Ruijie Reyee RG-EW3000GX PRO 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

The manual offers configuration information (including model, description, port type, software interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

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 Quick Setup (As a Primary Router) 4

2.1 Connecting the Router 4

2.2 Configuring the Router for Internet Access 5

2.2.1 eWeb-based Internet Access Configuration 5

3 Quick Setup (As a Secondary Router) 12

3.2 Wired Repeater Configuration 12

3.2.1 Connecting to the Primary Router 12

3.2.2 Internet Access Configuration 12

3.3 Wireless Repeater Configuration 17

3.3.1 Connecting to the Primary Router 17

3.3.2 Internet Access Configuration 17

3.4 Verification and Testing 29

3.5 Managing the Device After Successful Setup 29
3.5.1 Connecting the Device 29
3.5.2 Logging In to the Web Interface 29
4 Wi-Fi Network Settings 30
4.1 Adding Wi-Fi Networks 30
4.1.1 Adding Game Wi-Fi Network 30
4.1.2 Adding Other Types of Wi-Fi Networks 30
4.2 Changing the SSID and Password 32
4.3 Enabling Band Steering 33
4.4 Hiding the SSID 34
4.4.1 Overview 34
4.4.2 Getting Started 34
4.4.3 Configuration Steps 34
4.5 Configuring the Wi-Fi Blocklist or Allowlist 35
4.5.1 Overview 35
4.5.2 Configuration Steps 36
4.6 Optimizing the Wi-Fi Network 37
4.6.1 Overview 37
4.6.2 Getting Started 38
4.6.3 Configuration Steps 38
4.7 Configuring the Healthy Mode 41
4.8 Enabling Roaming Optimization 42
4.9 Configuring Wi-Fi/IGMP 42
4.9.1 Overview 42

4.9.2 Configuration Steps 43
5 Configuring Work Mode 44
5.1 Access Point 44
5.2 Wireless Repeater 45
5.3 WISP 47
6 Configuring Network Settings 51
6.1 Configuring WAN Settings 51
6.1.1 Configuring Internet connection types 51
6.1.2 Changing the MAC Address 52
6.1.3 Modifying MTU 53
6.1.4 Configuring a Private Line 54
6.1.5 Configuring the VLAN Tag 55
6.1.6 Configuring Load Balancing Settings 56
6.2 Changing the Address of a LAN Port 57
6.3 Connecting to IPTV 58
6.3.1 Getting Started 58
6.3.2 IPTV Configuration Steps (VLAN Type) 59
6.3.3 IPTV Configuration Steps (IGMP Type) 59
6.4 Configuring IPv6 60
6.4.1 Configuring the IPv6 of the WAN Port 60
6.4.2 Click Save.Configuring the IPv6 of the LAN Port 61
6.4.3 Viewing DHCPv6 Clients 62
6.5 Configuring Auto Bandwidth Control 62
6.5.1 Viewing Network Latency 63

6.5.2 Configuring Designated Devices 63
6.5.3 Viewing Auto Bandwidth Control Device Details 64
6.5.4 Disabling Auto Bandwidth Control 64
6.6 Setting Blocking Schedules 65
6.6.1 Setting a Blocking Schedule 65
6.6.2 Removing a Blocking Schedule 66
6.7 Configuring DHCP Server 66
6.7.1 Overview 66
6.7.2 Configuration Steps 66
6.8 Configuring DNS Server 69
6.8.1 Local DNS Server 69
6.8.2 Configuring DNS Proxy 69
6.9 Configuring Port Mapping 70
6.9.1 Overview 70
6.9.2 Getting Started 70
6.9.3 Configuration Steps 70
6.9.4 Verification and Testing 72
6.9.5 Solution to a Test Failure 72
6.9.6 DMZ Configuration Steps 72
6.10 Configuring DDNS 72
6.10.1 Overview 72
6.10.2 Getting Started 72
6.10.3 Configuration Steps 73
6.11 Configuring Connectivity Detection 73

6.12 Configuring ARP Binding 74
6.12.1 Overview 74
6.12.2 Configuration Steps 74
6.13 Configuring Static Routing 75
6.14 Policy-based Routing 77
6.14.1 Overview 77
6.14.2 Configuration Steps 77
6.15 Enabling Smart Traffic Control 80
6.15.1 Enabling Smart Flow Control 80
6.15.2 Custom Policy 80
6.16 Enabling Port-Based Flow Control 81
6.17 Enabling Hardware Acceleration 81
6.18 Enabling Reyee Mesh 82
6.19 Configuring Reyee Mesh 3.0 82
6.19.1 Parallel Networking 83
6.19.2 AP Networking 85
6.20 Configuring UPnP 86
6.20.1 Overview 86
6.20.2 Configuration Steps 86
6.21 Enabling Wi-Fi Switch 87
6.22 Switching to AP Mode 87
6.23 Configuring Auto NAT66 88
6.24 Configuring PPTP VPN 88
6.24.1 Overview 88

6.24.2 Configuring PPTP Server 88
6.24.3 Configuring PPTP Client 90
6.25 Configuring OpenVPN 91
6.25.1 Overview 91
6.25.2 Configuring OpenVPN (Server Mode) 91
6.25.3 Configuring OpenVPN (Client Mode) 95
6.25.4 Typical Configuration Example 96
6.26 Other Settings 101
7 Configuring Diagnostics 103
7.1 Enabling Alerts 103
7.2 Diagnosing Network Problems 104
7.3 Network Diagnosis Tools 105
7.3.1 Ping 105
7.3.2 Traceroute 105
7.3.3 DNS Lookup 106
7.3.4 HTTP/HTTPS Detection 106
7.4 Packet Capture Tool 108
8 System Settings 110
8.1 Switching to PC View 110
8.2 System Logs 110
8.2.1 Viewing System Logs 110
8.2.2 Configuring System Logs 111
8.3 Configuring the Login Password 115
8.4 Configuring Session Timeout Duration 115

8.5 Remote Access 116
8.6 Configuring Backup and Import 116
8.7 Restoring Factory Settings 117
8.8 Configuring System Time 117
8.9 Configuring Reboot 118
8.10 Configuring Scheduled Reboot 118
8.10.1 Getting Started 118
8.10.2 Configuration Steps 119
8.11 Performing Online Upgrade and Displaying the System Version 119
8.12 Turning On/Off the Indicator 120
8.13 Switching System Language 120
8.14 Configuring the Compatibility Mode 121
8.15 Configuring Cloud Service 122
8.15.1 Overview 122
8.15.2 Configuration Steps 122
8.15.3 Unbinding Cloud Service 123
8.16 Switching to Accessibility Mode 124
8.17 Connectivity Detection 124
9 FAQs 126
9.1 How Do I Restore the Router to Factory Settings? 126
9.2 What Should I Do If I Forgot the Password? 126
9.3 How Do I Manage the Router When Used As a Range Extender After Installation is Successful? 126
9.4 What Should I Do If the System LED Keeps Flashing After the Router is Powered On? 126
10 Appendix 127

10.1 User Ports 127

10.2 User Privacy Log 127

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-EW3000GX PRO	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 8.17 Connectivity Detection.

2. New Feature — HTTP/HTTPS Detection

ReyeeOS 1.420 supports the **HTTP/HTTPS Detection** feature. For details, see 7.3.4 HTTP/HTTPS Detection.

3. Changed Feature — Disable Reset

ReyeeOS 1.420 supports the **Disable Reset** feature. For details, see 8.7 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-EW3000GX PRO	1.xx

1.2.2 Software Feature Change

1. New Feature —Accessibility Mode

ReyeeOS 1.390 supports accessibility mode. For details, see 8.16 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-EW3000GX PRO	1.xx

1.3.2 Software Feature Change

ReyeeOS 1.380 is the baseline version of this configuration guide. Compared with ReyeeOS 1.316, ReyeeOS 1.380 has the following new and changed features:

1. New Feature — Compatibility Mode

ReyeeOS 1.380 supports compatibility mode. For details, see 8.14 Configuring the Compatibility Mode.

2. New Feature — System Log

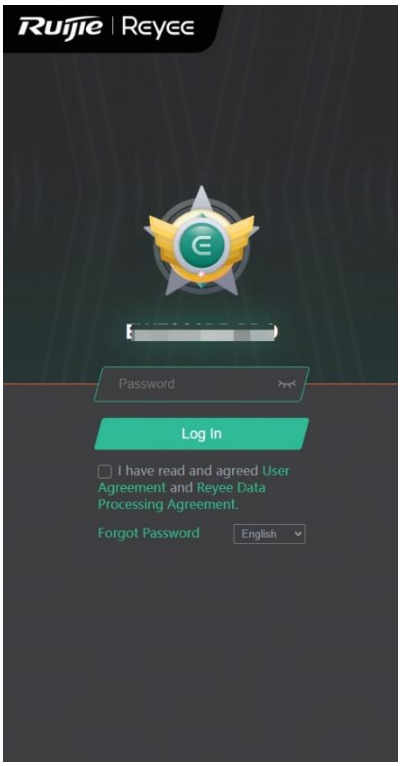
ReyeeOS 1.380 supports the System Log function. For details, see Section 8.2 System Logs.

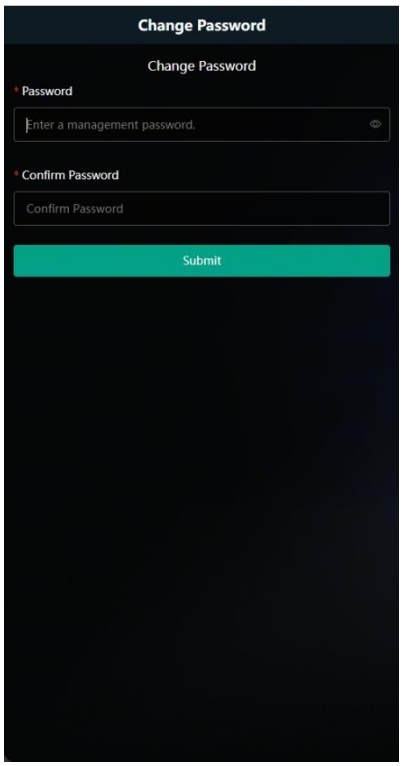
3. New Feature — Cloud Service

This version supports the cloud service feature. For details, see 8.15 Configuring Cloud Service.

4. 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 2 Quick Setup (As a Primary Router) and 3 Quick Setup (As a Secondary Router).


Ruijie | Reyee
Password
Log In
I have read and agreed User Agreement and Reyee Data Processing Agreement.
Forgot Password
English


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

2 Quick Setup (As a Primary Router)

When the device serves as the primary router, it is directly connected to a modem to provide wireless or wired Internet access for mobile phones, computers, and other devices.

To configure the device as the primary router for fast Internet access, follow these steps:

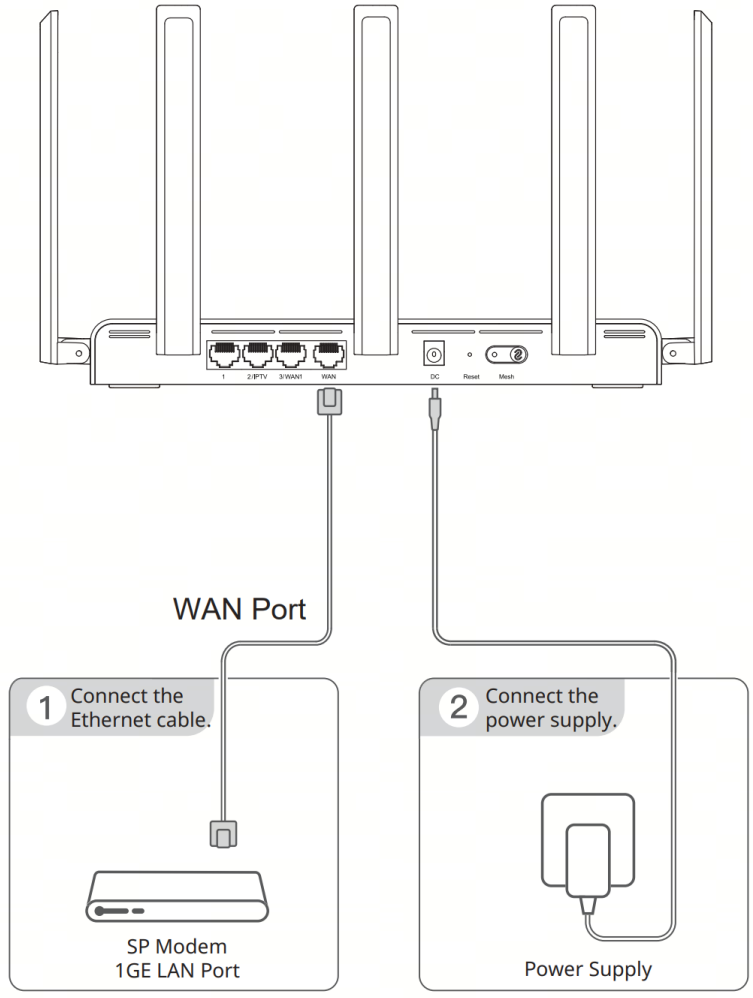
(1) Connect the router. For detailed configuration steps, see 2.1 Connecting the Router.

(2) Configure the router. For detailed configuration steps, see 2.2 Configuring the Router for Internet Access.

2.1 Connecting the Router

(1) Connect the supplied power cord to the DC connector of the router to supply power.

(2) Connect the WAN port (yellow port) of the router to the LAN port of the ISP's modem using an Ethernet cable.



(3) Wait for 2 to 3 minutes. The router will start up and broadcast Wi-Fi signals. The Service Set Identifier (SSID) of the default Wi-Fi network is **@Ruijie-sxxxx**. xxxx indicates the last four digits of the device's MAC address, which can be found on the nameplate at the bottom of the device.

Note

An ISP's modem typically provides the broadband authentication service. When connected to the ISP's modem, a router automatically connects to the Internet. In this case, you can access the Internet by connecting to the default Wi-Fi signal broadcast by the router. If the ISP's modem does not provide the broadband authentication service, you need to dial up to the Internet or configure an IP address for the device. For details, see 2.2 Configuring the Router for Internet Access.

2.2 Configuring the Router for Internet Access

The Internet access mode of the router must be configured according to the requirements of the broadband ISP. Otherwise, Internet access may fail. Therefore, before configuration, contact your ISP to confirm the Internet access mode and obtain the necessary configuration parameters.

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.
- **L2TP**: First, check whether the uplink device (like a modem) connects via DHCP or static IP.
  - DHCP: Enter the username, password, and server IP or domain name provided by the L2TP service provider.
  - Static IP: In addition to the username, password, and server IP or domain name from the L2TP service provider, enter the static IP address assigned by the uplink device, subnet mask, gateway IP address, and DNS server address.

2.2.1 eWeb-based Internet Access Configuration

1. Logging In to the Configuration Page

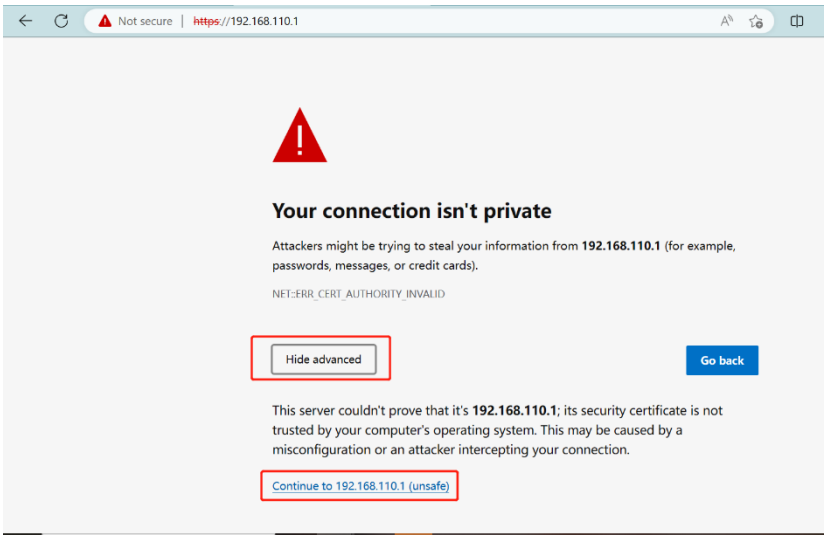
(1) You can open the management page and complete Internet access configuration only after connecting a smartphone or laptop to the router. You can connect a smartphone or laptop to the router in the following way.
  - **Wireless Connection:** On a smartphone or laptop, search for the Wi-Fi network **@Ruijie-s**XXXX (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) After a PC is connected to the router in the initial state, the setup page is displayed. If the setup page is not displayed, enter the IP address of the router (default: 192.168.110.1) or https://192.168.110.1 in the address bar of your browser, and press **Enter**. The login page is displayed.

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.

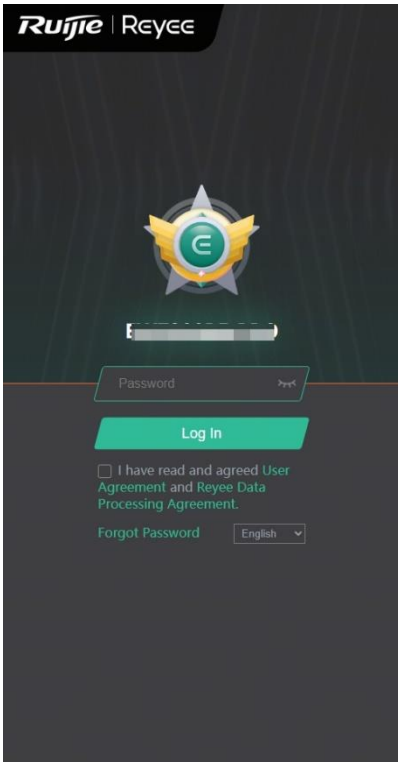
If you enter https://192.168.110.1 in the address bar of your browser, and press Enter, the following page will be displayed. Choose Advanced > Continue to 192.168.110.1(unsafe) to access the login page.



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

Note

The default password is required for the first login. The default password can be found on the nameplate at the bottom of the router. If no default password is shown, use **admin**.



2. Configuring the Device Password

Specification

If the default password is already shown on the nameplate at the bottom of the router, this step will be skipped. To change the password, see 8.3 Configuring the Login Password.

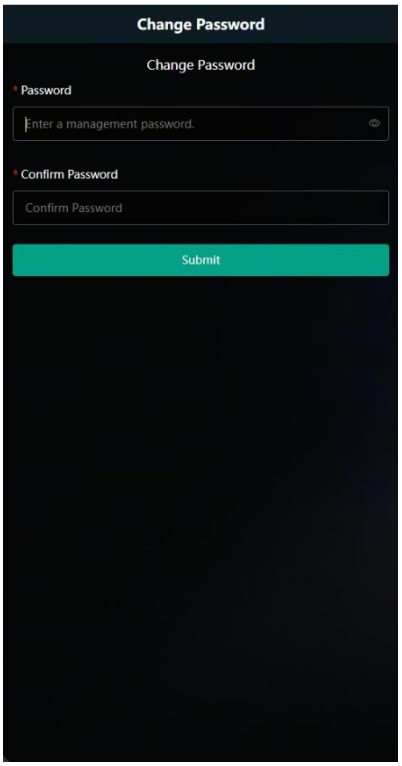
Caution

- The password is used to log in to the device's eWeb. Make sure to remember it.
- If you forget the IP address or password, hold down the **Reset** button for more than 10 seconds to restore the router to factory settings. After restoration, you can use the default IP address and password to log in.
- Restoring factory settings will delete existing configuration. You will be required to configure Internet access again at your next login. Therefore, exercise caution when performing this operation.

Set the router's password and tap **Submit**.

Note

For security purposes, set a device password with at least eight characters, including numbers, letters, and special characters.



3. Configuring the Internet Connection Type

Specification

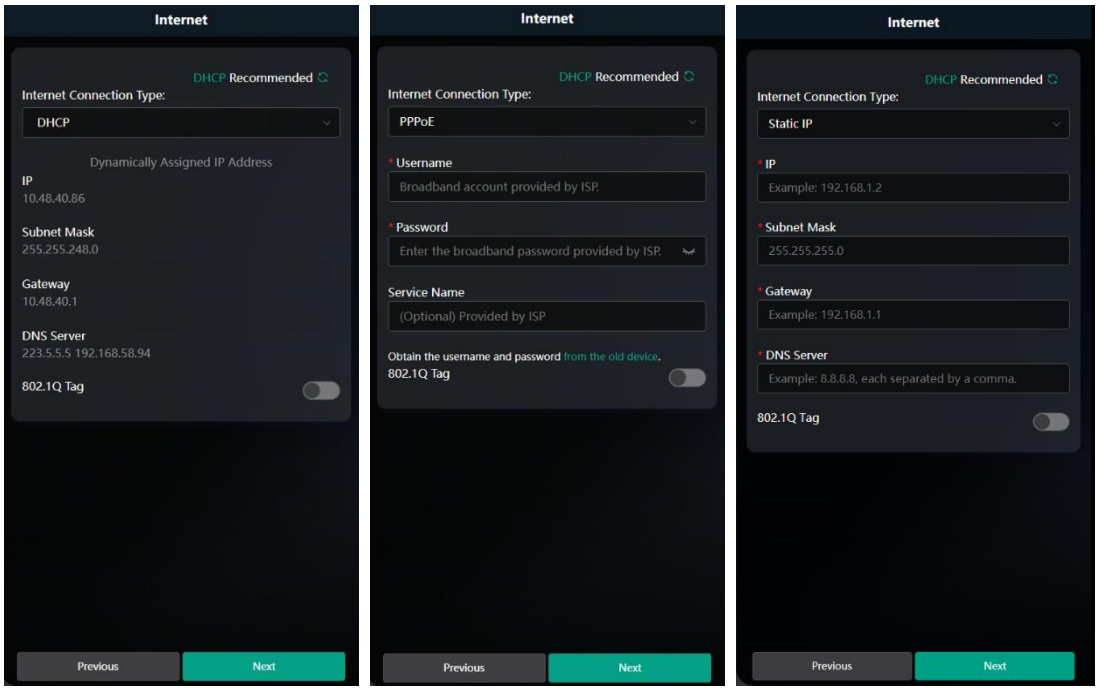
When the device is detected to be connected to the Internet, this step will be skipped automatically.

Select an Internet access mode and tap **Next**.

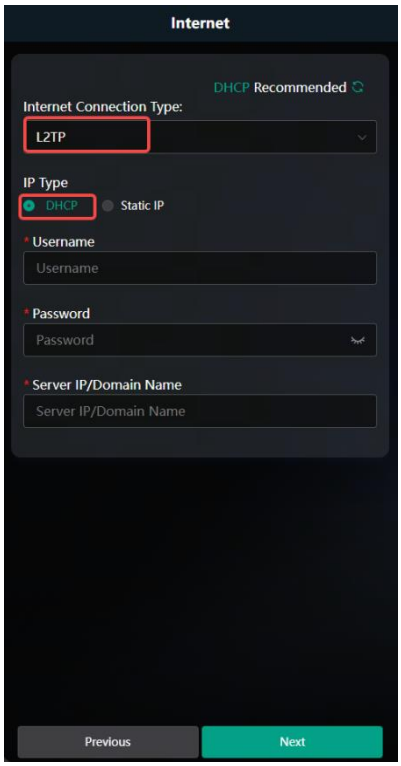
- **DHCP**: The uplink DHCP server automatically assigns an IP address to the device, with no configuration parameters required.

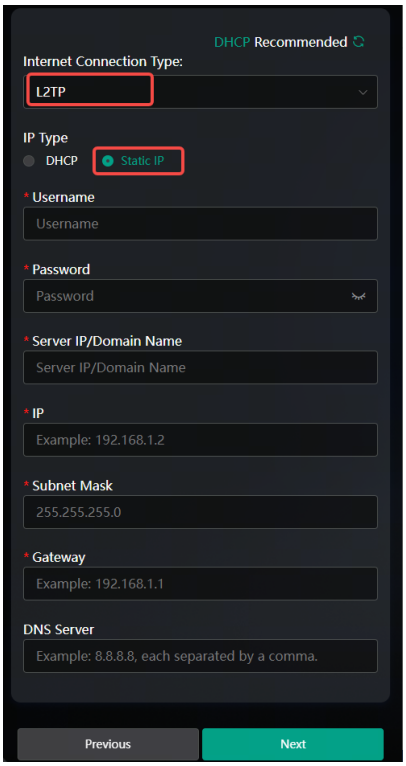
> **Caution**
>
> If the IP address delivered by the primary router is 192.168.110.0, the router will automatically change the IP address of its LAN port to 192.168.111.1 to avoid IP address conflict. Do not change the configuration of the primary router. You can differentiate routers by checking the router model and Wi-Fi information on the home page.

- **PPPoE**: 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.



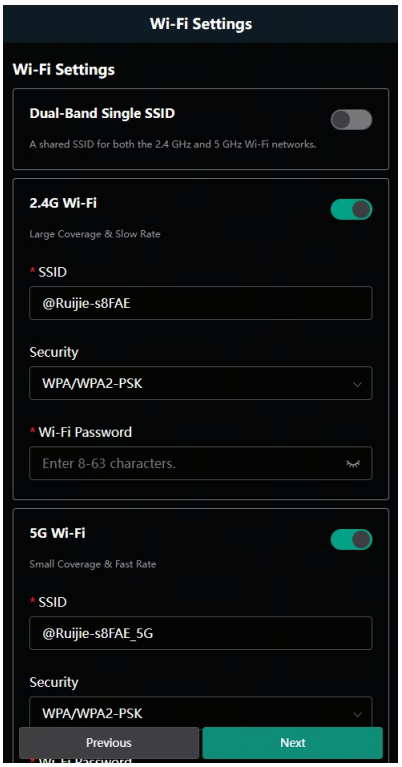
- **L2TP:** Select the IP address allocation type based on the L2TP VPN server information provided by the ISP:
  - DHCP: Enter the username, password, and server IP or domain name provided by the L2TP service provider, and click **Next**.
  - Static IP: In addition to the username, password, and server IP or domain name provided by the L2TP service provider, enter the static IP address assigned by the uplink device (like a modem), subnet mask, gateway IP address, and DNS server address for internet access, and click **Next**.





4. Configuring a Wi-Fi Network

Set the SSID and password, and tap **Next**.





- **Dual-Band Single SSID**: After this feature is enabled, the 2.4G SSID will be consistent with the 5G SSID and the 5G band will be preferred. The 2.4G signal is strong but easily interfered by various wireless signals. The 5G band boasts fast speed, low latency and less interference.

You are advised to disable **Dual-Band Single SSID**. When this function is disabled, you can disable 2.4G or 5G Wi-Fi networks separately, and set different passwords for 2.4G and 5G SSIDs.

When **Dual-Band Single SSID** is enabled, you can enable **Band Steering** in the meanwhile. The 5G-capable client will access 5G radio preferentially after the function is enabled. For details, see 4.3 Enabling Band Steering.

Note

The terms “2.4G” and “5G” mentioned in this document only refer to the channels with the frequency of 2.4 GHz and 5 GHz, and have nothing to do with the 5G (fifth generation) Mobile Communication Technology.

- **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.

- **SSID** and **Wi-Fi Password** in **Game Wi-Fi**: The gaming SSID and password will be automatically set to the primary device's SSID with the suffix "_Game" and password, respectively. Tap the corresponding input fields to modify the values.
- **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.

5. 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.

