configuring the extender, configure the primary router and test that the primary router can access the Internet.
- Put the secondary router at a place where it can detect the primary router's Wi-Fi signal with at least 2 bars of signal strength; no Ethernet cable is required.
- Connect the secondary router to the power supply. After 1 to 2 minutes, when the system LED stays solid on, the device has completed startup.

4.2 Internet Access Configuration

(1) You can open the management page and complete Internet access configuration only after connecting a smartphone or laptop to the router. You can connect a smartphone or laptop to the router in the following way.

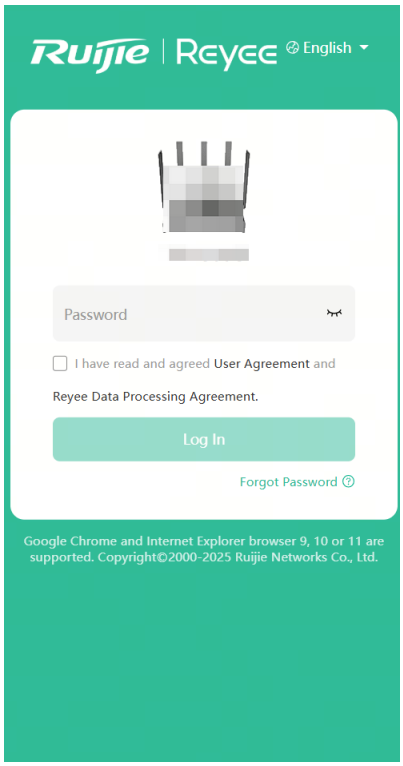
- **Wireless Connection:** On a smartphone or laptop, search for the Wi-Fi network **@Ruijie-s*XXXX*** (XXXX is the last four digits of the MAC address of each device). The default SSID and login address can be found on the bottom label of the router.
- **Wired Connection:** Connect a local area network (LAN) port of the router to the network port of the PC, and configure **Obtain an IP address automatically** on the PC.

(2) Open a browser and enter the device's default IP address (192.168.110.1) in the address bar.

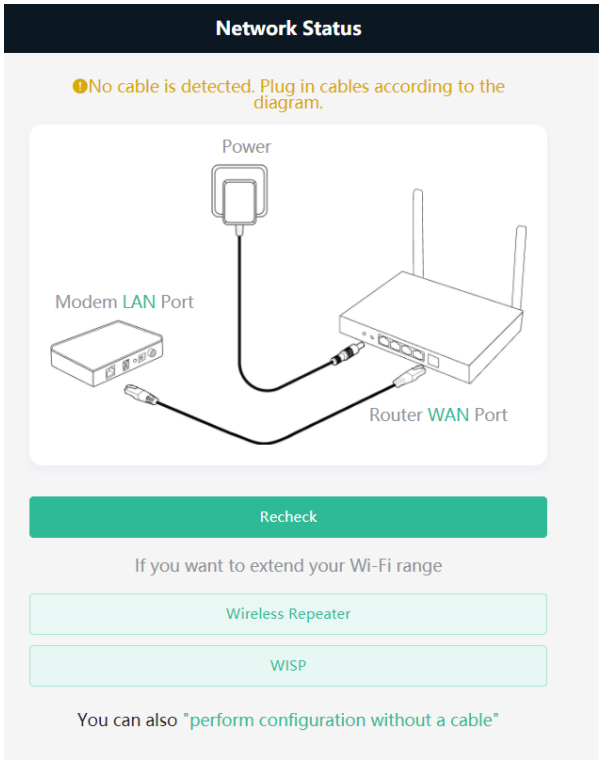
(3) Enter the device login password and tap **Log In** to configure the router.

Note

The default password can be found on the nameplate at the bottom of the router.

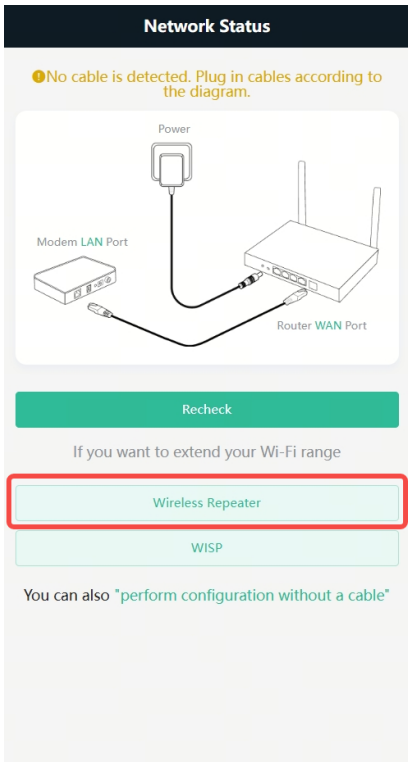


(4) The device supports two wireless repeater modes: **Wireless Repeater** and **WISP**. Configure the device according to your actual needs.



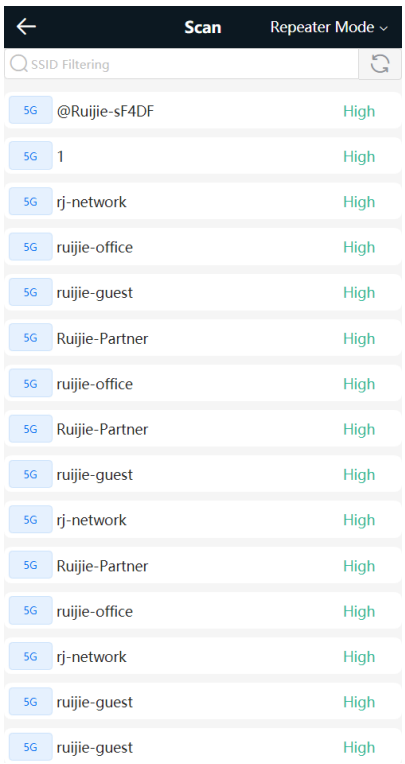
4.2.2 Wireless Repeater

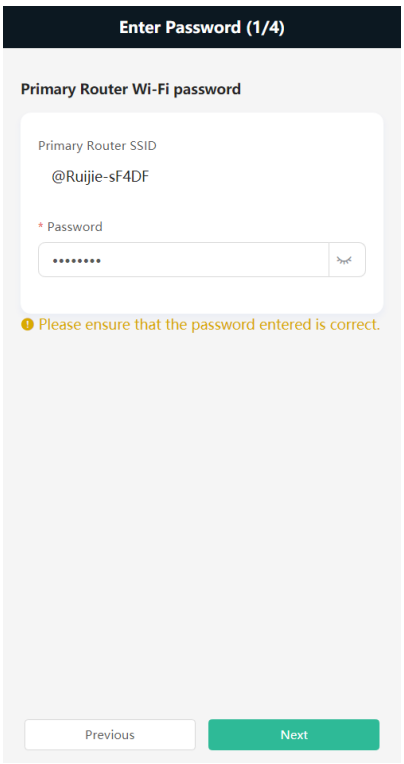
(1) Select **Wireless Repeater**.



(2) Select the SSID of the primary router, and enter the Wi-Fi password to connect to the primary router. Tap **Next**.

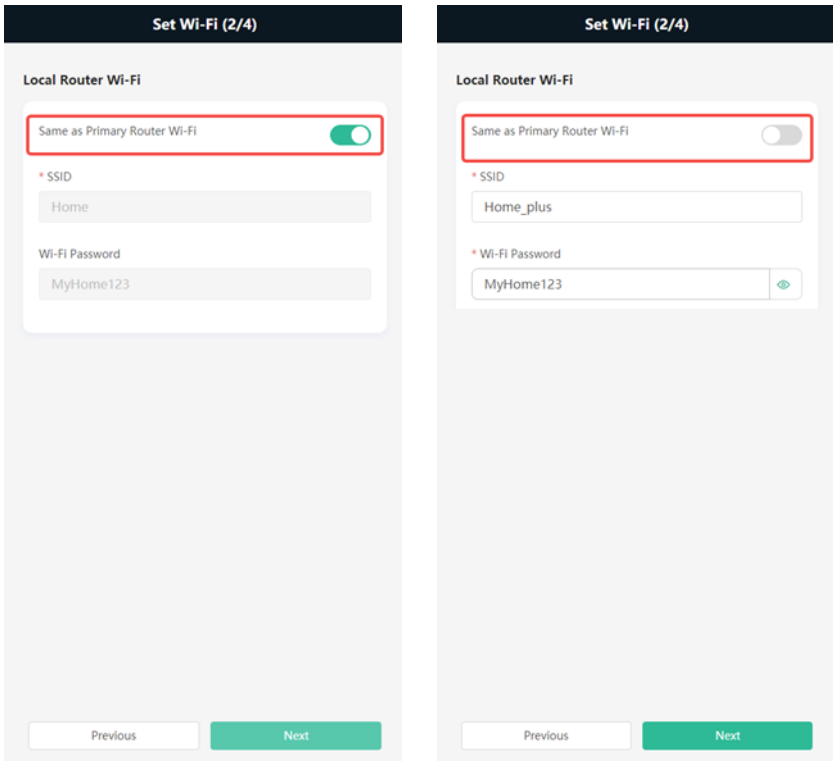
In wireless repeater mode, only Wi-Fi signals are extended and the DHCP function is disabled. The IP addresses of all clients connected to the primary and secondary routers are assigned by the primary router. If the device connects to the primary router in wireless repeater mode, the WAN port of the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



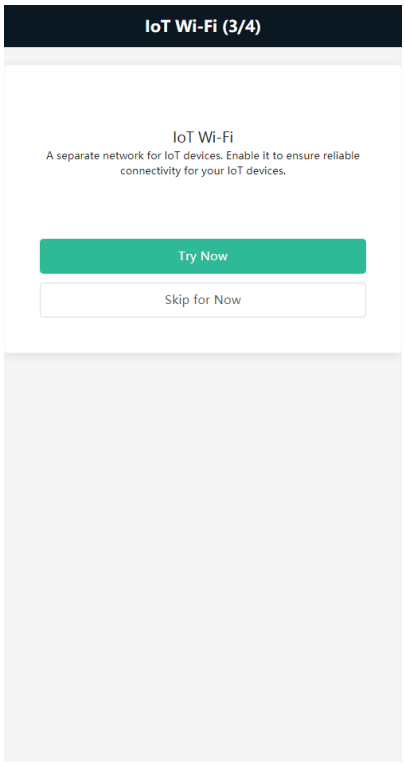


(3) Set the Wi-Fi network of the secondary router and tap **Next**.

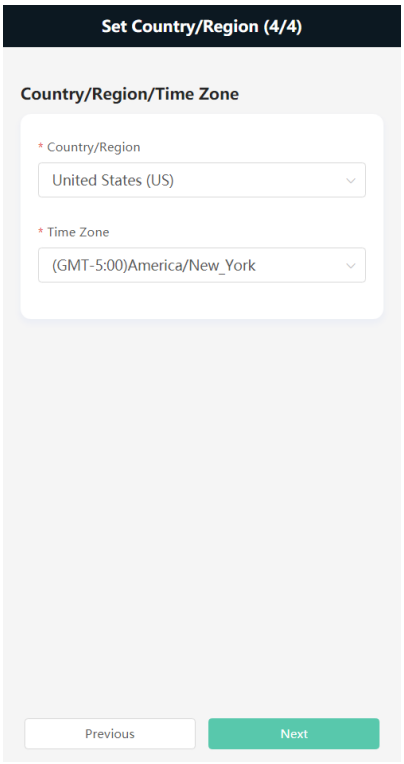
- Toggle on **Same as Primary Router Wi-Fi**. The SSID and password of the secondary router will be the same as those of the primary router.
- Toggle off **Same as Primary Router Wi-Fi**. You need to set a separate SSID and password for the secondary router.



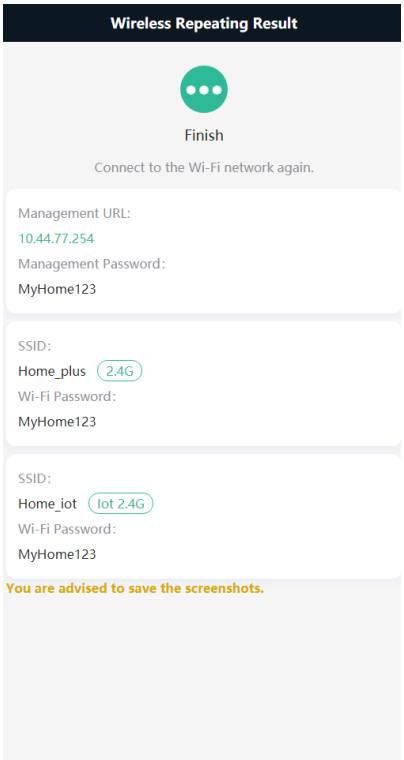
(4) Enable IoT Wi-Fi as required. For detailed configuration, see 3.3.4 Configuring IoT Wi-Fi.



(5) Set **Country/Region** and **Time Zone.** You are advised to choose the correct country or region, as well as the appropriate time zone. Tap **Next**.



(6) Wait for 1 to 2 minutes. When the system LED of the secondary router turns solid green, the Wi-Fi extension is successful. After configuration is complete, the Wi-Fi networks configured on the router will automatically restart. Reconnect to a network with a new SSID using the configured password. Tap **Management URL** to go to the eWeb management page.



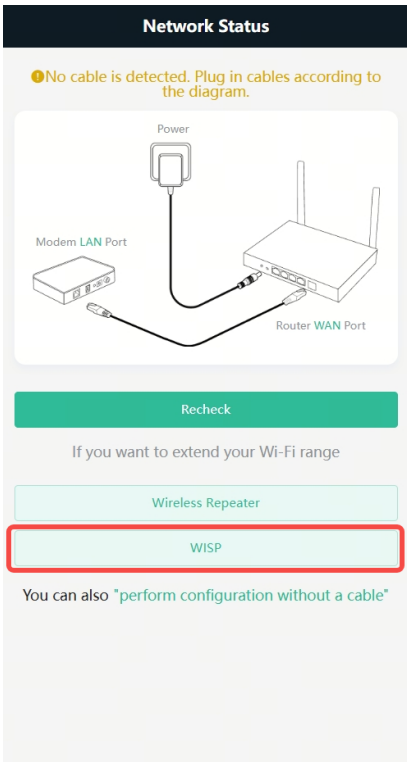
4.2.3 WISP

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

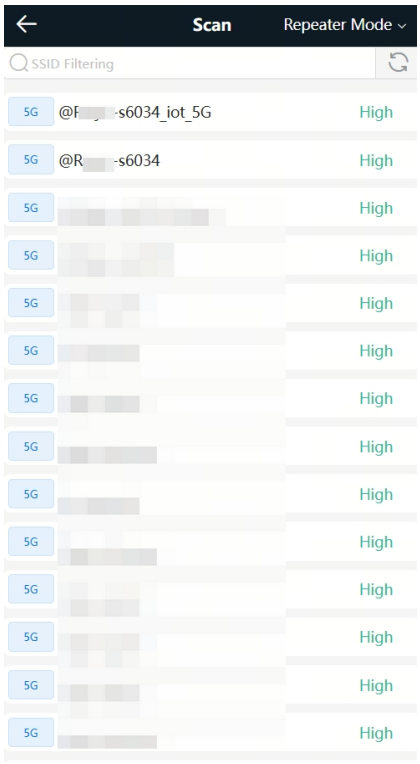
Note

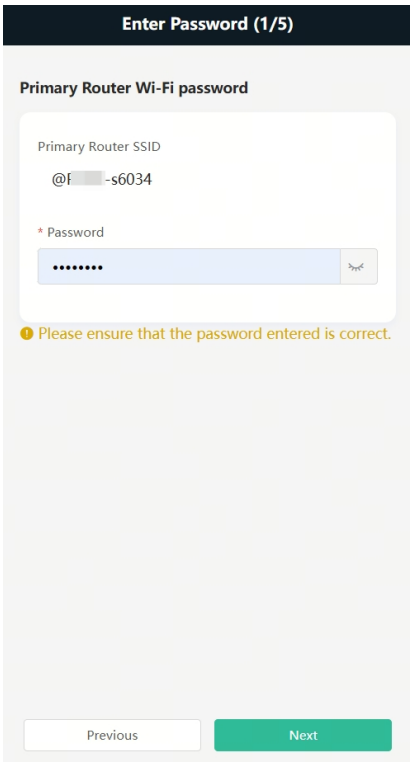
In the WISP mode, the device still supports routing and DHCP. The clients connected to the primary router are assigned IP addresses by the primary router; the clients connected to the secondary router are assigned IP addresses by the secondary router.

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

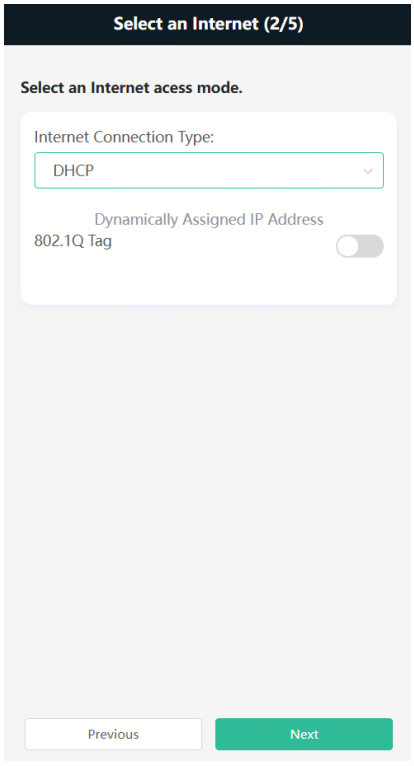


(2) Select the SSID of the primary router, and enter the Wi-Fi password to connect to the primary router. Tap **Next**.

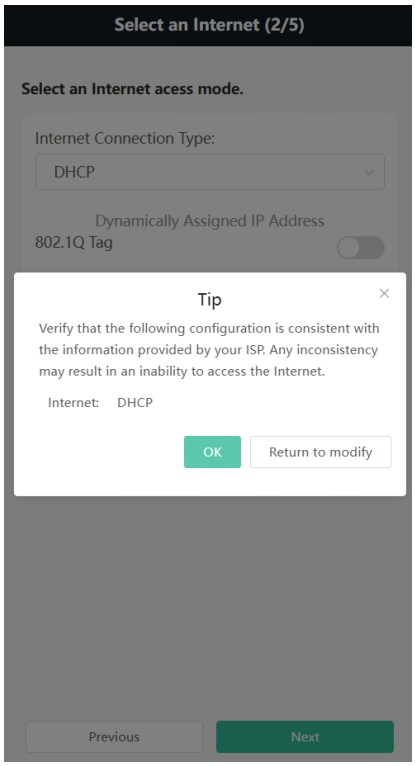




(3) Select an Internet access mode. For details, see 3.3.2 2. Wireless Router Mode.

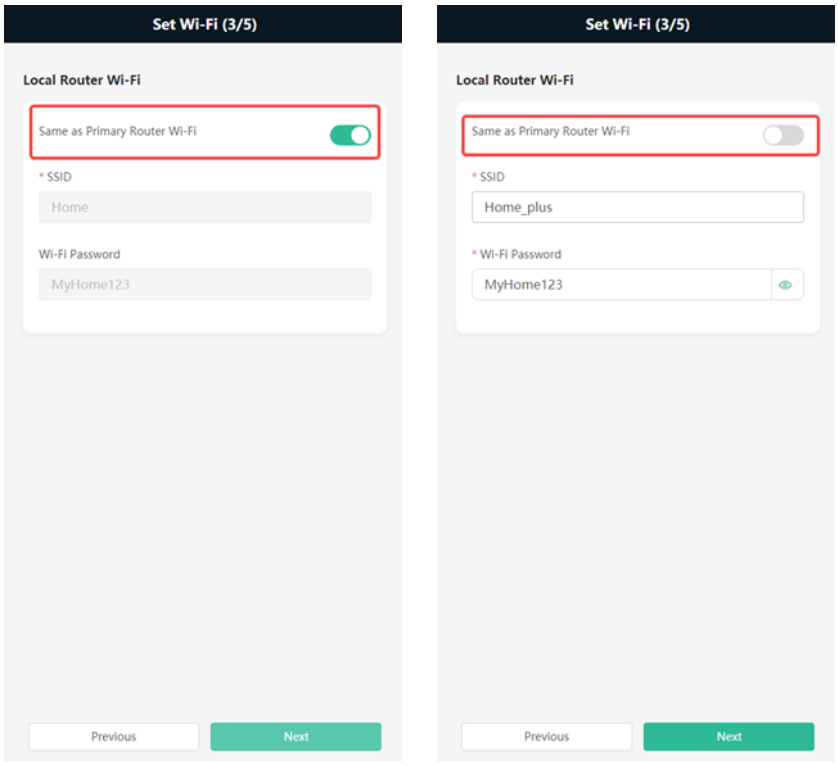


(4) Tap **Next**. Verify the Internet settings. Then, tap **OK**.

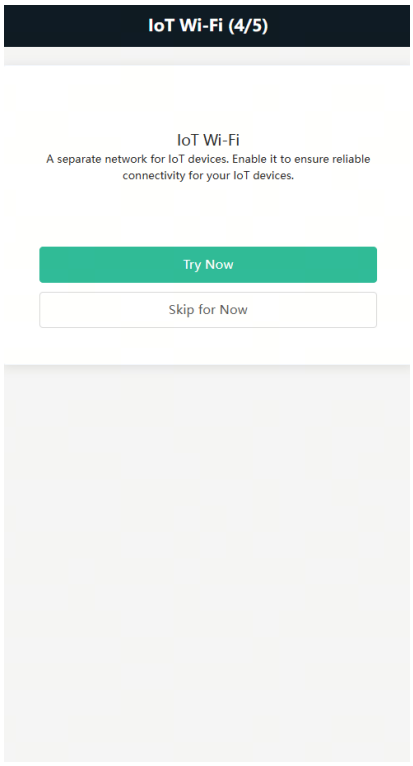


(5) Set the Wi-Fi network of the secondary router and tap **Next**.

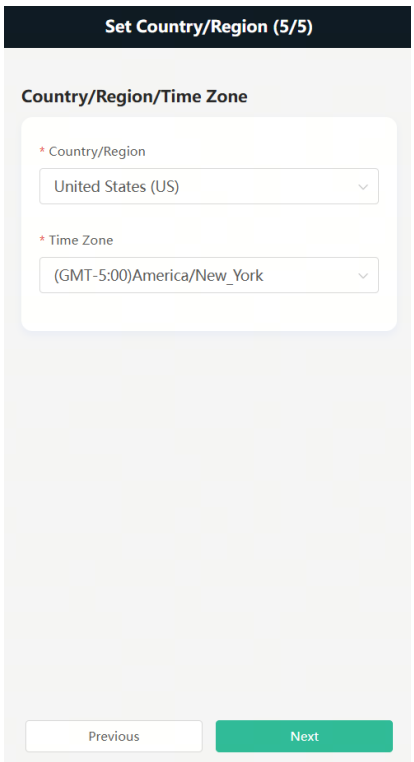
- Toggle on **Same as Primary Router Wi-Fi**. The SSID and password of the secondary router will be the same as those of the primary router.
- Toggle off **Same as Primary Router Wi-Fi**. You need to set a separate SSID and password for the secondary router.



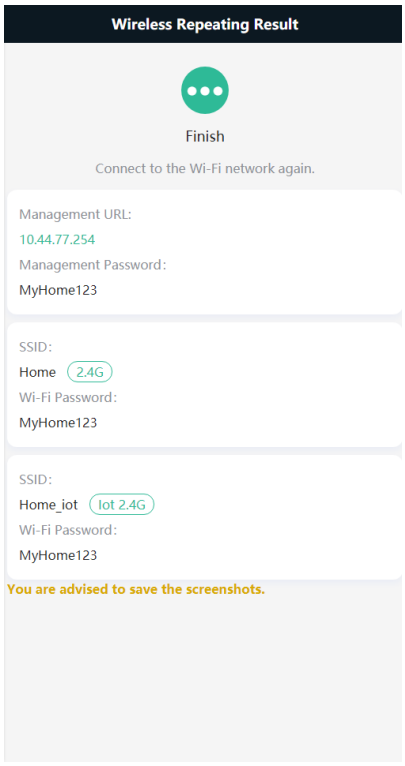
(6) Enable IoT Wi-Fi as required. For detailed configuration, see 3.3.4 Configuring IoT Wi-Fi.



(7) Set **Country/Region** and **Time Zone.** You are advised to choose the correct country or region, as well as the appropriate time zone. Tap **Next**.



(8) Wait for 1 to 2 minutes. When the system LED of the secondary router turns solid green, the Wi-Fi extension is successful. After configuration is complete, the Wi-Fi networks configured on the router will automatically restart. Reconnect to a network with a new SSID using the configured password. Tap **Management URL** to go to the eWeb management page.



4.3 Verification and Testing

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

5 Wi-Fi Network Settings

5.1 Changing the SSID and Password

Mobile Phone View: Choose **Wi-Fi**.