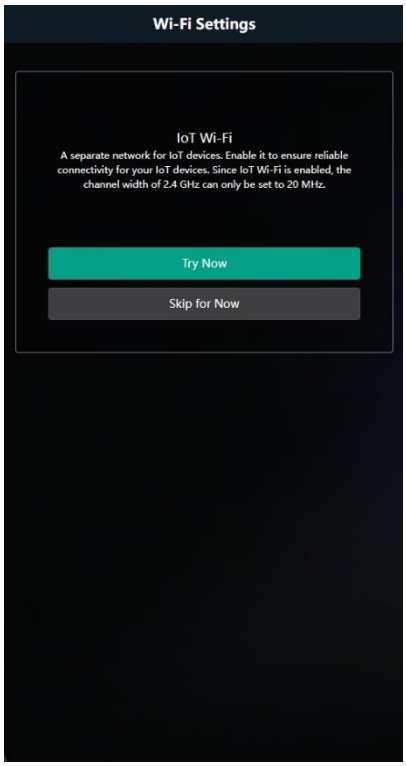
(1) Tap **Try Now** to configure the IoT Wi-Fi network.

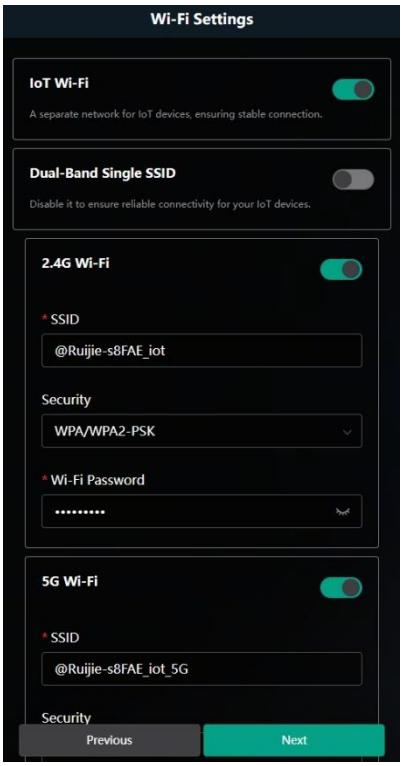
Note

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

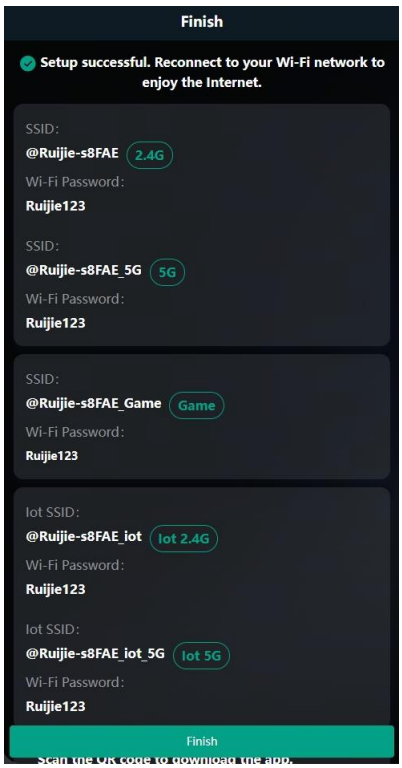
(2) Toggle on **IoT Wi-Fi**, configure the Wi-Fi parameters, and tap **Next**.

To provide smart home clients with a better network experience, you are advised to toggle off **Dual-Band Single SSID** and configure separate SSIDs and passwords for the 2.4 GHz and 5 GHz bands.





(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 Quick Setup (As a Secondary Router)

When the primary router's wireless signal cannot cover the entire home, adding a secondary router can extend network coverage, providing stable wireless or wired connections for clients in coverage holes, such as smartphones and computers.

The steps of configuring a device as the secondary router for fast Internet access are as follows:

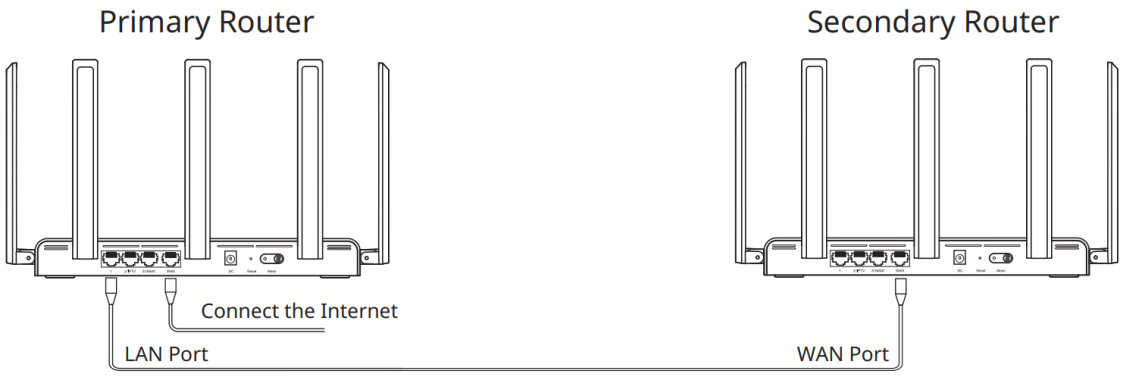
(1) Before configuring this router as a secondary router, configure the primary router and verify that the primary router can access the Internet. Otherwise, the secondary router cannot be connected to the Internet.

(2) Choose the mode for the secondary router to extend the primary router's network coverage based on your actual scenario. The following two modes are supported:

- **Wired repeater**: If there are pre-installed Ethernet cables in your home, connect the secondary router's WAN port to the primary router's LAN port using an Ethernet cable. This wired mode extends the network coverage of the primary router and provides more stable connectivity. For detailed configuration, see 3.2 Wired Repeater Configuration.
- **Wireless repeater**: If it is not feasible to connect the primary and secondary routers using an Ethernet cable, the secondary router can extend the primary router's Wi-Fi coverage by functioning as a wireless repeater. For detailed configuration, see 3.3 Wireless Repeater Configuration.

3.2 Wired Repeater Configuration

3.2.1 Connecting to the Primary Router



(1) Use an Ethernet cable to connect the WAN port of the secondary router to the LAN port of the primary router.

(2) 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.

3.2.2 Internet Access Configuration

1. Wired Repeater Using Reyee Mesh

Note

- If the primary router is a Ruijie home router that supports Reyee Mesh, perform the following configuration steps.

- To use Reyee Mesh, the secondary router must be in factory default state. If the secondary router has been configured, press and hold the Reset button on the device for more than 10 seconds to restore it to factory settings.

(1) Connect the secondary router to the primary router as instructed in 3.2.1 Connecting to the Primary Router.

(2) Press the **Reyee Mesh** button on the primary router to establish a wired connection. The Reyee Mesh LEDs on both the primary and secondary routers will begin to blink.

(3) Wait until the Reyee Mesh LEDs on both the primary and secondary routers stay solid on. Reyee Mesh setup is complete. The default SSID and password of the secondary router are automatically synchronized to be the same as those on the primary router.

2. Web-based Wired Repeater

Note

If the primary router is not a Ruijie home router, perform the following configuration steps.

(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.

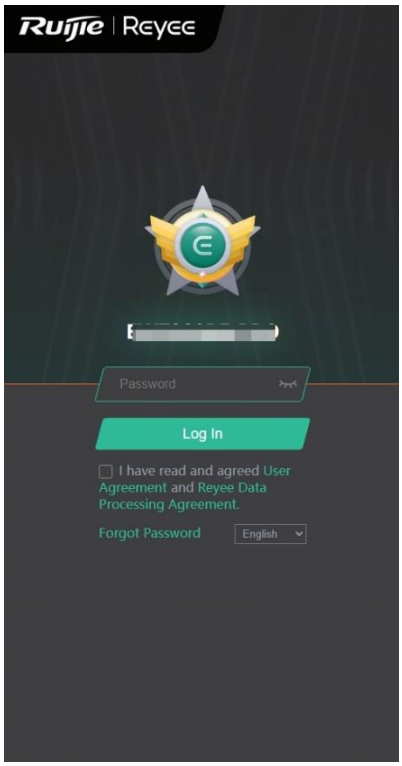
- **Wireless Connection:** On a smartphone or laptop, search for the Wi-Fi network **@Ruijie-s**XXXX (XXXX is the last four digits of the MAC address of each device). The default SSID and login address can be found on the bottom label of the router.
- **Wired Connection:** Connect a local area network (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 is required for the first login. The default password can be found on the nameplate at the bottom of the router. If no default password is shown, use **admin**.



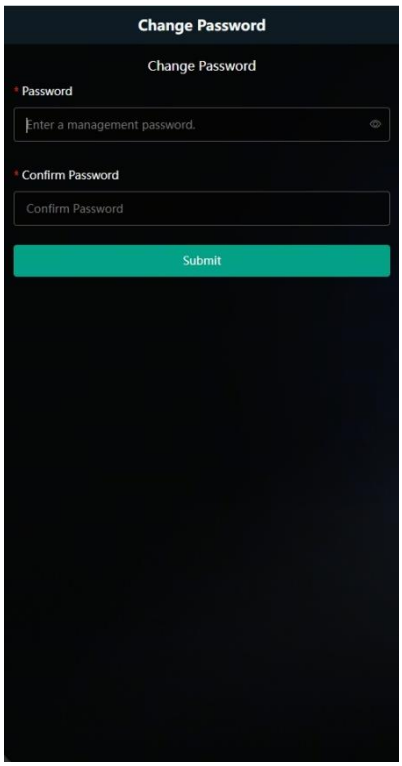
(4) Set the router's password and tap **Submit**.

Specification

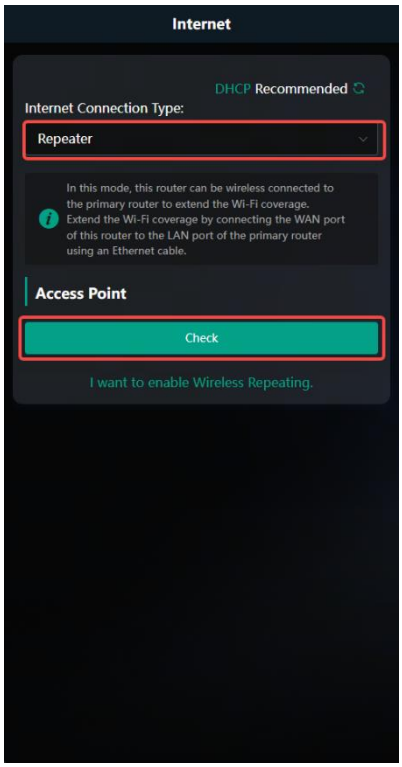
If the default password is already shown on the nameplate at the bottom of the router, this step will be skipped. To change the password, see 8.3 Configuring the Login Password.

Caution

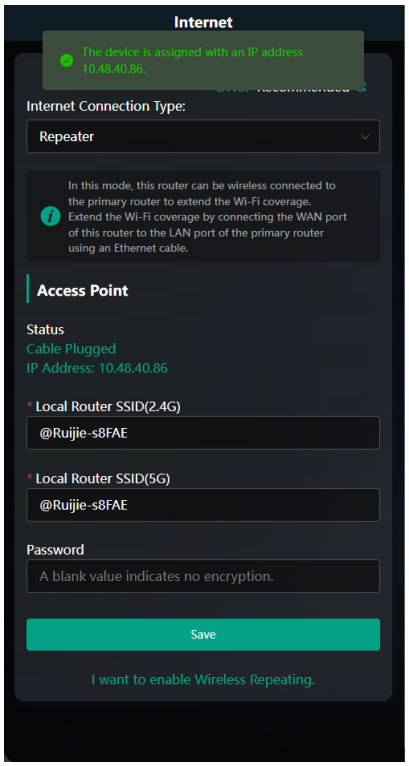
- The password is used to log in to the device's eWeb. Make sure to remember it. If you forget the password, press and hold the Reset button on a device for more than 10 seconds to restore it to factory settings. Restoring factory settings will delete all configurations and you will be required to configure again at your next login. Therefore, exercise caution when performing this operation.
- For security purposes, set a device password with at least eight characters, including numbers, letters, and special characters.



(5) Set Internet Connection Type to Repeater, and tap Check.



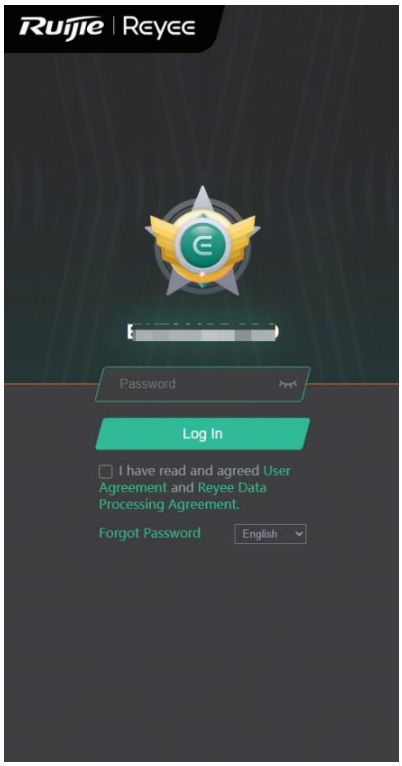
(6) The device will automatically detect the connection mode with the primary router and the obtained IP address. Set the SSID and password of the secondary router. Then, tap **Save**.



(7) After the configuration is complete, you will be redirected to the eWeb management page. Use the password set in step (4) to log in. At the same time, the Wi-Fi networks configured on the device will automatically restart. Reconnect to a network with the new SSID using the configured password.

Note

If step (4) is skipped during configuration, you can log in to the eWeb management page using the default password shown on the nameplate at the bottom of the device.



3.3 Wireless Repeater Configuration

3.3.1 Connecting to the Primary Router

(1) 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.

(2) 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.

3.3.2 Internet Access Configuration

1. Wireless Connection Using Reyee Mesh

Note

- When both the primary router and secondary router are Reyee Home Wi-Fi routers, you can enable the Reyee Mesh feature to extend the Wi-Fi range of the primary router.
- To use Reyee Mesh, the secondary router must be in factory default state. If the secondary router has been configured, press and hold the Reset button on the device for more than 10 seconds to restore it to factory settings.

(1) Briefly press the Reyee Mesh button on the primary router. The Reyee Mesh LEDs on both the primary and secondary routers will begin to blink.

(2) Wait until the Reyee Mesh LEDs on both the primary and secondary routers stay solid on. Reyee Mesh setup is complete. The SSID and password of the secondary router are automatically synchronized with those of the primary router.

(3) Place the secondary router in a location where the Wi-Fi signal needs to be extended, and power it on.

2. Web-based Wireless Connection

Note

When the primary router is a non-Reyee Home Wi-Fi router, to wireless connect this router to the primary router, you can log in to its web interface and connect this router to the Wi-Fi network of the primary 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.

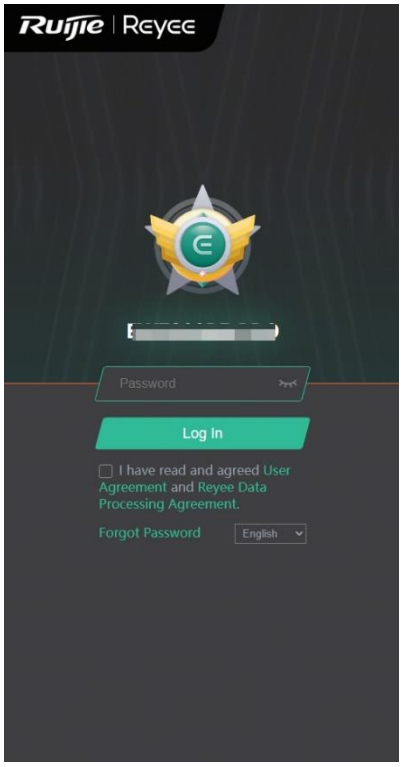
- **Wireless Connection:** On a smartphone or laptop, search for the Wi-Fi network **@Ruijie-s**XXXX (XXXX is the last four digits of the MAC address of each device). The default SSID and login address can be found on the bottom label of the router.
- **Wired Connection:** Connect a local area network (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 is required for the first login. The default password can be found on the nameplate at the bottom of the router. If no default password is shown, use **admin**.



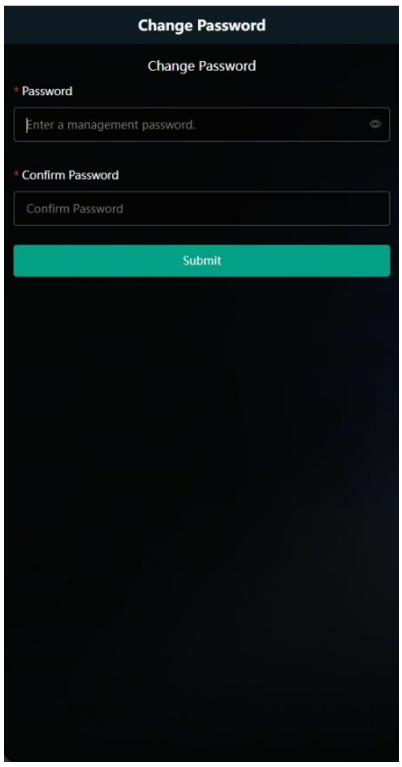
(4) Set the router's password and tap **Submit**.

Specification

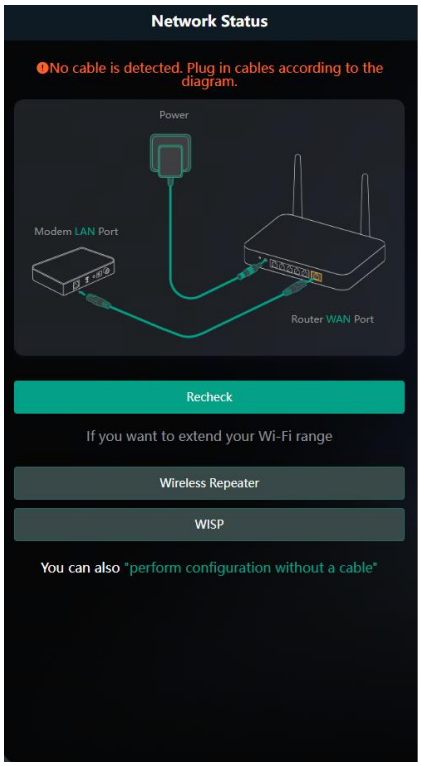
If the default password is already shown on the nameplate at the bottom of the router, this step will be skipped. To change the password, see 8.3 Configuring the Login Password.

Caution

- The password is used to log in to the device's eWeb. Make sure to remember it. If you forget the password, press and hold the Reset button on a device for more than 10 seconds to restore it to factory settings. Restoring factory settings will delete all configurations and you will be required to configure again at your next login. Therefore, exercise caution when performing this operation.
- For security purposes, set a device password with at least eight characters, including numbers, letters, and special characters.

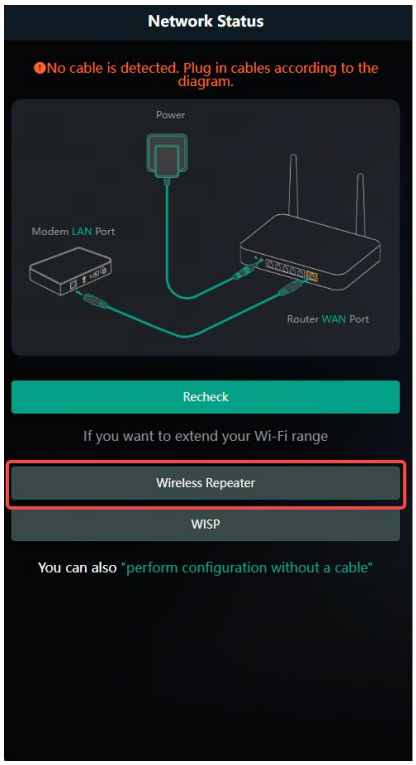


(5) The device supports two wireless repeater modes: Wireless Repeater and WISP. Configure the device according to your actual needs.



- Wireless Repeater

a. Select **Wireless Repeater**.

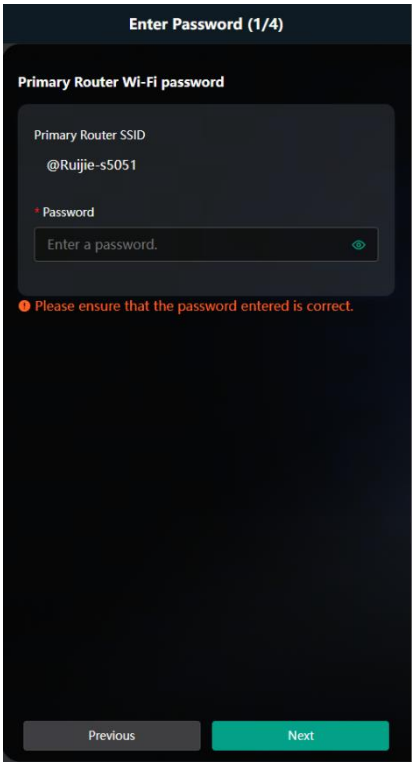


b. Select the SSID of the primary router, and enter the Wi-Fi password to connect to the primary router. Tap **Next**.

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

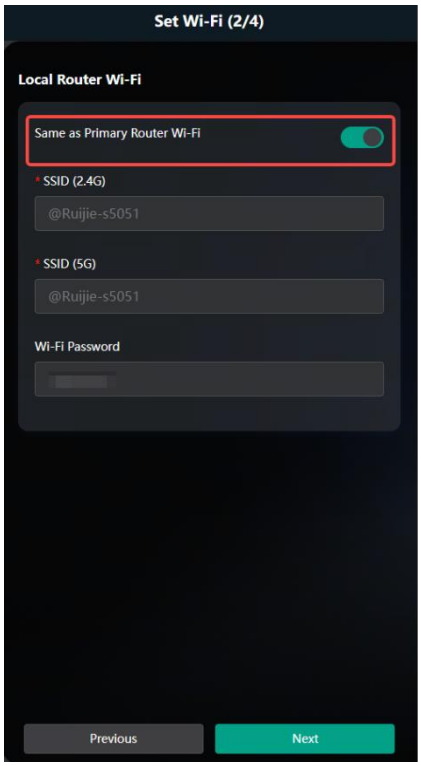
connects to the primary router in wireless repeater mode, the WAN port of the device keeps unchanged. If WAN cable is plugged in, the device automatically switches to the wired repeater mode.





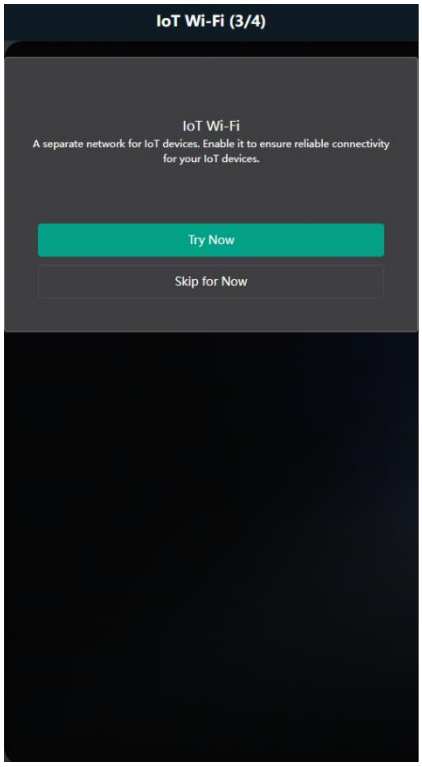
c. Set the Wi-Fi network of the secondary router and tap **Next**.

- 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.

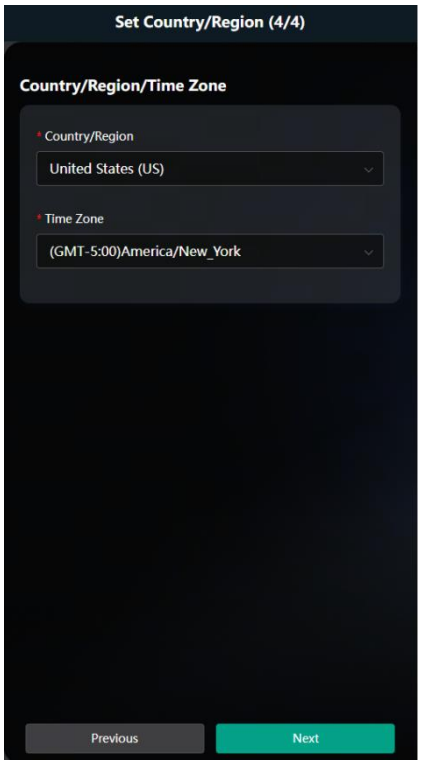




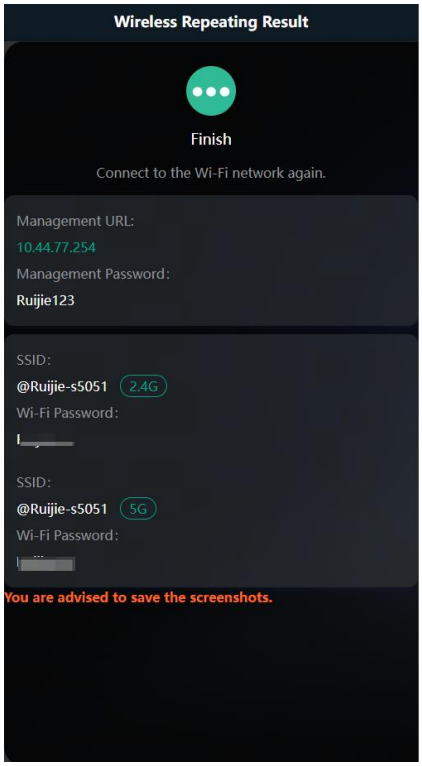
d. Enable IoT Wi-Fi as required. For detailed configuration, see 2.2.1 5. Configuring IoT Wi-Fi.



e. 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**.



f. 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.



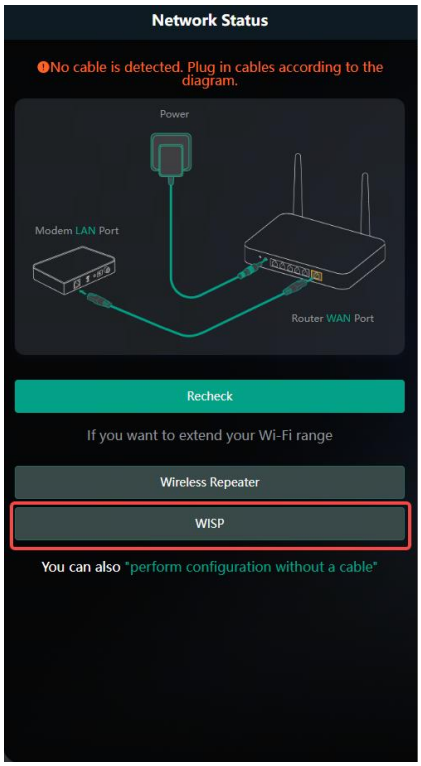
- WISP

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

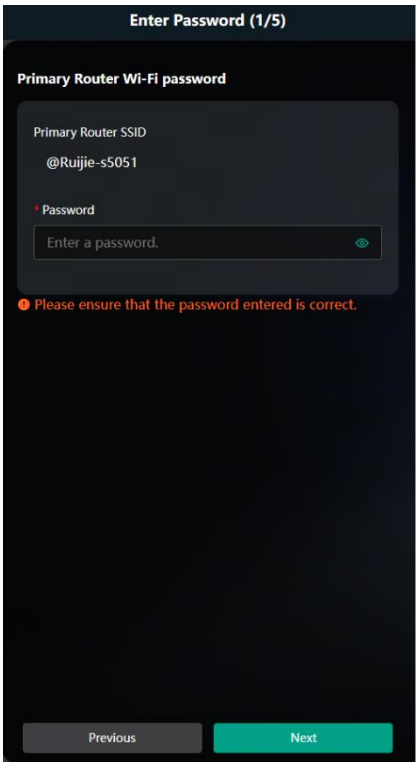
In the WISP mode, the device still supports routing and DHCP. The clients connected to the primary router are assigned IP addresses by the primary router; the clients connected to the secondary router are assigned IP addresses by the secondary router.

g. Tap **WISP**. Select the Wi-Fi of the primary router.



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

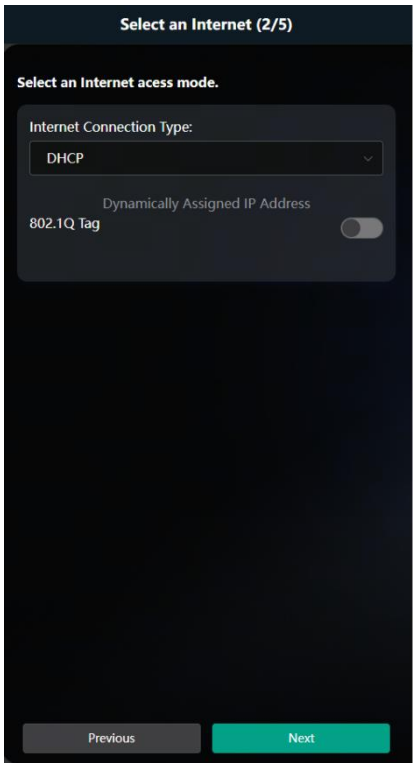




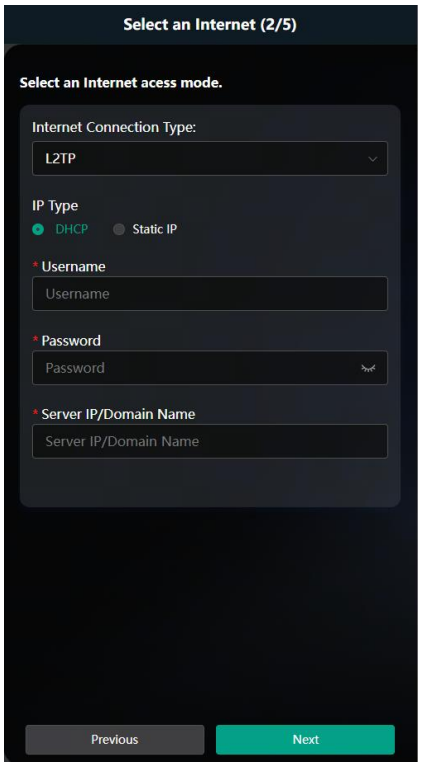
i. Select an Internet access mode. For details, see 2.2.1 3. Configuring the Internet Connection Type.

- Select DHCP and the extender will automatically obtain an IP address.
- If the primary router cannot assign IP addresses, select **Static IP**.

If the Internet connection type provided by the ISP is L2TP, then select **L2TP**. Select the IP address allocation type based on the actual situation, and enter the username, password, and other information.

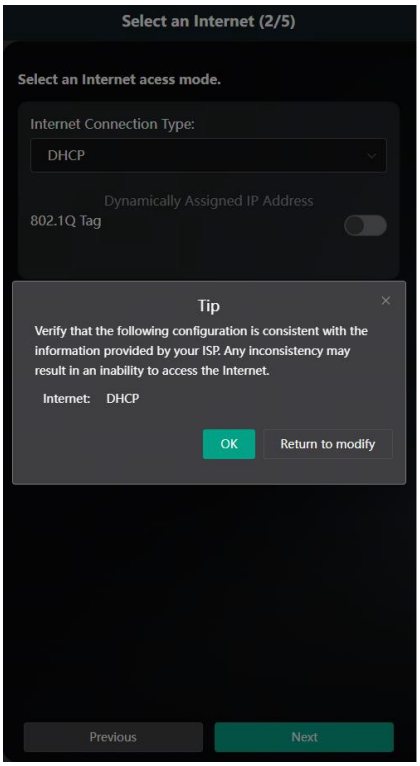








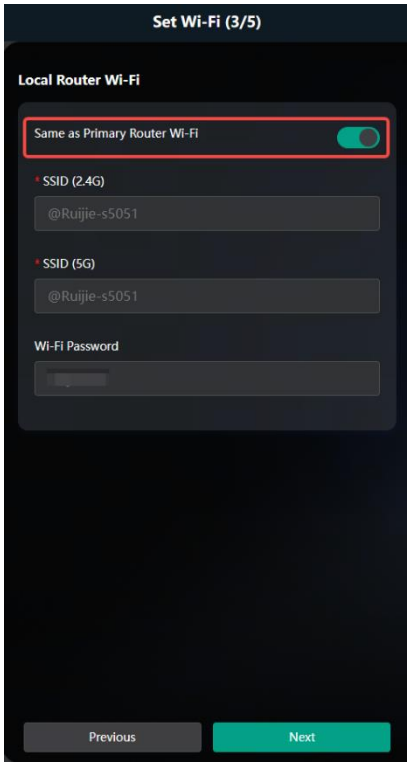
j. Tap **Next**. Verify the Internet settings. Then, tap **OK**.



k. Set the Wi-Fi network of the secondary router and tap **Next**.

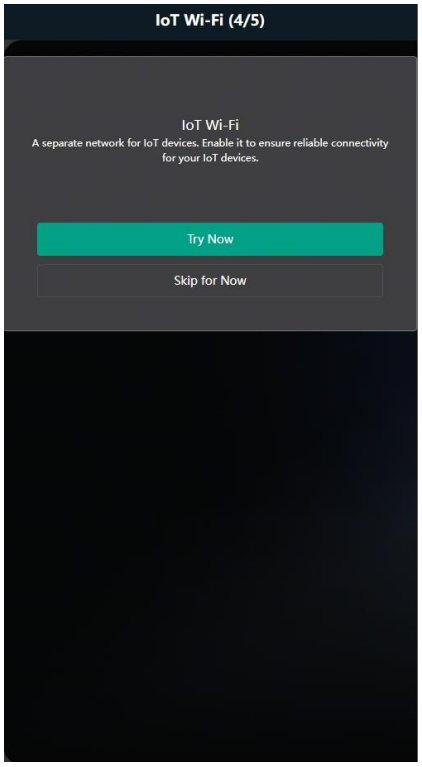
- Toggle on **Same as Primary Router Wi-Fi**. The SSID and password of the secondary router will be the same as those of the primary router.
- Toggle off **Same as Primary Router Wi-Fi**. You need to set a separate SSID and password for the

secondary router.

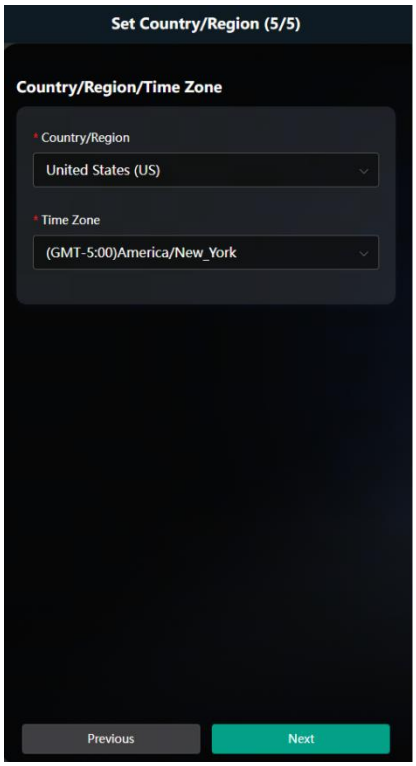




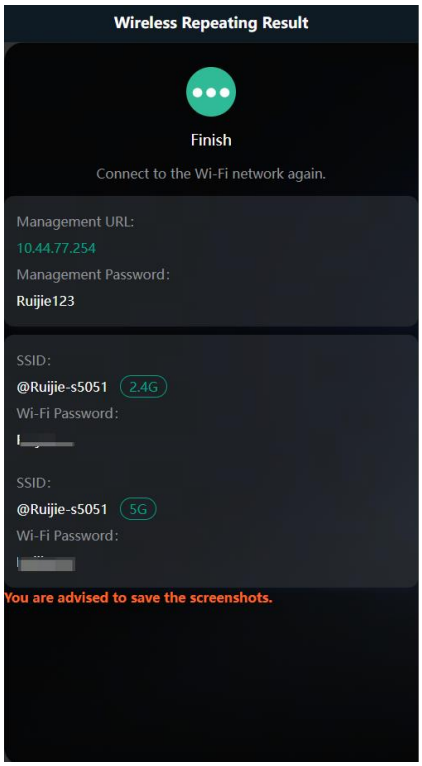
l. Enable IoT Wi-Fi as required. For detailed configuration, see 2.2.1 5. Configuring IoT Wi-Fi.



m. 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**.



n. 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.



3.4 Verification and Testing

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

3.5 Managing the Device After Successful Setup

After successful setup, you can manage the router by accessing its web interface.

3.5.1 Connecting the Device

Connect your smartphone or PC to the router via a wired or wireless connection.

- Wired Connection

  Connect your PC to the LAN/WAN port of the router using an Ethernet cable, and configure **Obtain an IP address automatically** on the PC.

- Wireless Connection

  On your smartphone or PC, search for and connect to the Wi-Fi network of the router.

3.5.2 Logging In to the Web Interface

- Login using the default IP address

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

- **Login using an obtained IP address**

If you fail to log in using the default IP address, you can obtain an IP address from the primary router for login. The steps are as follows:

(1) Log in to the web interface of the primary router to find the current IP address of the router.

(2) Enter this IP address in the address bar of your browser, and press **Enter**. The login page is displayed.

If you encounter any issues during this process, feel free to seek help from the official website at https://reyee.ruijie.com or reach out to customer service by emailing service_rj@ruijienetworks.com.

4 Wi-Fi Network Settings

4.1 Adding Wi-Fi Networks

This router supports four types of Wi-Fi networks, which are default Wi-Fi, Game Wi-Fi, Guest Wi-Fi and Smart Home Wi-Fi networks.

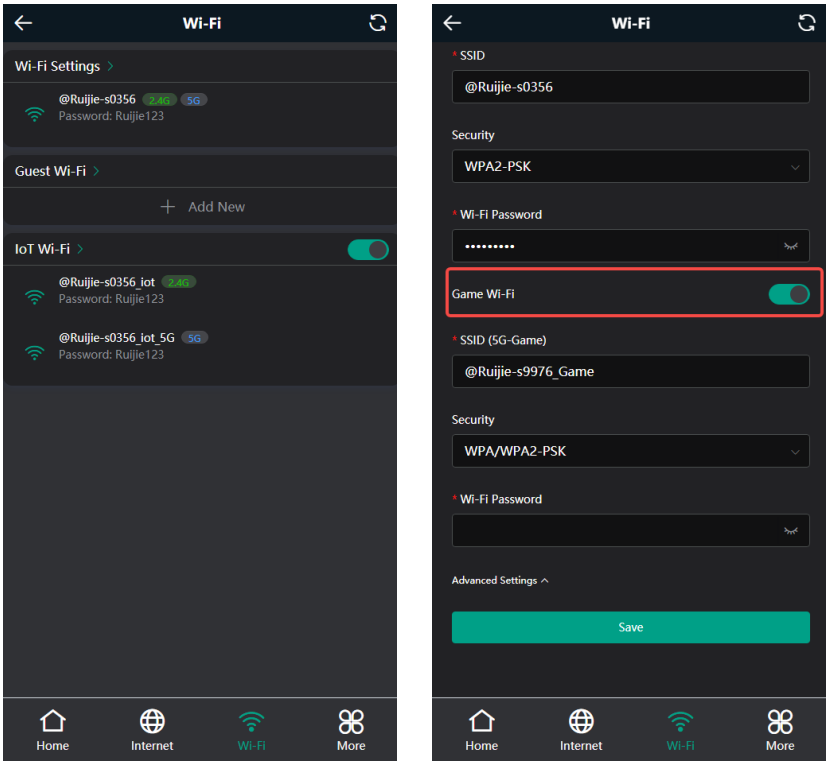
Smartphone View: Choose **Wi-Fi** > **Wi-Fi Settings**.

Click the target Wi-Fi network.

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

4.1.1 Adding Game Wi-Fi Network

On the **Wi-Fi Settings** page, choose **Wi-Fi** > **Wi-Fi Settings**, enable **Game-Wi-Fi** and change the SSID and password of the Game Wi-Fi.



4.1.2 Adding Other Types of Wi-Fi Networks

1. Overview

In addition to the Game Wi-Fi network, this router also supports other three types of Wi-Fi networks: primary Wi-Fi network, guest Wi-Fi network, and IoT Wi-Fi network. Only one Wi-Fi network can be configured for each type.

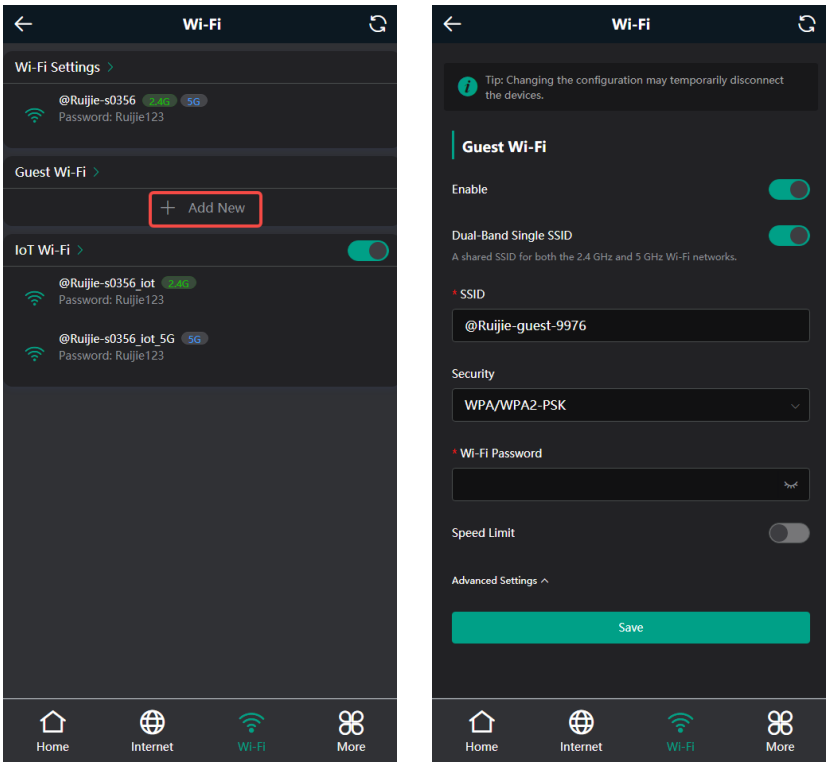
- **Primary Wi-Fi**: The primary Wi-Fi network is listed in the first line of the page and is enabled by default.
- **Guest Wi-Fi**: This Wi-Fi network is provided for guests and is disabled by default. It supports user isolation, that is, access users are isolated from each other. They can only access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

access each other, improving security.

- **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.

2. Configuration Steps

Click **Add New** and set the SSID and password.



- **Dual-Band Single SSID**: After this feature is enabled, the 2.4 GHz SSID will be consistent with the 5 GHz SSID and the 5 GHz band will be preferred. The 2.4 GHz signal is strong but easily interfered by various wireless signals. The 5 GHz band boasts fast speed, low latency and less interference.

  You are advised to disable **Dual-Band Single SSID**. When this function is disabled, you can disable 2.4G or 5G Wi-Fi networks separately, and set different passwords for 2.4 GHz and 5 GHz SSIDs.

  When **Dual-Band Single SSID** is enabled, you can enable **Band Steering** in the meanwhile. The 5G-capable client will access 5 GHz radio preferentially after the function is enabled. For details, see 4.3 Enabling Band Steering.

- **Effective Time:** For the **Primary Wi-Fi** network and **IoT Wi-Fi**, options include **Always**, **Weekdays**, **Weekends** 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 and IoT Wi-Fi.

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

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

- **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.

- **Wi-Fi 6**: You can enable Wi-Fi 6 to enjoy high-speed Internet access.
- **XPress**: After this function is enabled, the device sends game packets preferentially, providing more stable wireless network for games.

4.2 Changing the SSID and Password

Smartphone View: Choose **Wi-Fi** > **Wi-Fi Settings**.

Click the target Wi-Fi network.

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

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

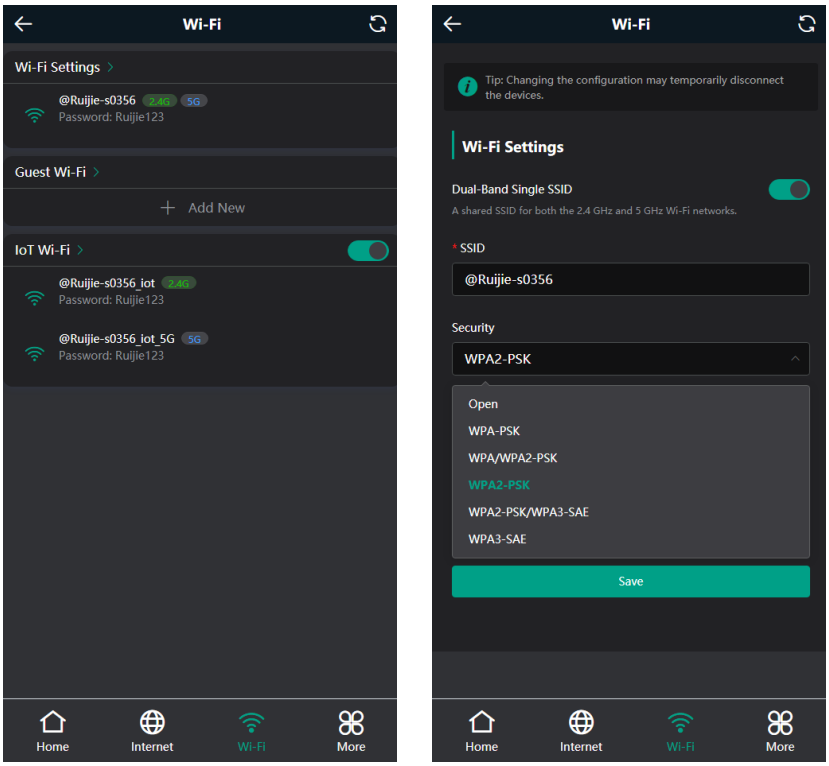
Caution

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

You can set the encryption type and Wi-Fi password for different types of Wi-Fi networks such as 2.4 GHz Wi-Fi, 5 GHz Wi-Fi, Game Wi-Fi and Smart Wi Fi.

The encryption types supported include: Open, WPA-PSK, WPA/WPA2-PSK, WPA2-PSK, WPA2-PSK/WPA3-SAE, and WPA3-SAE. You are advised to enable encryption and set a strong password to improve network security.

The password must be a string of 8 to 63 characters, which can contain uppercase and lowercase letters, digits, and English characters, but cannot contain special characters such as single quotation marks ('), double quotation marks (''), or spaces.



4.3 Enabling Band Steering

Caution

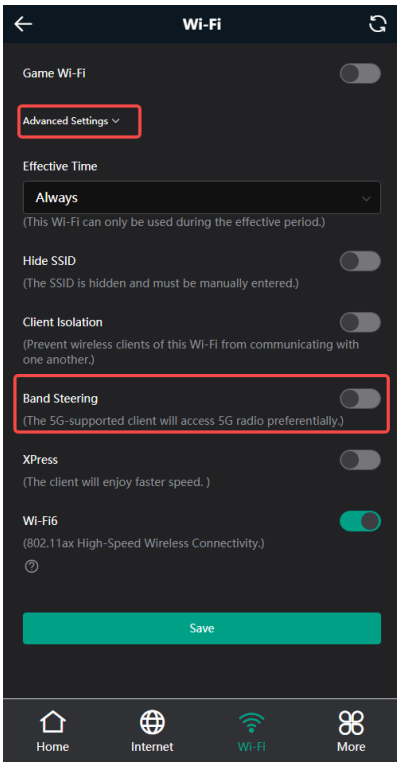
Before enabling the band steering, you must enable the **Dual-Band Single SSID**. Because the client can automatically choose to steer to either band only when the 2.4G and 5G bands use the same SSID.

Smartphone View: Choose **Wi-Fi** > **Wi-Fi Settings**.

Click the target Wi-Fi network.

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

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



4.4 Hiding the SSID

4.4.1 Overview

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

4.4.2 Getting Started

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

4.4.3 Configuration Steps

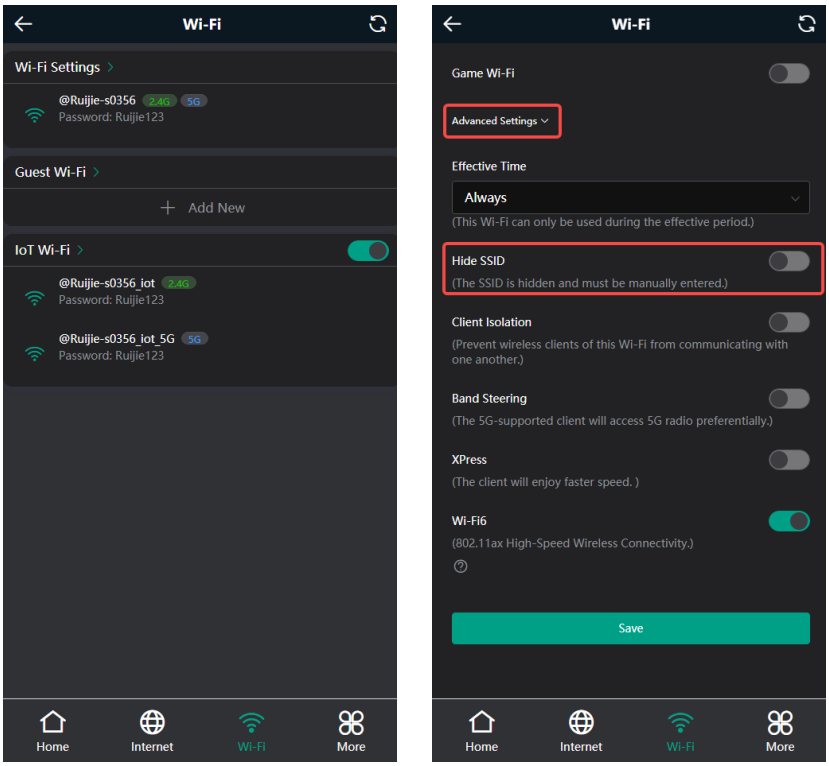
Smartphone View: **Wi-Fi** > **Wi-Fi Settings**

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

On the **Wi-Fi Settings** page, enable **Hide SSID**, and click **Save**. 2.4 GHz Wi-Fi, 5 GHz Wi-Fi and Game Wi-Fi will be hidden.

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**.

4.5 Configuring the Wi-Fi Blocklist or Allowlist

4.5.1 Overview

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

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

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.

4.5.2 Configuration Steps

Smartphone View: Choose More > Switch to PC view > More > WLAN > Blocklist / Allowlist.

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

The following takes the blocklist configuration as an example. If you want to configure an allowlist, follow the same steps.

(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.

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.

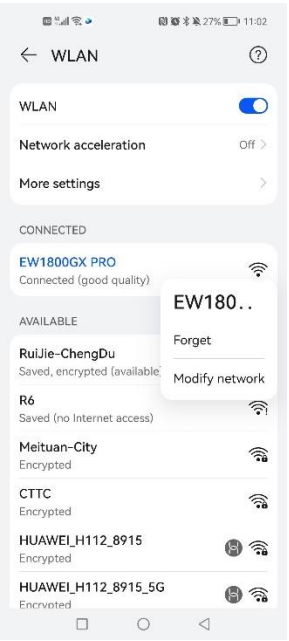
Caution

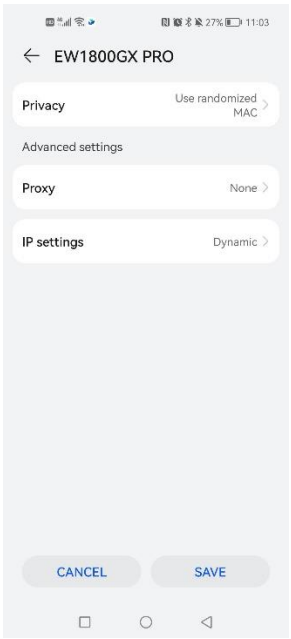
This configuration prevents some devices from connecting to the Wi-Fi network. Exercise caution when performing this operation.

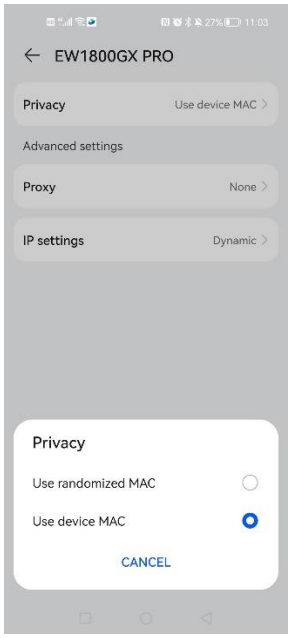
Note

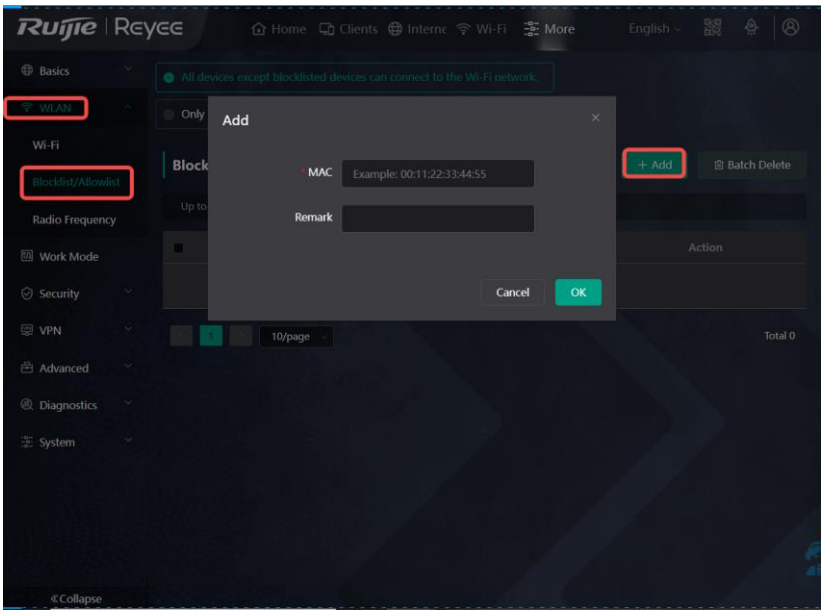
To use this function, you must disable the randomized MAC address on the mobile device. The following example shows how to disable the randomized MAC address on an Android device.

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.