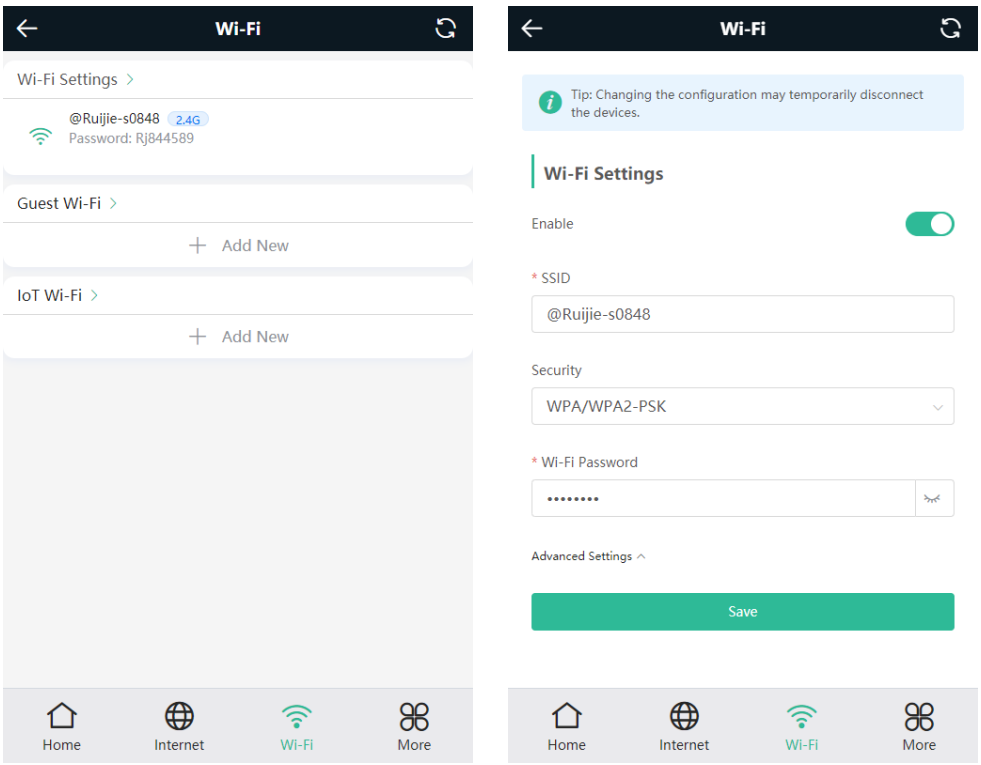
PC View: Choose **More** > **WLAN** > **Wi-Fi** > **Wi-Fi Settings/Guest Wi-Fi/IoT Wi-Fi**.

Click the target Wi-Fi network.

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.



5.2 Hiding the SSID

5.2.1 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.

5.2.2 Getting Started

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

5.2.3 Configuration Steps

Mobile Phone View: Choose **Wi-Fi**.

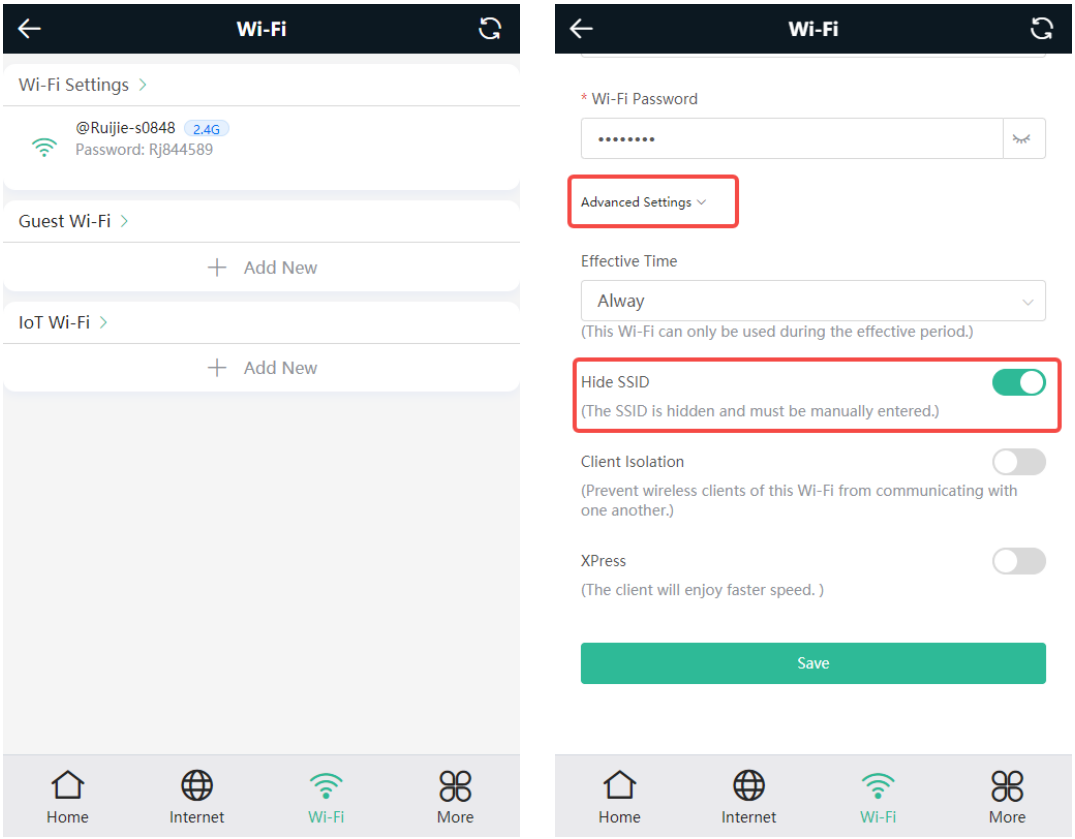
PC View: Choose **More** > **WLAN** > **Wi-Fi** > **Wi-Fi Settings/Guest Wi-Fi/IoT Wi-Fi**.

Click the target Wi-Fi network.

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**.

5.3 Adding a Wi-Fi Network

5.3.1 Overview

The router supports three types of Wi-Fi networks: primary Wi-Fi network, guest Wi-Fi network, and IoT 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.

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

5.3.2 Configuration Steps

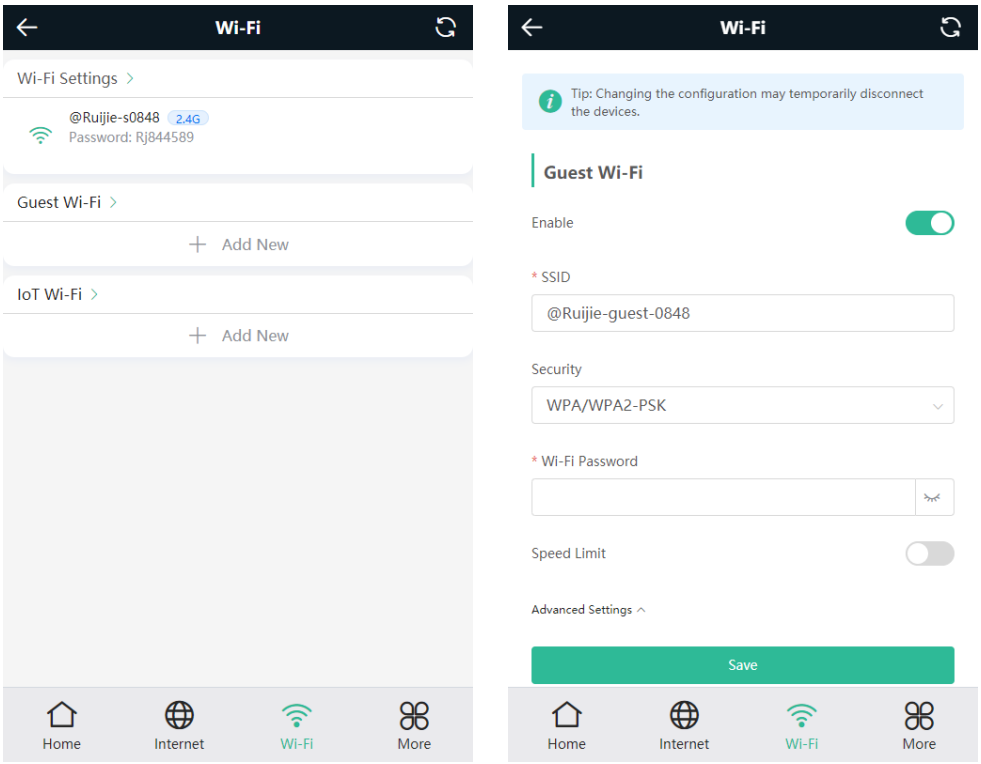
Mobile Phone View: Choose **Wi-Fi**.

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

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

Note

To ensure security, you are advised to configure a Wi-Fi password that contains at least eight characters, including digits, letters, and special characters.

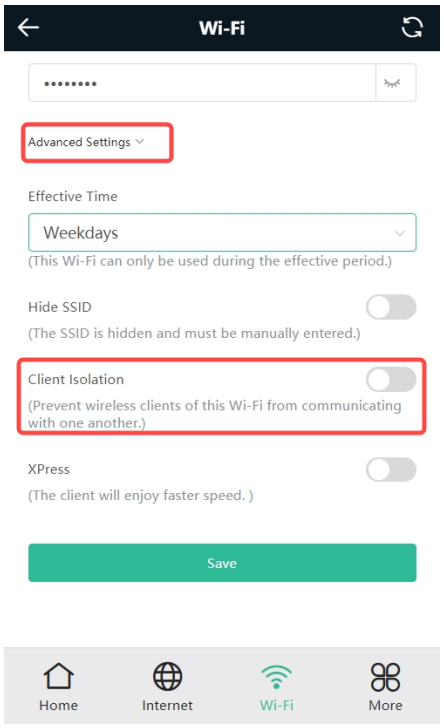


- **Effective Time:** For the host Wi-Fi network and IoT Wi-Fi, options include Weekdays, Weekends, All Time and Custom. When Custom is selected, you can select a custom effective time. This Wi-Fi can only be used during the effective period

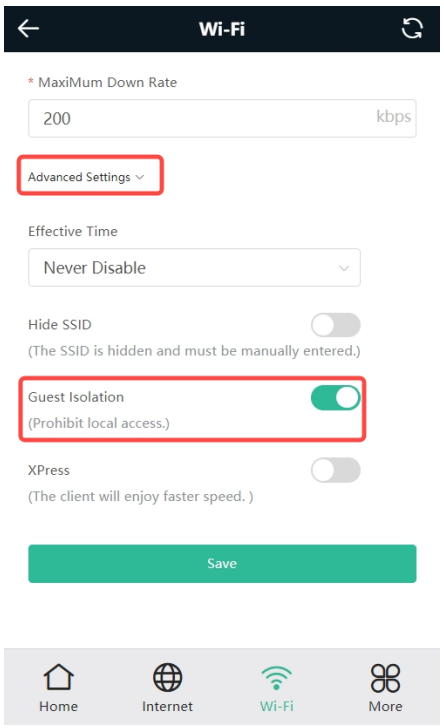
  The guest Wi-Fi network can be turned off as scheduled. Options include Never Disable, Disable 1 Hour Later, Disable 6 Hours Later, Disable 12 Hours later and Other Time. When the time expires, the guest network is off.

- **Client Isolation/Guest Isolation**: This feature is supported by **Wi-Fi Settings**/**Guest Wi-Fi**.

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

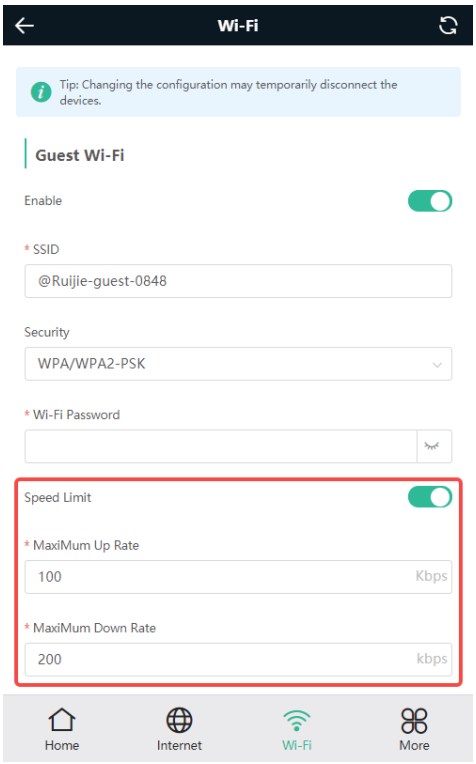


You can enable **Guest Isolation** in **Guest Wi-Fi** to enable wireless clients on the Guest Wi-Fi to access the Internet, and to prevent them from accessing the intranet and from communicating with each other.



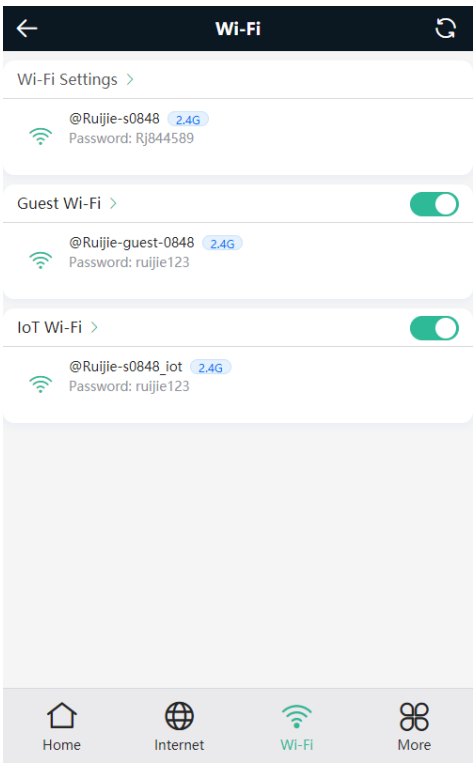
- **Speed Limit:** You can set a rate limit for the Guest Wi-Fi.

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



5.3.3 Verification and Testing

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



5.4 Configuring the Wi-Fi Blocklist or Allowlist

5.4.1 Overview

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

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

Note

To prevent an unknown client from invading your home network, you can create a Wi-Fi allowlist, and add common wireless clients such as home devices and IoT devices to the allowlist while blocking the access from all unknown clients.

5.4.2 Configuration Steps

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

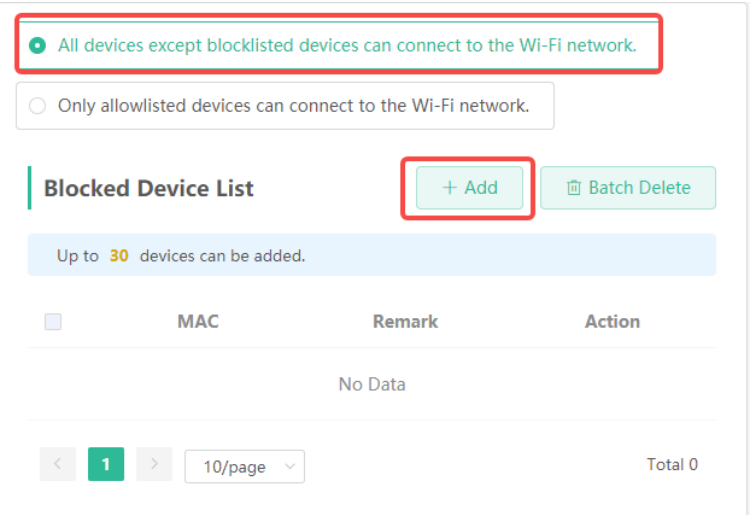
PC View: Choose **More** > **WLAN** > **Blocklist/Allowlist**.

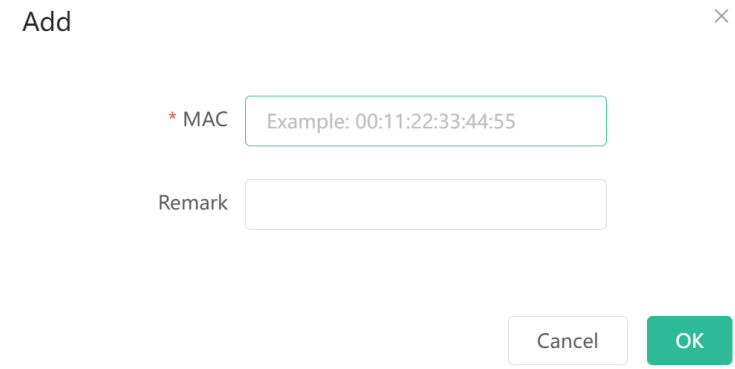
(1) Select the blocklist mode and click **Add**. The default mode is blocklist mode.

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.

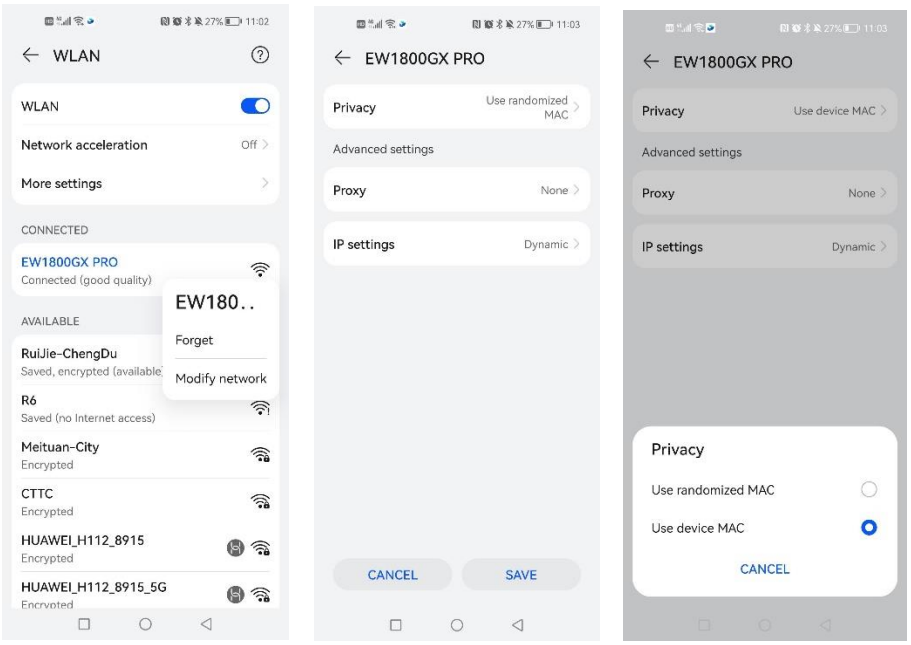




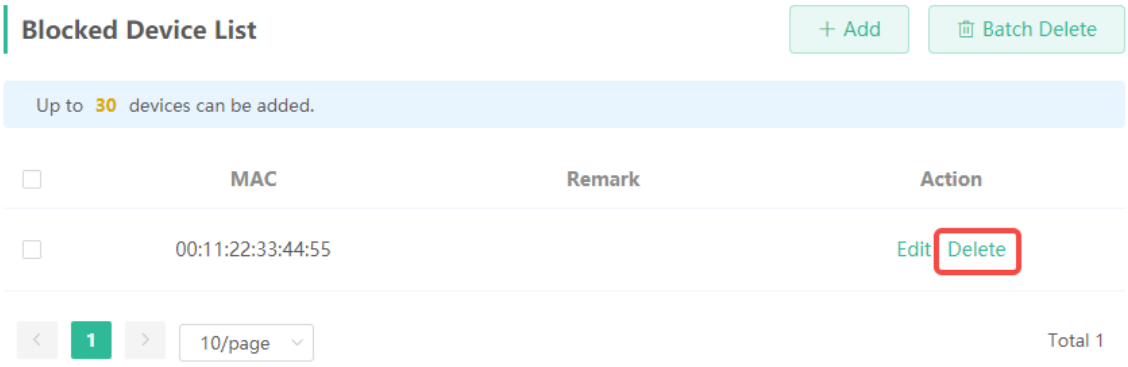
Note

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.



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



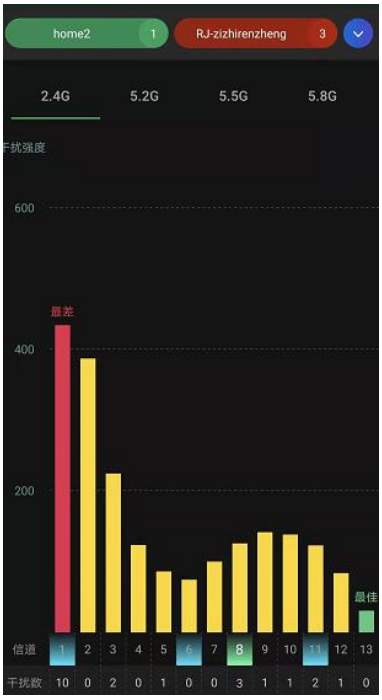
5.5 Optimizing the Wi-Fi Network

5.5.1 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 8.6 Configuring Scheduled Reboot. You can also analyze the wireless environment around the router and select appropriate parameters.

5.5.2 Getting Started

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



5.5.3 Configuration Steps

- Optimizing the radio channel

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

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

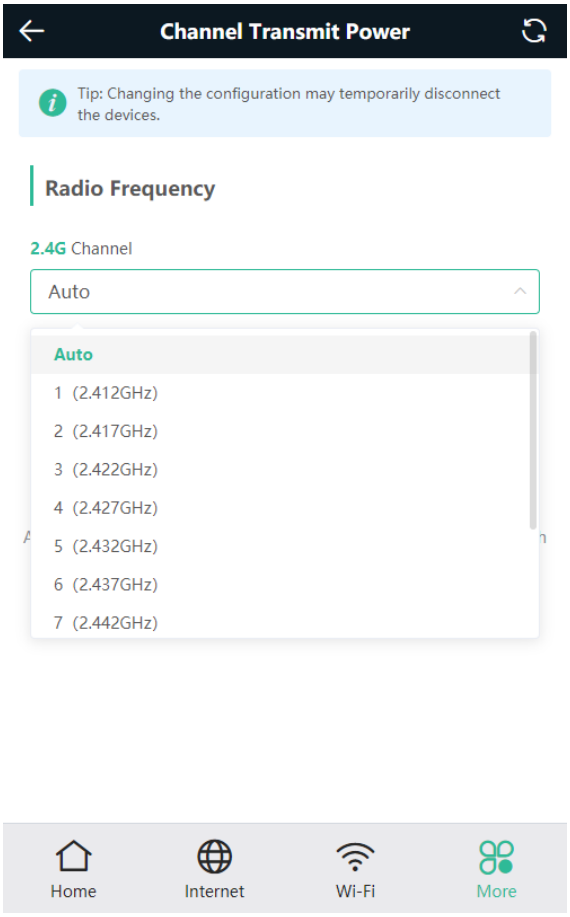
Choose the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. Excess clients connected to a channel can bring stronger wireless interference.

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**> **Radio Frequency**.

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

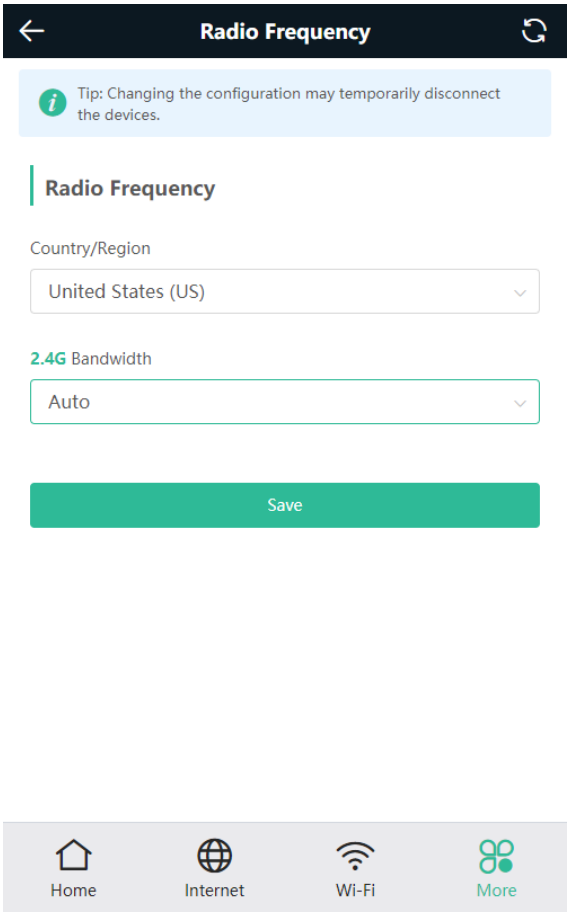
If the interference is severe, choose a lower channel bandwidth to avoid network stalling. You can select 20MHz and 40MHz bandwidths for the 2.4GHz band. The default value is "Auto", indicating that the bandwidth will be automatically selected based on the wireless environment.

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.



- Optimizing the transmit power

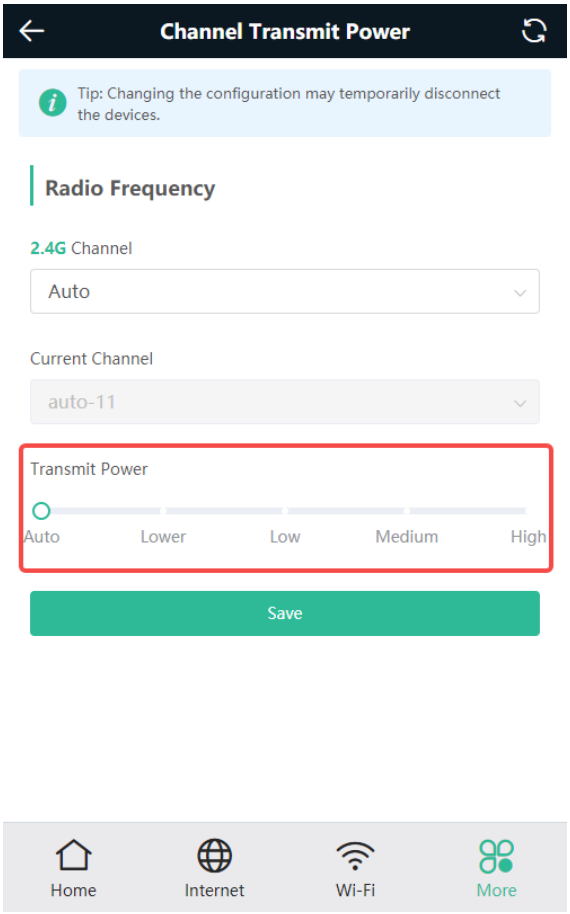
Mobile Phone View: Choose **More** > **Channel Transmit Power**.

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.

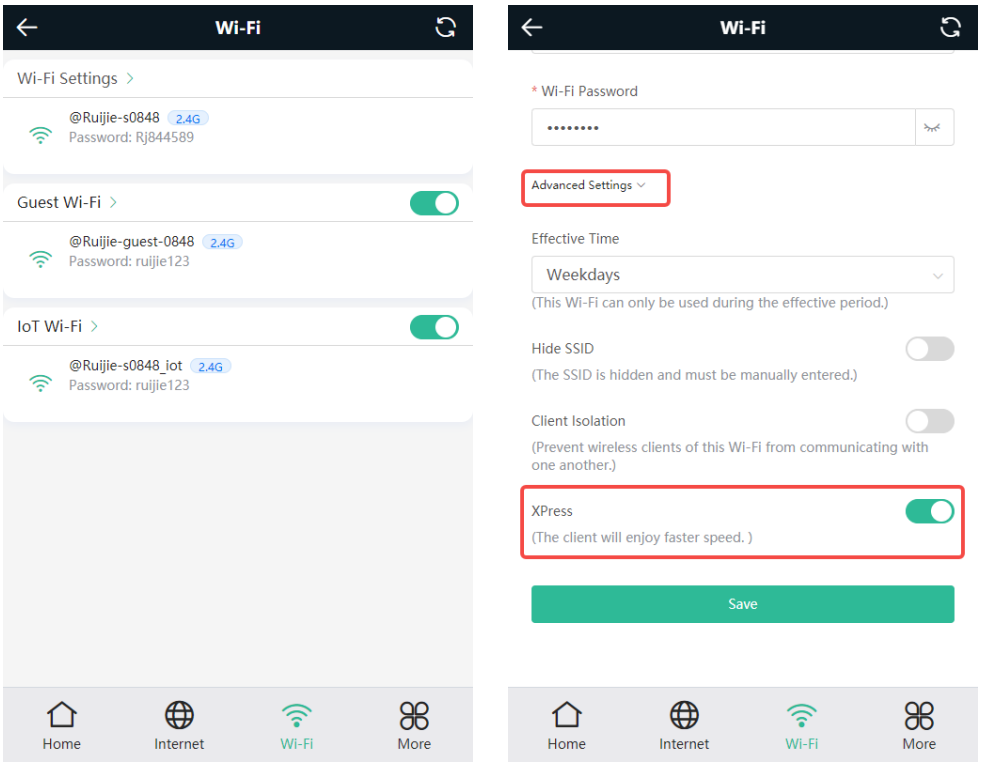


5.6 Configuring XPress

Mobile Phone View: Choose **Wi-Fi** > **Advanced Settings** > **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.



5.7 Configuring Wi-Fi/IGMP

5.7.1 Overview

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

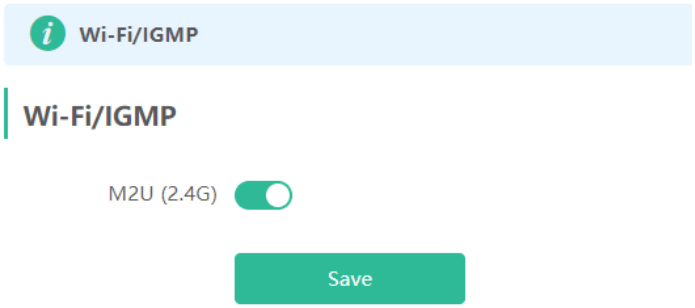
When it comes to routers, the terminals connected to them are fixed, so multicast packets only need to be forwarded to specific terminals. By enabling WIFI/IGMP and converting the multicast packets into unicast packets, the packets can then be forwarded to the designated terminals in the multicast group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

5.7.2 Configuration Steps

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

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

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



5.8 Configuring the Health Mode

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

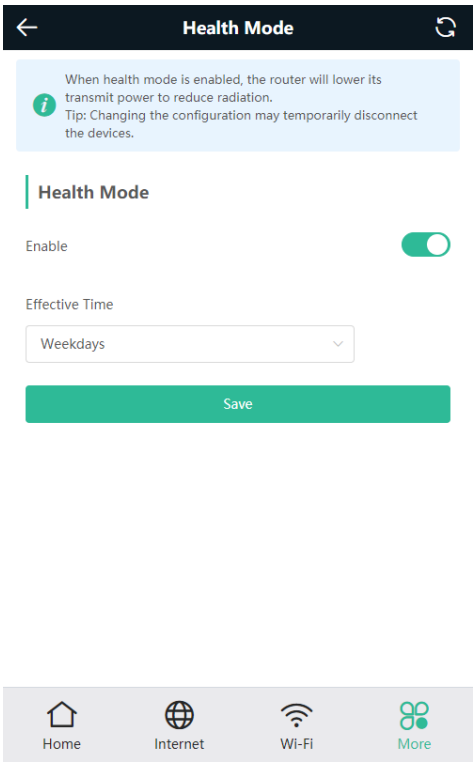
PC View: Choose **More** > **WLAN** > **Wi-Fi** > **Health Mode**.

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.



6 Networks Settings

6.1 Displaying SIM Card Information

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



6.2 Managing the SIM Card

Note

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

6.2.1 Configuring Network Access for a SIM Card

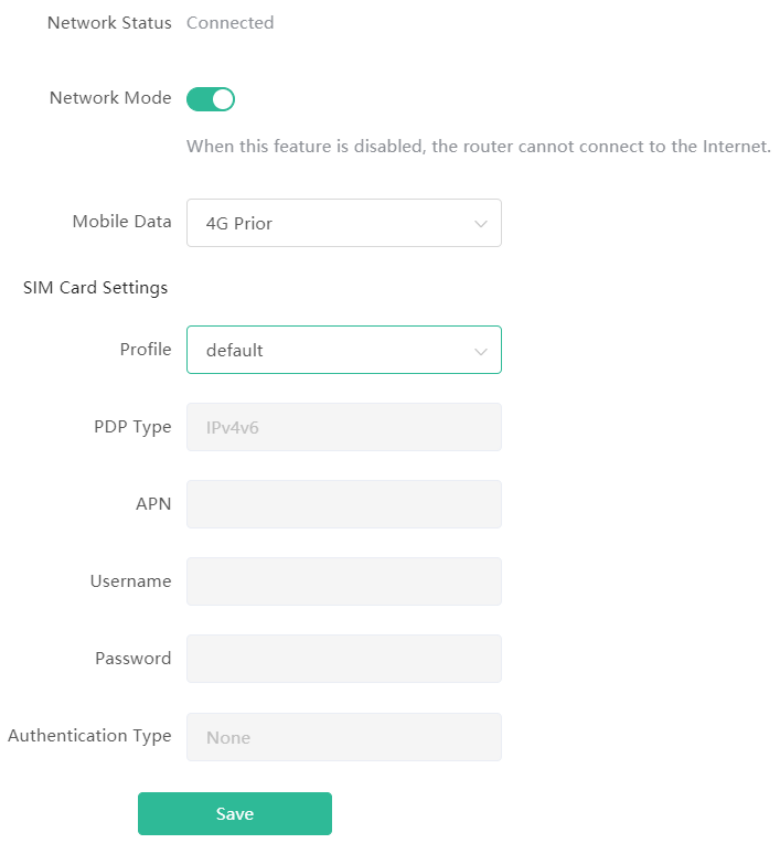
Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Basics** > **Network Access > Network Access**.

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

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

Caution

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



- **Mobile Data**

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

- **Profile**

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

- **PDP Type**

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

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

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

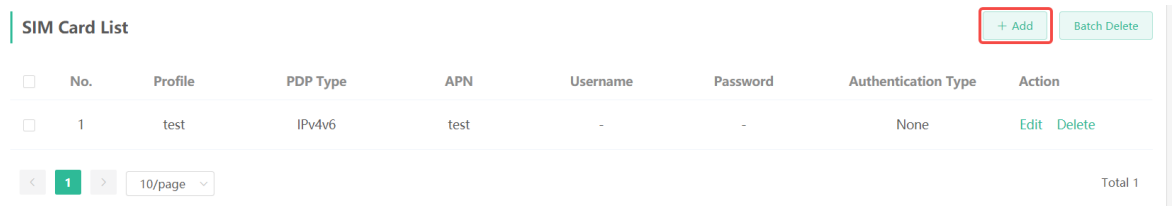
- **Authentication Type**
  - An authentication type refers to the authentication mode used when the router connects to the mobile network. Common authentication modes include Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP).
  - These authentication modes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

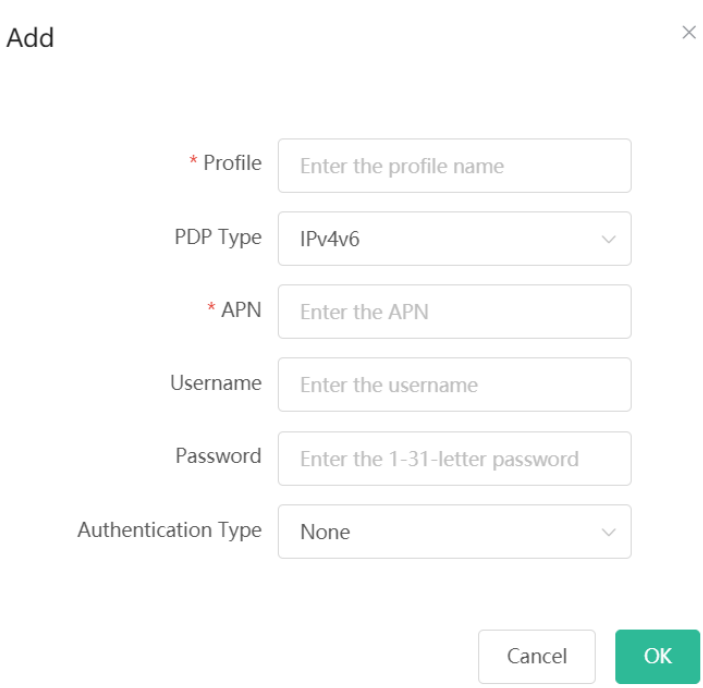
6.2.2 Displaying the SIM Card List

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

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

Click **Add** to create an SIM profile. Select the protocol type for establishing a data connection, and configure **APN**, **Username**, **Password**, and **Authentication Type**. For parameter descriptions, see 6.2.1 Configuring Network Access for a SIM Card.





6.3 Managing the PIN

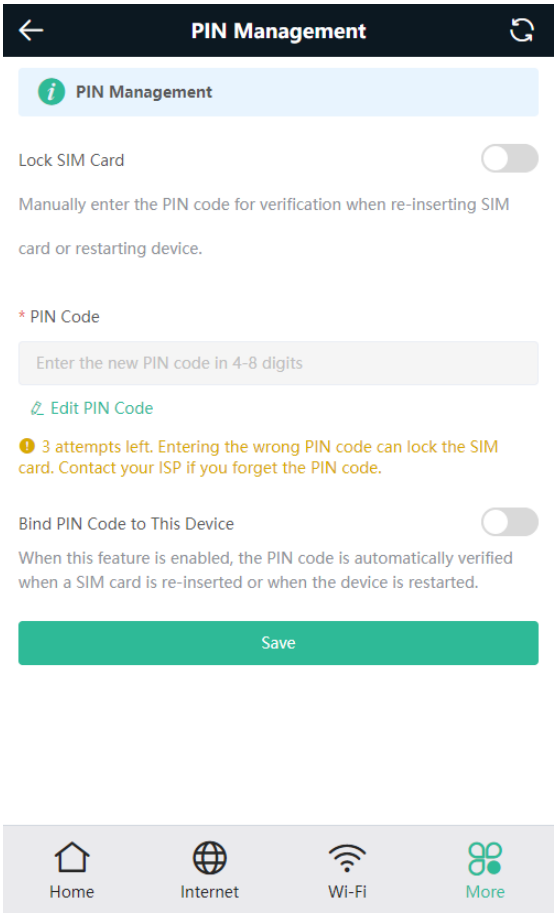
Note

This function is only supported when the router works in **3G/4G Router Mode**.

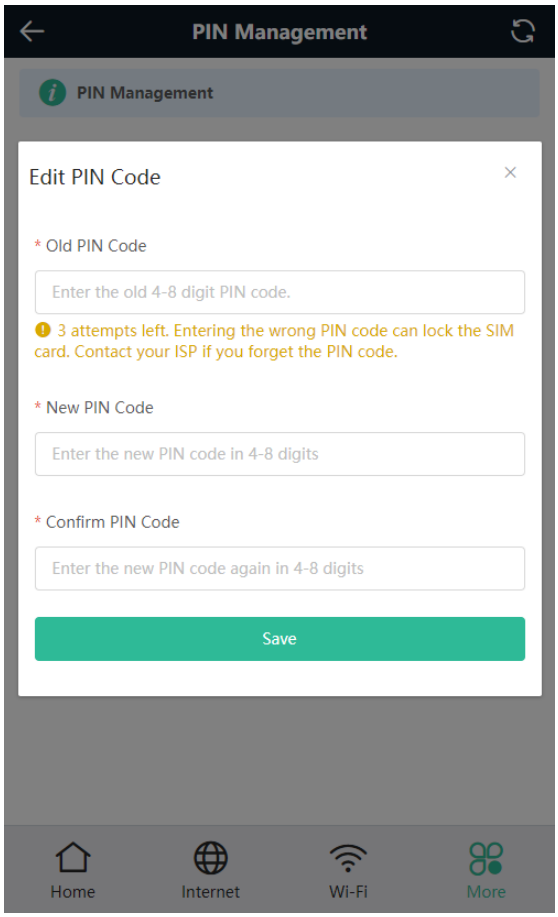
Mobile Phone View: Choose **More > PIN Management.**

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

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



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



Caution

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

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

Note

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

6.4 Managing SMS

Note

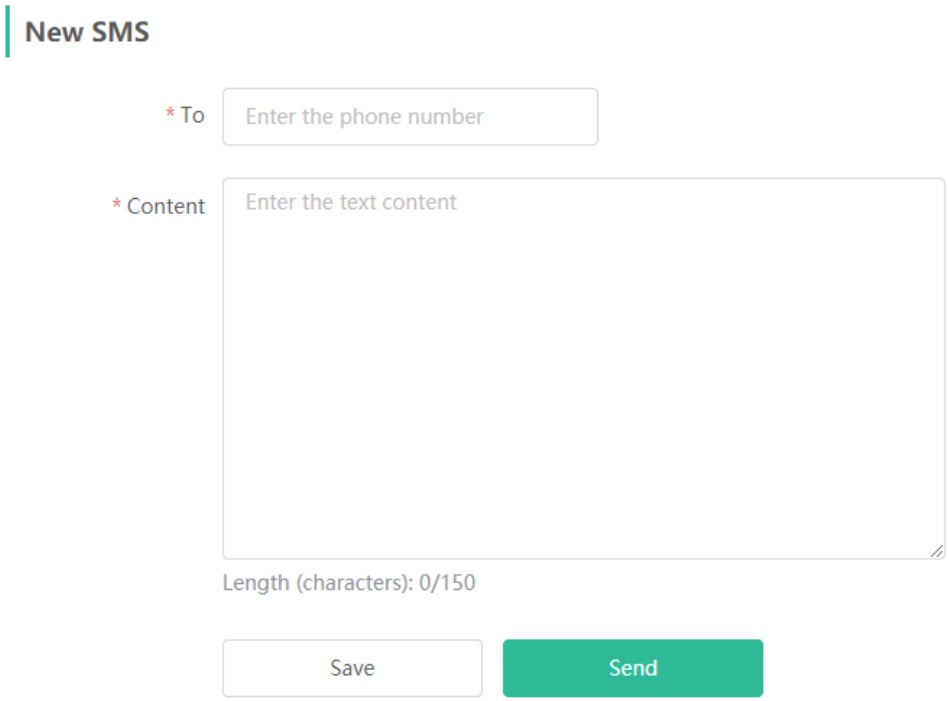
This function is only supported when the router works in **3G/4G Router Mode**.

6.4.1 Creating an SMS Message

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

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

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

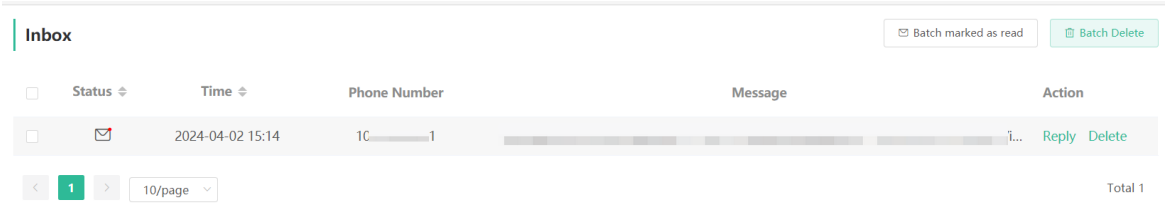


6.4.2 Displaying the Inbox

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

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

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

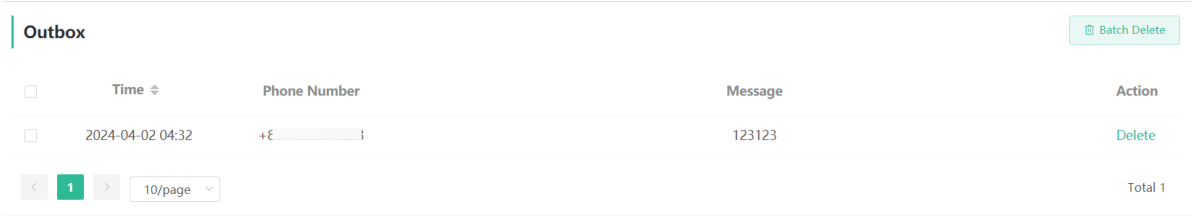


6.4.3 Displaying the Outbox

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

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

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

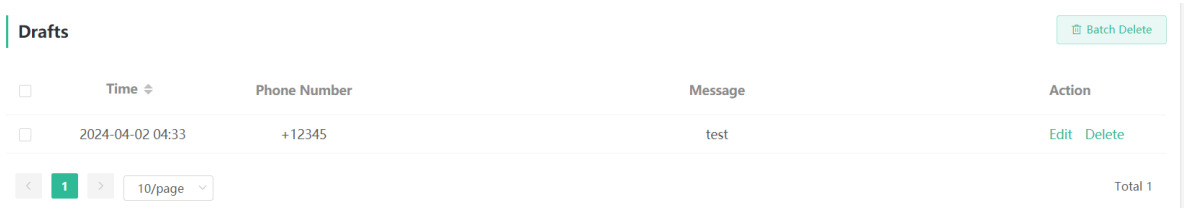


6.4.4 Displaying the Drafts Box

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

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

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



6.5 Configuring Internet Connection Type

Note

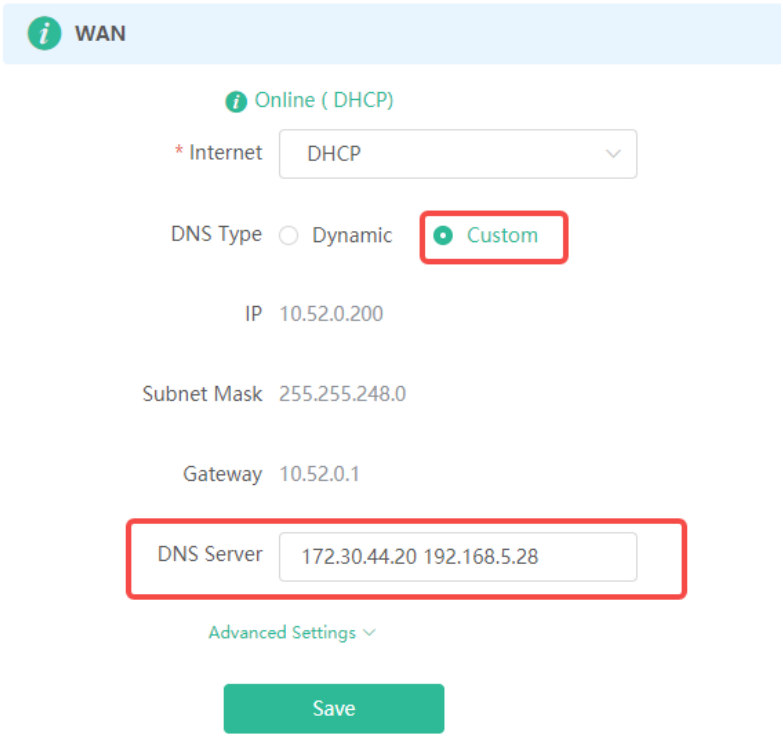
This function is only supported when the router works in **Wireless Router Mode**.

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 3.3.2 2. Wireless Router Mode.

For **DCHP** Internet connection types, you can manually configure a DNS.



6.6 Changing the MAC Address

Note

This function is only supported when the router works in **Wireless Router Mode**.

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**.

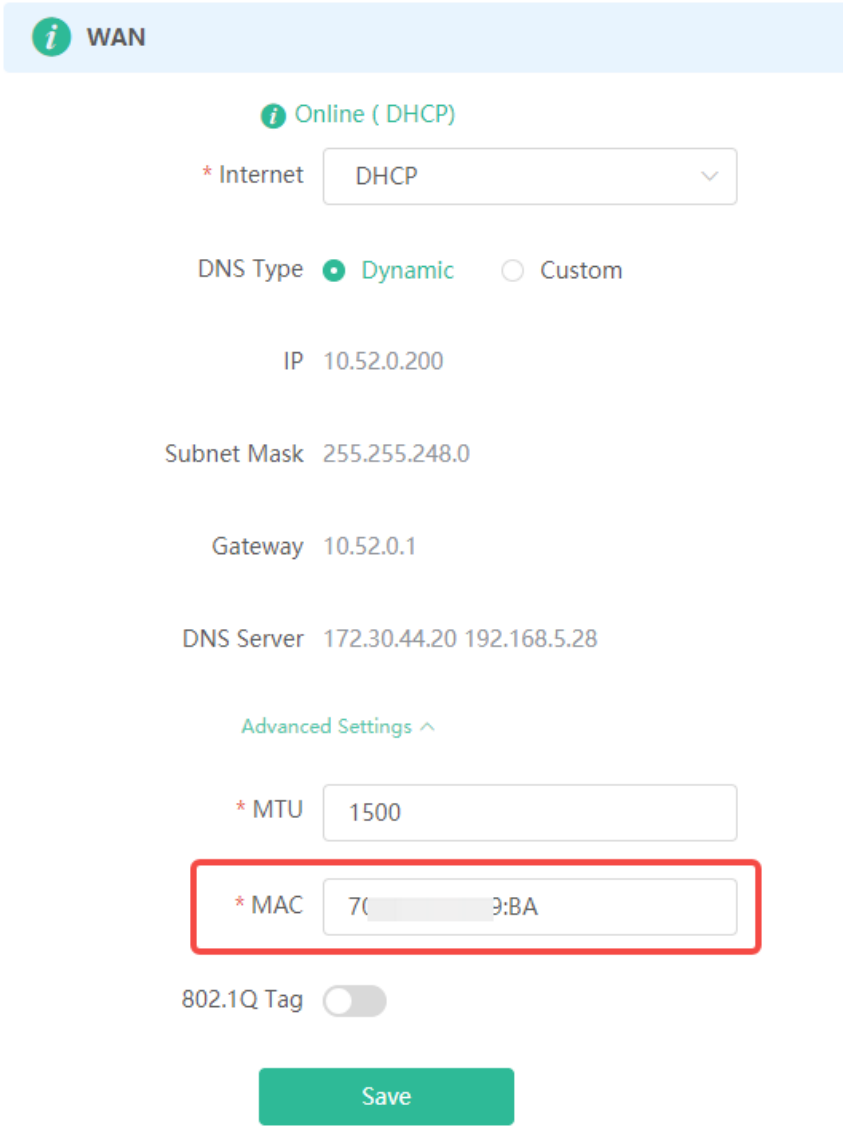
PC View: Choose **More** > **Basics** > **WAN** > **Advanced Settings**.

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.