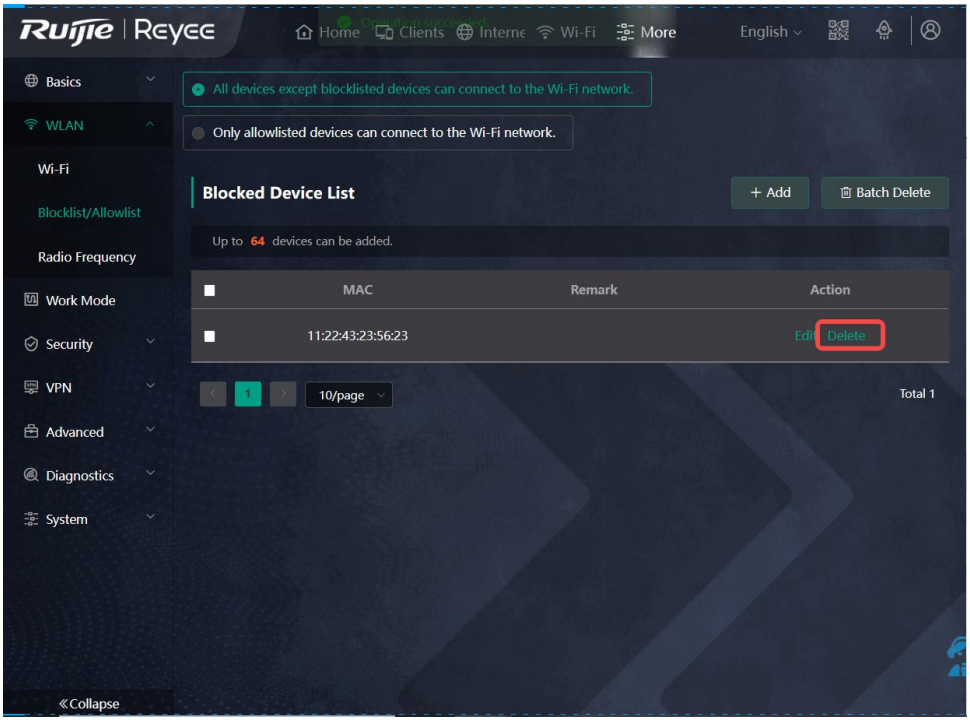








(2) Click **Delete**. The client can connect to the Wi-Fi network again.



4.6 Optimizing the Wi-Fi Network

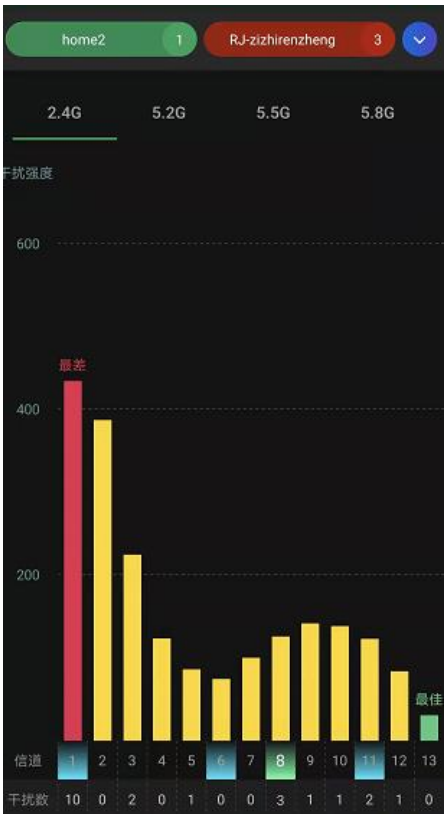
4.6.1 Overview

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

details, see 8.10 Configuring Scheduled Reboot. You can also analyze the wireless environment around the router and select appropriate parameters.

4.6.2 Getting Started

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



4.6.3 Configuration Steps

- Optimizing the radio channel

Smartphone View: Choose **More** > **Channel Transmit Power**.

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

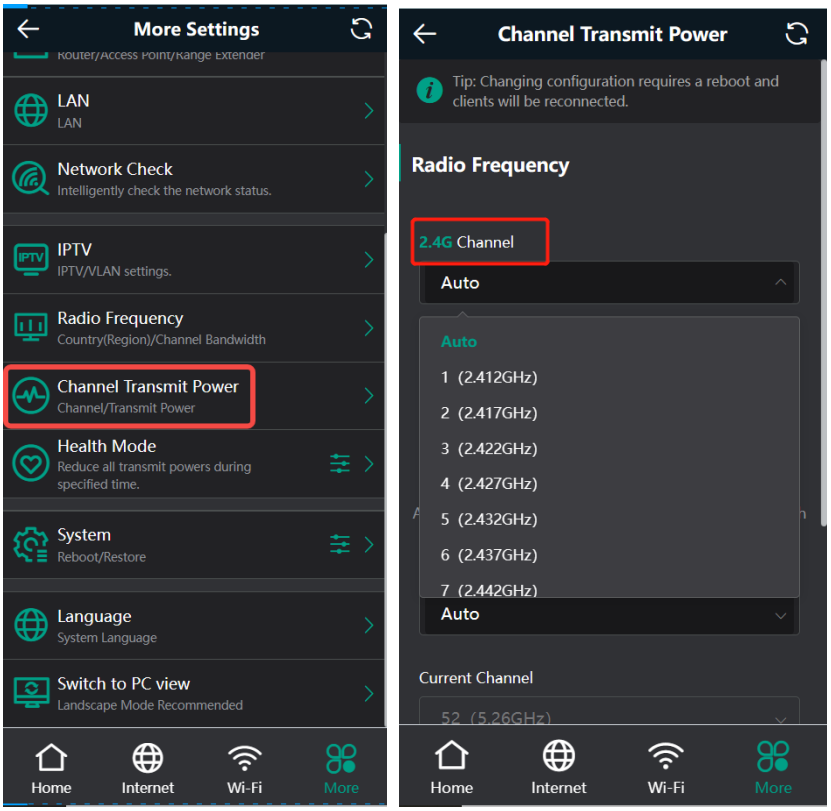
Choose the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. Excess clients connected to a channel can bring stronger wireless interference.

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

Smartphone 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.

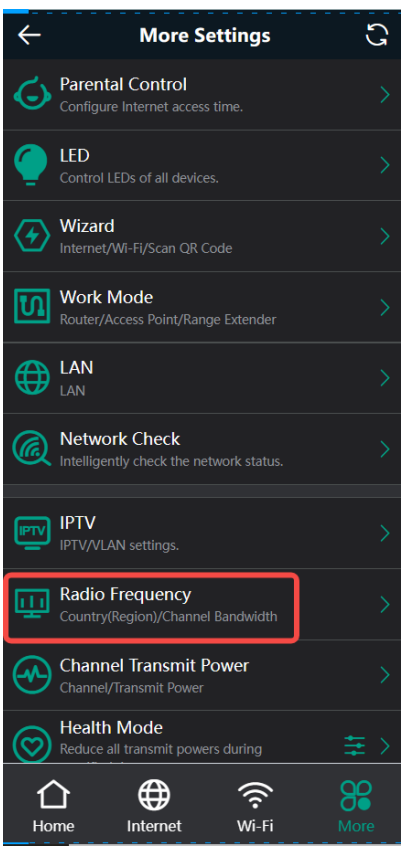
You can select 20 MHz and 40 MHz bandwidths for the 2.4 GHz band, or 20 MHz, 40 MHz, 80 MHz and 160 MHz for the 5 GHz band. The default value is "Auto", indicating that the bandwidth will be automatically selected based on the wireless environment.

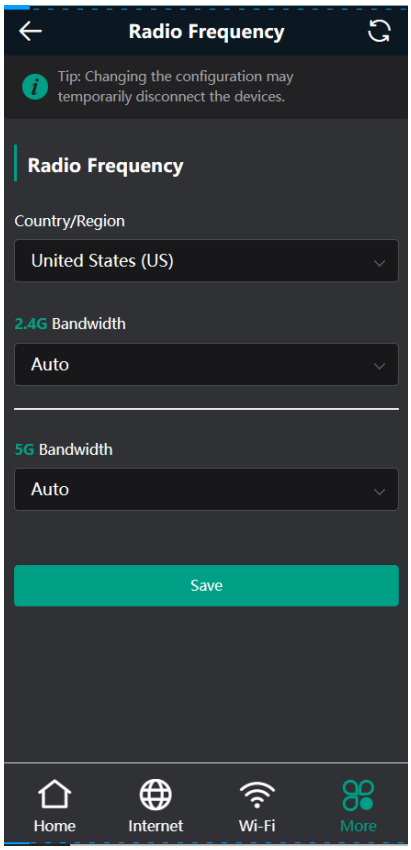
The Wi-Fi network speed is more stable when the channel bandwidth is smaller, and a larger channel bandwidth makes the device more prone to interference. You are advised to select 20 MHz bandwidth for the 2.4 GHz band.

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

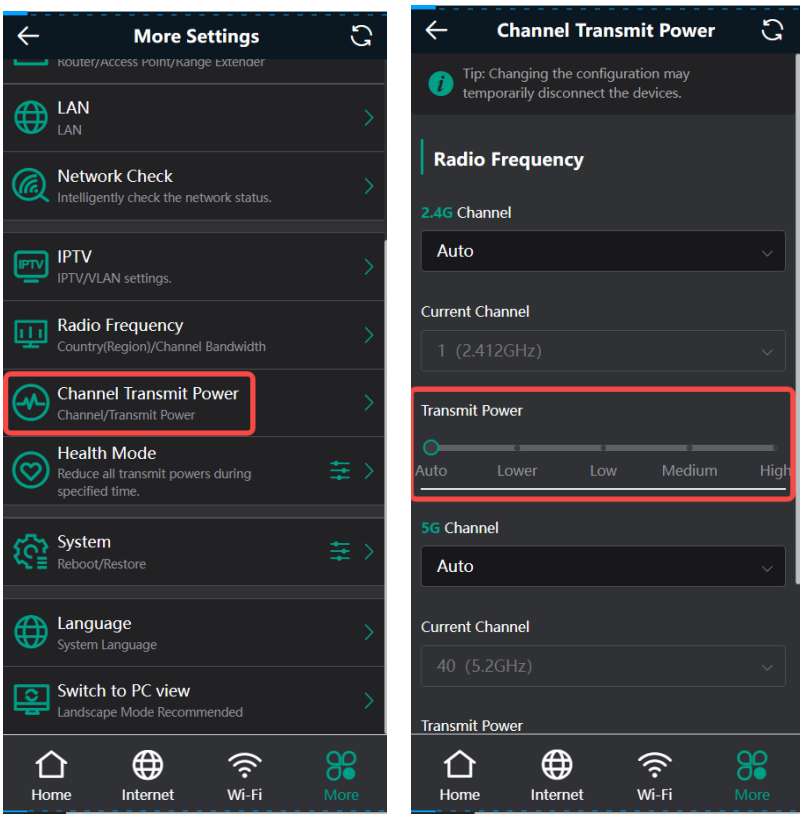
Smartphone View: Choose **More** > **Channel Transmit Power**.

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.



4.7 Configuring the Healthy Mode

Smartphone View: Choose **More** > **Healthy Mode**.

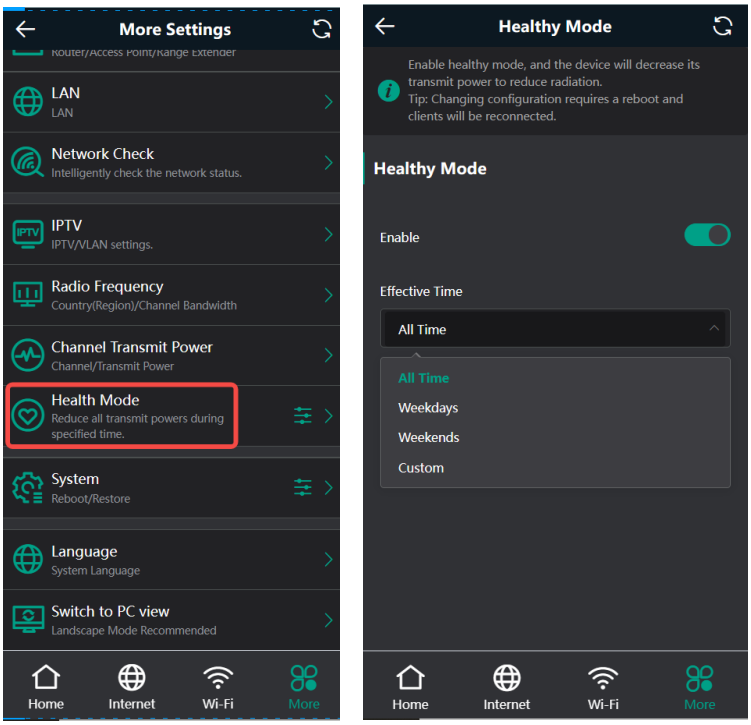
PC View: Choose **More** > **WLAN** > **Wi-Fi** > **Healthy Mode**.

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

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

Note

All Mesh Routers have undergone stringent radiation detection and evaluation, and comply with IEC/EN62311, EN 50385 and other standards. Wi-Fi networks will not affect human health and you can be rest assured to use them.

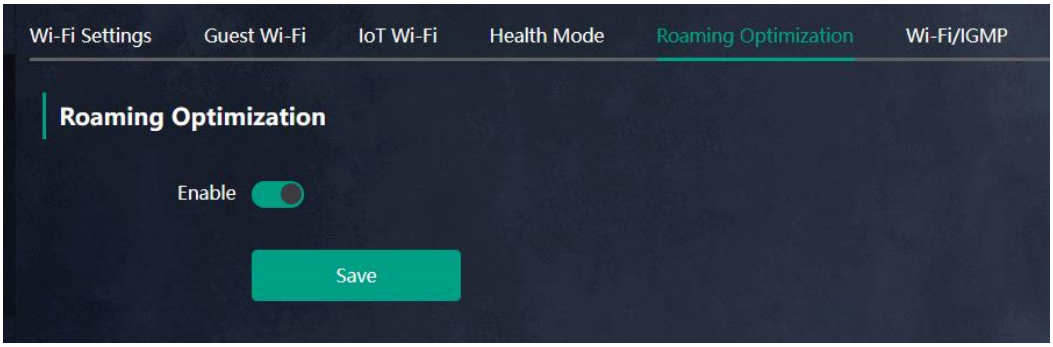


4.8 Enabling Roaming Optimization

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

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

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



4.9 Configuring Wi-Fi/IGMP

4.9.1 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.

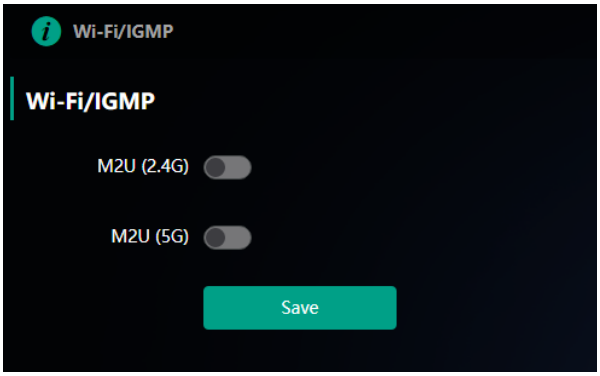
4.9.2 Configuration Steps

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

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

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

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



5 Configuring Work Mode

5.1 Access Point

Smartphone View: Choose **More** > **Work Mode**.

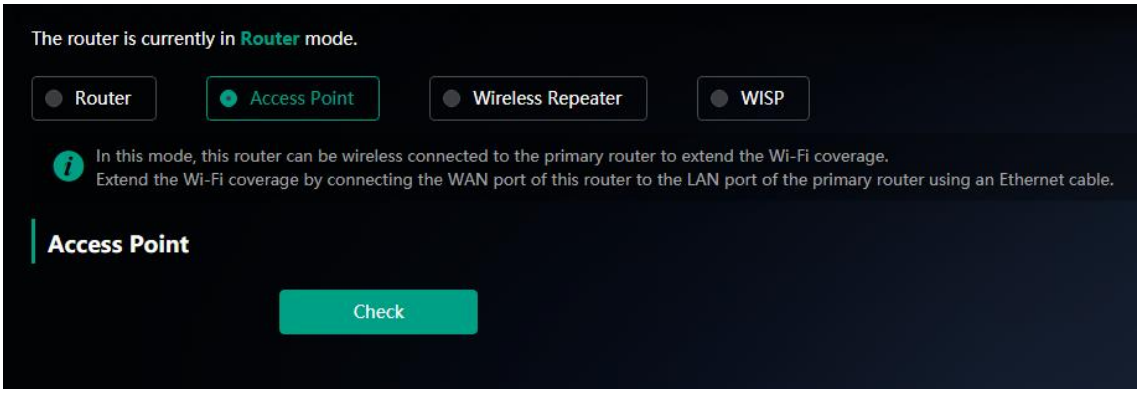
PC View: Choose **More** > **Work Mode**.

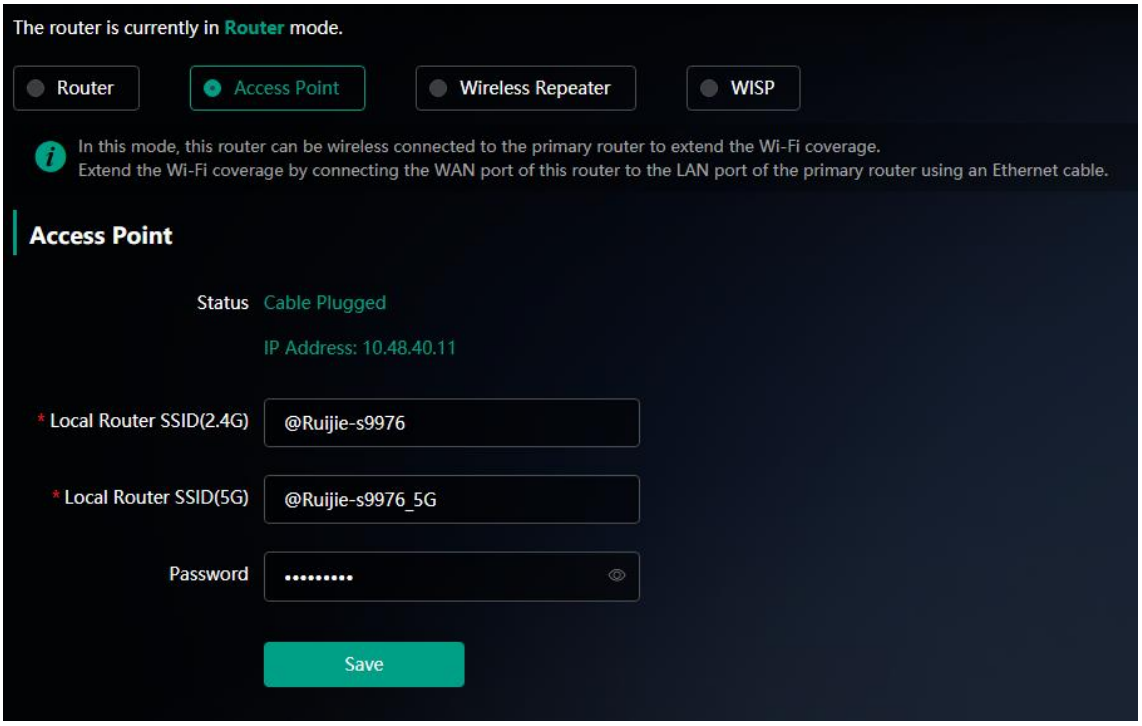
Connect the WAN port of this router to a LAN port of the primary router using an Ethernet cable.

Choose **Access Point** > **Check**, verify the Wi-Fi settings of this router, and click **Save**.

Caution

After the Wi-Fi settings are saved, clients connected to this router will be briefly disconnected. The Internet connection of these clients can be restored by reconnecting them to the Wi-Fi network of the primary router.





5.2 Wireless Repeater

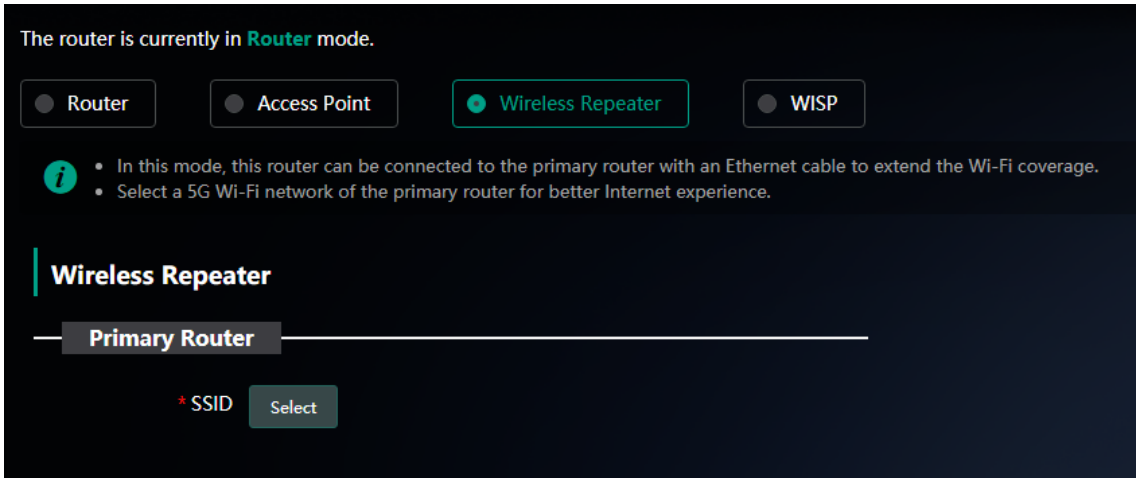
Smartphone View: Choose **More** > **Work Mode**.

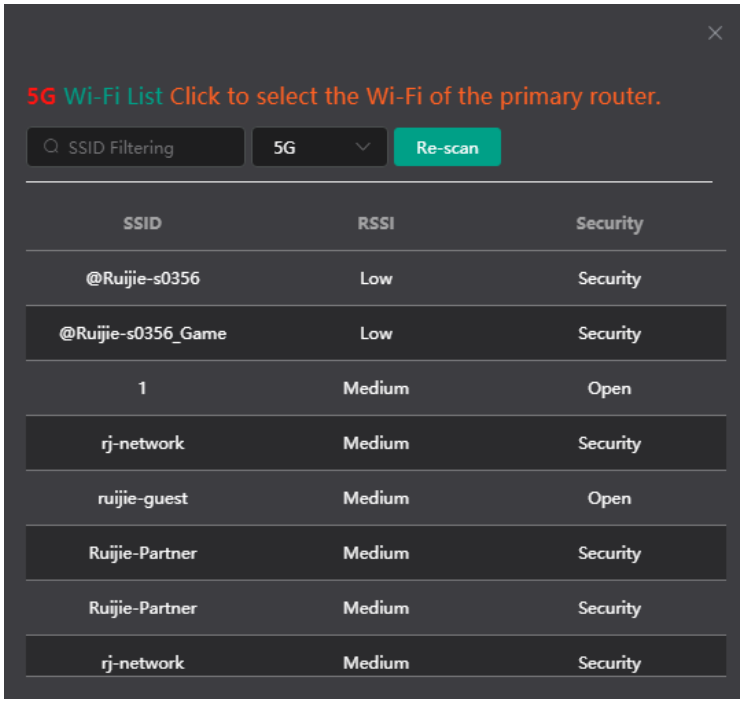
PC View: Choose **More** > **Work Mode**.

Note

- For wireless repeater, first unplug the Ethernet cable from the router.
- Before configuring wireless repeater, obtain the Wi-Fi network name and password of the primary router.

(1) Click **Wireless Repeater**. Verify that the Ethernet cable is unplugged, then click **Cable Unplugged**. Click **Select**, the Wi-Fi list is displayed. By default, a 5 GHz Wi-Fi list is displayed. To view a 2.4 GHz Wi-Fi list, click the **5 GHz** drop-down box and select **2.4 GHz**. You are advised to select a 5 GHz Wi-Fi network of the primary router for better internet experience.

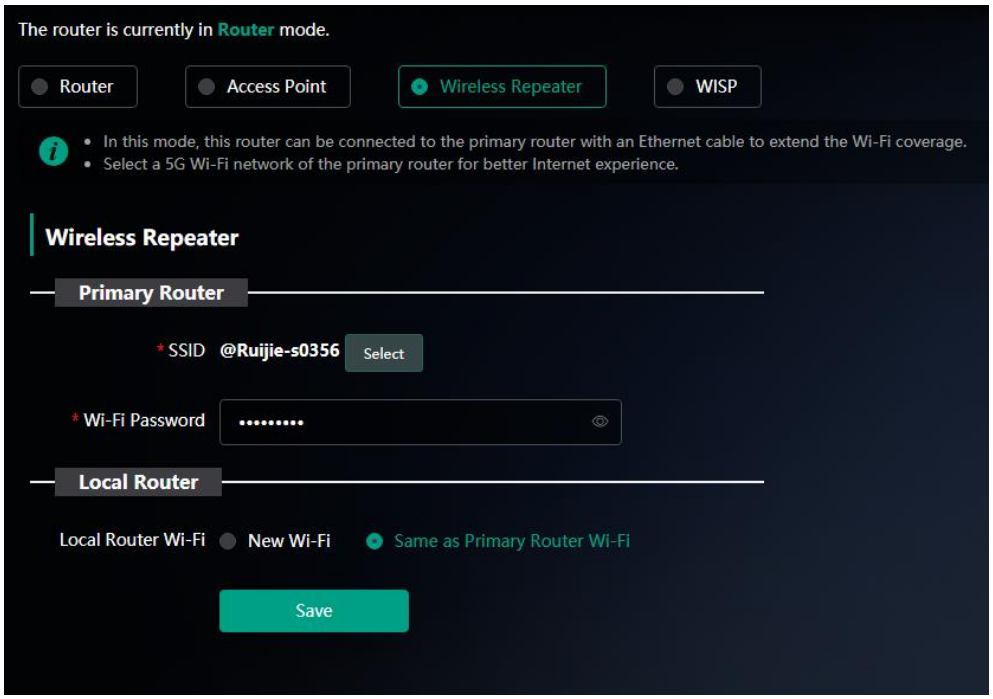




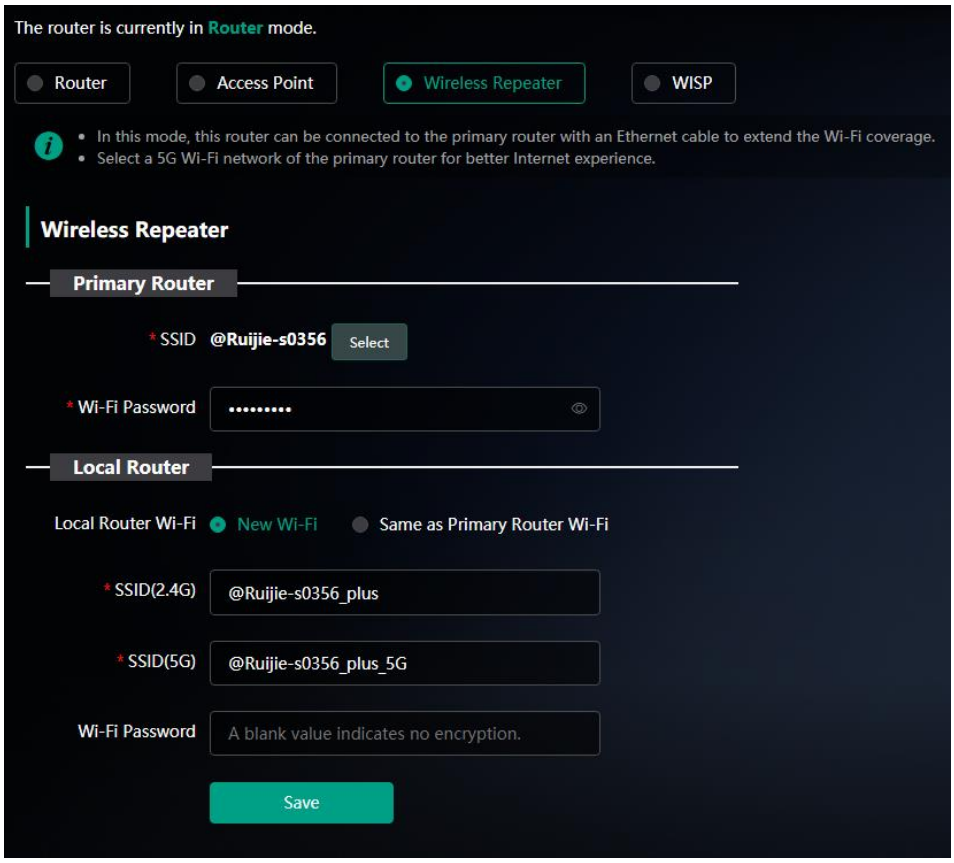
(2) Select the Wi-Fi network of the primary router to be relayed. The **Local Router** configuration item is displayed. If the primary router's Wi-Fi network is encrypted, enter the Wi-Fi password.