6.7 Changing the MTU

Note

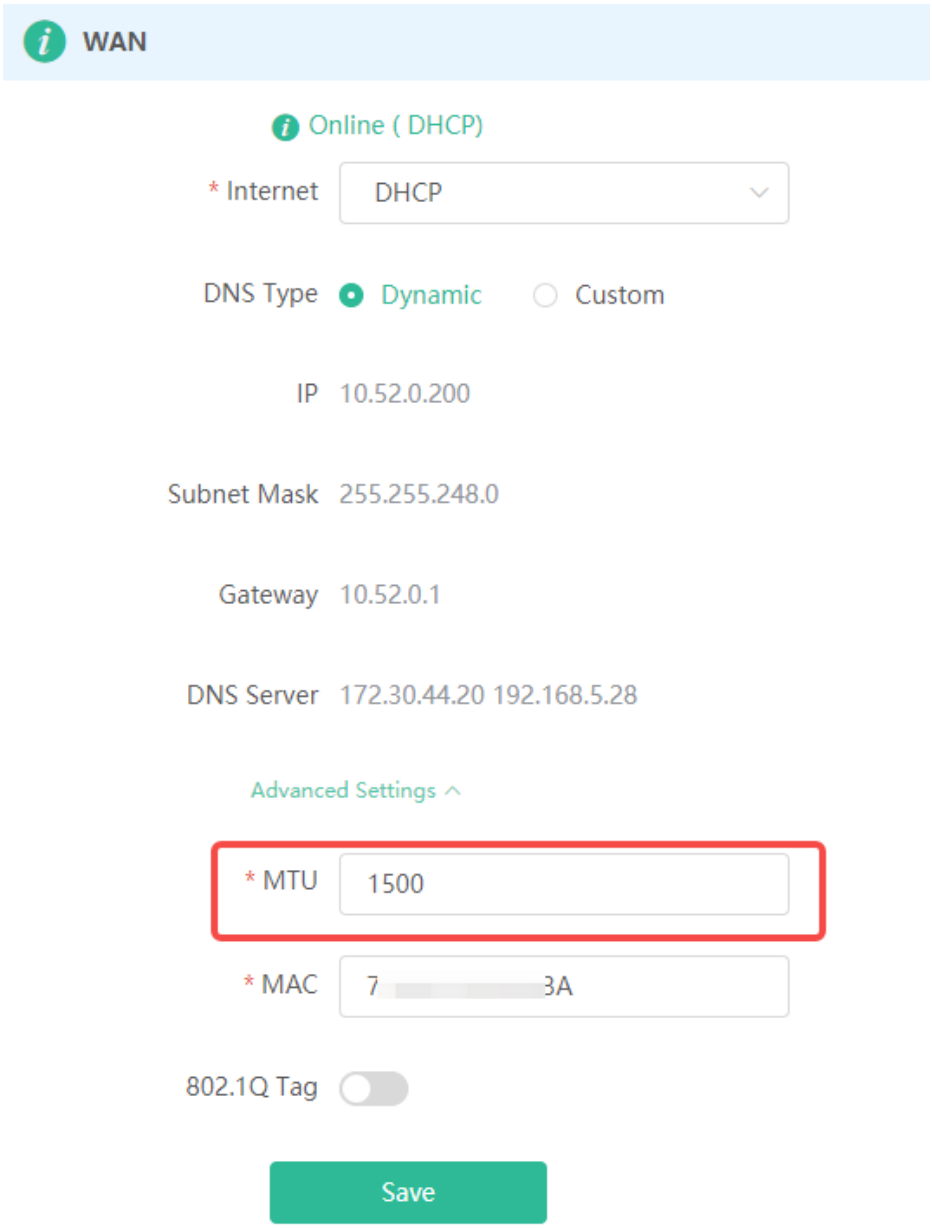
This function is only supported when the router works in **Wireless Router Mode**.

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.



6.8 Changing the Address of a LAN Port

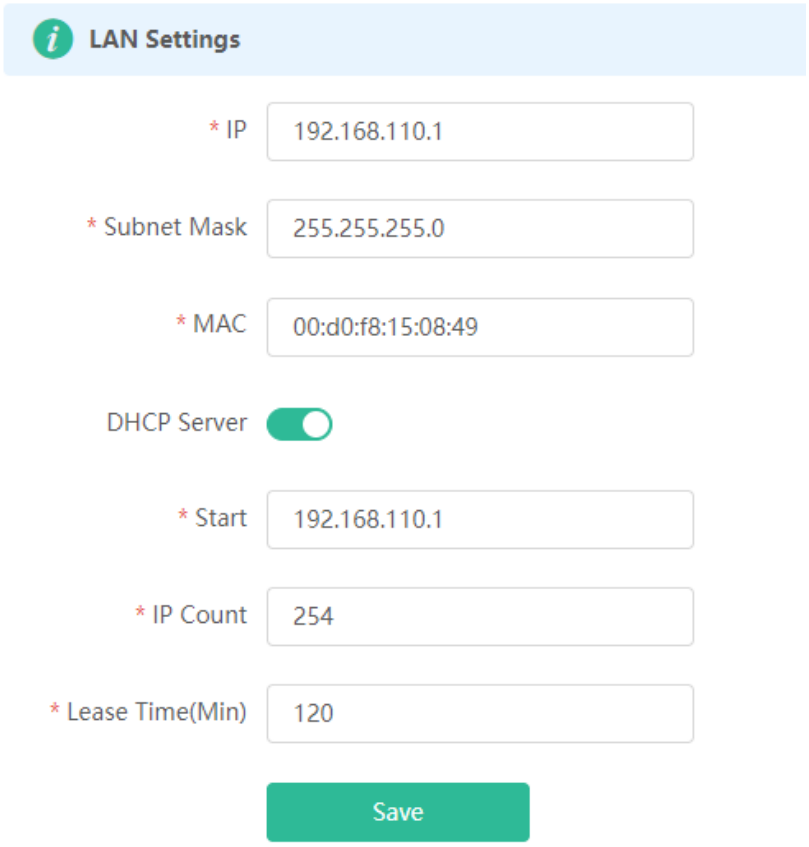
Mobile Phone View: Choose **More** > **LAN**.

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

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 web interface 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.



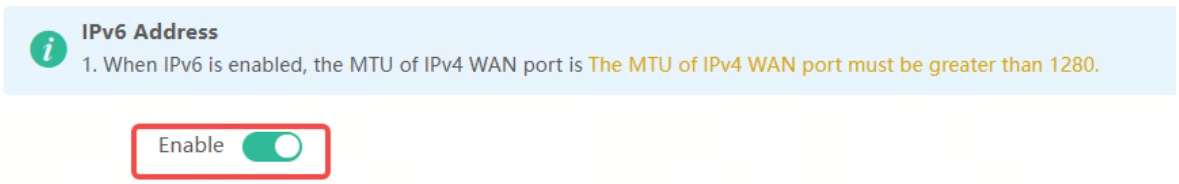
6.9 Configuring IPv6 Address

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** > **WAN Settings**.

PC View: **More** > **Basics** > **IPv6** > **WAN Settings**.

Toggle on **Enable** to enable the IPv6 feature.



6.9.1 Configuring the IPv6 Address of the WAN Port

Smartphone View: Choose **More** > **Switch to PC** > **More** > **Basics** > **IPv6** > **WAN Settings**.

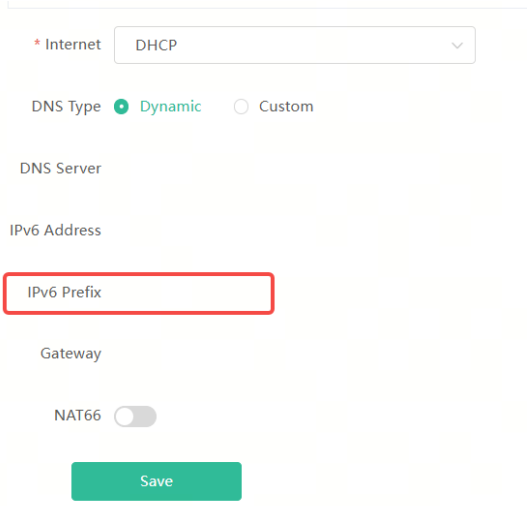
PC View: **More** > **Basics** > **IPv6** > **WAN Settings**.

(1) Set Internet connection type:

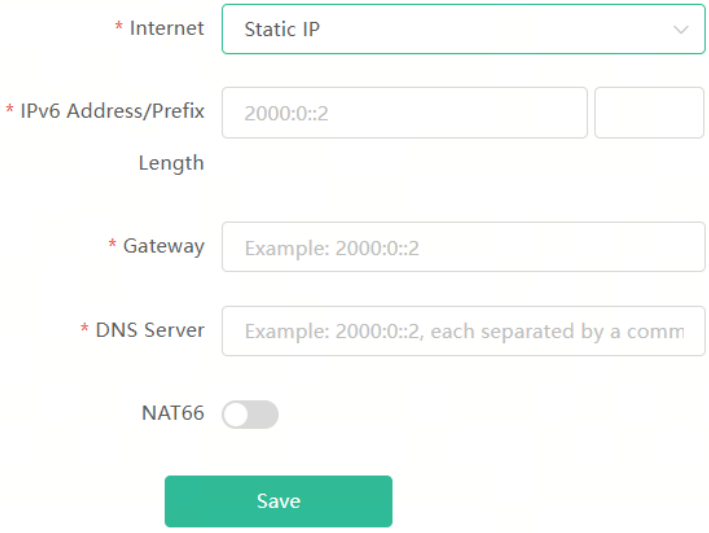
- If you select **DHCP**, and the device will get an IPv6 from the upstream device.

Note

When **IPv6 Prefix** is empty, the WAN port has not obtained an IPv6 prefix. In this case, you can toggle on NAT66 and manually configure an IPv6 prefix on the **LAN Settings** tab page. If the fault persists, you are advised to consult the local ISP about the IPv6 status of the network.



- If you select **Static IP**, please configure the IPv6, gateway address and DNS server address manually.



- If you select **NULL**, the IPv6 function will be disabled on the WAN port.

6.9.2 Click Save.Configuring the IPv6 Address of the LAN Port

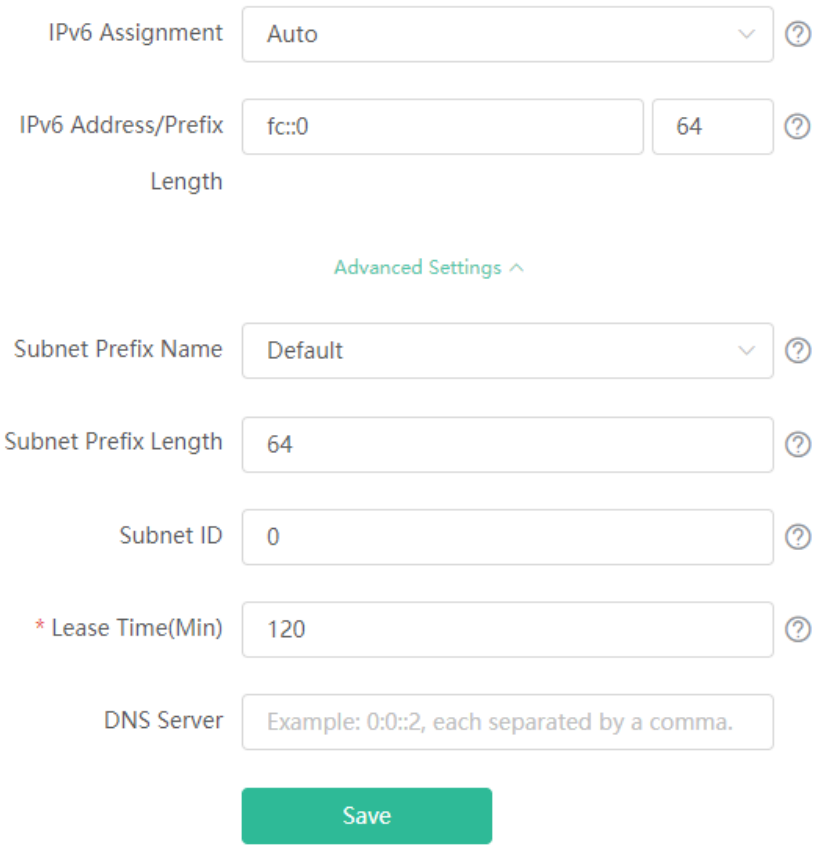
Mobile Phone View: Choose **More** > **Switch to PC** > **More** > **Basics** > **IPv6** > **LAN Settings**.

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

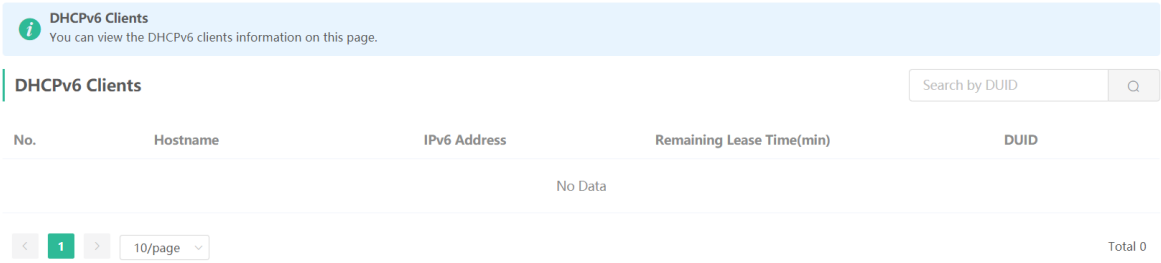


6.9.3 Viewing DHCPv6 Clients

Mobile Phone View: Choose **More** > **Switch to PC** > **More** > **Basics** > **IPv6** > **DHCPv6 Clients**.

PC View: **More** > **Basics** > **IPv6** > **DHCPv6 Clients**.

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



6.10 Enabling Parental Control

Mobile Phone View: Choose **Home** > **Client List**.

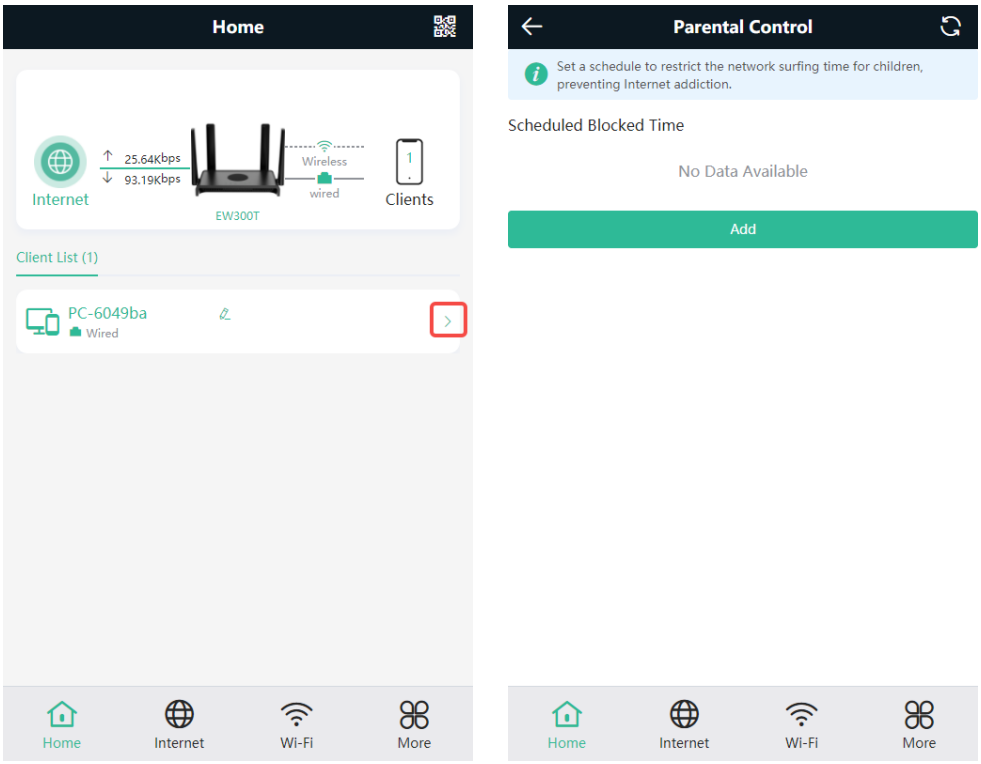
PC View: Choose **Clients** > **Add Blocking Schedule.**

Caution

- This function is only supported 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.

Click the right arrow icon next to the client device to access the **Parenteral Control** configuration page. Click **Add** on the page that opens to set Internet block periods.

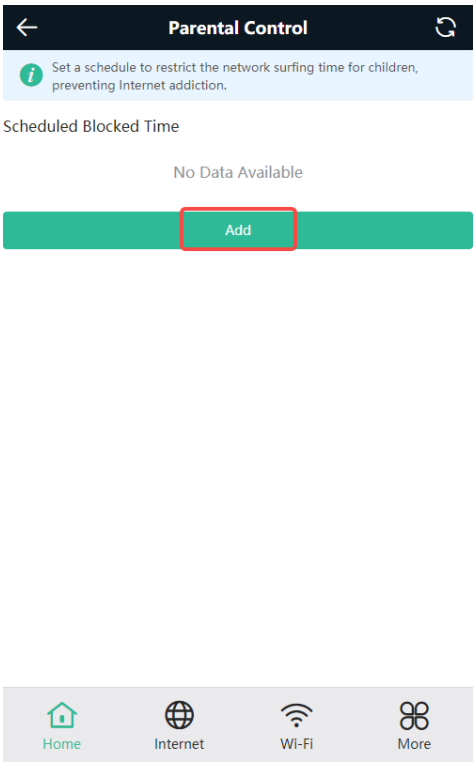


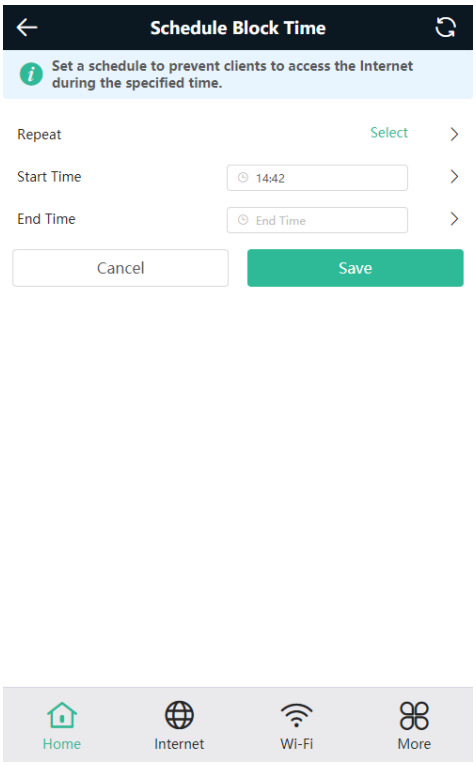
6.10.1 Setting the Internet Block Periods

1. Setting the Internet Block Rules

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

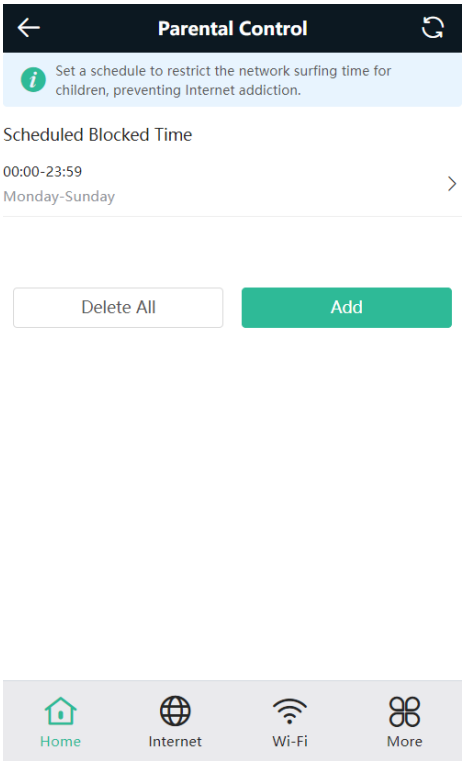
You can select certain days of the week or customize the Internet block periods.





6.10.2 Disabling Parental Control

To disable parental control, tap **Delete ALL** to lift the restrictions on the client.



6.11 Configuring Port Mapping

6.11.1 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.

6.11.2 Getting Started

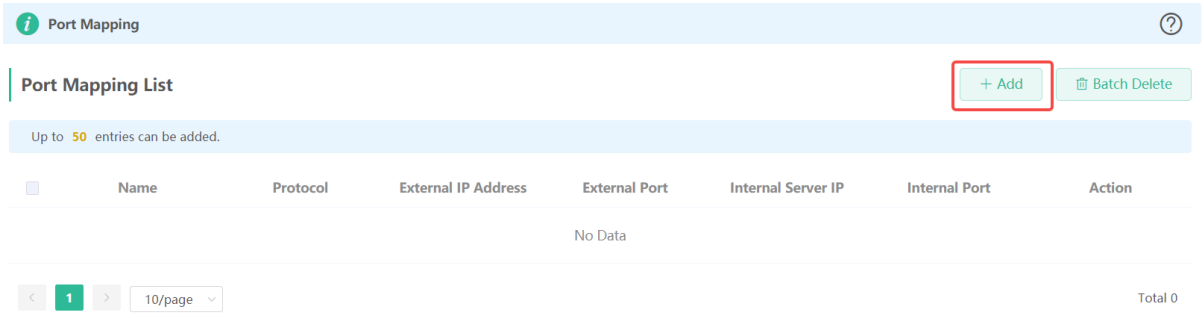
- Confirm the IP address of the target device in the internal network and service port ID.
- Ensure that port mapping is available in the internal network.
- Verify that your router has a public IP address. If the IP address is dynamic, changing it may cause port mapping failure. In this case, you are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

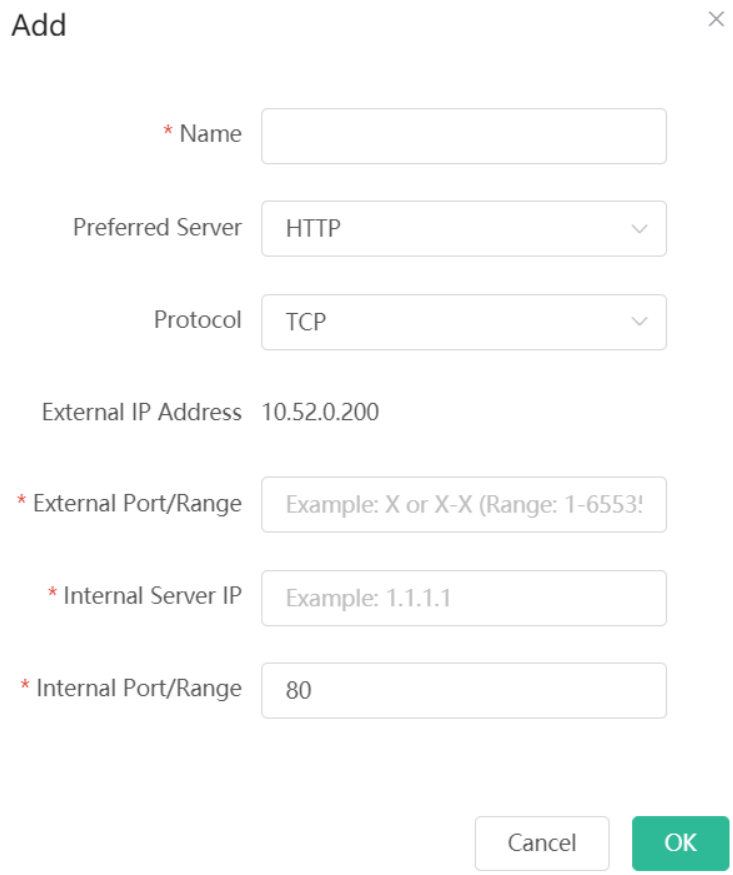
6.11.3 Configuration Steps

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

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

6.11.4 Verification and Testing

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

6.11.5 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.

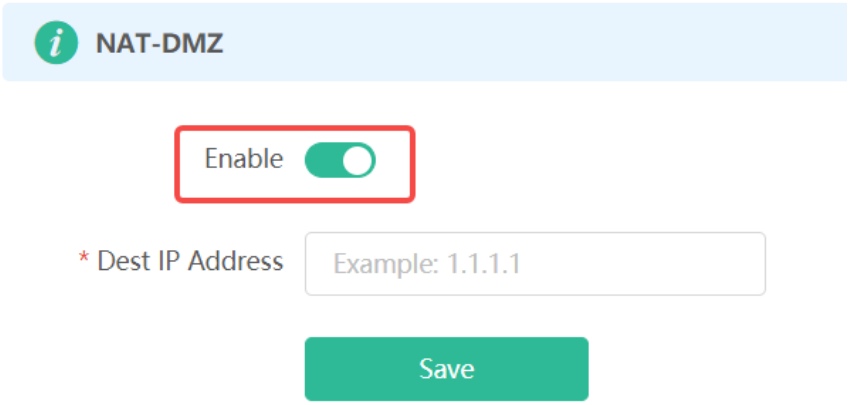
(3) Enable the DMZ service. For details, see 6.11.6 DMZ Configuration Steps. The common cause is that port configuration is incorrect or incomplete.

6.11.6 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**.



6.12 Configuring DHCP Server

6.12.1 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.

6.12.2 Configuration Steps

1. Configuring the DHCP Server Function

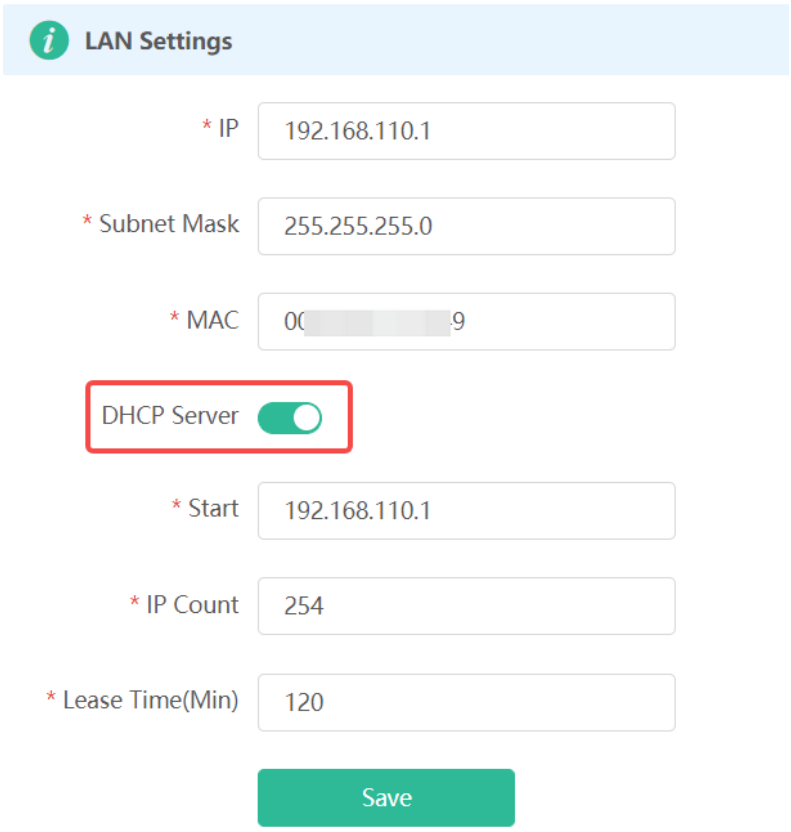
Mobile Phone View: Choose **More** > **LAN**.

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.



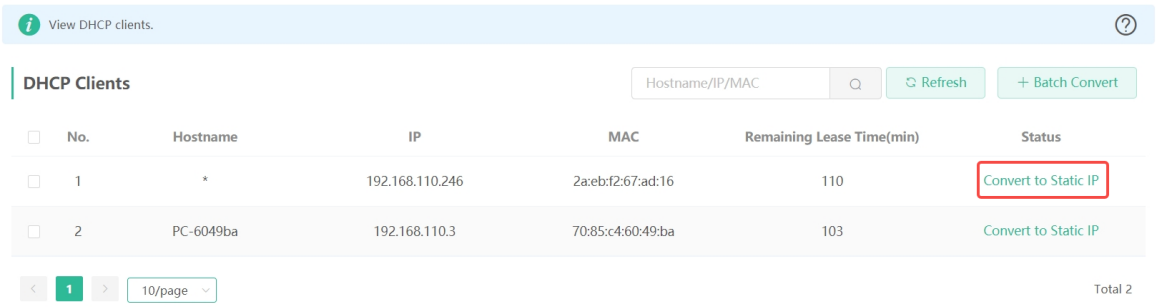
- **Start**: Enter the start IP address of the DHCP address pool. A client obtains an IP address from the address pool. If all the addresses in the address pool are used up, the client will fail to obtain the IP address.
- **IP Count**: Enter the number of IP addresses in the address pool. The default 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.

2. Displaying Online DHCP Clients

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

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

Check information about an online client. Click **Convert to Static IP**. Then, the client obtains the IP address each time connecting to the router.

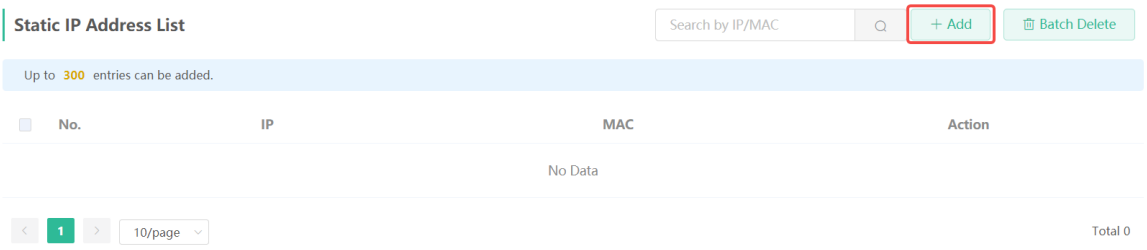


3. Displaying the DHCP Static IP Address Table

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

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

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



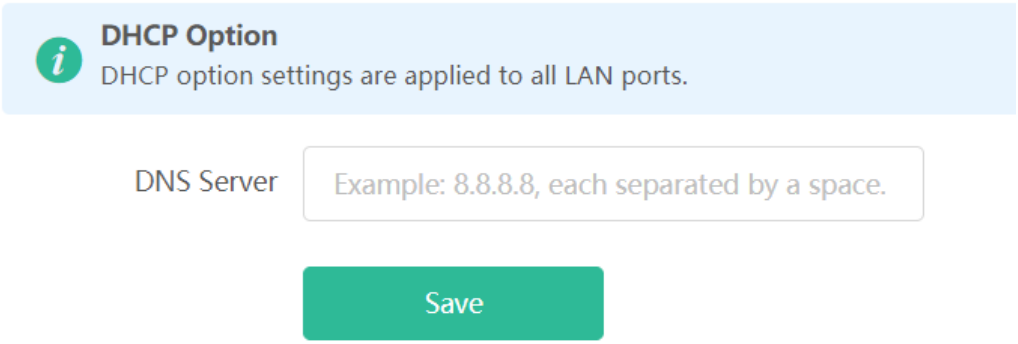
6.13 Configuring DHCP Option

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.



6.14 Configuring DNS

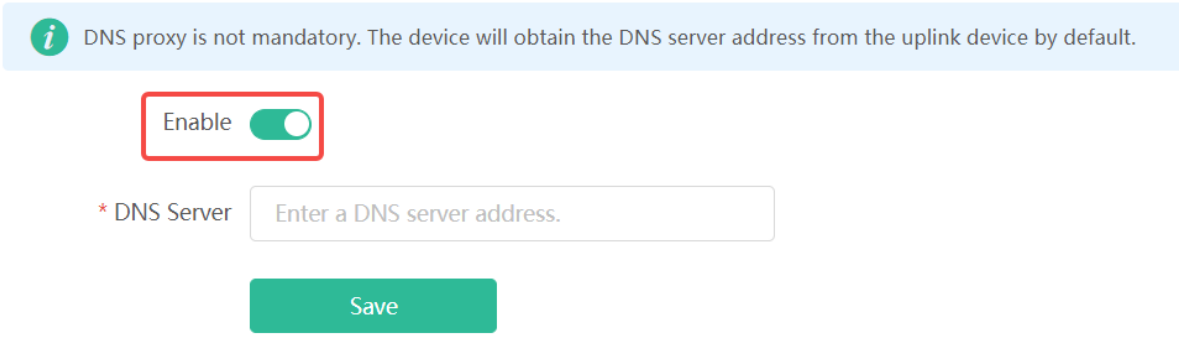
The domain name system (DNS) proxy configuration is not mandatory. The device obtains the DNS server address from the uplink device by default.

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.



6.15 Configuring DDNS

6.15.1 Overview

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

6.15.2 Getting Started

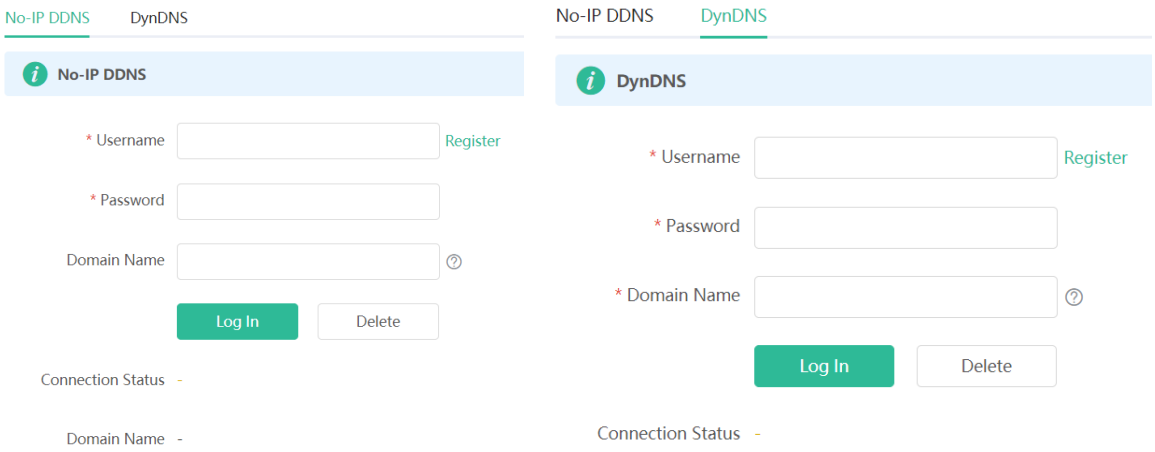
Register an account and domain name at Dyn or No-IP official website.

6.15.3 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.



6.16 Configuring ARP Binding

6.16.1 Overview

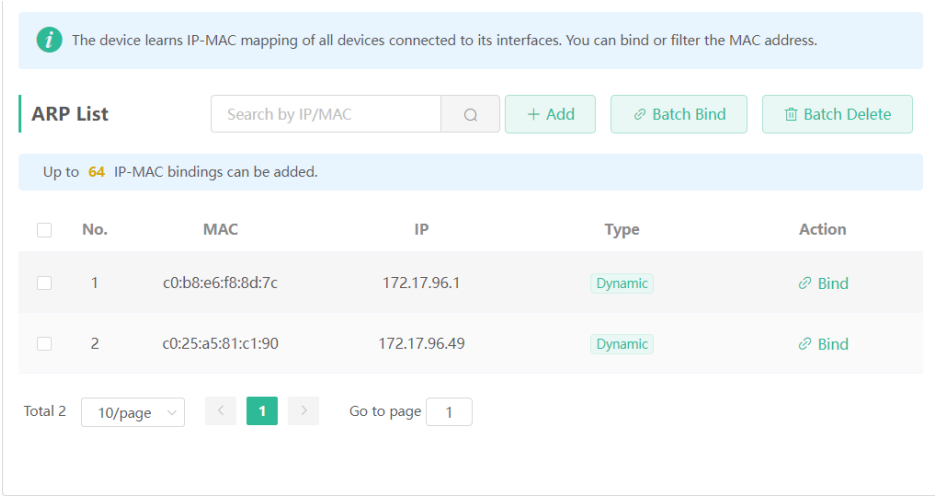
The router learns the ARP table from all devices connected to its ports. You can search for a device by its MAC address, perform ARP binding.

6.16.2 Configuration Steps

Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Security** >**ARP List**.

PC View: Choose **More** > **Security** >**ARP List**.

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



6.17 Connecting to IPTV

Note

This function is not supported when the router works in **3G/4G Router Mode**.

IPTV is an Internet television service provided by ISP.

6.17.1 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.

6.17.2 IPTV Configuration Steps (VLAN Type)

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

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

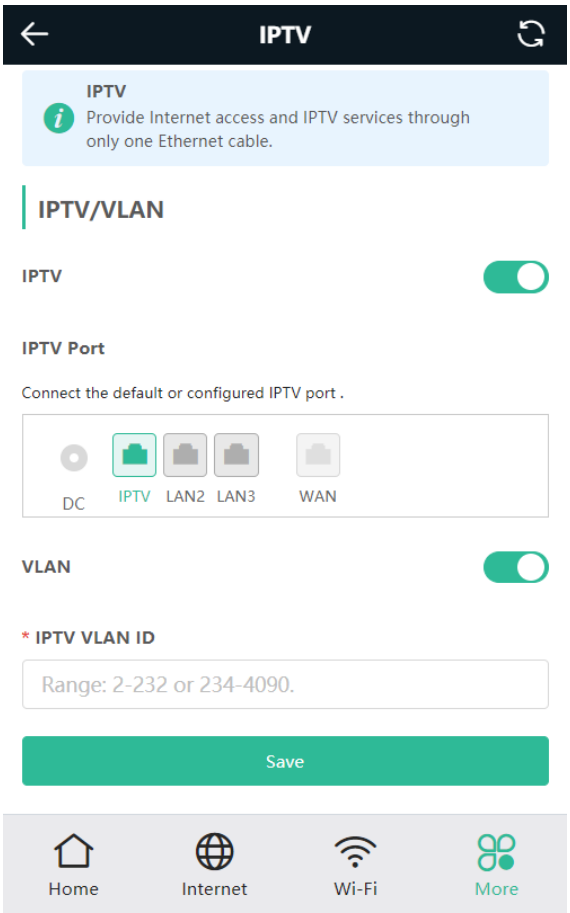
Click to enable IPTV, and select the LAN port to be connected to the IPTV STB.

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.

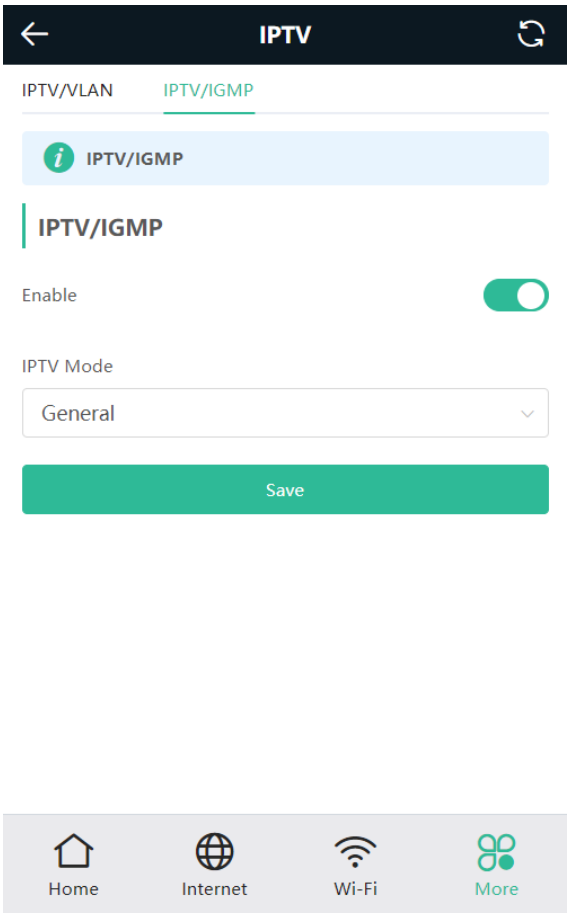


6.17.3 IPTV Configuration Steps (IGMP Type)

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

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

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



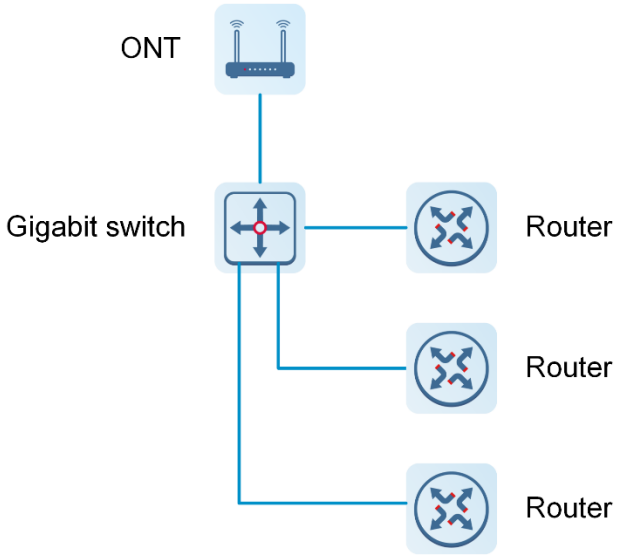
6.18 Configuring Reyee Mesh 3.0

6.18.1 Configuration Steps

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

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

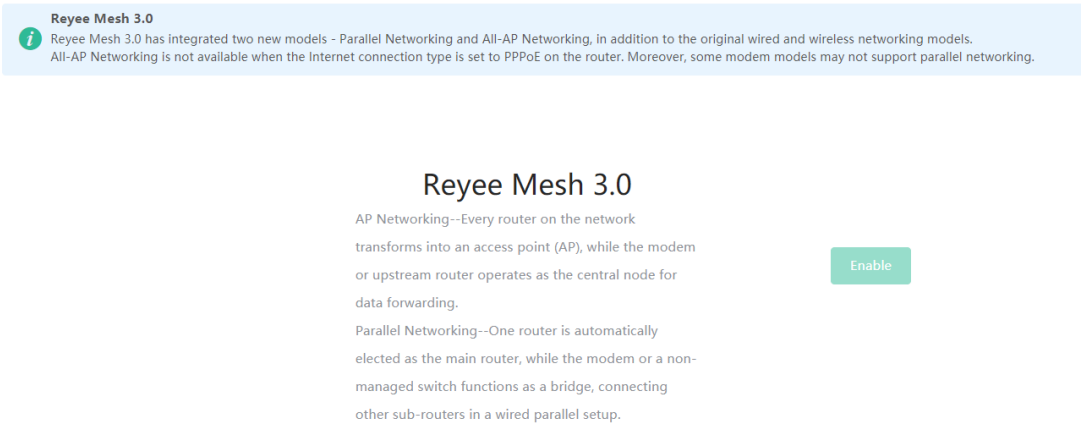
Connect the routers as indicated in the following figure:



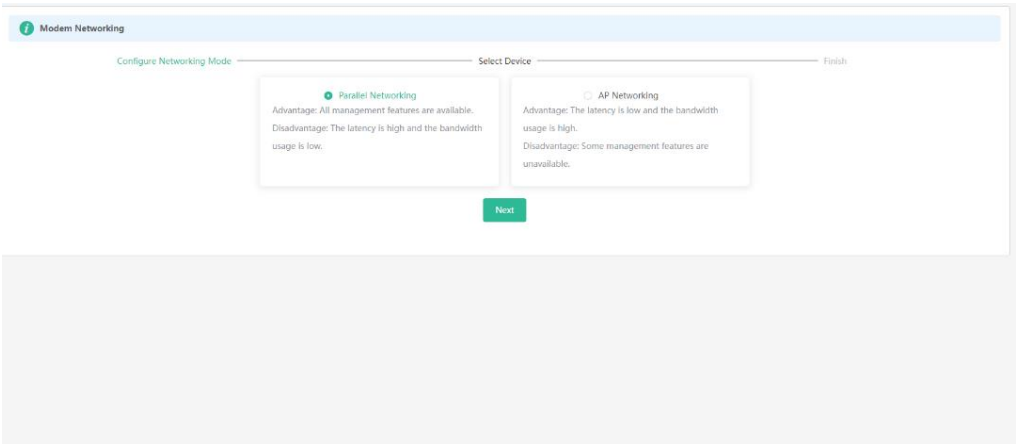
1. Parallel Networking

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.

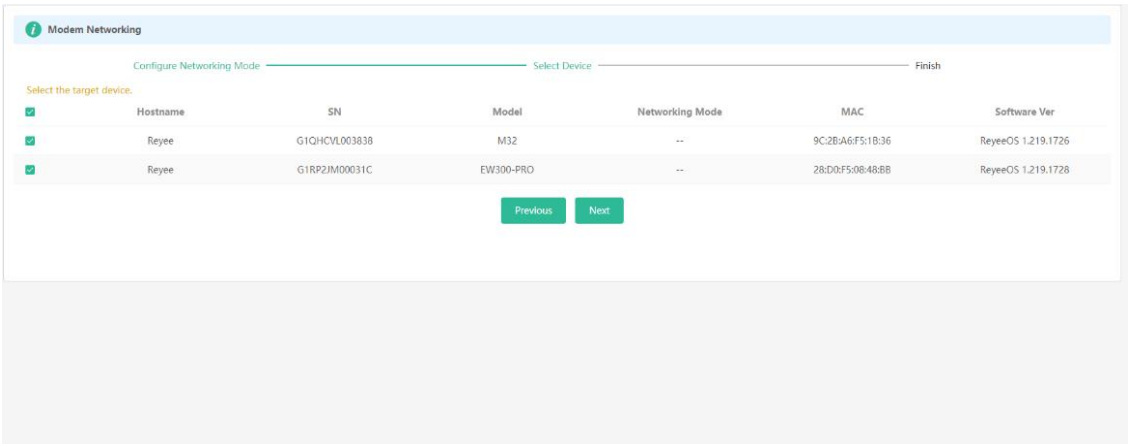
(1) Click **Enable** to enable Reyee Mesh 3.0.



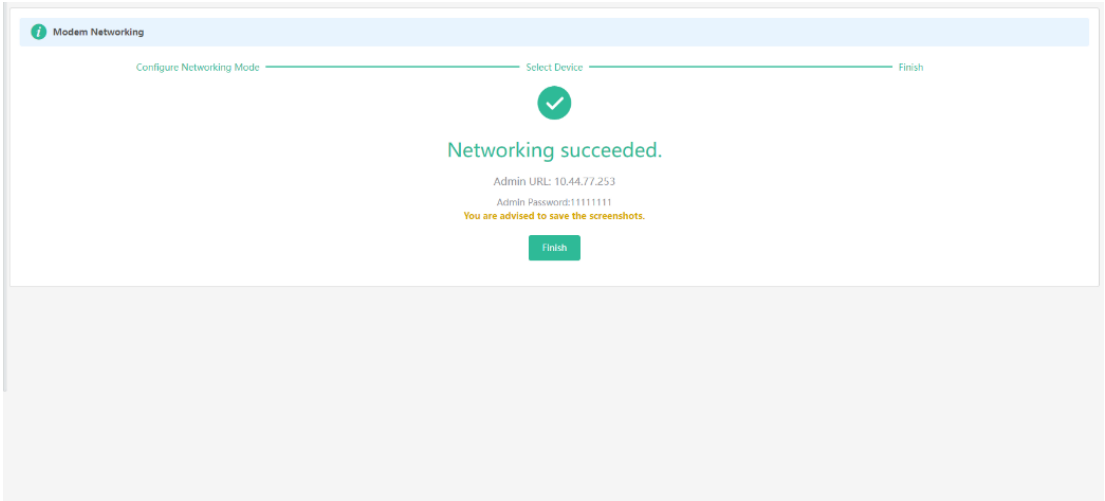
(2) Choose Parallel Networking, and click Next.



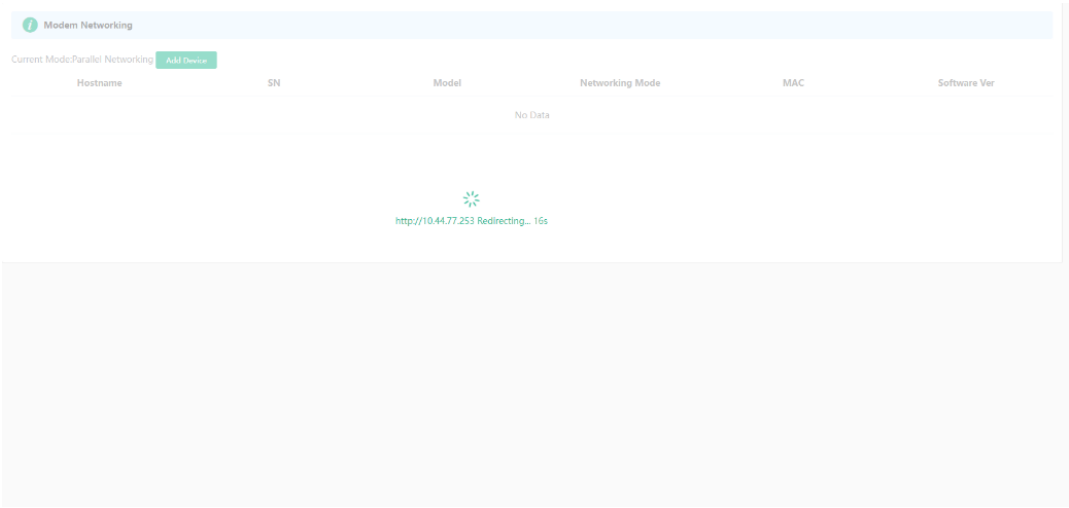
(3) Check routers for the networking.



(4) Click **Next**.



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

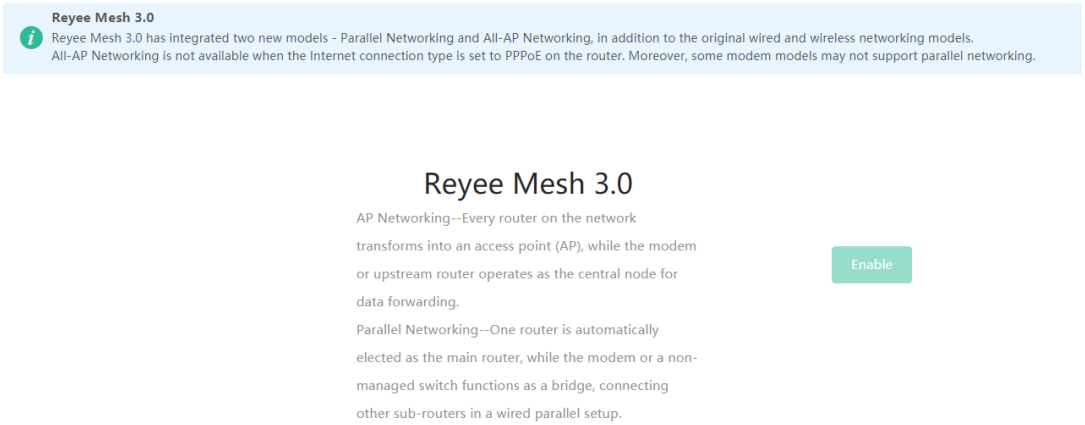


(6) On the master router page that opens, enter the password to log in.