(3) Configure the Wi-Fi network of the local router. You can configure the local router's Wi-Fi network to be a new Wi-Fi network or same as the primary router's Wi-Fi network.

- 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 you click **Save**, the Wi-Fi network of the local router will be disconnected, and clients need to be connected to the new Wi-Fi network. You are advised to remember the configured SSID and password. Please exercise caution.
- You are advised to place the router in a location where at least two bars of the signal strength LED are on, in order to prevent severe signal loss during relaying. Otherwise, relay failure or poor signal quality may occur after Wi-Fi extension.

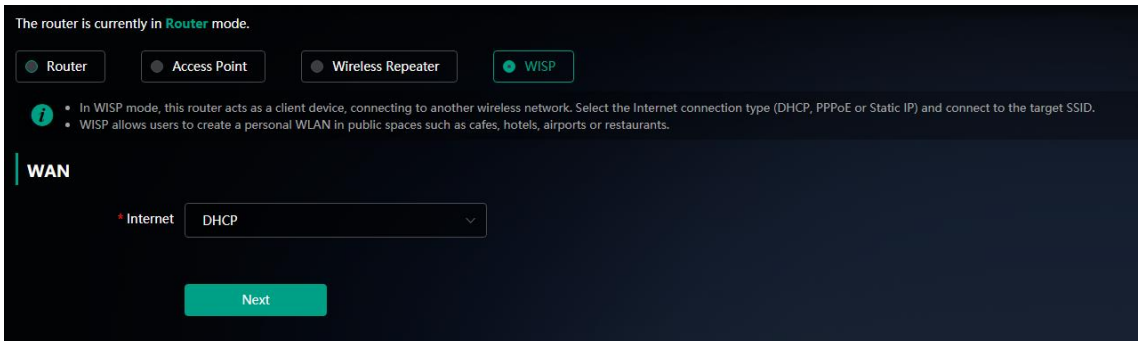
5.3 WISP

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

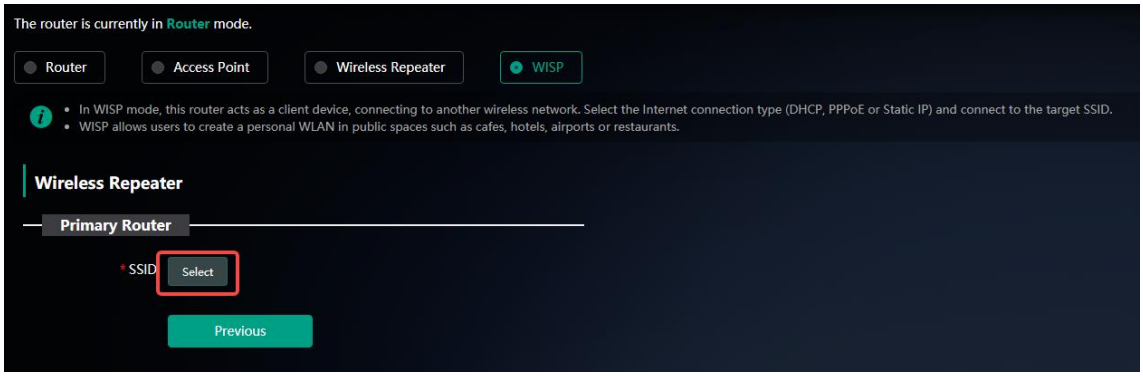
PC View: More >Work Mode

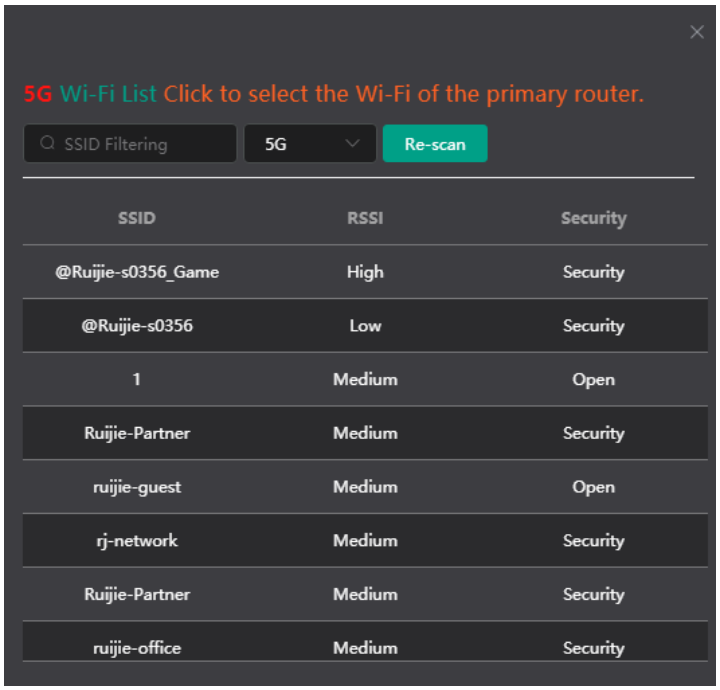
WISP allows users to establish their own WLAN for Internet access in public spaces, including coffee, hotel, airport or restaurant.

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



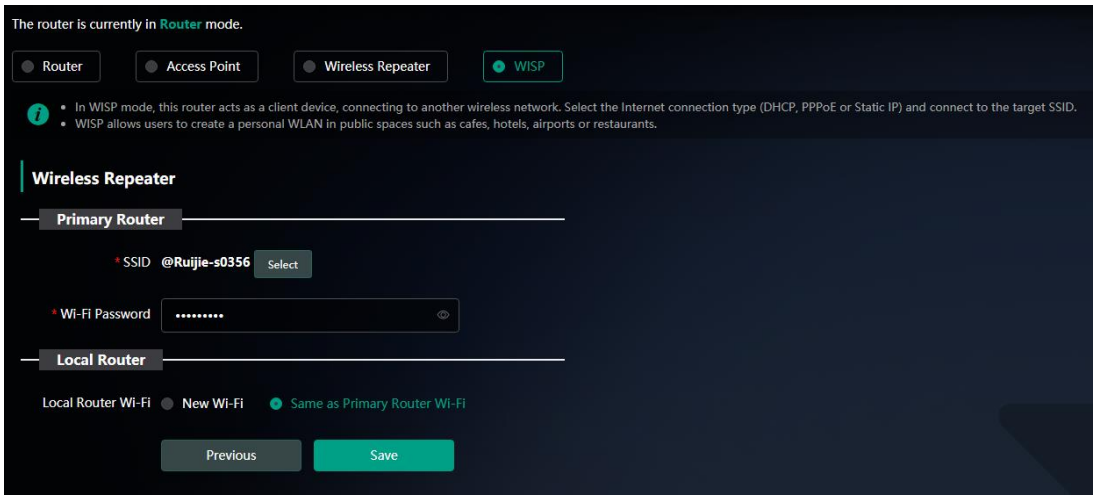
(2) Select the Wi-Fi signal of the primary router and enter its Wi-Fi password.



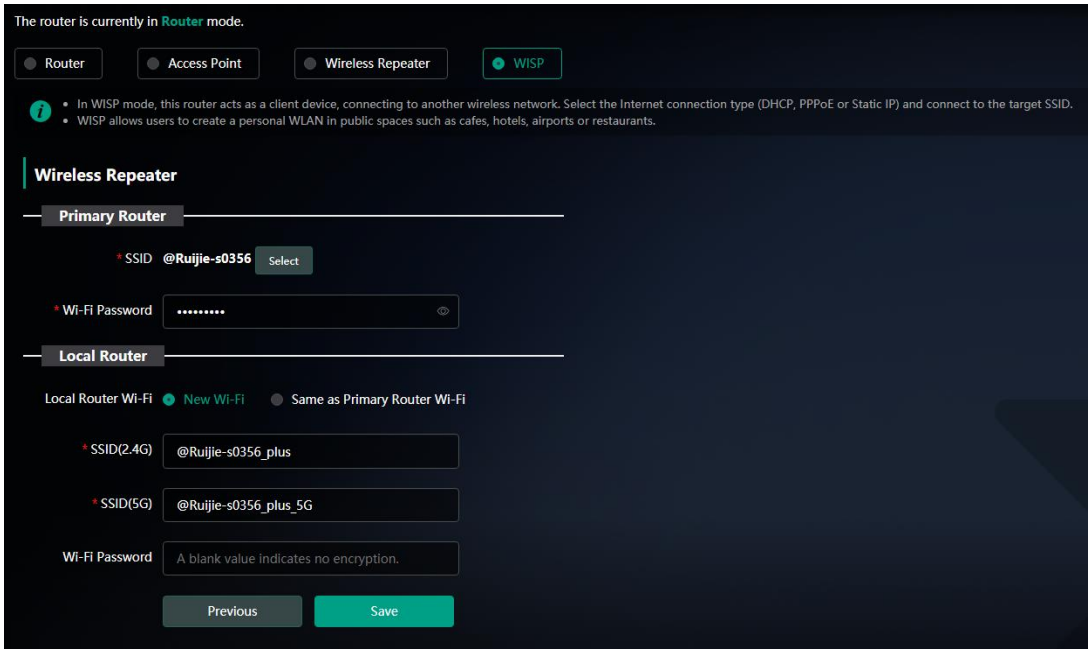


(3) You can configure a new Wi-Fi network or have a Wi-Fi network the same as that of the primary router:

- 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.



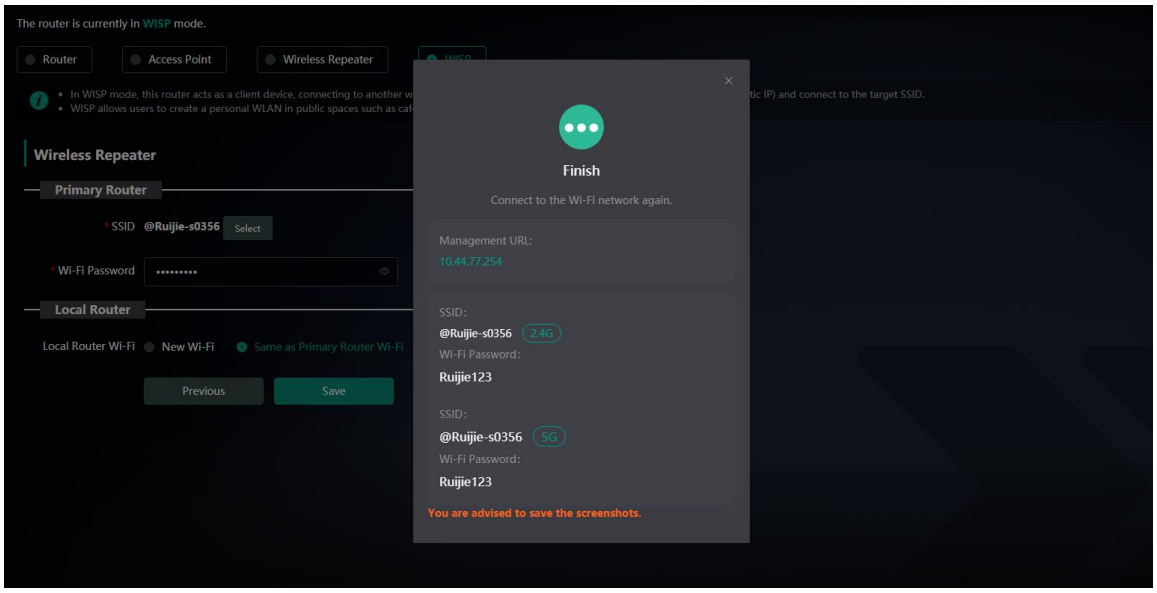
- If you select **New Wi-Fi**, you can set a local SSID and password. Clients will search out a Wi-Fi signal different from the primary router Wi-Fi signal.



(4) Click **Save**.

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.


The router is currently in WISP mode.
Router
Access Point
Wireless Repeater
Wireless Repeater
Primary Router
SSID @Ruijie-s0356
Select
Wi-Fi Password
Local Router
Local Router Wi-Fi
New Wi-Fi
Same as Primary Router Wi-Fi
Previous
Save
Finish
Connect to the Wi-Fi network again.
Management URL:
10.44.77.254
SSID:
@Ruijie-s0356
2.4G
Wi-Fi Password:
Ruijie123
SSID:
@Ruijie-s0356
5G
Wi-Fi Password:
Ruijie123
You are advised to save the screenshots.

6 Configuring Network Settings

6.1 Configuring WAN Settings

Caution

This feature is supported in router mode.

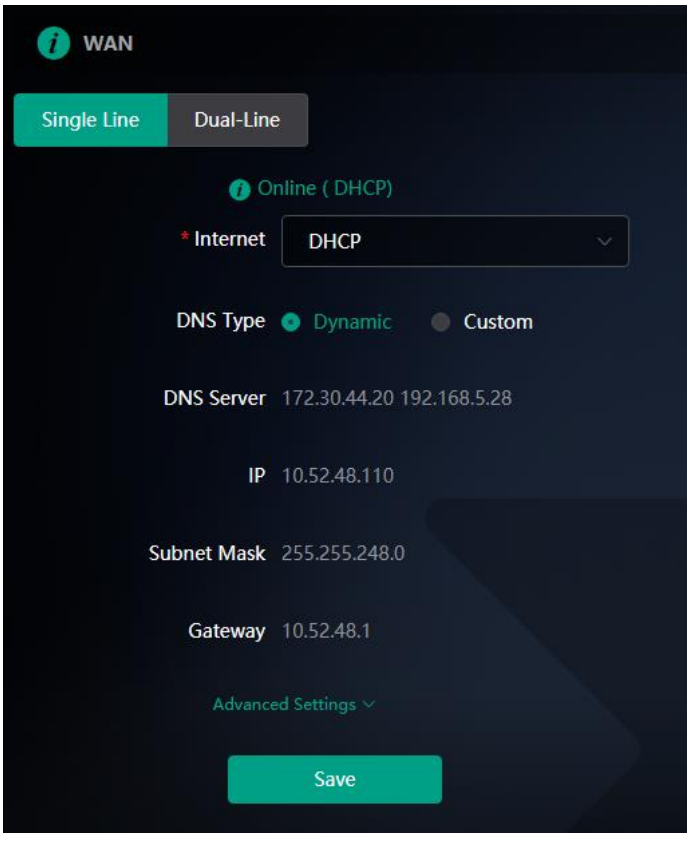
Smartphone View: Choose More > Switch to PC view > More > Basics > WAN > WAN Settings.

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

6.1.1 Configuring Internet connection types

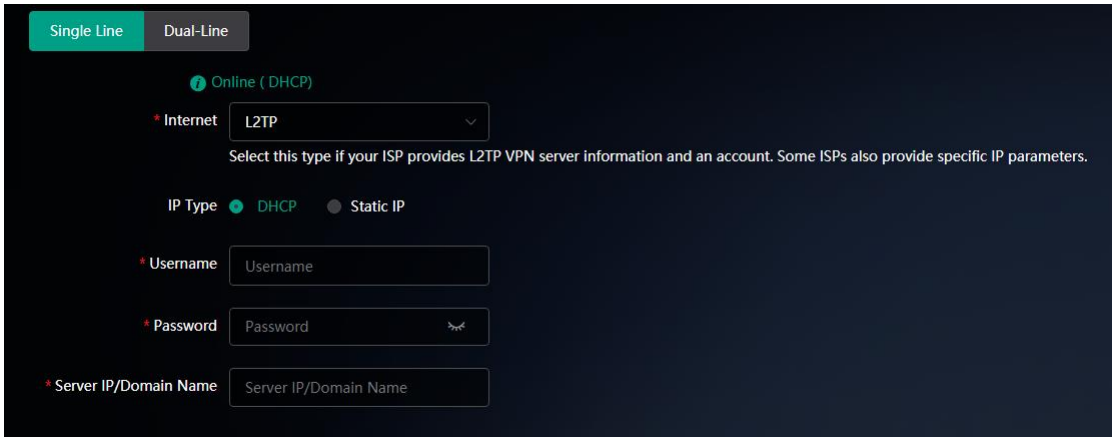
This router supports single and dual WAN links, allowing dual links to operate simultaneously. In dual-link mode, in addition to setting the basic network parameters for each WAN port, you can also set the ISP and load balancing mode for the links.

The router supports four Internet connection types: PPPoE, DHCP, static IP, and L2TP. For details, see 2.2.1 3. Configuring the Internet Connection Type.

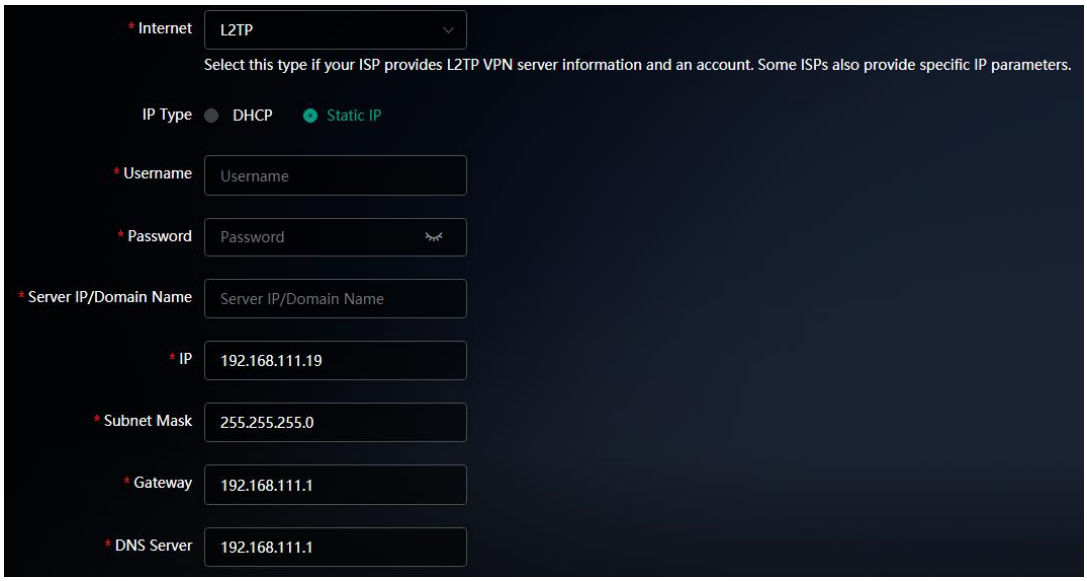


- **DHCP**: The router automatically obtains an IP address for Internet access.
- **PPPoE**: Enter the username and password provided by the ISP.
- **Static IP**: Enter the IP address, subnet mask, gateway, and DNS server.
- **L2TP:** Select the IP address allocation type based on the L2TP VPN server information provided by the ISP:

- DHCP: Enter the username, password, and server IP or domain name provided by the L2TP service provider, and click **Next**.



- Static IP: In addition to the username, password, and server IP or domain name provided by the L2TP service provider, enter the static IP address assigned by the uplink device (like a modem), subnet mask, gateway IP address, and DNS server address for internet access, and click **Next**.



6.1.2 Changing the MAC Address

Caution

- Changing the MAC address of the WAN port is only supported when the router is in router mode.
- This feature is only supported when the **Internet Connection Type** is set to **DHCP**, **PPPoE** or **Static IP**.

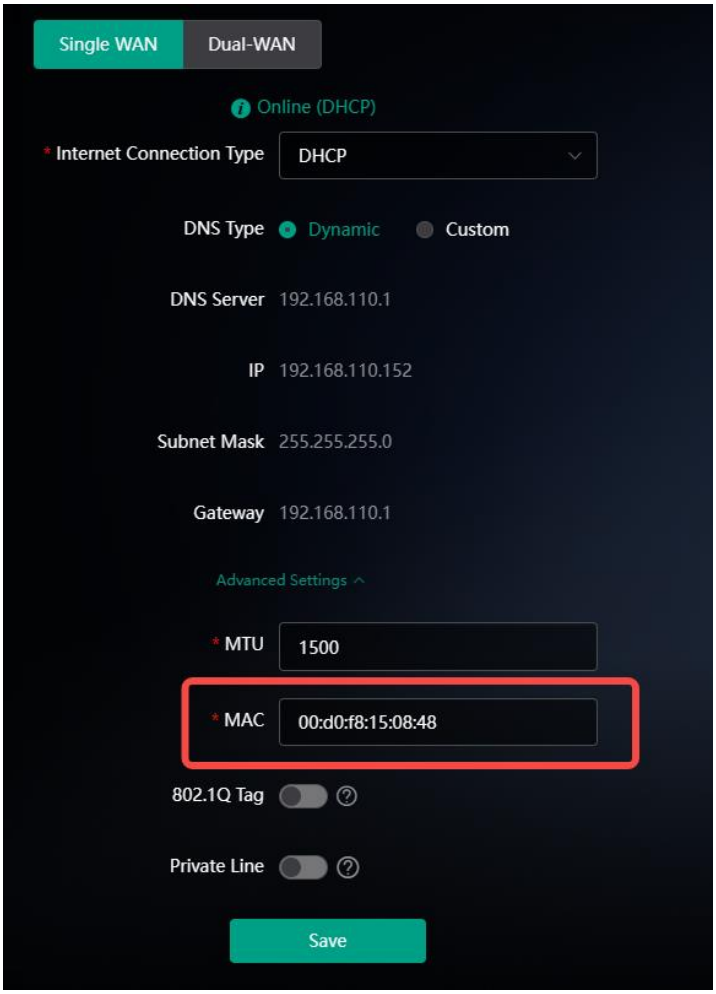
The ISP may restrict the access of devices with unknown MAC addresses to the Internet for the sake of security. In this case, you can change the MAC address of the WAN port to another address. You are advised to use the MAC address of an old router that is allowed to access the Internet (the MAC address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

Click **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.



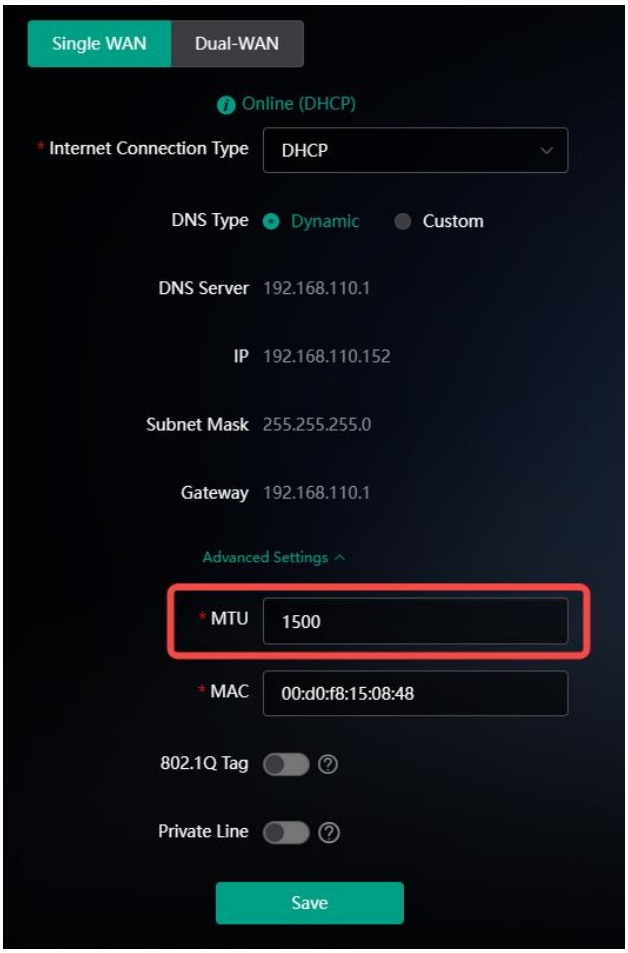
6.1.3 Modifying MTU

Caution

- This feature is supported in router mode.
- This function is only supported when the Internet Connection Type is set to DHCP, PPPoE, or Static IP.

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.

Click **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.



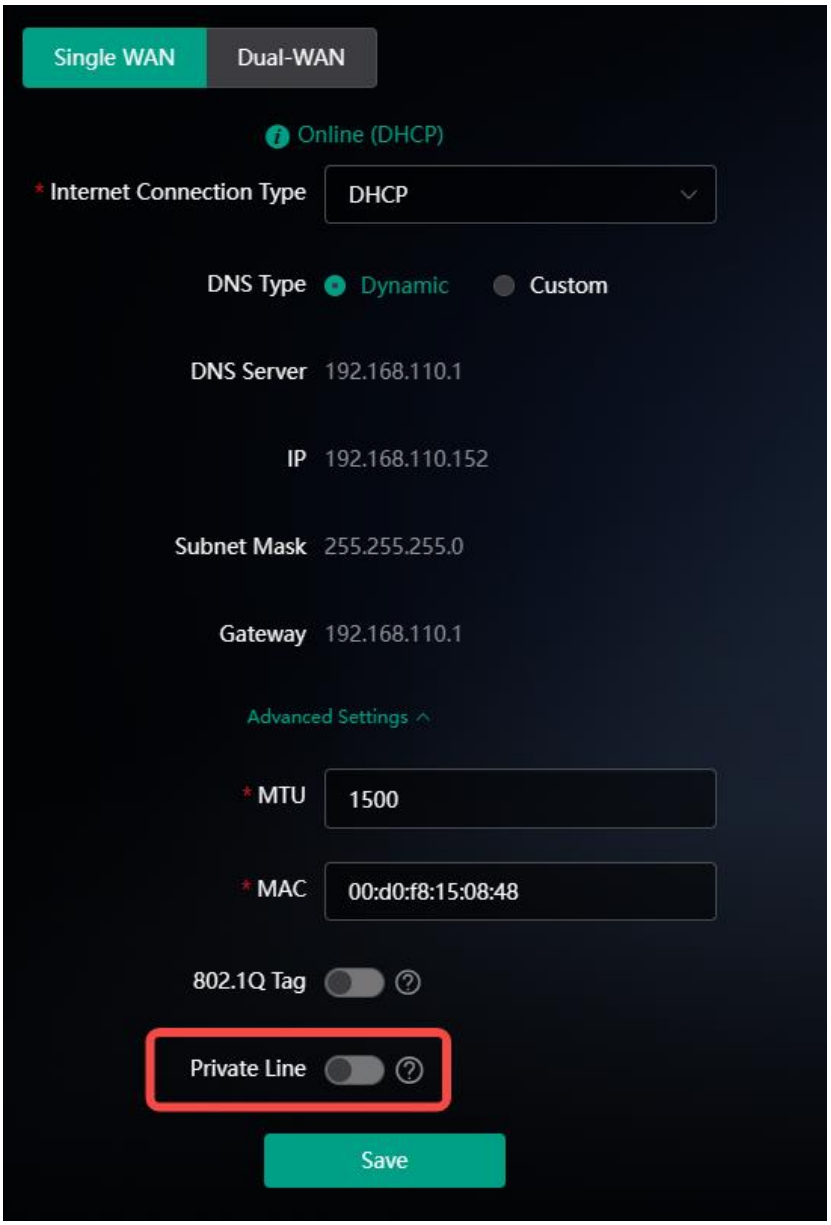
6.1.4 Configuring a Private Line

Caution

This function is only supported when the Internet Connection Type is set to DHCP, PPPoE, or Static IP.