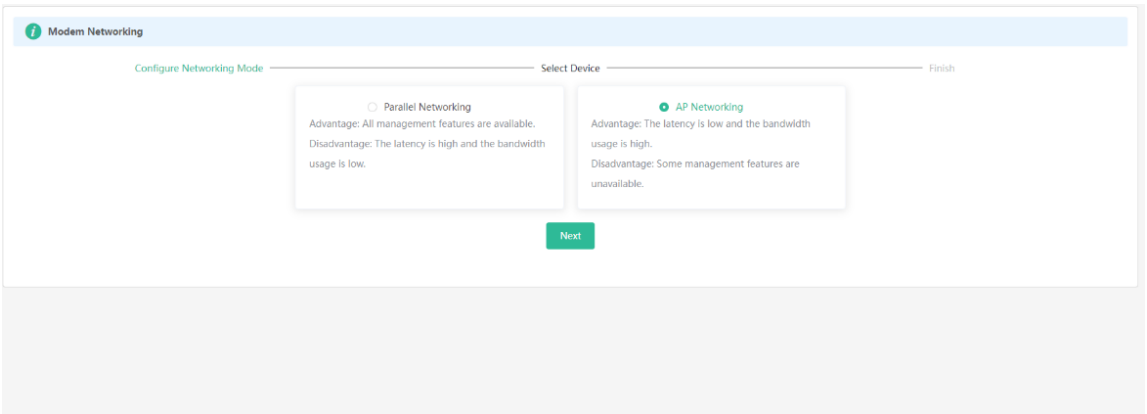
2. AP Networking

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

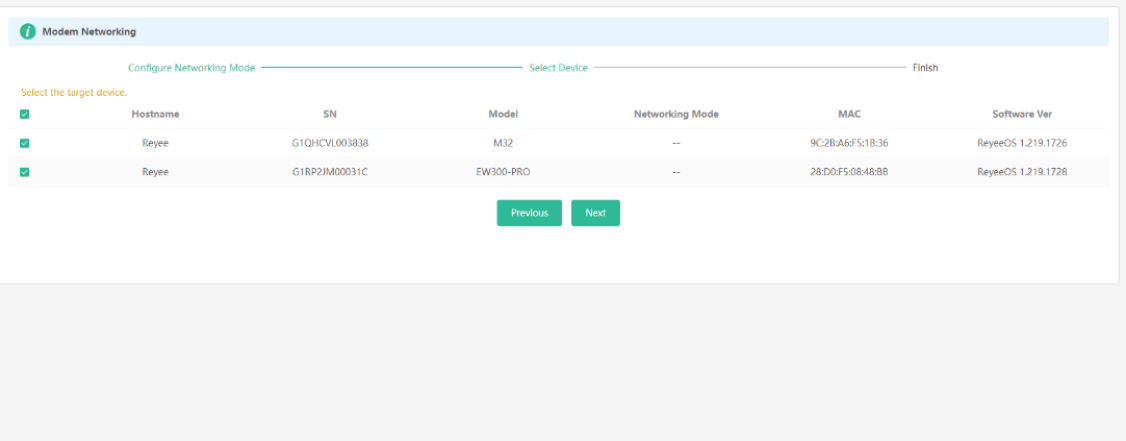
(1) Click **Enable** to enable Reyee Mesh 3.0.



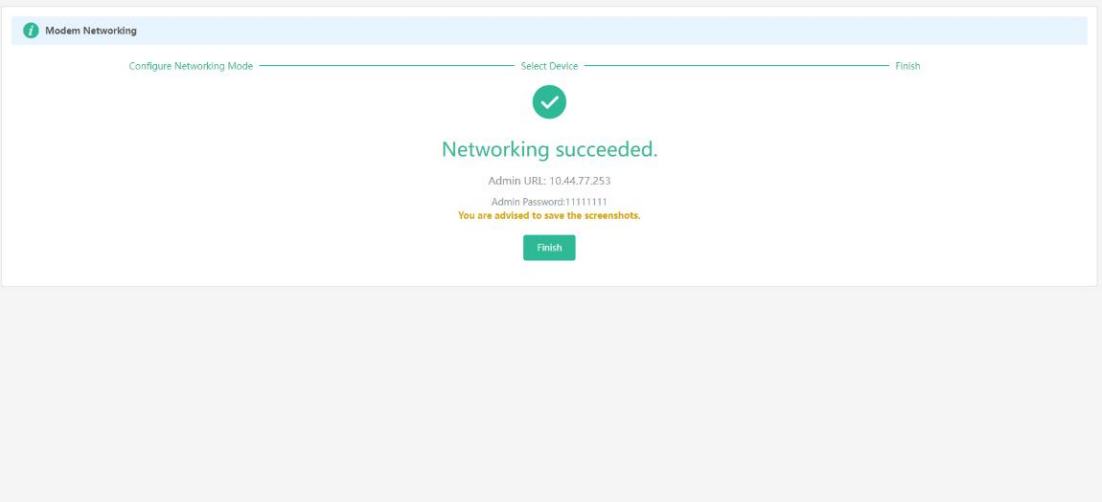
(2) Choose **AP networking**, and click **Next**.



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



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



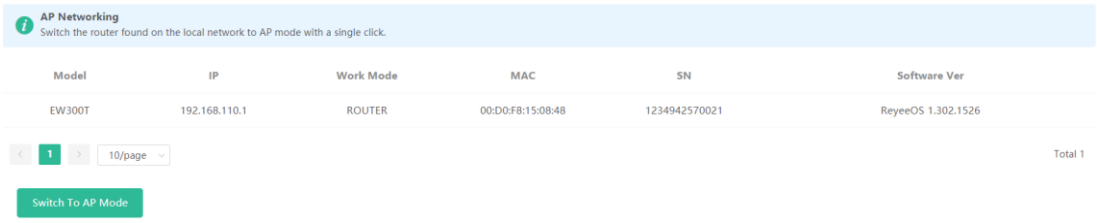
(5) On the master router page that opens, enter the password to log in.

6.19 Configuring AP Networking

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

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

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



6.20 Enabling Smart Flow Control

Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Advanced** > **Flow Control** > **Smart Traffic Control**.

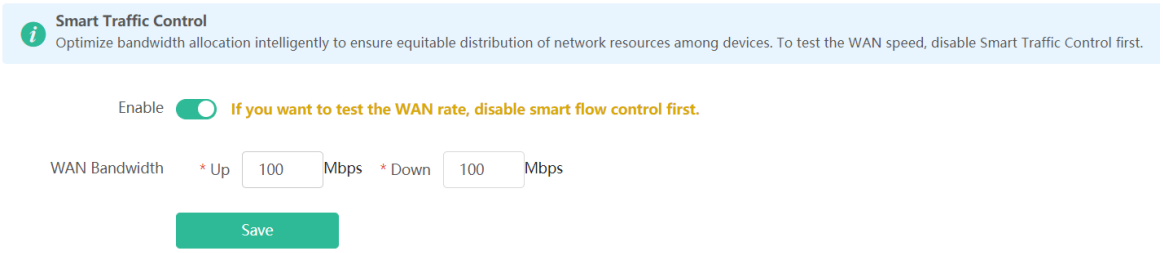
PC View: Choose **More** > **Advanced** > **Flow Control** > **Smart Traffic Control**.

1. Enabling Smart Traffic Control

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

Caution

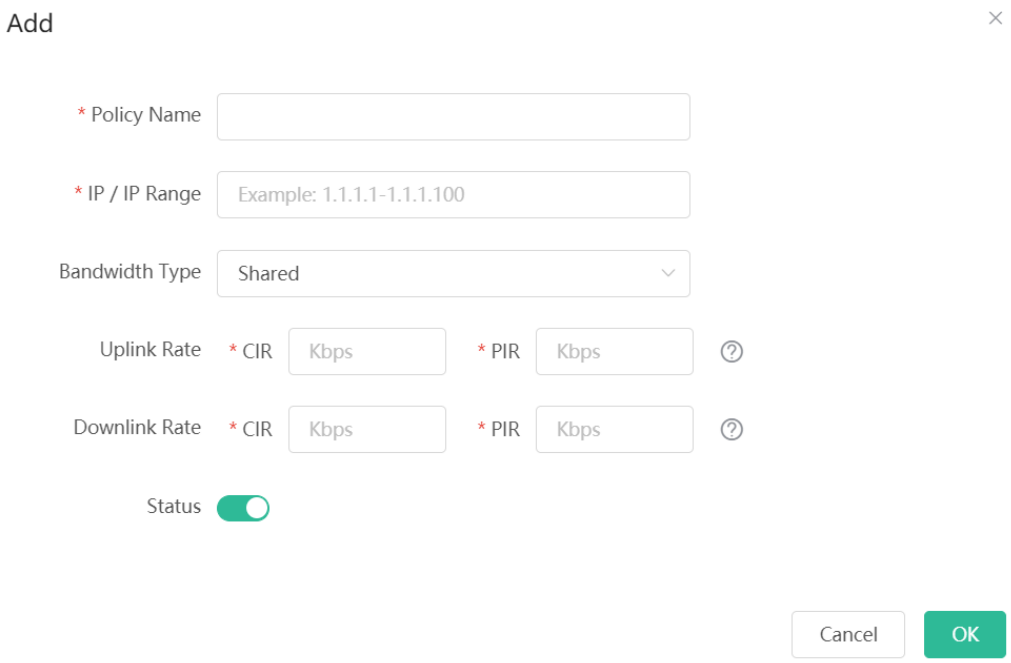
After smart flow control is enabled, speed measurement will be affected. Disable flow control if you want to do speed measurement.



2. Custom Policy

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





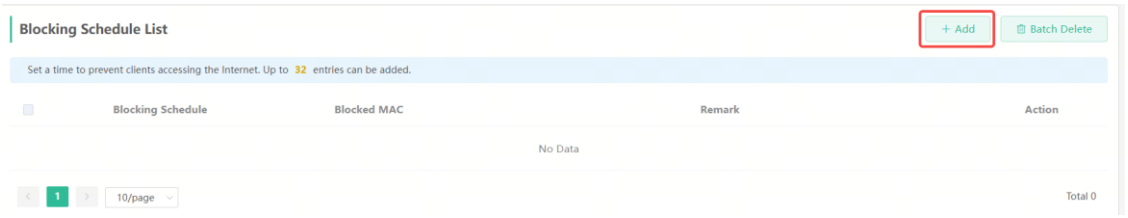
6.21 Setting Blocking Schedules

Smartphone View: Choose **More** > **Switch to PC** > **Advanced** > **Blocking Schedule**.

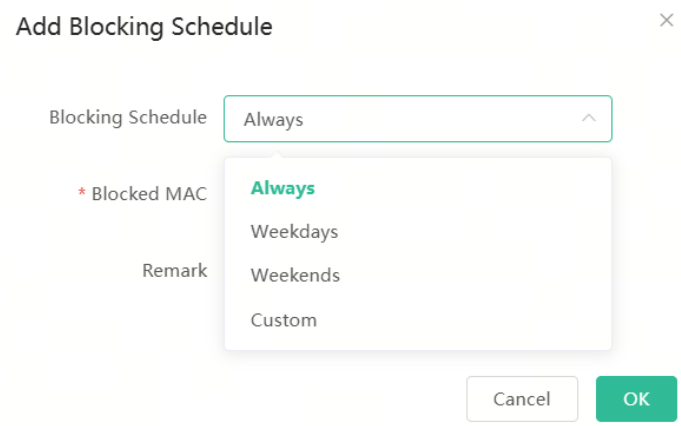
PC View: Choose **More** > **Advanced** > **Blocking Schedule**.

6.21.1 Setting a Blocking Schedule

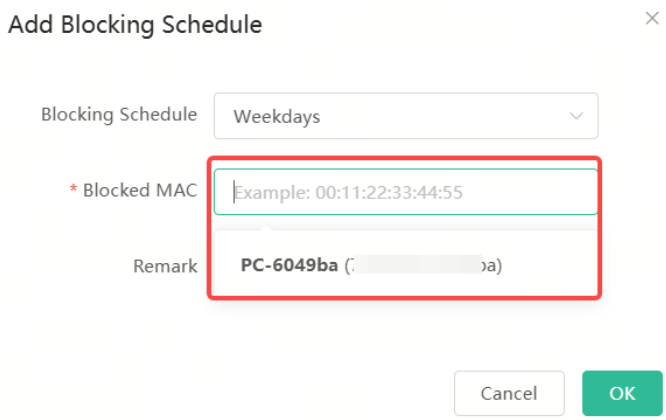
(1) Click **Add**.



(2) You can select all time slots, weekdays, weekends, or custom for the blocking schedule. When **Custom** is selected, you can choose recurring dates and time periods.



(3) Select a client or enter a MAC address for the blocking schedule.



(4) Click **OK** to save the changes.

6.21.2 Removing a Blocking Schedule

Click **Delete** next to a blocking schedule to remove it.

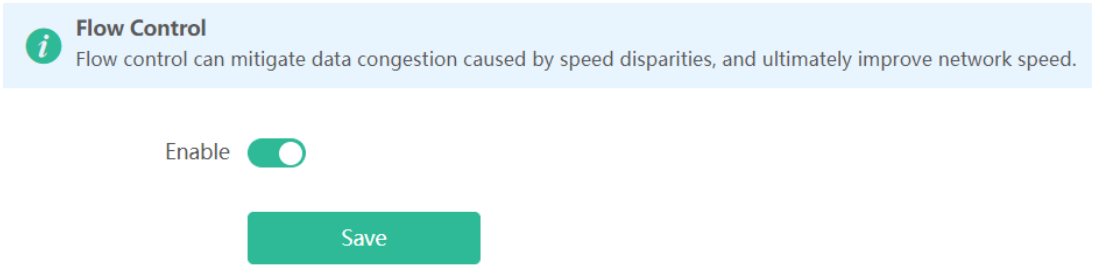


6.22 Enabling Port-Based Flow Control

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.



6.23 Configuring UPnP

6.23.1 Overview

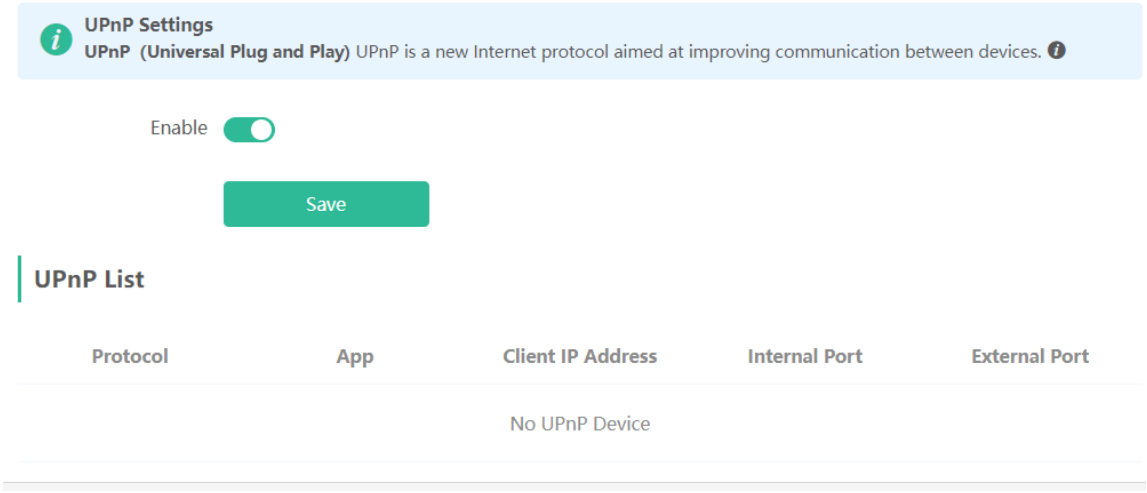
The universal plug and play (UPnP) function can map the port used by a client for Internet access according to the client's request so that related applications run faster or more stably. Common applications that support UPnP include MSN Messenger.

6.23.2 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.



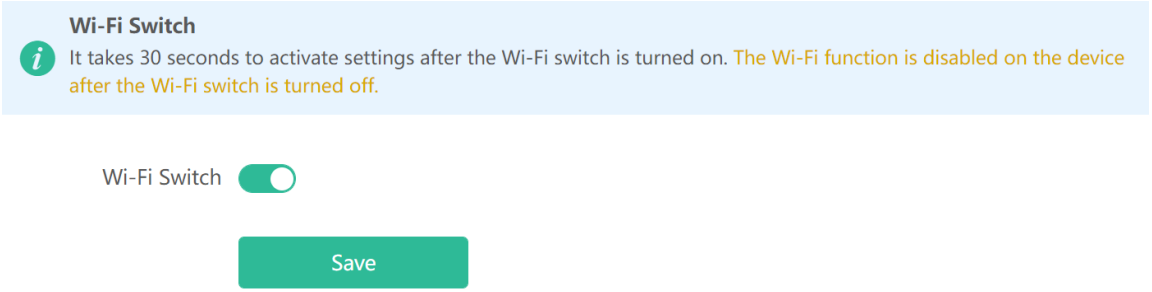
6.24 Enabling Wi-Fi Switch

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.



7 Configuring the Repeater Mode

7.1 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.

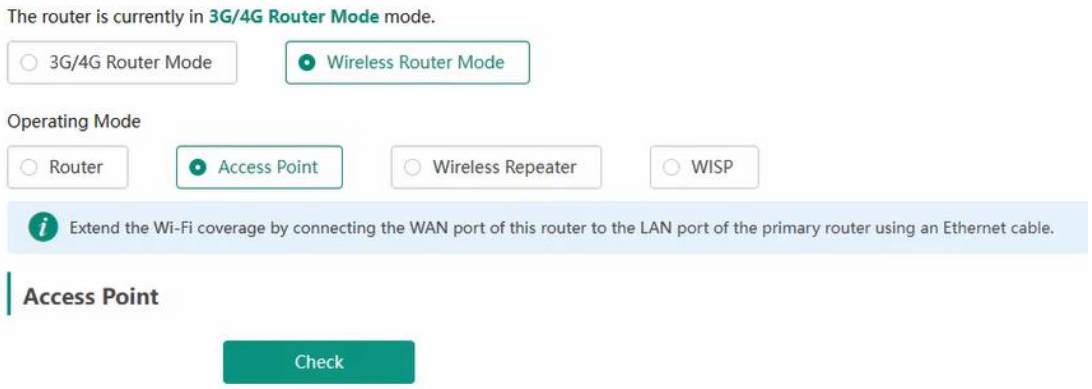
Mobile Phone View: Choose **More** > **Work Mode**

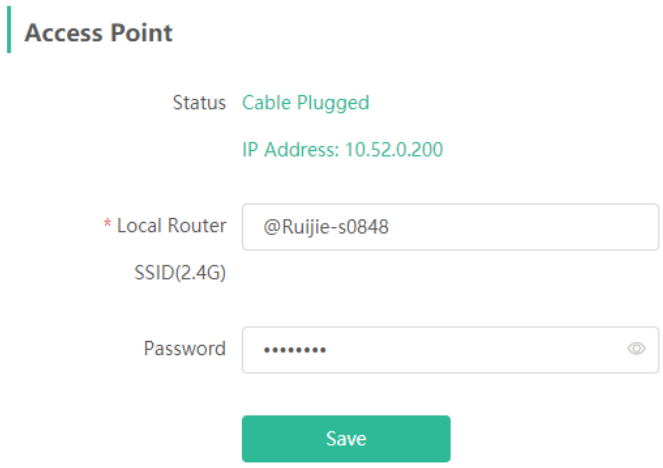
PC View: **More** >**Work Mode**

Set the **Work Mode** to **Wireless Router Mode**, and the **Operating Mode** to **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.





7.2 Wireless Repeater

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

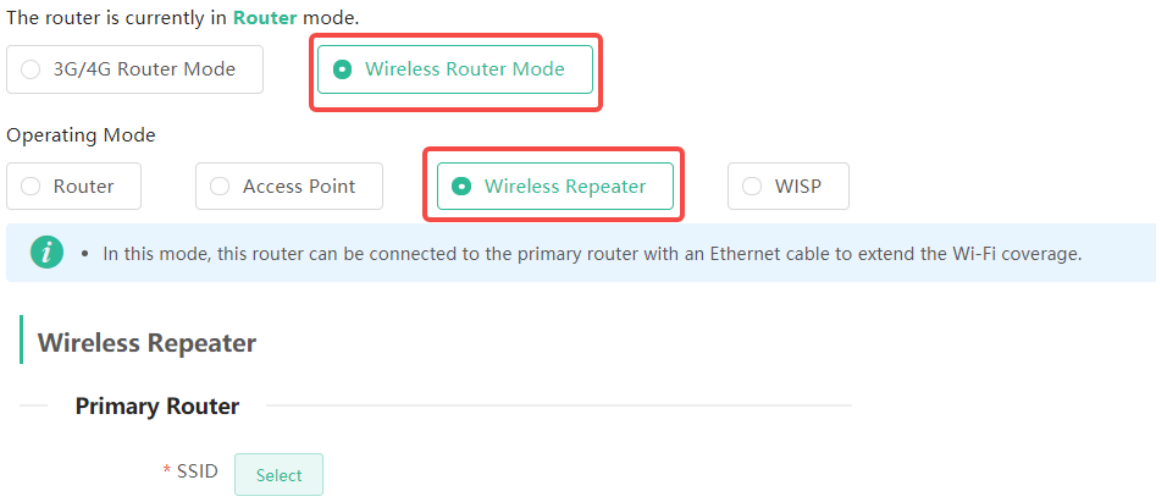
Note

- 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 > Work Mode**

PC View: **More >Work Mode**

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

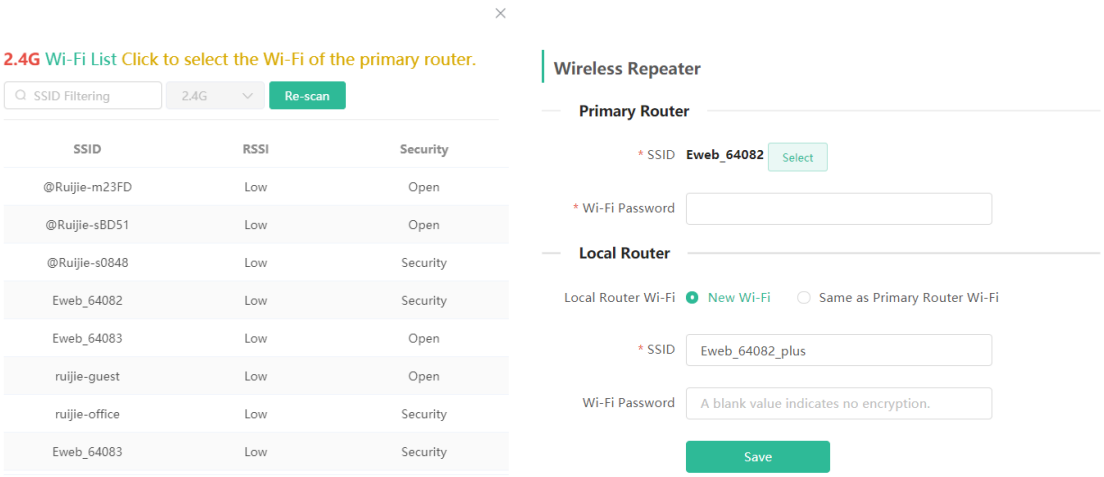


(2) Select the Wi-Fi signal of the primary router and enter its Wi-Fi password. You can configure a new Wi-Fi network or have a Wi-Fi network the same as that of the primary router:

- 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.



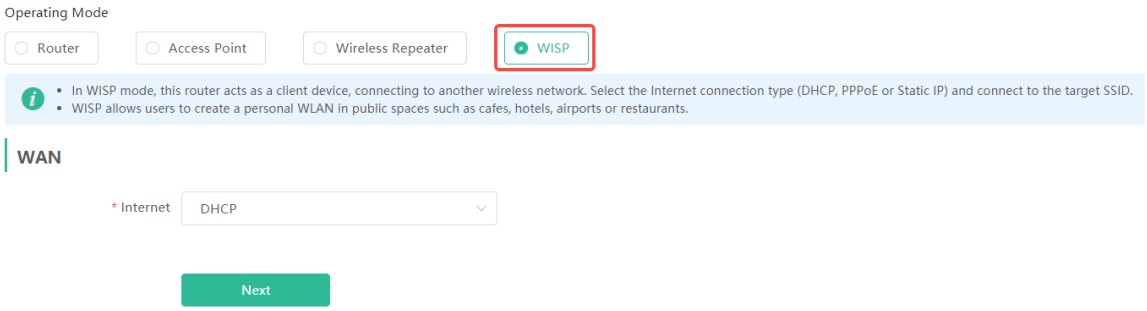
7.3 WISP

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** > **Work Mode**

PC View: **More** > **Work Mode**

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

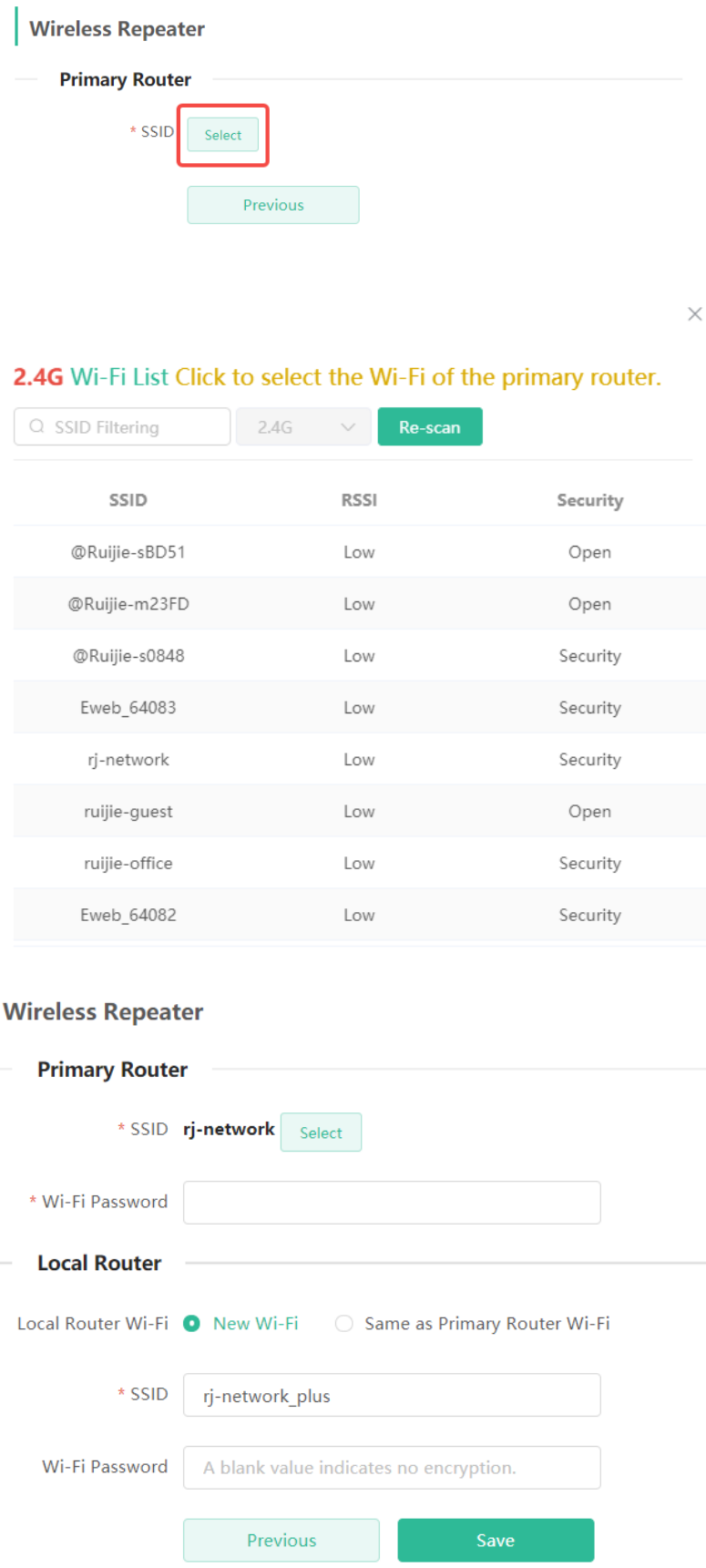


(2) Select the Wi-Fi signal of the primary router and enter its Wi-Fi password. You can configure a new Wi-Fi network or have a Wi-Fi network the same as that of the primary router:

- 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 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
Select
Previous
2.4G Wi-Fi List Click to select the Wi-Fi of the primary router.
SSID Filtering
2.4G
Re-scan
SSID
RSSI
Security
@Ruijie-sBD51
Low
Open
@Ruijie-m23FD
Low
Open
@Ruijie-s0848
Low
Security
Eweb_64083
Low
Security
rj-network
Low
Security
ruijie-guest
Low
Open
ruijie-office
Low
Security
Eweb_64082
Low
Security
Wireless Repeater
Primary Router
* SSID
rj-network
Select
* Wi-Fi Password
Local Router
Local Router Wi-Fi
New Wi-Fi
Same as Primary Router Wi-Fi
* SSID
rj-network_plus
Wi-Fi Password
A blank value indicates no encryption.
Previous
Save

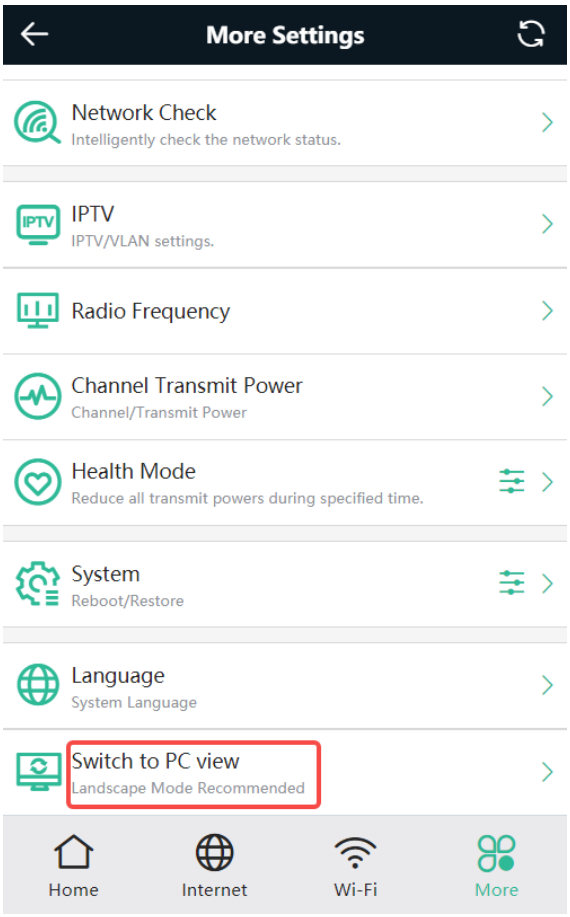
8 System Settings

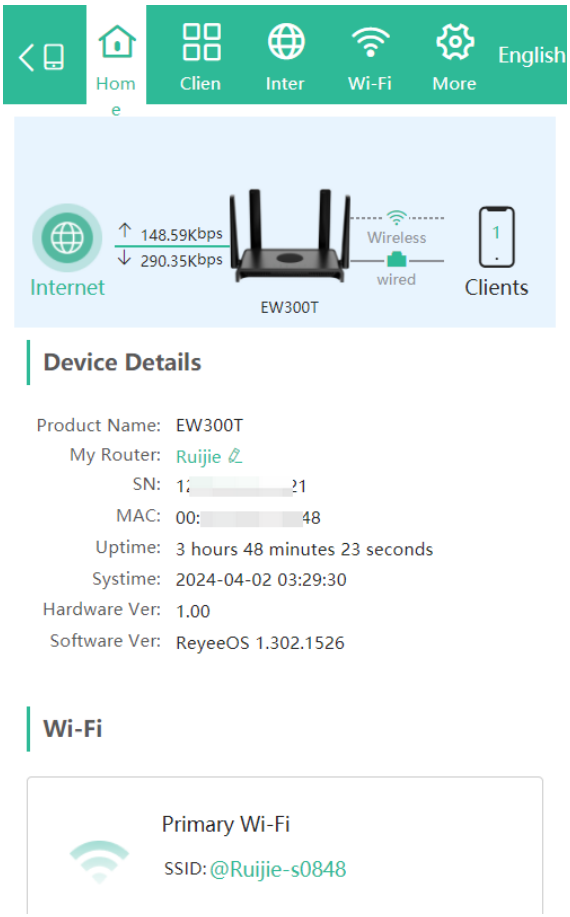
8.1 Switching to PC View

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).





8.2 Configuring the Login Password

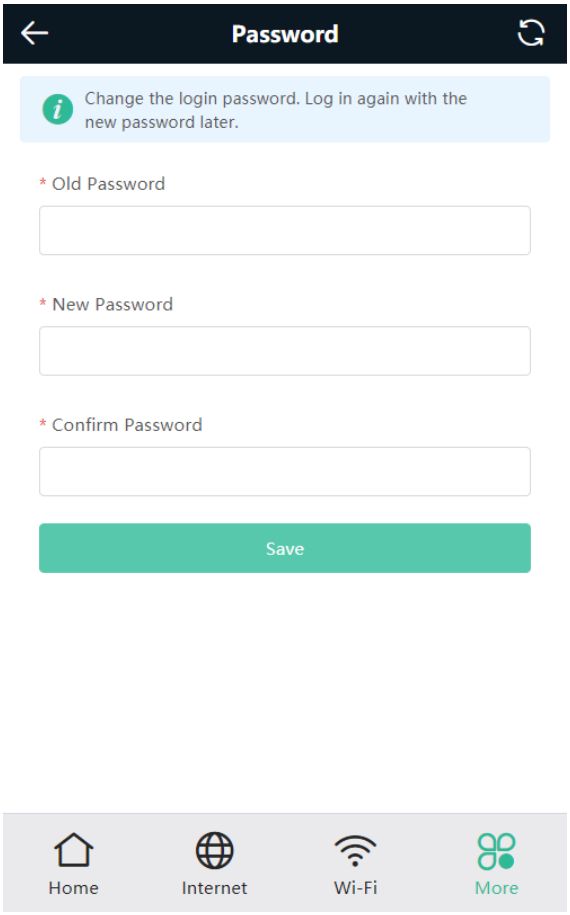
Note

To ensure security, you are advised to configure a management password that contains at least eight characters, including digits, letters, and special characters.

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

PC View: Choose **More** > **System** > **Login** > **Management Password**.

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



8.3 Remote Access

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

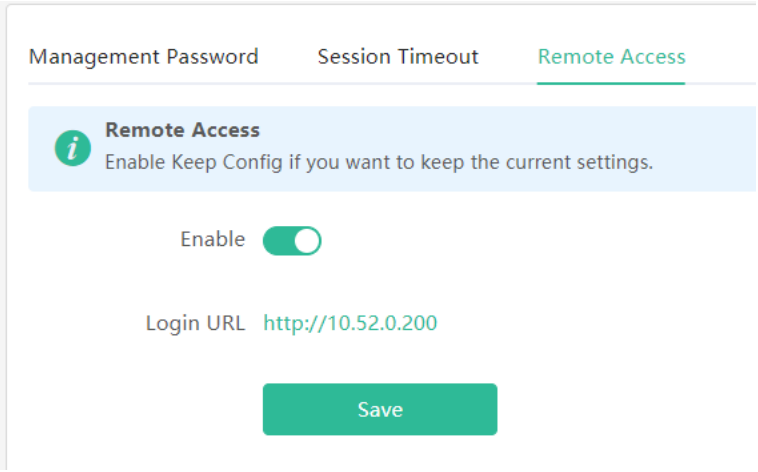
PC View: Choose **More** > **System** > **Login > Remote Access**.

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

Caution

This function 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 8.2 Configuring the Login Password to configure a strong and secure device management password.

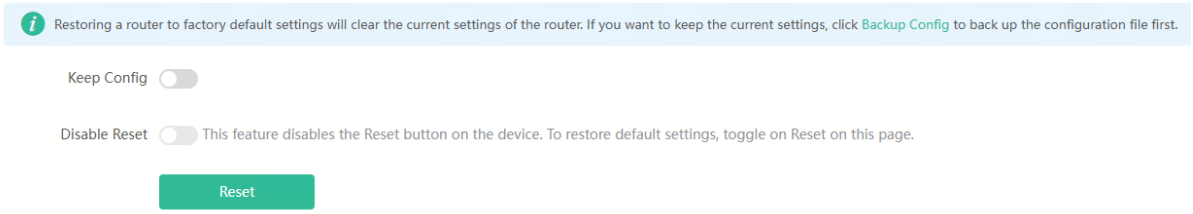


8.4 Restoring Factory Settings

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

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

Click to enable **Keep Config** 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

- If the **Dis**able Reset feature is enabled on Ruijie Cloud ISP, devices running ReyeeOS 1.420 or later cannot be restored to factory settings using the physical Reset button. However, the Reset feature on eWeb remains available.
- This operation will clear existing settings and restart the device. Therefore, exercise caution when performing this operation.

Note

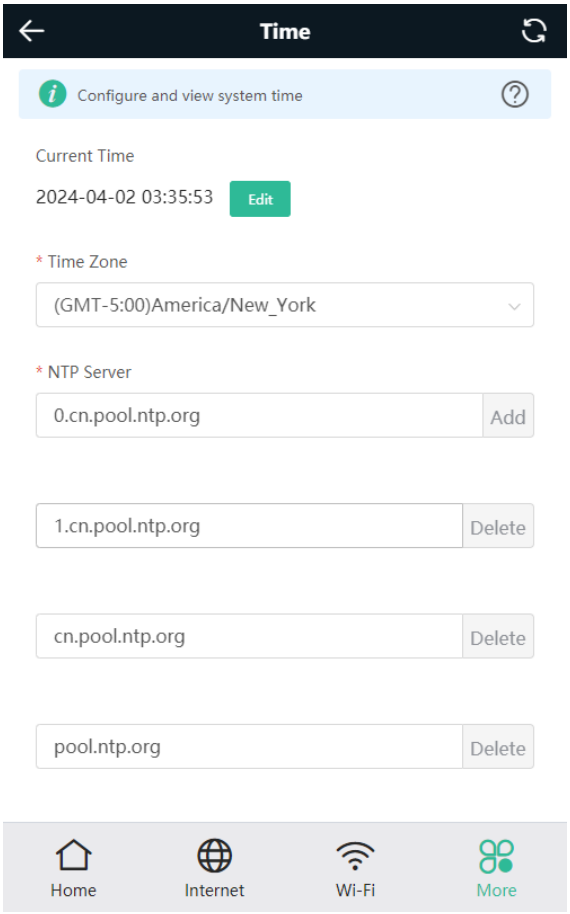
If resetting all routers in the network is unsuccessful, the judgment method is the SSID of the primary router factory resets (The default SSID can be found on the bottom label of the router.), the SSID of the extender is not factory reset name, you can hold down the Reset button of the extender for more than 10 seconds to restore factory settings.

8.5 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.



8.6 Configuring Scheduled Reboot

8.6.1 Getting Started

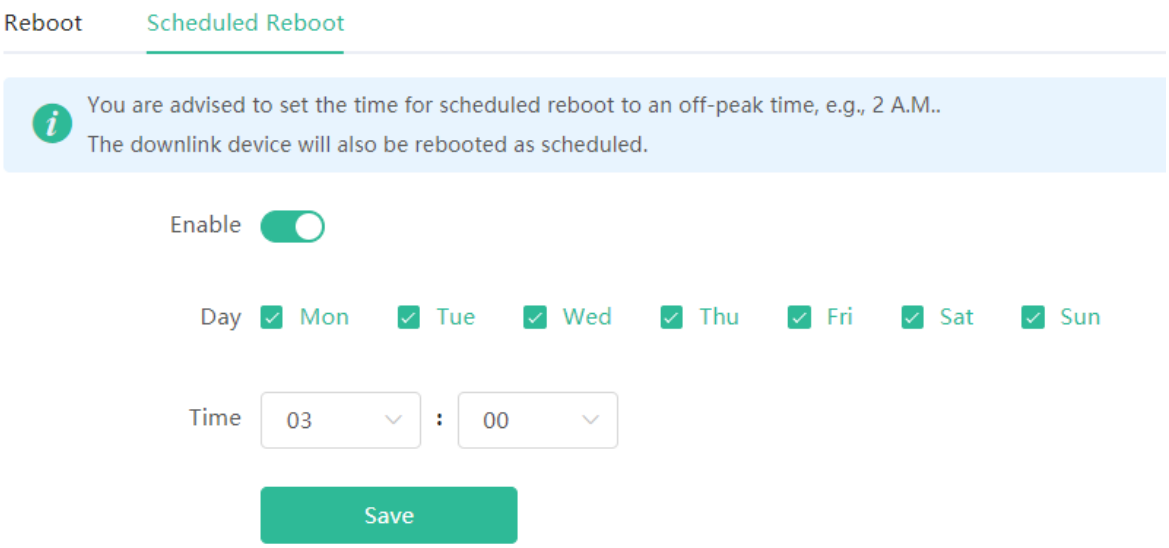
Confirm that the system time is accurate to avoid network interruption caused by device reboot at the wrong time. For details, see 8.5 Configuring System Time.

8.6.2 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.



8.7 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.

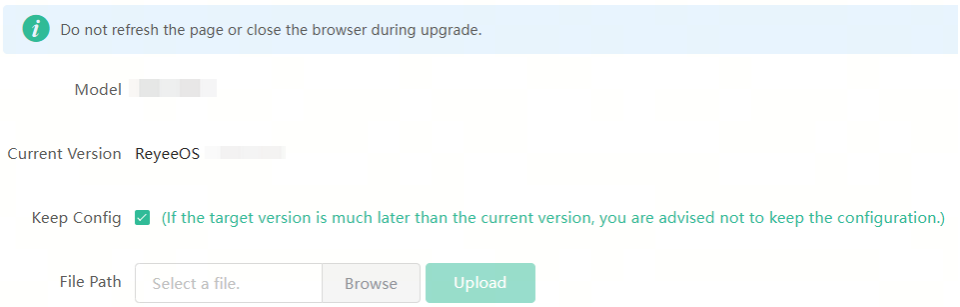


8.8 Performing Local Upgrade

Smartphone View: Choose **More** > **Switch to PC view** > **More** > **System** > **Local Upgrade**.

PC View: Choose **More** > **System** > **Upgrade** > **Local Upgrade**.

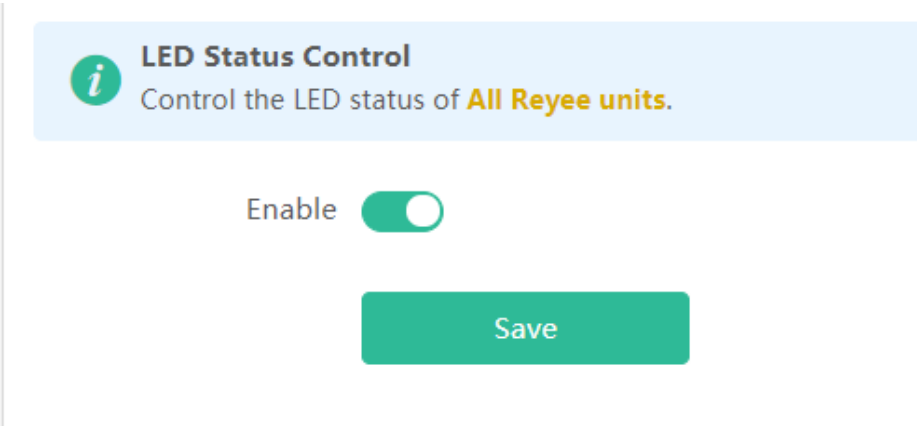
You can view the current software version and device model. If you want to upgrade the device with the configuration retained, select **Keep Config**. Click **Browse**, select an upgrade package on the local PC, and click **Upload** to upload the file. The device will be upgraded.



8.9 Turning On/Off the Indicator

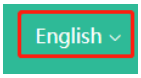
Mobile Phone View: Choose **More** > **LED**

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

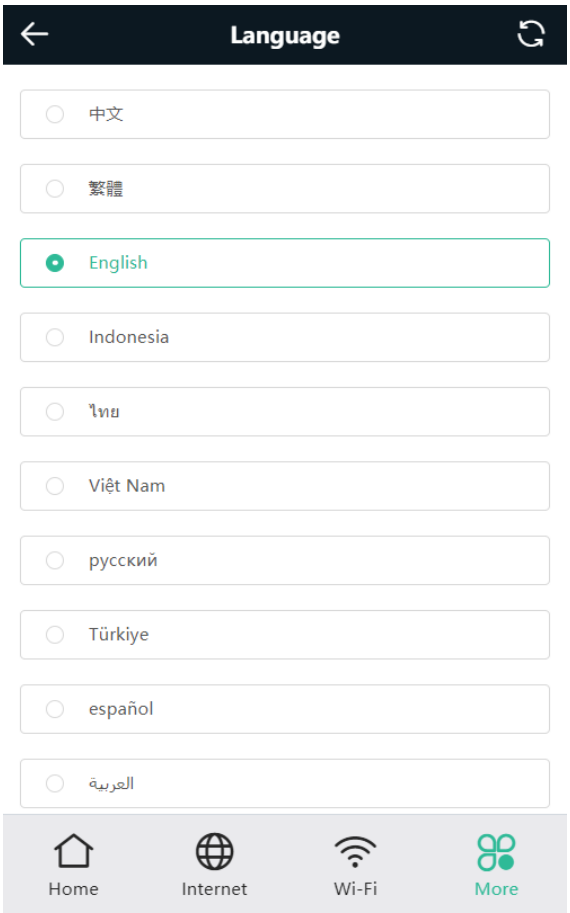


8.10 Switching System Language

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.

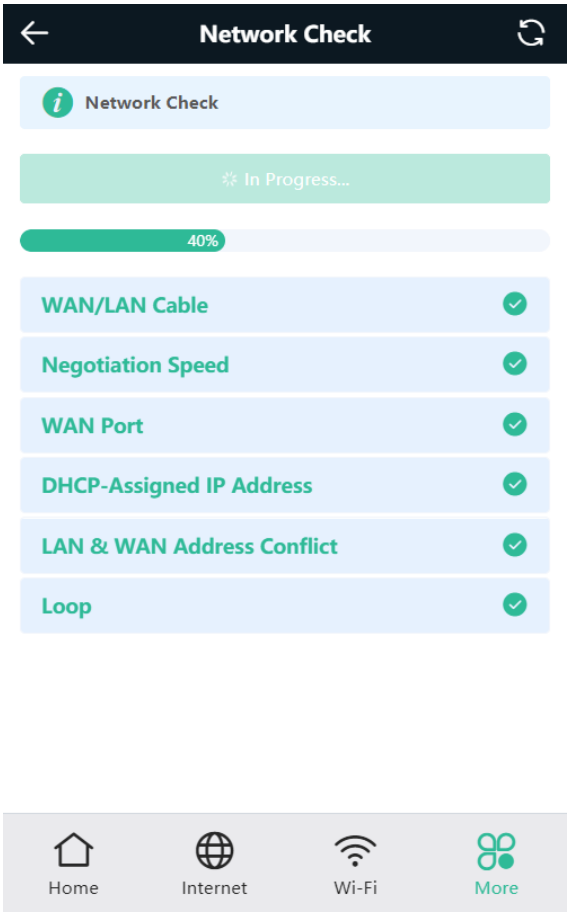


8.11 Diagnosing Network Problems

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



8.12 Network Diagnosis Tools

Caution

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

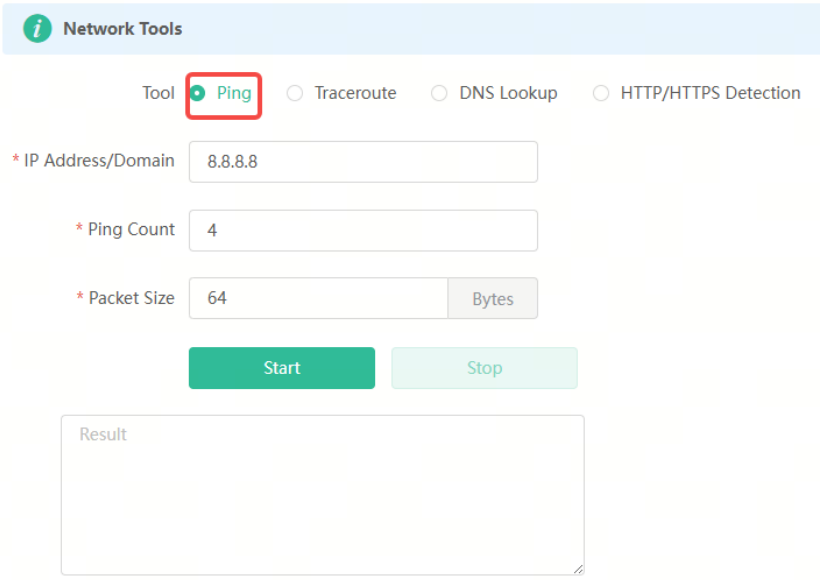
8.12.1 Ping

Smartphone View: Choose **More** > **System** > **Network Tools**.

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

The **Ping** command is used to detect the network connectivity.

Select **Ping** as the diagnosis mode, select the IP type, enter the destination IP address or website address, configure the ping count and packet size, and click **Start** to test the network connectivity between the device and the IP address or website. If "Ping failed" is displayed, the device is not reachable to the IP address or website.



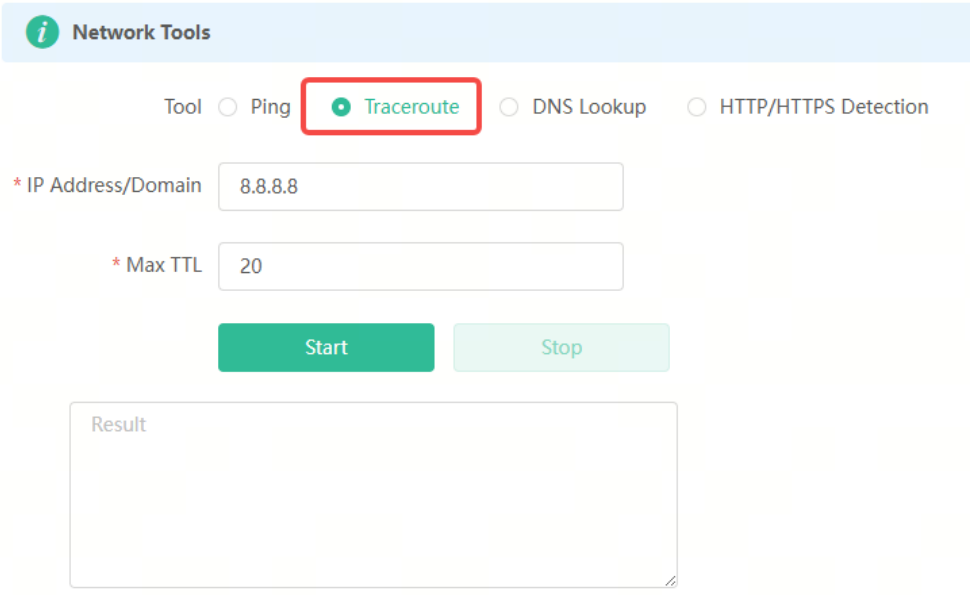
8.12.2 Traceroute

Smartphone View: Choose **More** > **System** > **Network Tools**.