Private lines can access specific intranets, but cannot access the Internet. Private lines have a higher level of network security.

Choose **Advanced** > **Private Line** to set the current WAN link as a private line.



6.1.5 Configuring the VLAN Tag

Caution

This function is only supported when the Internet Connection Type is set to DHCP, PPPoE, or Static IP.

Some ISPs require that packets transmitted to their networks carry VLAN IDs. In this case, you can click **Advanced Settings**, enable the **802.1Q Tag** function and set a **VLAN ID** and **Priority** for the WAN port. By default, the VLAN tag function is disabled. You are advised to keep the VLAN tag function disabled unless otherwise specified.



6.1.6 Configuring Load Balancing Settings

In the case of multiple lines, after **ISP Routing** is enabled, the remaining traffic will be distributed according to the load mode.

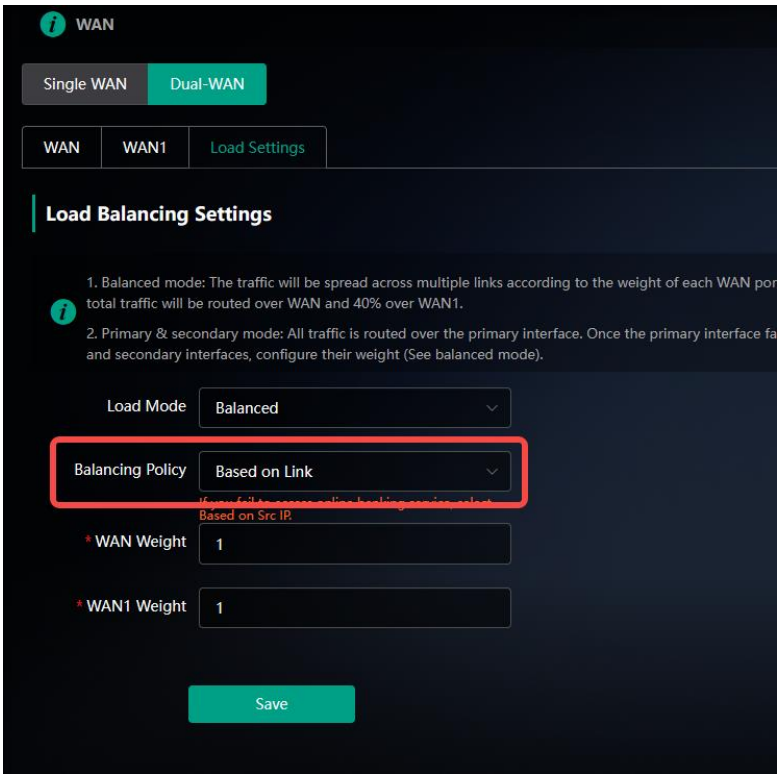


Table6-1 Description of Load-balancing Mode

Load Mode	Description
Balanced	Traffic is allocated in proportion to the weight of each WAN port. The higher the weight is, the more traffic is allocated. The weight of each WAN port must be specified in this mode. For example, if the weights of WAN and WAN1 ports in the dual-line mode are set to 3 and 2 respectively, then traffic will be allocated at 3:2, with 60% traffic routed to WAN port, and 40% traffic routed to WAN1 port.
Primary & secondary	When the primary interface is normal, all the traffic will be routed to the primary interface. If the primary interface fails, traffic is automatically routed to the secondary interface. In this mode, each WAN port must be specified as a primary or secondary interface. If there are multiple primary or secondary interfaces, a weight must be set for each interface (same as the balanced mode).

6.2 Changing the Address of a LAN Port

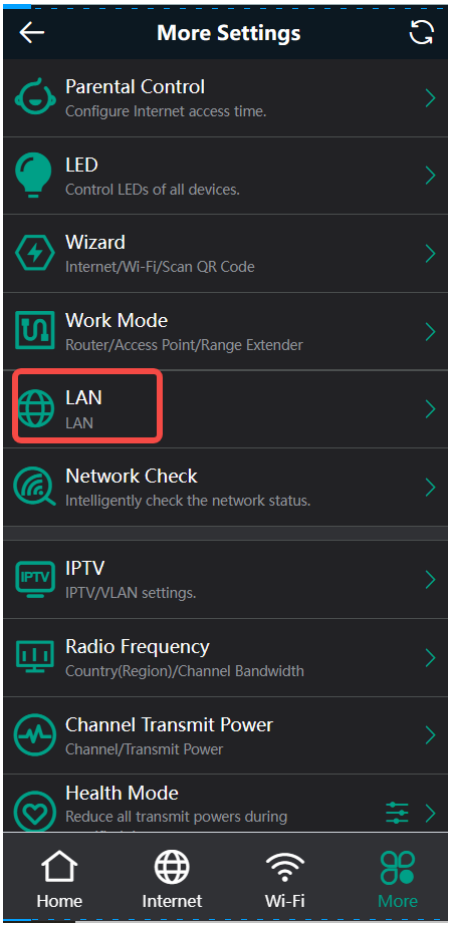
Smartphone View: Choose **More** > **LAN**.

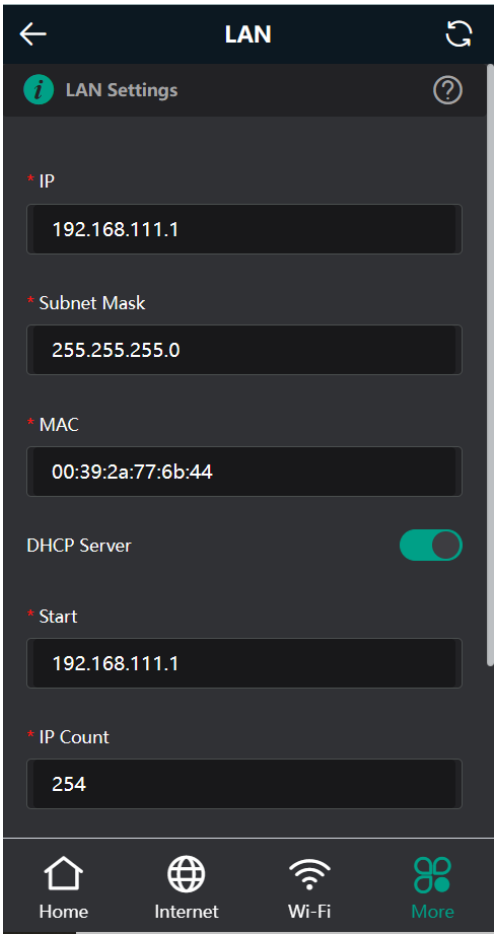
PC View: Choose **More** > **Basics** > **LAN**.

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





6.3 Connecting to IPTV

Caution

- This feature is supported in router mode.
- IPTV traffic is forwarded by hardware and is not counted in the traffic statistics collection on the WAN port.

IPTV is an Internet television service provided by ISP.

6.3.1 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.

6.3.2 IPTV Configuration Steps (VLAN Type)

Smartphone View: Choose **More** > **IPTV** > **IPTV/VLAN**.

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

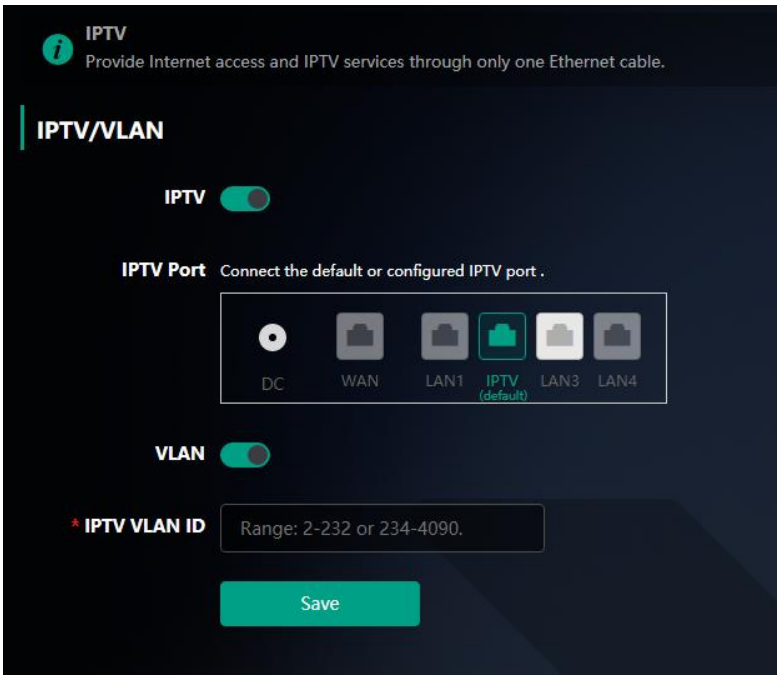
Click to enable IPTV, and select the LAN port to be connected to the IPTV STB.

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 LAN2.

Caution

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

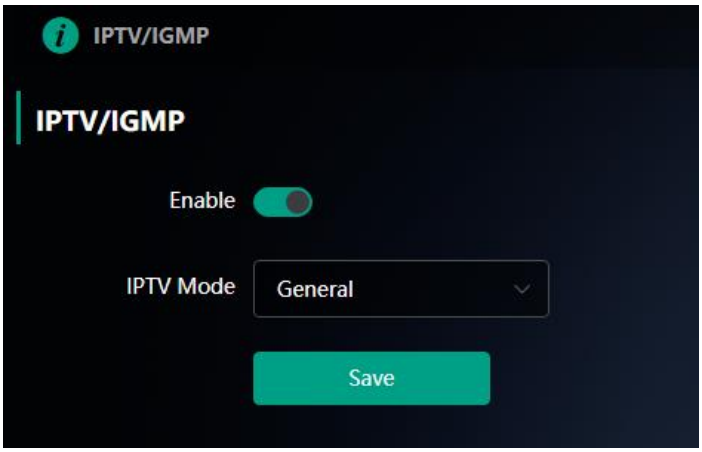


6.3.3 IPTV Configuration Steps (IGMP Type)

Smartphone 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.



6.4 Configuring IPv6

Caution

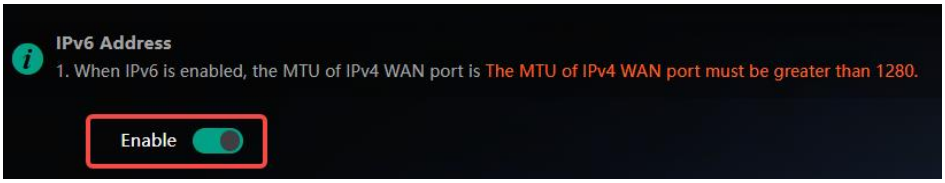
- This feature is supported in router mode.
- When IPv6 is enabled, The MTU of IPV4 WAN port need higher than 1280.

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

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

PC View: More > Basics > IPv6

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



6.4.1 Configuring the IPv6 of the WAN Port

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

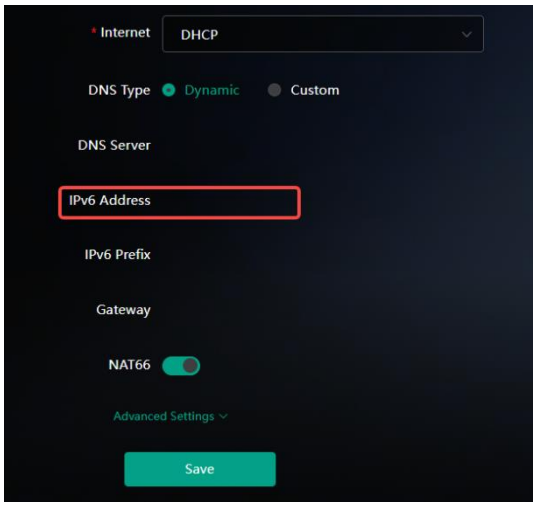
PC View: More > Basics > IPv6 > WAN Settings.

(1) Set Internet connection type:

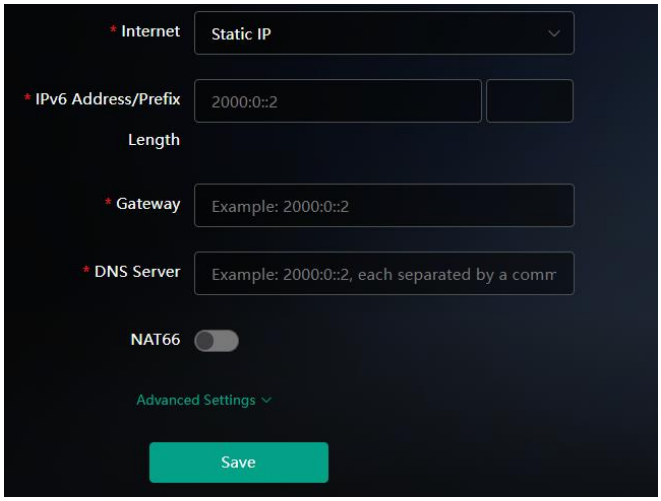
- If you select **DHCP**, and the device will get an IPv6 from the upstream device.

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.

6.4.2 Click Save.Configuring the IPv6 of the LAN Port

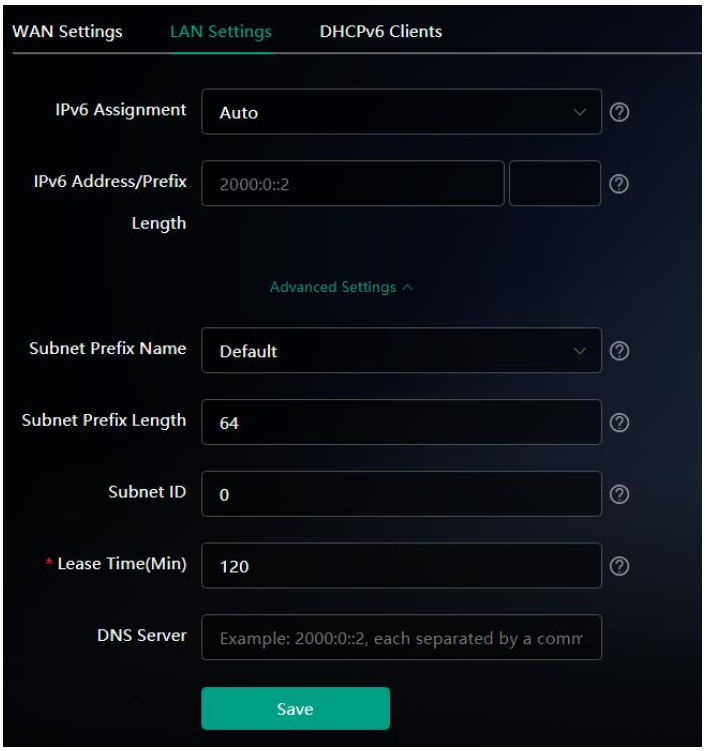
Smartphone View: Choose More > Switch to PC > More > Basics > IPv6 > LAN Settings.

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.

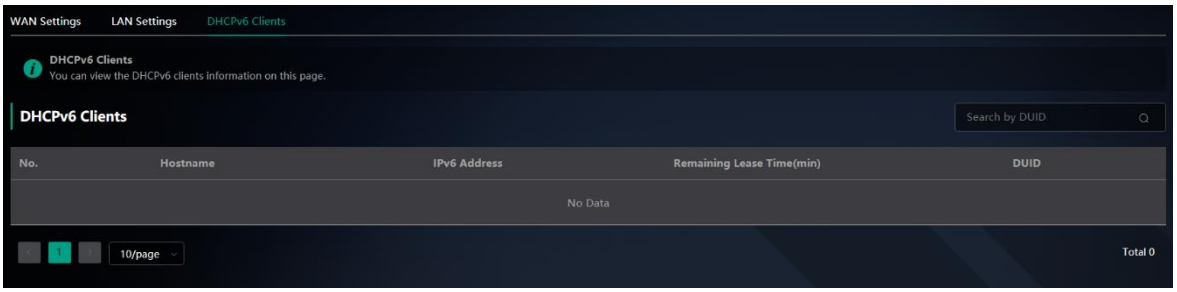
IPv6/Prefix Length: If the router fails to obtain an IPv6 prefix, you can configure one manually. Set the subnet prefix length to a value smaller than or equal to 64.

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



6.4.3 Viewing DHCPv6 Clients

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



6.5 Configuring Auto Bandwidth Control

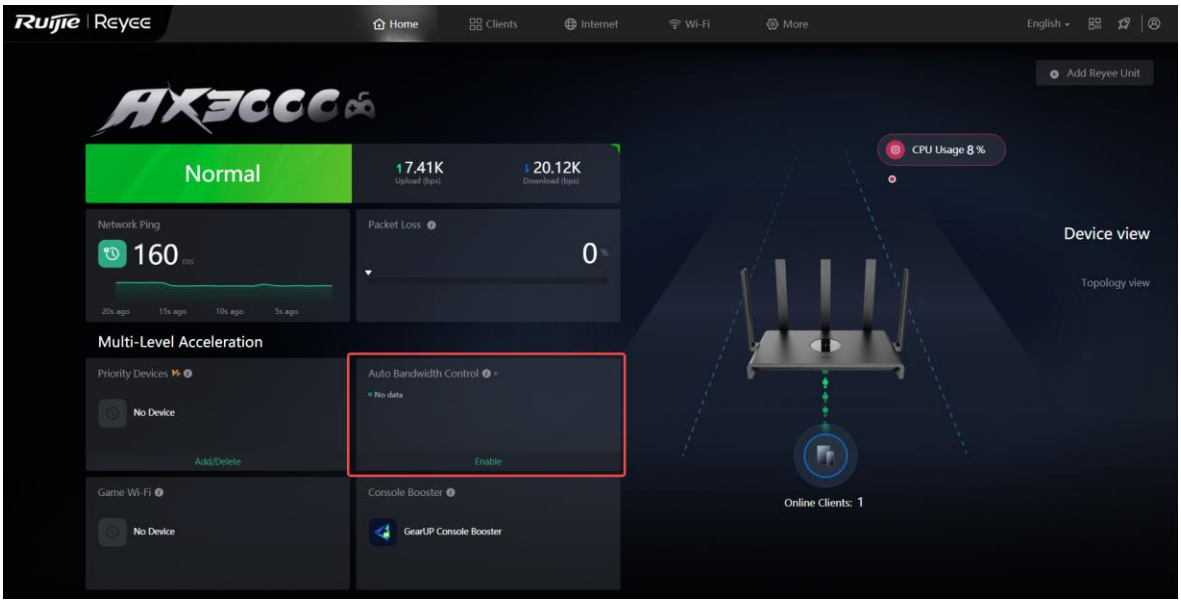
Caution

This feature is supported in router mode.

Smartphone View: Choose **More** > **Switch to PC** > **Home** > **Auto Bandwidth Control**

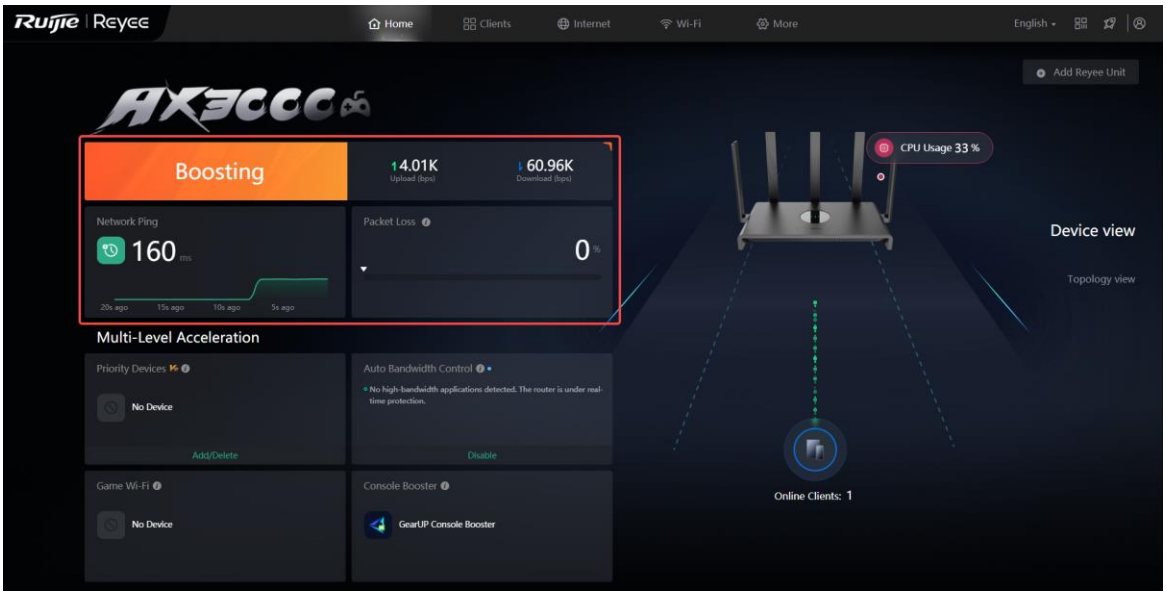
PC View: **Home page** > **Auto Bandwidth Control**

Click **Enable**. Ensure an uninterrupted gaming experience by prioritizing your game and suppressing high-traffic applications that may cause disruptions.



6.5.1 Viewing Network Latency

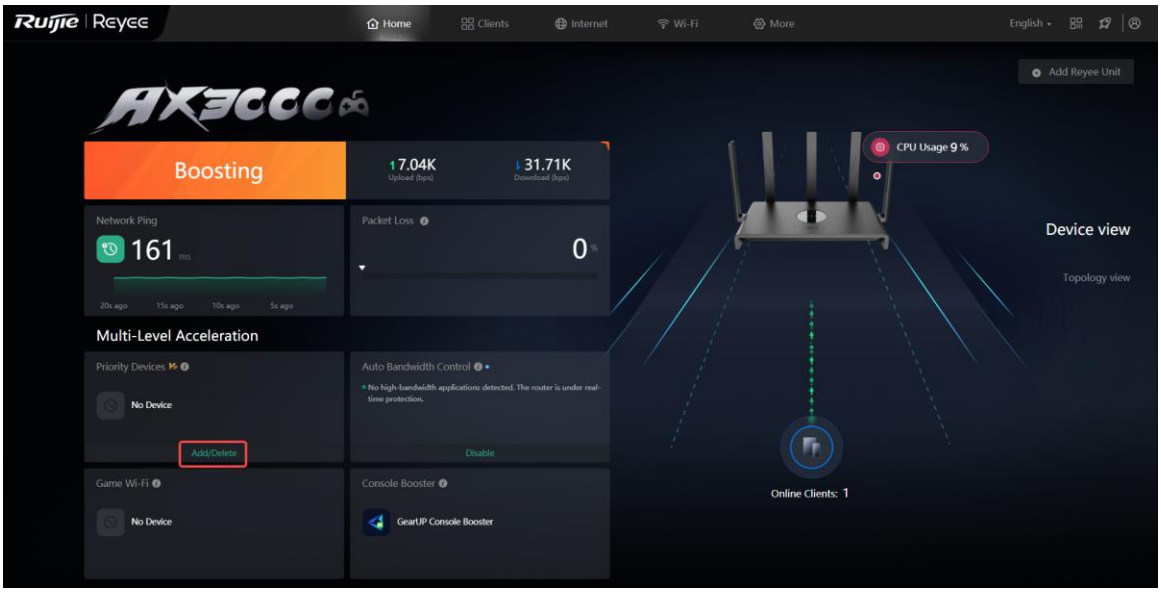
After **Auto Bandwidth Control** is enabled, you can view details such as network latency and packet loss rate of the router.



6.5.2 Configuring Designated Devices

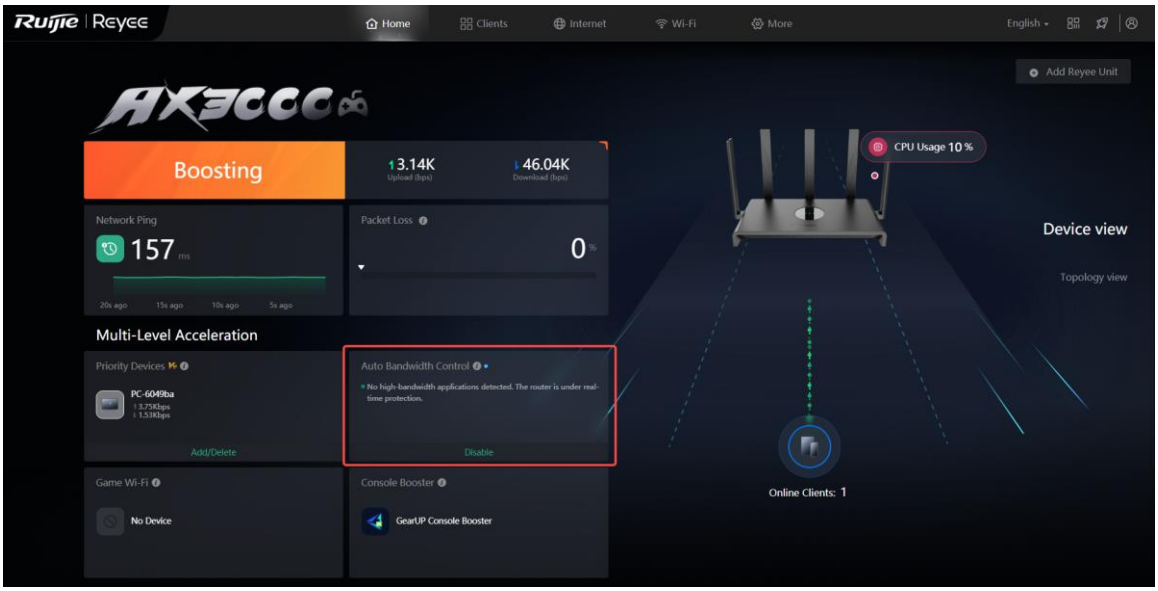
Clients in the designated device list will be prioritized and protected from the interference of other heavy traffic (such as downloading large videos). A maximum of 4 designated devices can be added.

Click **Add Device+** in the **Designated Devices** pane, select the target devices, and click **Save**.