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

The **Traceroute** function is used to identify the network path from one device to another. On a simple network, the network path may pass through only one routing node or none at all. On a complex network, packets may pass through dozens of routing nodes before reaching their destination. The traceroute function can be used to judge the transmission path of data packets during communication.

Select **Traceroute** as the diagnosis mode, select the IP type, and enter a destination IP address or the maximum TTL value used by the URL and traceroute, and click **Start**.



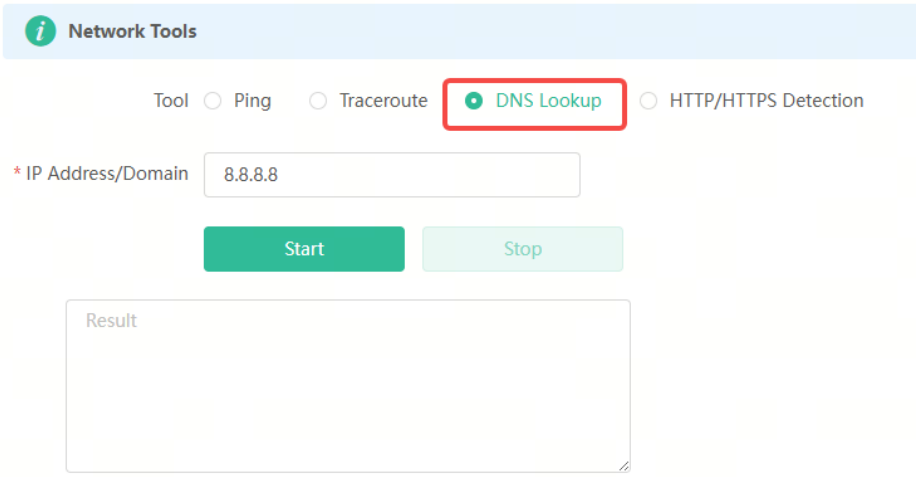
8.12.3 DNS Lookup

Smartphone View: Choose **More** > **System** > **Network Tools**.

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

DNS Lookup is used to query the information of network domain name or diagnose DNS server problems. If the device can ping through the IP address of the Internet from your web page but the browser cannot open the web page, you can use the DNS lookup function to check whether domain name resolution is normal.

Select **DNS Lookup** as the diagnosis mode, enter a destination IP address or URL, and click **Start**.



8.12.4 HTTP/HTTPS Detection

Specification

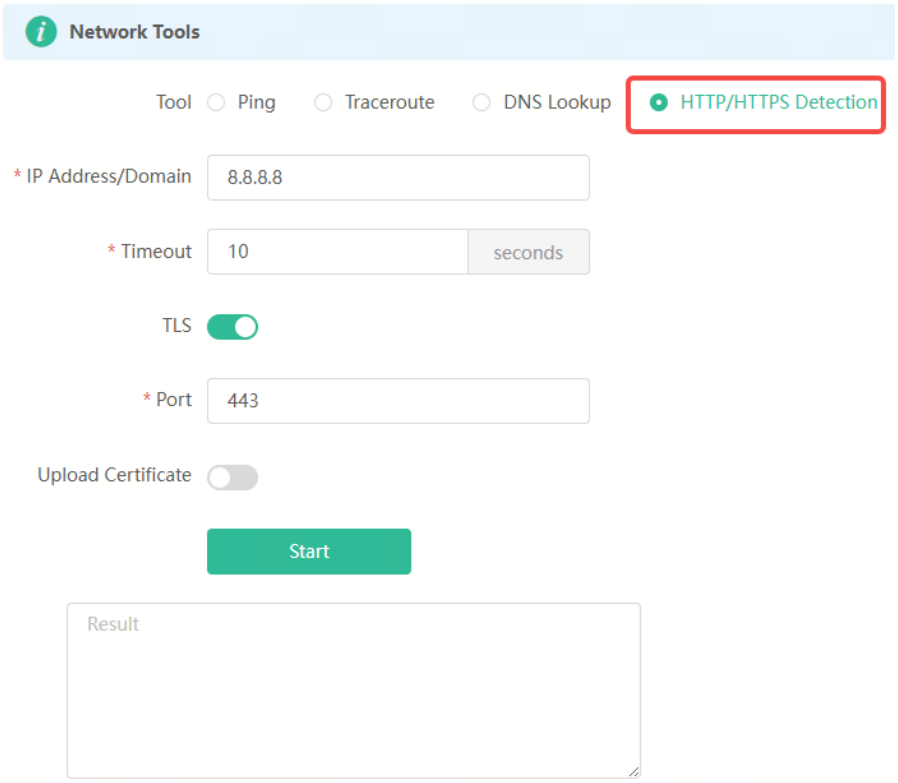
The device running ReyeeOS 1.420 version or later supports this feature.

Smartphone View: Choose **More** > **System** > **Network Tools**.

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

The HTTP/HTTPS detection tool verifies whether a web service runs properly by sending HTTP or HTTPS requests to a specified target server and receiving responses. It helps identify issues where a network can be pinged successfully but web pages cannot be accessed.

(1) Set **Tool** to **HTTP/HTTPS Detection**.



(2) Configure other parameters and click **Start**.

Table 8-1 HTTP/HTTPS Detection Parameters

Parameter	Description
IP Address/Domain	Specifies the IP address or domain name of the web server to be detected.
Timeout	Specifies the maximum waiting time for a server response. If no complete response is received within this period, the request is considered to have timed out, avoiding prolonged blocking.
TLS	When HTTPS is used, this parameter controls whether to enable the TLS encrypted handshake.
Port	The default port is 443 for HTTPS. Enter the port number used by the web server.
Upload Certificate	When TLS is enabled, you can choose whether to upload a certificate to verify the web server or allow the server to authenticate the device.

(3) Check the detection result displayed in the detection result box. The status descriptions are as follows:

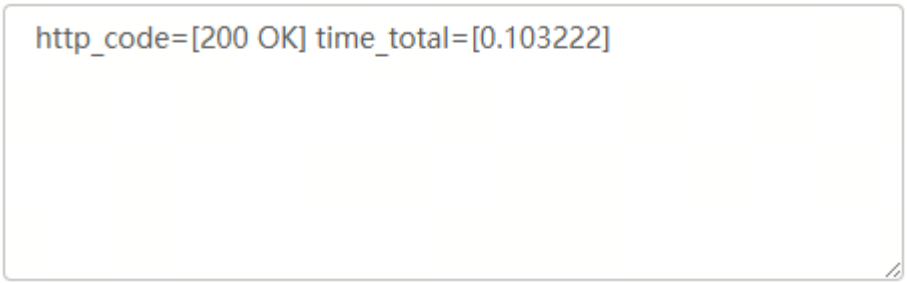


Table 8-2 HTTP/HTTPS Detection Results

Parameter	Description
http_code=000	Failed to receive the response from the server.
http_code=2xx	Success status codes ● 200: OK (Request succeeded) ● 201: Created (Request succeeded and a resource was created) ● 202: Accepted (Request accepted but processing is not complete) ● 204: No Content (Request succeeded but no response body is returned)
http_code=3xx	Redirection status codes ● 301: Moved Permanently (Permanent redirection) ● 302: Found (Temporary redirection) ● 303: See Other (Use a GET request to obtain the resource) ● 304: Not Modified (Resource not modified)
Others	Refer to curl error codes.

8.12.5 Packet Capture Tool

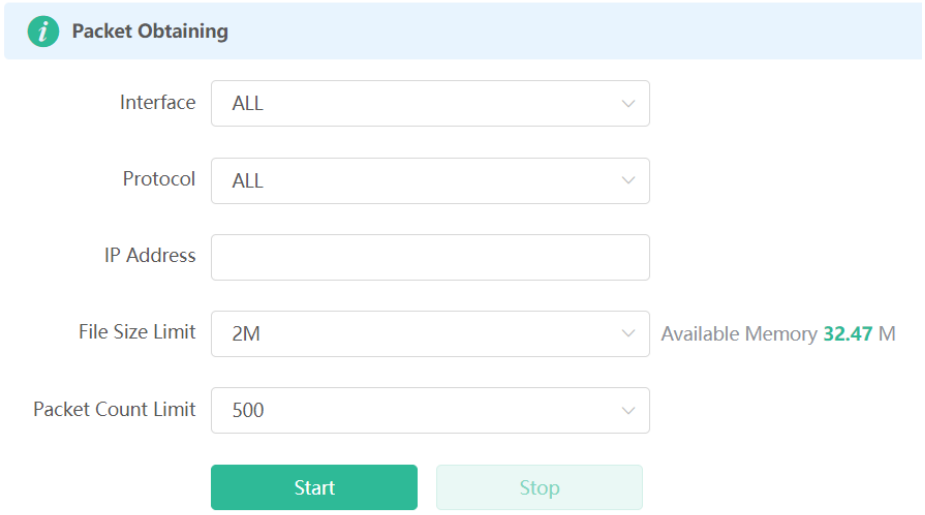
Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Diagnostics** > **Packet Obtaining.**

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.



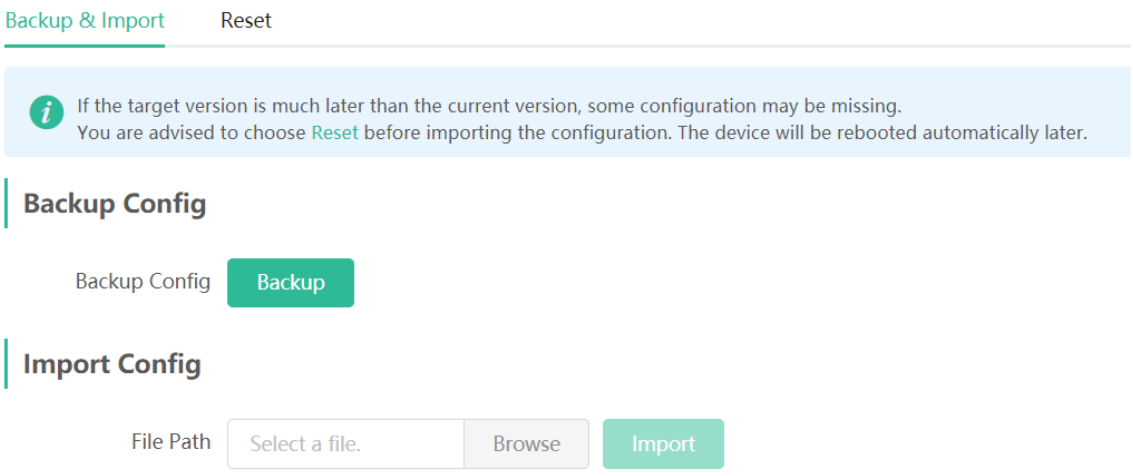
8.13 Configuring Config Backup and Import

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.

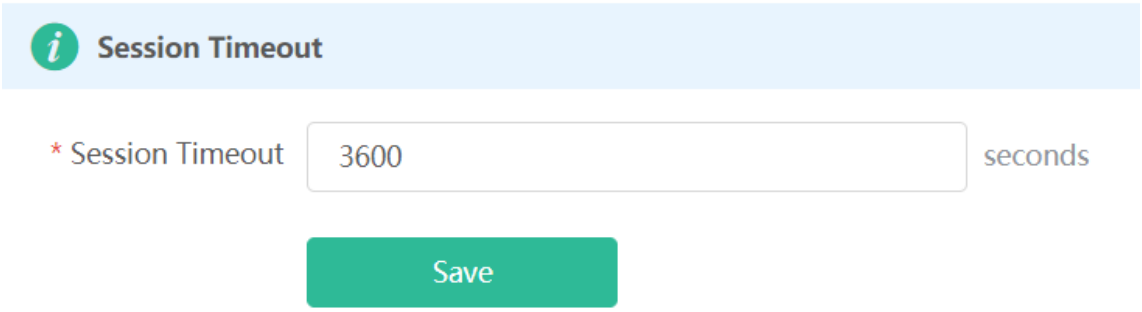


8.14 Configuring Session Timeout Duration

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.



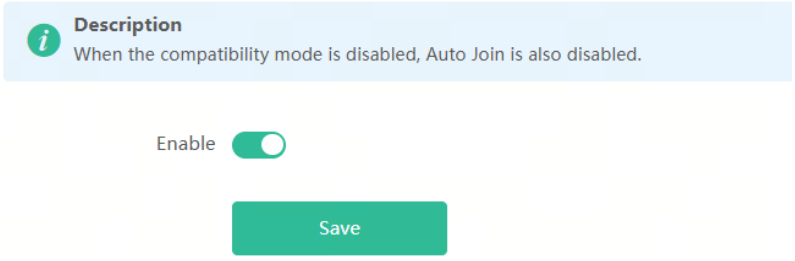
8.15 Configuring the Compatibility Mode

Smartphone View: Choose **More** > **Switching to PC View** > **More > System** > **Compatibility Mode**.

PC View: Choose **More** > **System** > **Compatibility Mode**.

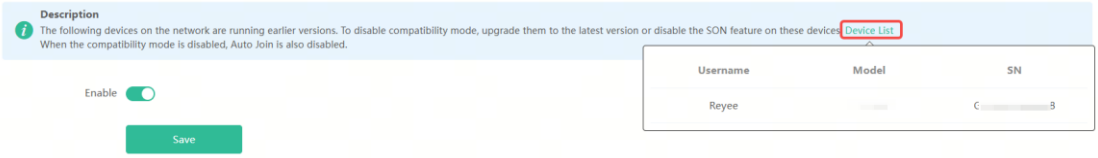
Enabling compatibility mode can improve interoperability between devices running the early and latest versions during networking. If the compatibility mode is disabled, **Auto Join** will be disabled as well.

- When no device on the network runs a software version earlier than ReyeeOS 1.380, the user interface will be displayed as follows:



- When a device on the network runs a software version earlier than ReyeeOS 1.380, the user interface will be displayed as shown below.

  If the compatibility mode is disabled, devices running software version earlier than ReyeeOS 1.380 cannot join the network or be managed by Ruijie Reyee App in local mode. You are advised to click **Device List**, upgrade the devices in the list to the latest version, and then disable the compatibility mode. For details about the device upgrade, see 8.8 Performing Local Upgrade.



8.16 Configuring Cloud Service

8.16.1 Overview

The Cloud Service feature provides powerful remote network management and operation capabilities, making it convenient and efficient to manage geographically dispersed networks with diverse device types. This feature supports wireless devices, switches, and gateways, enabling unified network management and visualized monitoring and operation. Additionally, it also offers various components such as real-name authentication, dedicated Wi-Fi, and passenger flow analysis, allowing for flexible expansion of network services.

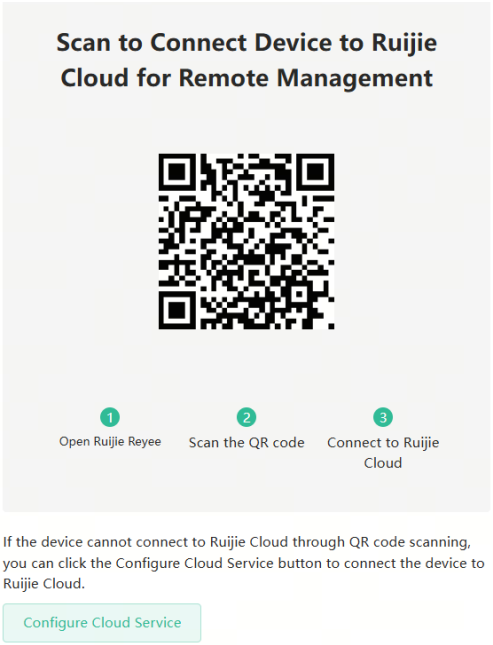
By configuring Cloud Service, you can conveniently mange networks through Ruijie Cloud or the Ruijie Reyee app.

8.16.2 Configuration Steps

Smartphone View: Choose **More** > **Switching to PC View** > **More > System** > **Cloud Service**.

PC View: Choose **More** > **System** > **Cloud Service**.

If the device is not currently associated with a cloud account, simply follow the on-screen instructions to add it to the network. Open up the Ruijie Reyee app, click the scan icon at the upper left corner on the **Project** page, and enter the device's management password.

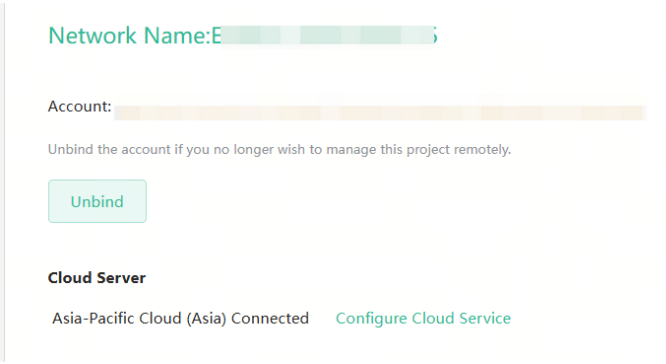


If the device cannot connect to Ruijie Cloud through QR code scanning you can click the **Configure Cloud Service** button to connect the device to Ruijie Cloud.

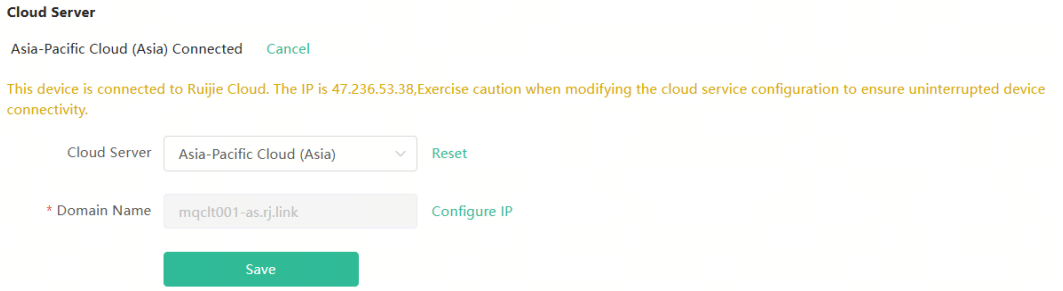
Once the device is associated with a cloud account, it will automatically be bound to a cloud server based on its geographic location.

Caution

Exercise caution when modifying cloud service configurations as improper modifications may lead to connectivity issues between the device and the cloud service.



To change the Cloud Service configurations, select the cloud server from the **Cloud Server** drop-down list, and click **Save**.

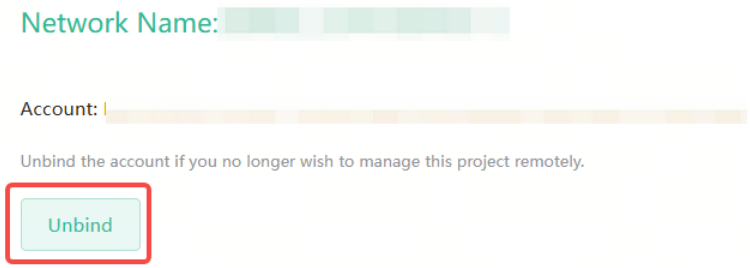


8.16.3 Unbinding Cloud Service

Smartphone View: Choose **More** > **Switching to PC View** > **More > System** > **Cloud Service**.

PC View: Choose **More** > **System** > **Cloud Service**.

You can click **Unbind** to unbind the account if you no longer wish to manage this project remotely.



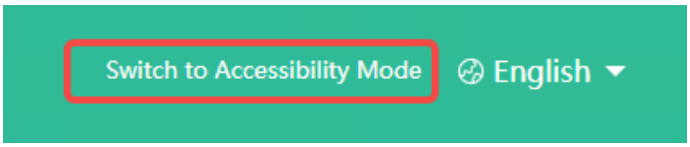
8.17 Switching to Accessibility Mode

Specification

The device running ReyeeOS 1.390 version or later supports this feature.

Accessibility mode is designed to help users with visual, physical, or other disabilities configure the router on eWeb more easily.

Click **Switch to Accessibility Mode** in the upper-right corner of the web page to enter accessibility mode.



8.18 Connectivity Detection

Specification

The device running ReyeeOS 1.420 version or later supports this feature.

Smartphone View: Choose **More** > **Switching to PC View** > **More** > **System** > **Connectivity Detection**.

PC View: Choose **More** > **System** > **Connectivity Detection**.

This function is used to actively detect the availability of network links, helping the device determine whether the WAN port is online.

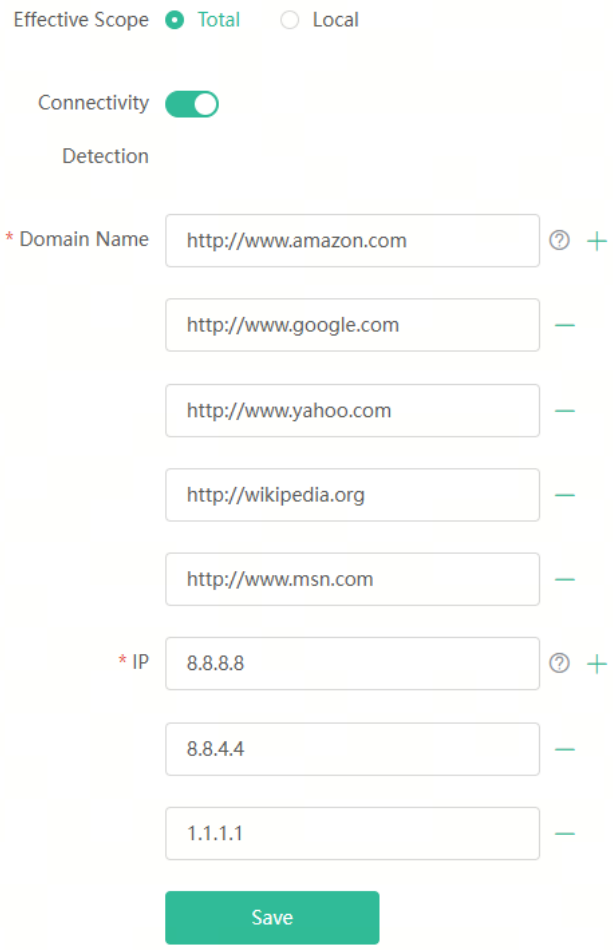


Table 8-3 Connectivity Detection Configuration

Parameter	Description
Effective Scope	● Total: Connectivity Detection takes effect globally. The detection result displays the connectivity status of all devices across the network. ● Local: Connectivity Detection takes effect locally. The detection result displays the connectivity status of the current device.
Connectivity Detection	Enable or disable Connectivity Detection.
Domain Name	The device sends a detection request to the specified domain name and determines connectivity based on the returned result.
IP	The device sends a detection request to the specified IP address and determines connectivity based on the returned result.

9 Expert Mode

The expert mode can be enabled by pressing the combination of keys on the web interface. The expert mode is disabled by default. If you encounter a fault and cannot troubleshoot the fault, contact Ruijie customer service engineers for remote support.

10 FAQs

10.1 How Do I Restore the Router to Factory Settings?

Use a needle-shaped object to press and hold the router's **Reset** button for more than 10 seconds, then release it after the system LED flashes quickly. Wait for the router's system LED to become solid on, then perform network settings on the router. The SSID of the router in the factory state can be found on the label on the back of the router.

10.2 What Should I Do If I Forgot the Password?

- Forgot the management password of the web interface: Enter the Wi-Fi password and try again. If the password is still incorrect, restore the router to factory settings. The management password will also be restored to the default management password.
- Forgot the Wi-Fi password:
  - Enter the default Wi-Fi password on the label on the back of the router and try again.
  - Scan the QR code on the label on the back of the router, and change the Wi-Fi password on the Reyee Router App.
  - If the fault persists, restore the router to factory settings. The management password will also be restored to the default Wi-Fi password.

10.3 What Should I Do If the System LED Keeps Flashing After the Router is Powered On?

Restore the router to factory settings and power on it again.
If the system LED still fails to turn solid on, you can contact us through the following channels:

- After-sales website: https://reyee.ruijie.com/en-global/support
- Manual service: https://reyee.ruijie.com/en-global/rita
- Community: https://community.ruijienetworks.com
- Service hotline: https://www.ruijienetworks.com/support/hotline

11 Appendix

11.1 User Ports

Table 11-1 Default Open Port Information

Port Number	Protocol	Service
1883, 8883, 9883, 43561, 43562	TCP	Reyee SON service

Port Number	Protocol	Service
53	TCP, UDP	DNS domain name service
67	UDP	DHCP service
5248	UDP	Roaming service
5252	UDP	Layer 3 roaming service
3799	UDP	RADIUS service
80, 443, 2062	TCP	Web service
22867	TCP	AP mesh service
6378, 6379, 6390, 6391	TCP	Database service

11.2 User Privacy Log

To generate and store logs for certain privacy-related activities, users must first connect their devices to the cloud.