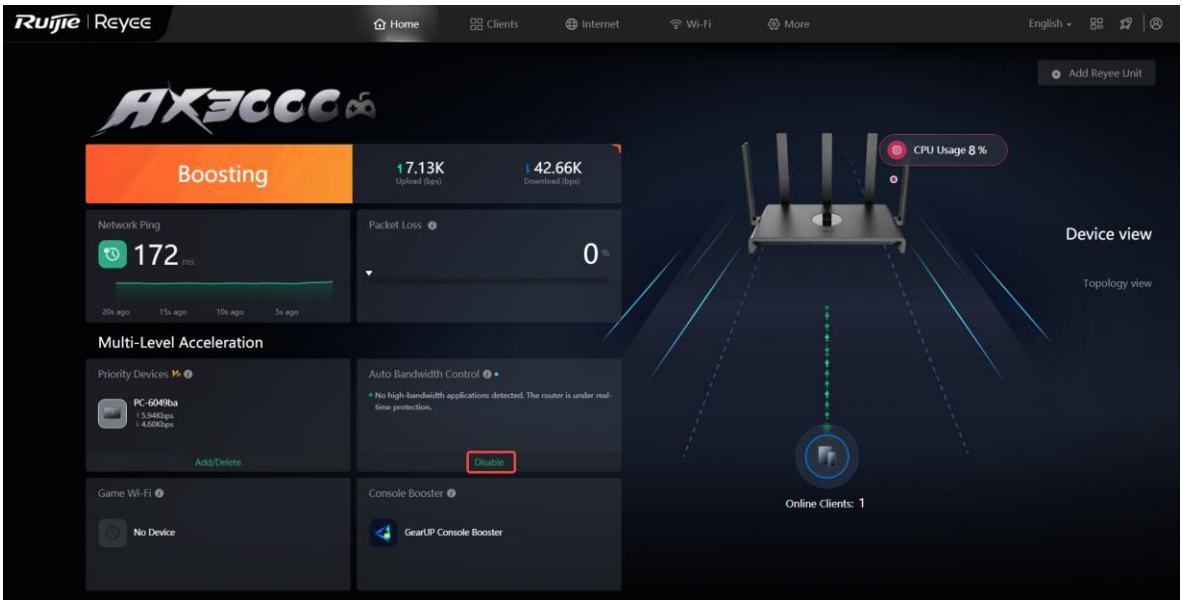
6.5.3 Viewing Auto Bandwidth Control Device Details

After **Auto Bandwidth Control** is enabled, you can view the boosted devices in the Auto Bandwidth Control list. You can click **View Log** to view the devices that are being boosted and device details.



6.5.4 Disabling Auto Bandwidth Control

Click **Disable** to disable the **Auto Bandwidth Control** feature.



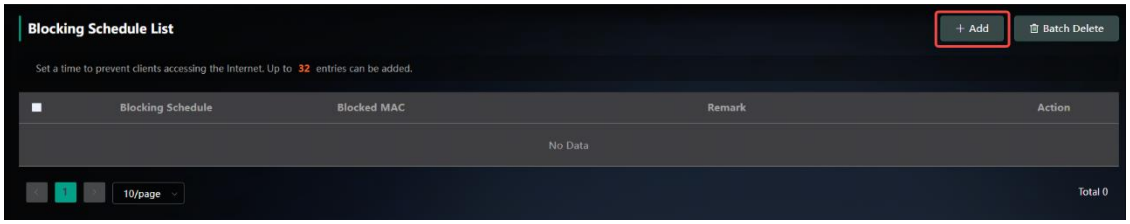
6.6 Setting Blocking Schedules

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

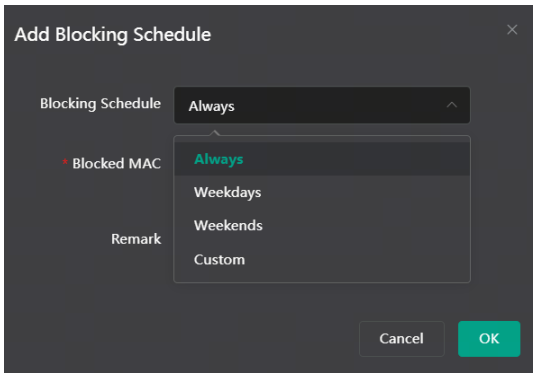
PC View: Choose More > Advanced > Blocking Schedule.

6.6.1 Setting a Blocking Schedule

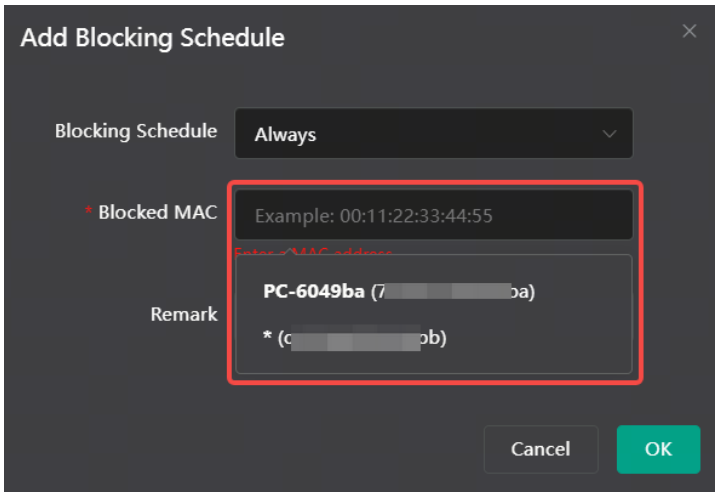
(1) Click **Add**.



(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.



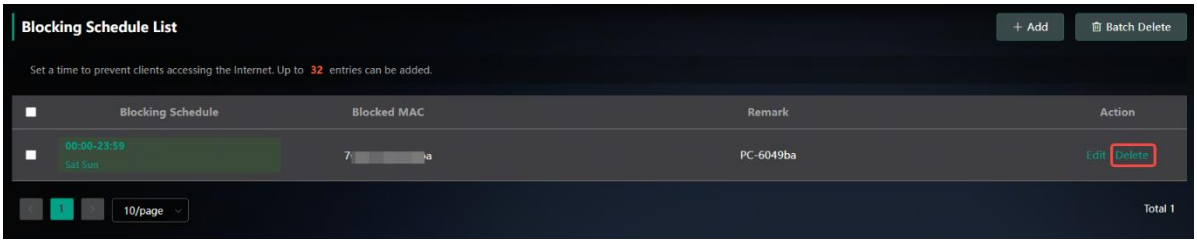
(3) Select a client or enter a MAC address for the blocking schedule.



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

6.6.2 Removing a Blocking Schedule

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



6.7 Configuring DHCP Server

Caution

This feature is supported in router mode.

6.7.1 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.

6.7.2 Configuration Steps

1. Configuring the DHCP Server Function

Smartphone View: Choose More > Switch to PC view > More > Basics > LAN > LAN Settings.

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

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

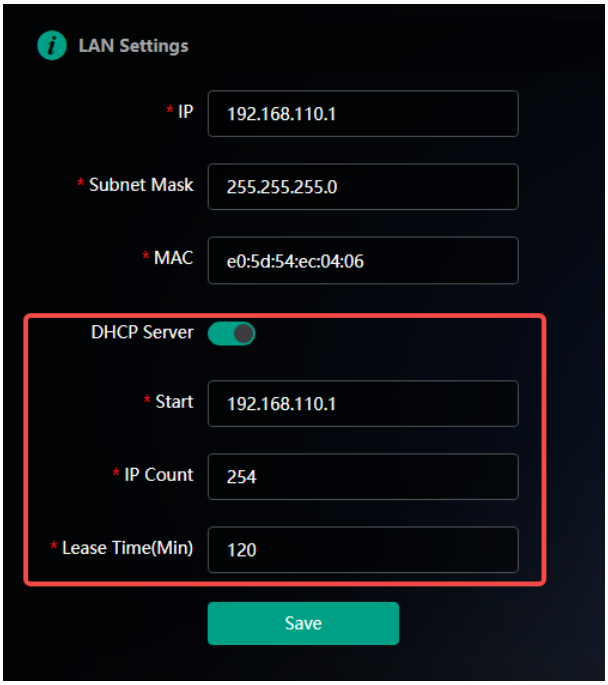
Caution

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

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

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

Lease Time (Min): Enter the address lease time period. When a client keeps connected, the lease is automatically renewed. If a lease is not renewed due to the client disconnection or network instability, the IP address will be reclaimed after the lease period expires. After the client connection is restored, the client requests an IP address again. The default lease period is 120 minutes.

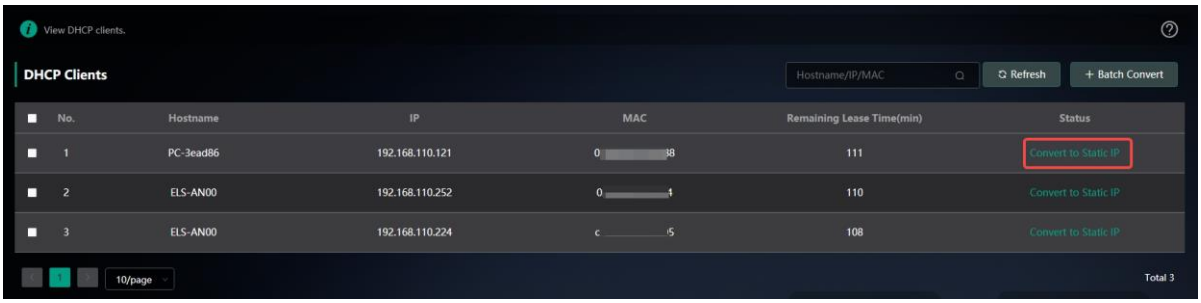


2. Displaying Online DHCP Clients

Smartphone View: Choose More > Switch to PC view > More > LAN > DHCP Clients.

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

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

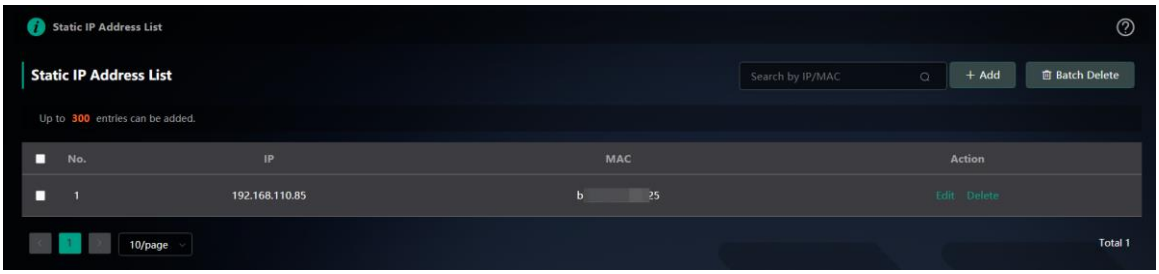


3. Displaying the DHCP Static IP Address Table

Smartphone View: Choose More > Switch to PC view > More > LAN > Static IP Addresses.

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

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



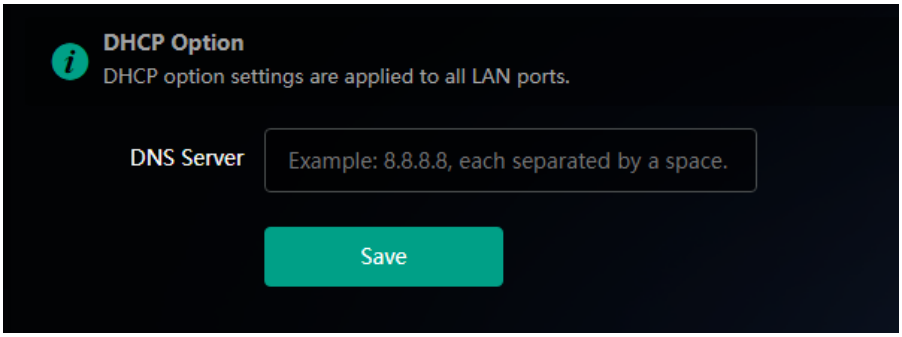
4. Configuring DHCP Option

Smartphone 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.



6.8 Configuring DNS Server

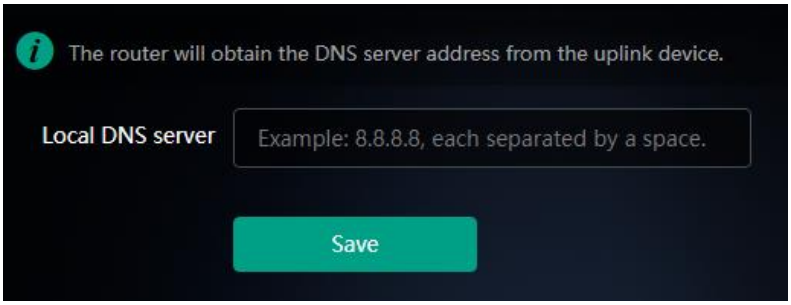
6.8.1 Local DNS Server

When the WAN port uses DHCP protocol or PPPoE protocol, the router will obtain the DNS server address automatically. If the DNS server address is not delivered by the primary router, or if you need to change the DNS server, you can set a new DNS server.

Smartphone View: Choose More > Switch to PC view > More > Advanced > Local DNS server.

PC View: Choose More > Advanced > Local DNS server

In the Local DNS server field, you can set the local DNS server address. Separate multiple address with a space, if any.



6.8.2 Configuring DNS Proxy

Caution

This feature is supported in router mode.

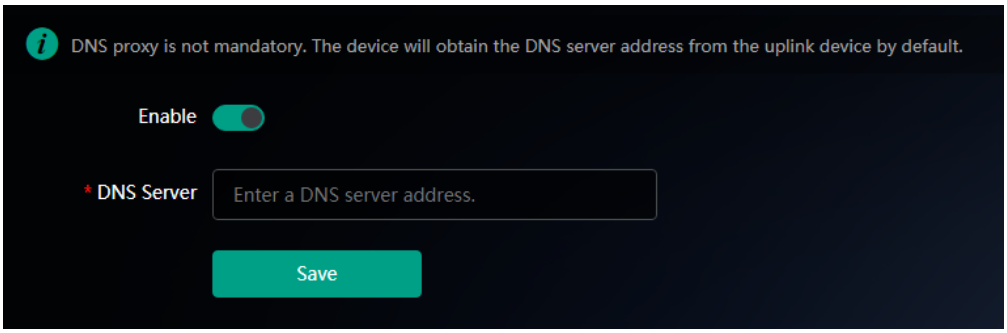
The domain name system (DNS) proxy configuration is not mandatory. The device obtains the DNS server address from the uplink device by default.

Smartphone 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.



6.9 Configuring Port Mapping

Caution

This feature is supported in router mode.

6.9.1 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.

6.9.2 Getting Started

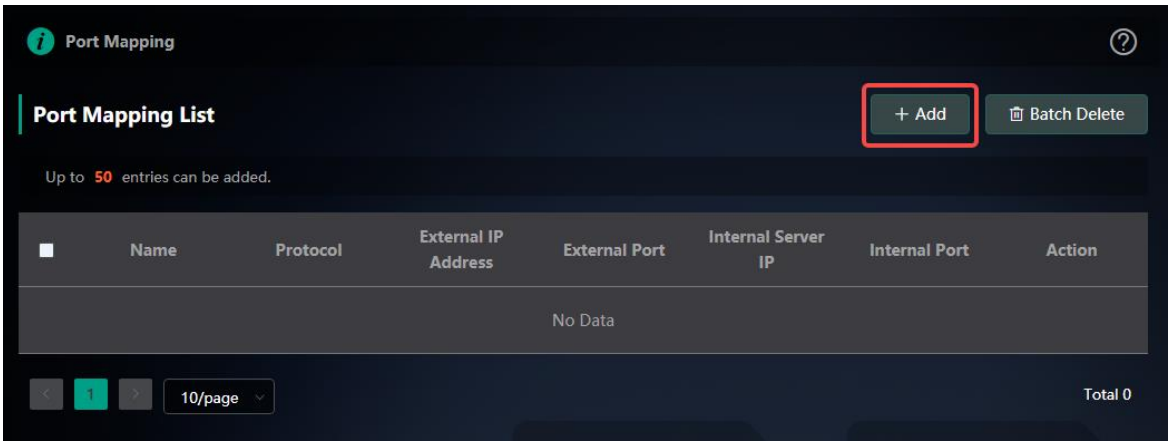
- Confirm the IP address of the target device in the internal network and service port ID.
- Ensure that port mapping is available in the internal network.
- Verify that your router has a public IP address. If the IP address is dynamic, changing it may cause port mapping failure. In this case, you are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

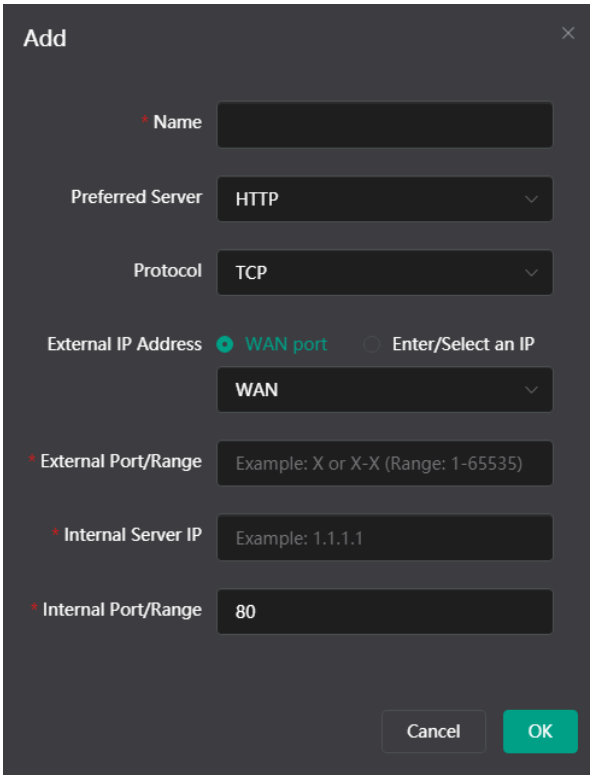
6.9.3 Configuration Steps

Smartphone View: Choose More > Switch to PC view > More > Advanced > Port Mapping.

PC View: Choose More > Advanced > Port Mapping.

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





Name: Enter a name for ease of maintenance.

Preferred Server: Select a service to be mapped, such as HTTP or FTP. The device will automatically fill in the internal port number of the service. If you are not sure of the service, you can select **Custom**.

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

External IP Address: IP address for externet access. If multiple egresses exist on the network, select a specific WAN port IP address as the IP address for externet access.

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.

6.9.4 Verification and Testing

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

6.9.5 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.

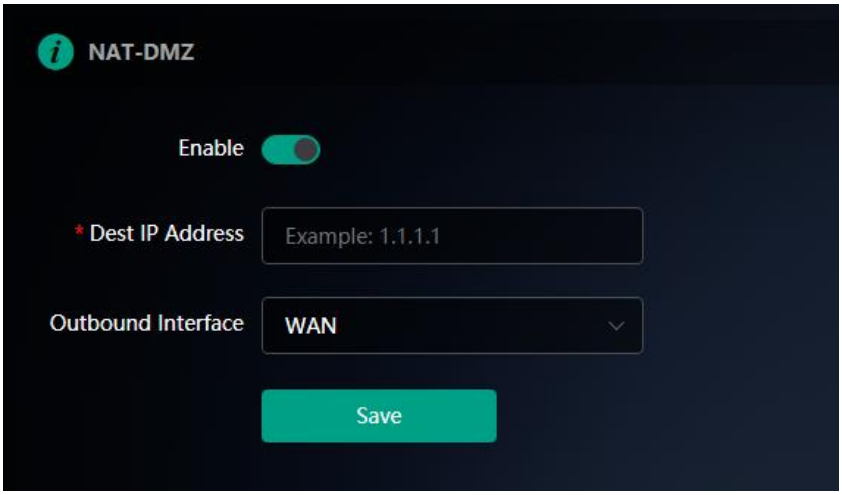
(3) Enable the DMZ service. For details, see 6.9.6 DMZ Configuration Steps. The common cause is that port configuration is incorrect or incomplete.

6.9.6 DMZ Configuration Steps

Smartphone 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 **Dest IP Address** of the internal server, select the **Outbound Interface**, and click **Save**.



6.10 Configuring DDNS

6.10.1 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.

6.10.2 Getting Started

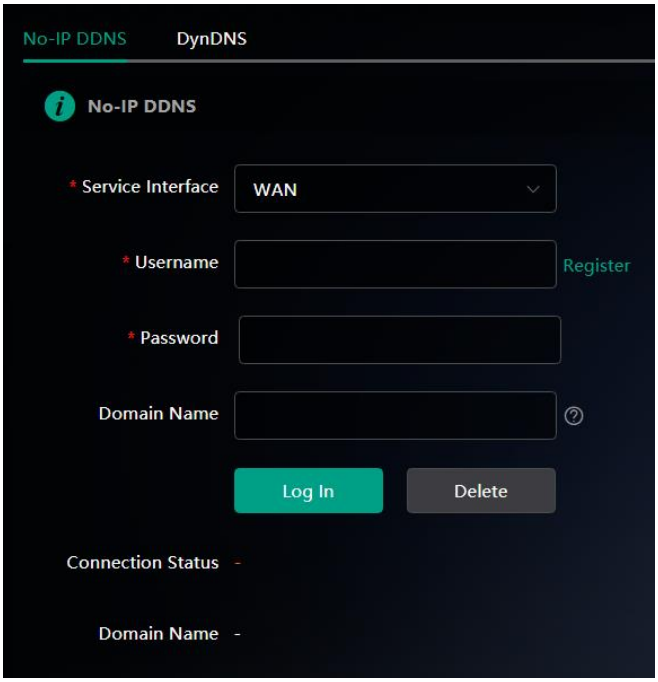
Register an account and domain name at Dyn or No-IP official website.

6.10.3 Configuration Steps

Smartphone 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.



6.11 Configuring Connectivity Detection

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

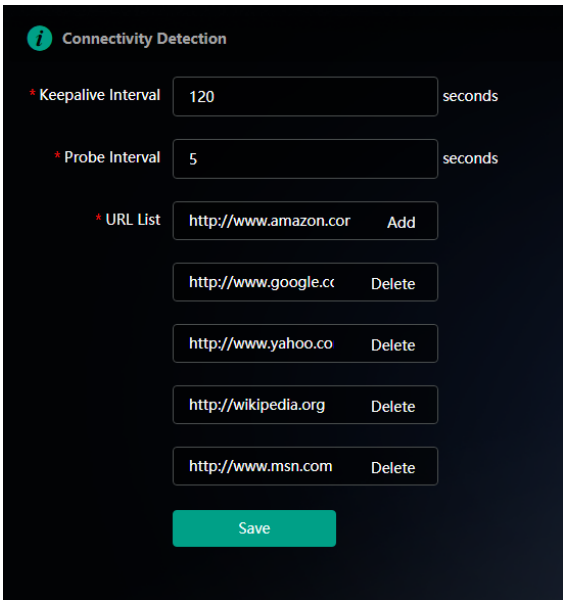
PC View: Choose More > Advanced > Connectivity detection.

Enter the values in the **Keepalive Interval**, **Probe Interval** and **URL List** fields, and click **Save** to save the settings.

Keepalive Interval: Interval for network connectivity detection when the network is reachable. The value range is 3 to 120 seconds.

Probe Interval: Interval for network connectivity detection when the network is unreachable. The value range is 1 to 30 seconds.

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



6.12 Configuring ARP Binding

Caution

This feature is supported in router mode.

6.12.1 Overview

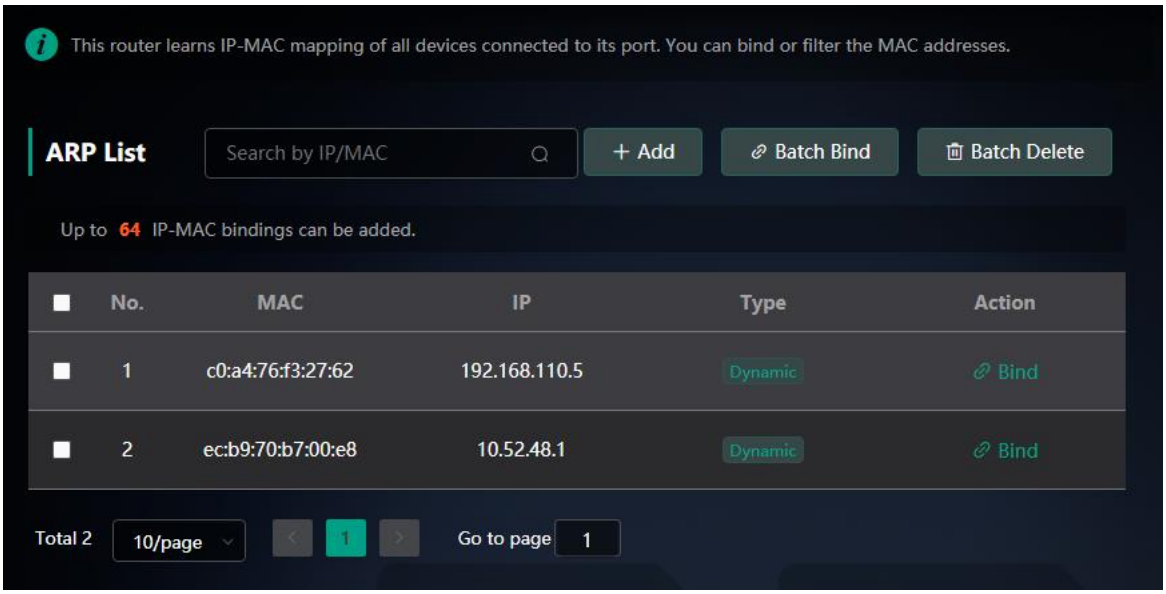
The router learns the ARP table from all devices connected to its ports. You can search for a device by its MAC address, perform ARP binding.

6.12.2 Configuration Steps

Smartphone View: Choose More > Switch to PC view > More > Security >ARP List.

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

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



6.13 Configuring Static Routing

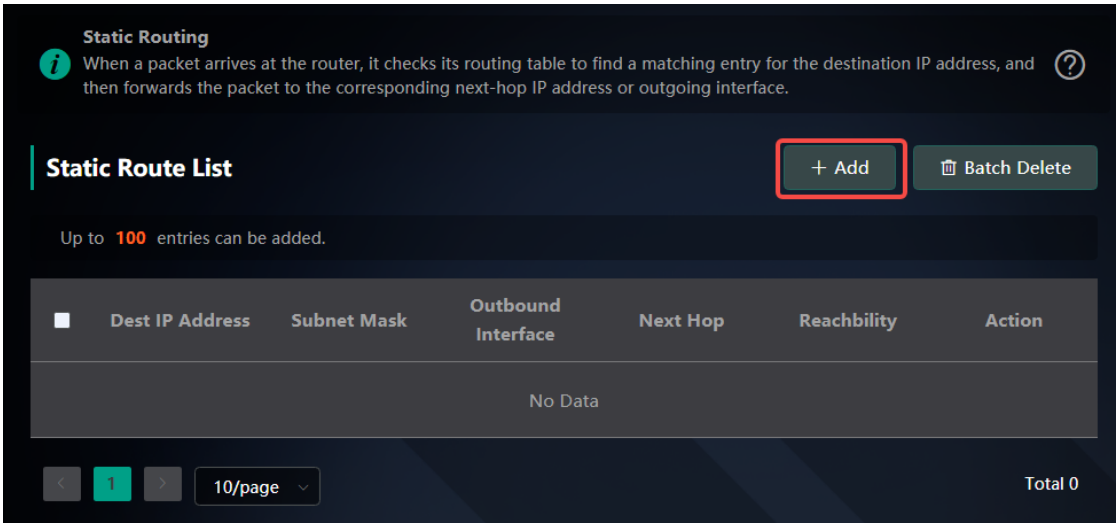
Smartphone View: Choose More > Switch to PC view > More > Advanced > Routing > Static Routing.

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

Caution

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

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



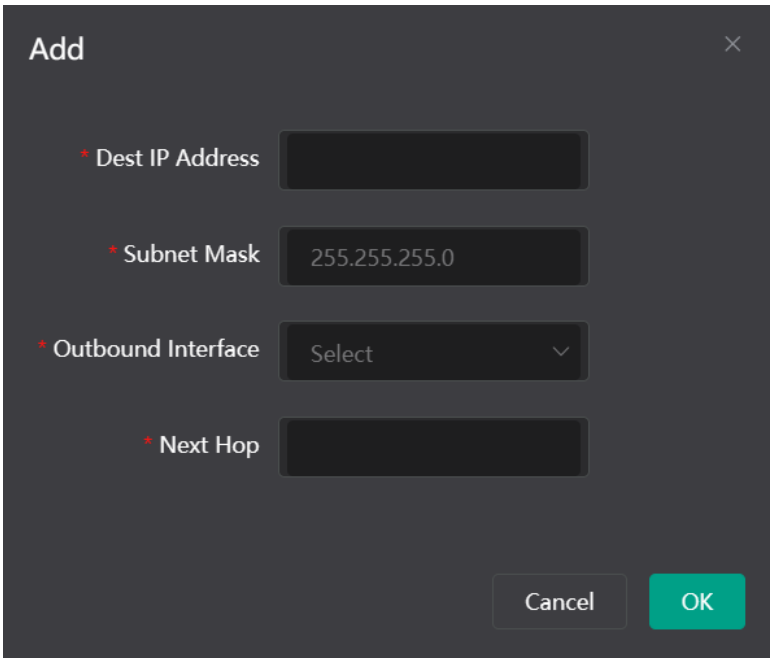
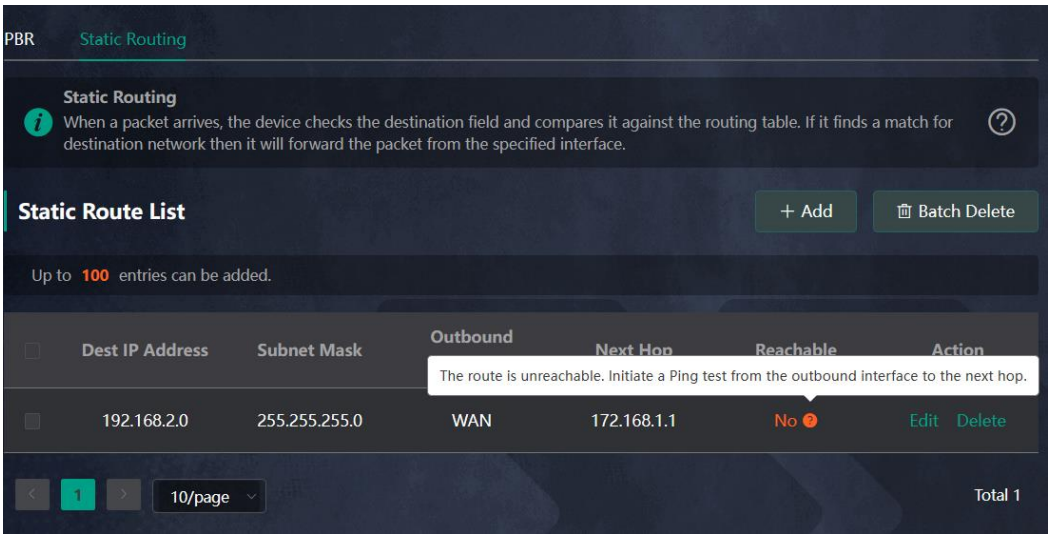


Table6-2 Description of Static Routing Configuration

Parameter	Description
Dest IP Address	The destination network of the packet. The destination IP address of the packet is matched based on the destination IP address and subnet mask.
Subnet Mask	The subnet mask of the destination network. The destination IP address of the packet is matched based on the destination IP address and subnet mask.
Outbound Interface	Interface over which packets are forwarded.
Next Hop	The IP address of the next-hop router to which the packet will be sent. If the outbound interface is a PPPoE interface, there is no need to configure the next-hop IP address.

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



6.14 Policy-based Routing

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

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

6.14.1 Overview

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

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

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

6.14.2 Configuration Steps

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

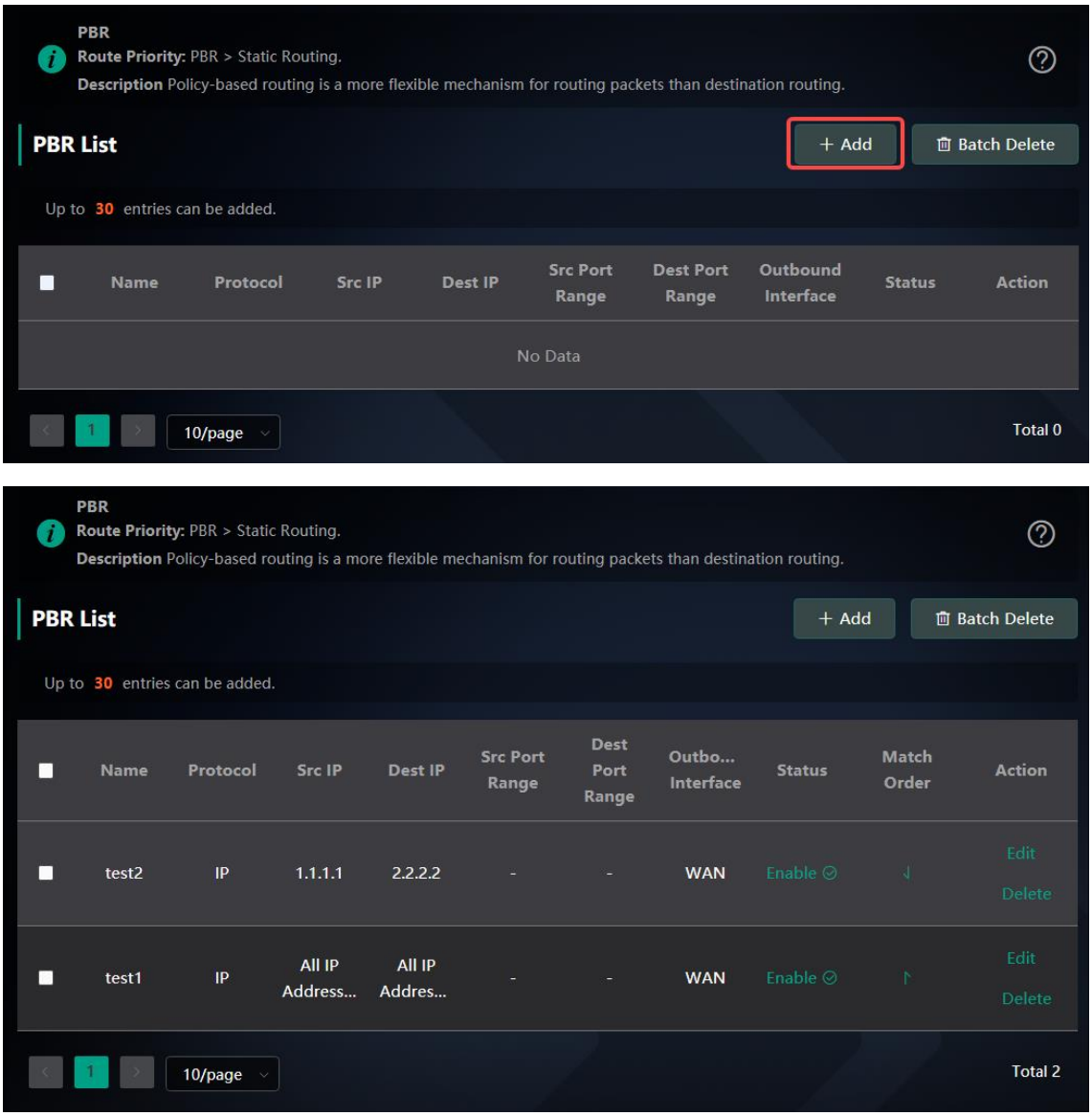


Table6-3 Description of Policy-based Routing

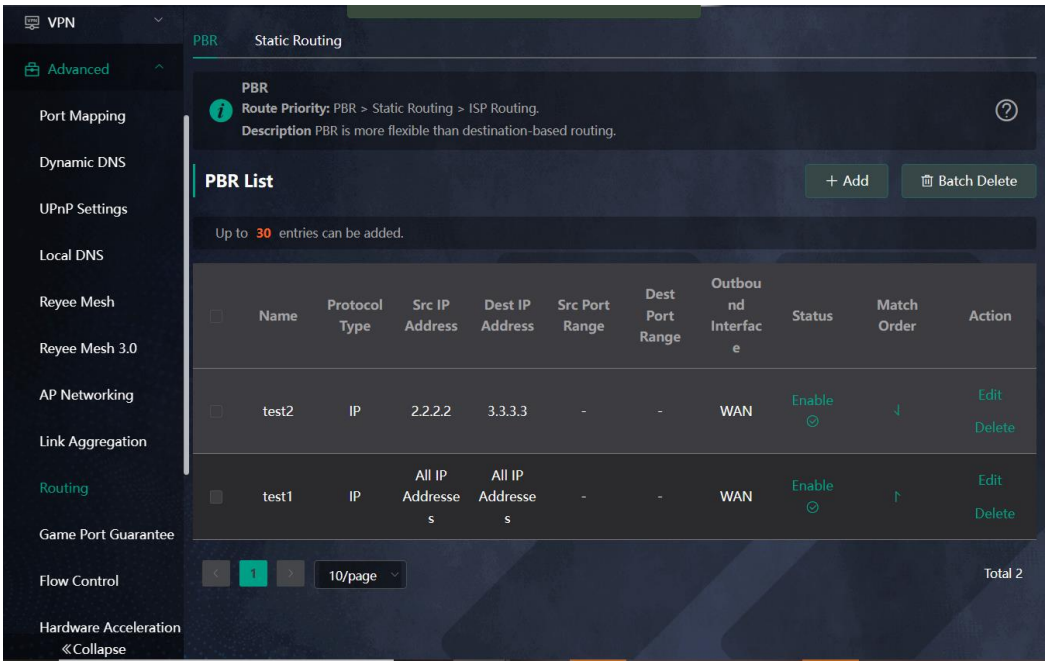
Parameter	Description
Name	The name of the PBR rule, as the identifier of the PBR route. The name must be unique.
Protocol Type	The protocol for the PBR route to take effect, which can be IP, ICMP, UDP, TCP, or a custom protocol type as needed.
Protocol Number	When the protocol type is **Custom**, the protocol number is required.
Src IP/IP Range	The source IP/IP range to which the PBR rule matches. By default, **All IP** is selected. ● All IP: Matches all source IP addresses. ● Custom: Matches source IP addresses in the specified range.
Custom Src IP	The source IP address or range is required when the matching source IP/IP range is **Custom**.

Parameter	Description
Dest IP/IP Range	The destination IP/IP range to which the PBR rule matches. By default, **All IP** is selected. ● All IP: Matches all destination IP addresses. ● Custom: Matches destination IP addresses in the specified range.
Custom Dest IP	The destination IP address or range is required when the matching destination IP/IP range is **Custom**.
Src Port Range	This field is displayed only when the protocol type is **TCP** or **UDP**. The value in this field is the source port range matching the PBR route.
Dest Port Range	This field is displayed only when the protocol type is **TCP** or **UDP**. The value in this field is the destination port range matching the PBR route.
Outbound Interface	Interface over which packets hit the PBR rule are forwarded.
Status	You can enable or disable the toggle switch next to **Status** to enable or disable the PBR rule.

Note

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

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



6.15 Enabling Smart Traffic Control

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

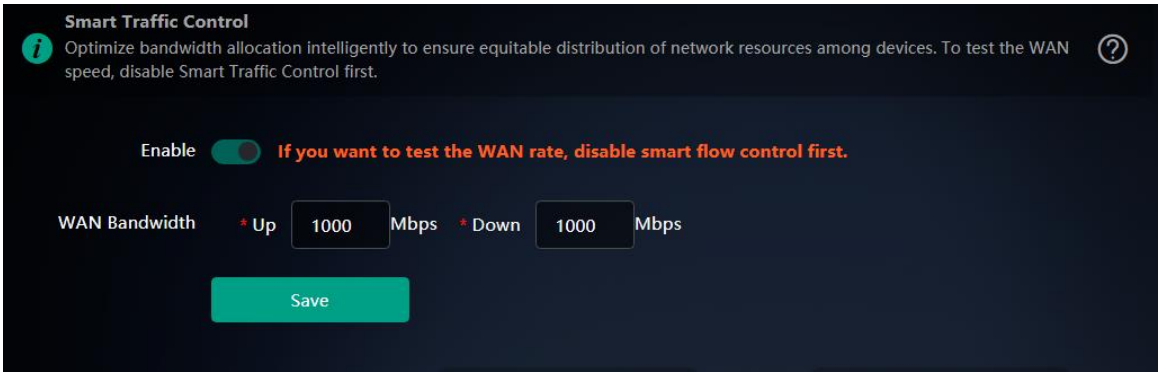
PC View: Choose More > Advanced > Flow Control > Smart Traffic Control.

6.15.1 Enabling Smart Flow Control

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

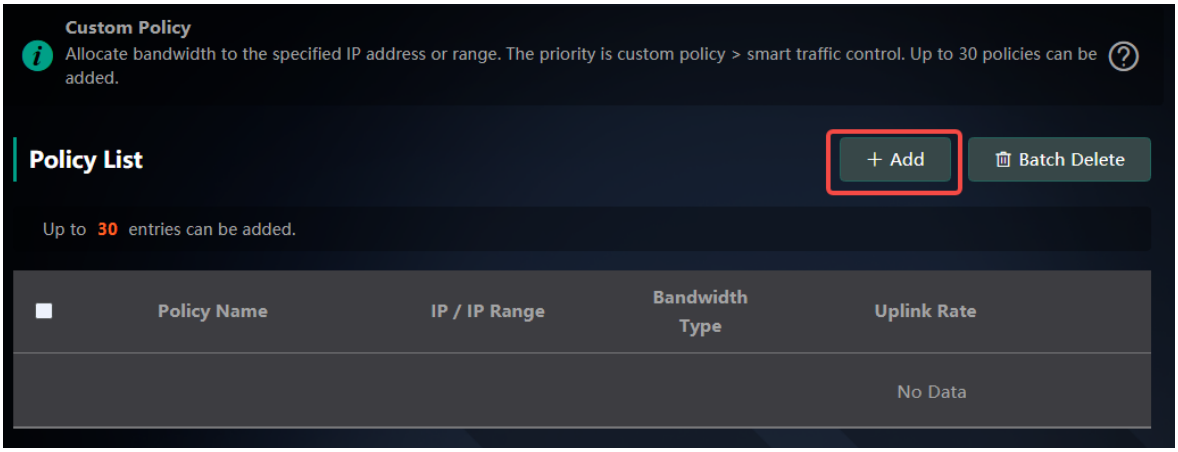
Caution

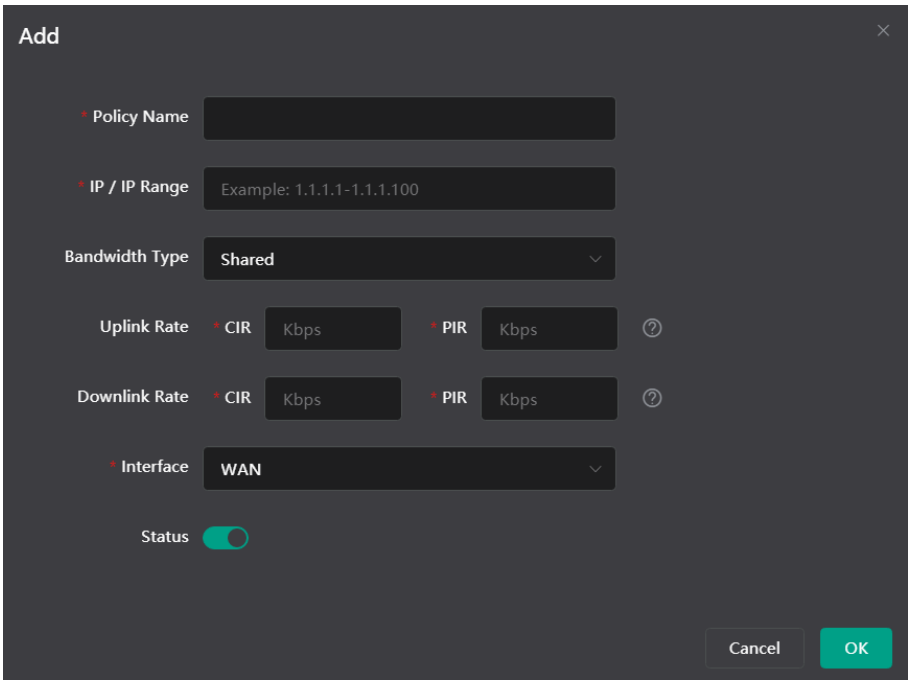
After smart traffic control is enabled, speed measurement will be affected. Disable flow control if you want to do speed measurement.



6.15.2 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.



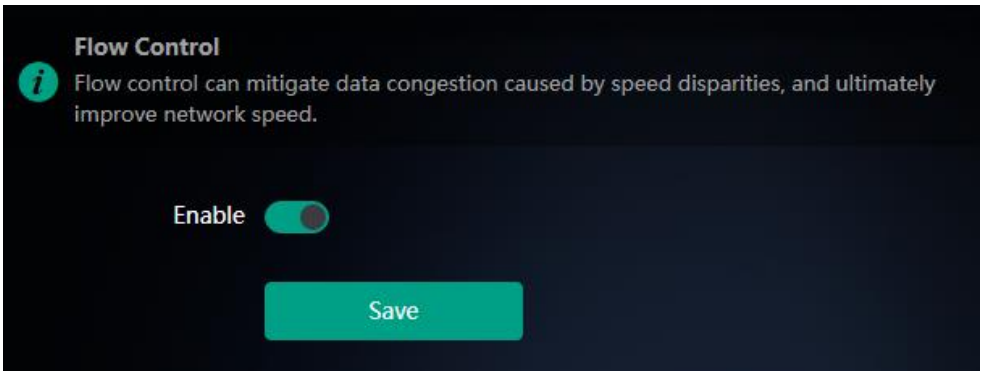


6.16 Enabling Port-Based Flow Control

Smartphone 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.



6.17 Enabling Hardware Acceleration

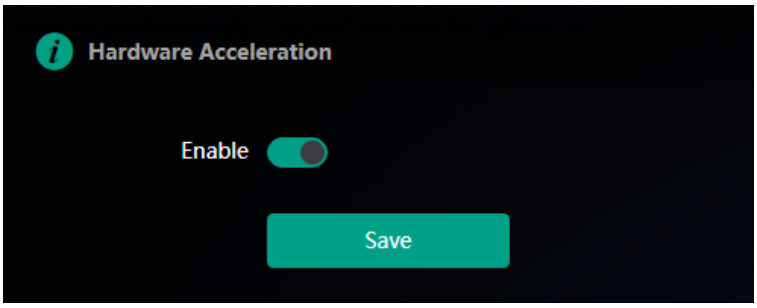
Caution

- This feature is supported in router mode.
- This feature is mutually exclusive with the **Auto Bandwidth Control** and **Priority Devices** feature. To Enable this feature, please turn off **Auto Bandwidth Control** and **Priority Devices** first.
- After hardware acceleration is enabled, IPv6 and smart flow control will be disabled.

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

PC View: Choose More > Advanced > Hardware Acceleration.

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

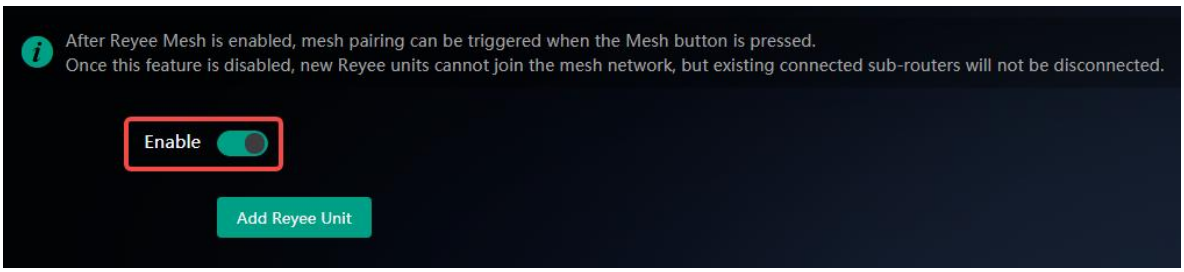


6.18 Enabling Reyee Mesh

Smartphone View: Choose More > Switch to PC view > More > Advanced > Reyee Mesh 3.0 > Reyee Mesh

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

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



Note

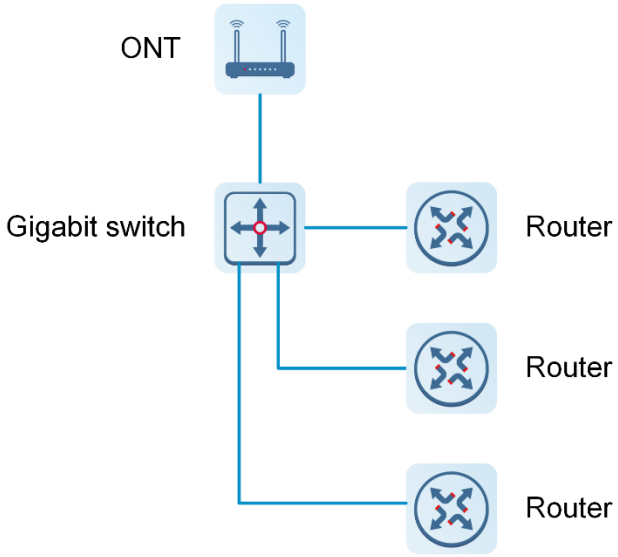
When Reyee Mesh is disabled, bridged mesh repeaters will not be disconnected.

6.19 Configuring Reyee Mesh 3.0

Smartphone View: Choose More > Switch to PC view > More > Advanced > Reyee Mesh 3.0

PC View: Choose More > Advanced > Reyee Mesh 3.0

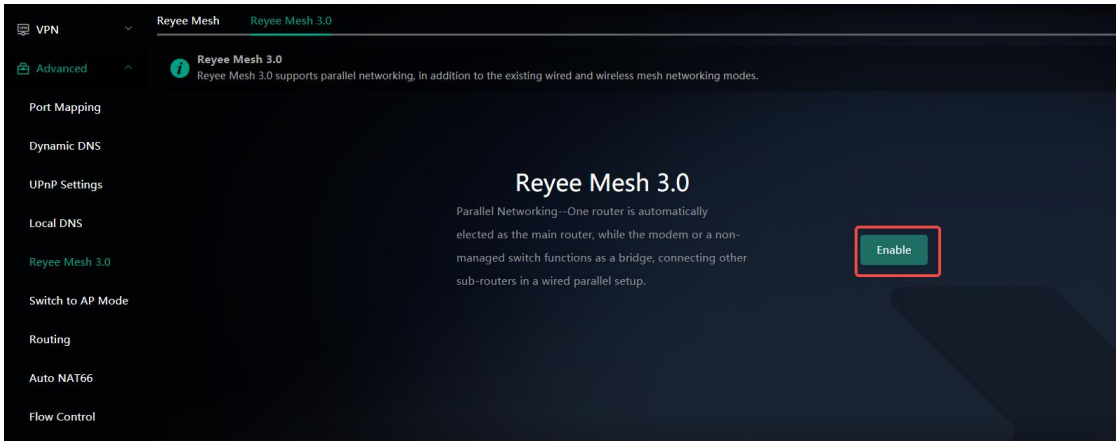
Connect the routers as indicated in the following figure:



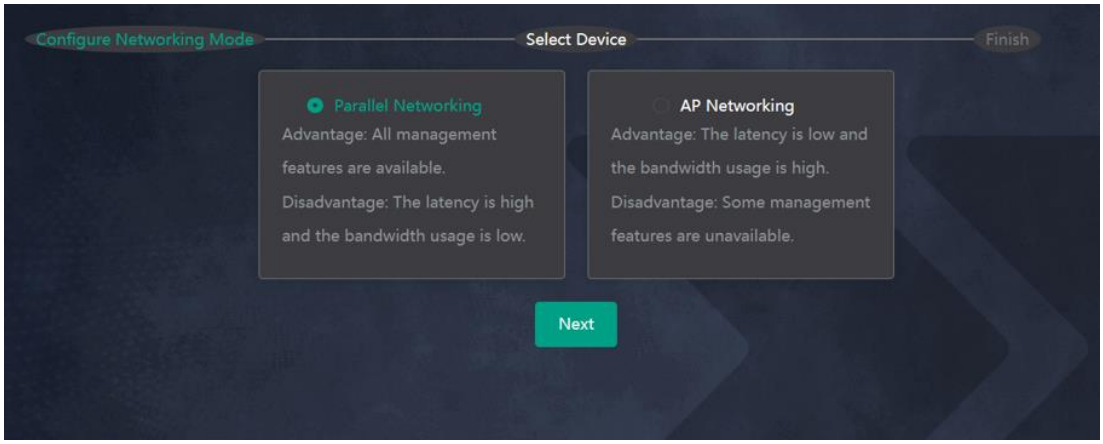
6.19.1 Parallel Networking

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

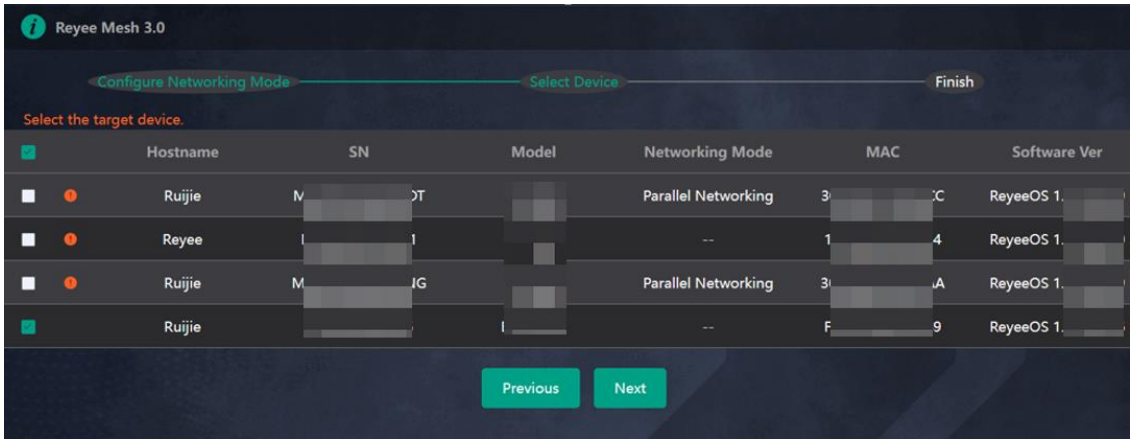
(1) Click **Enable** to enable Reyee Mesh 3.0.



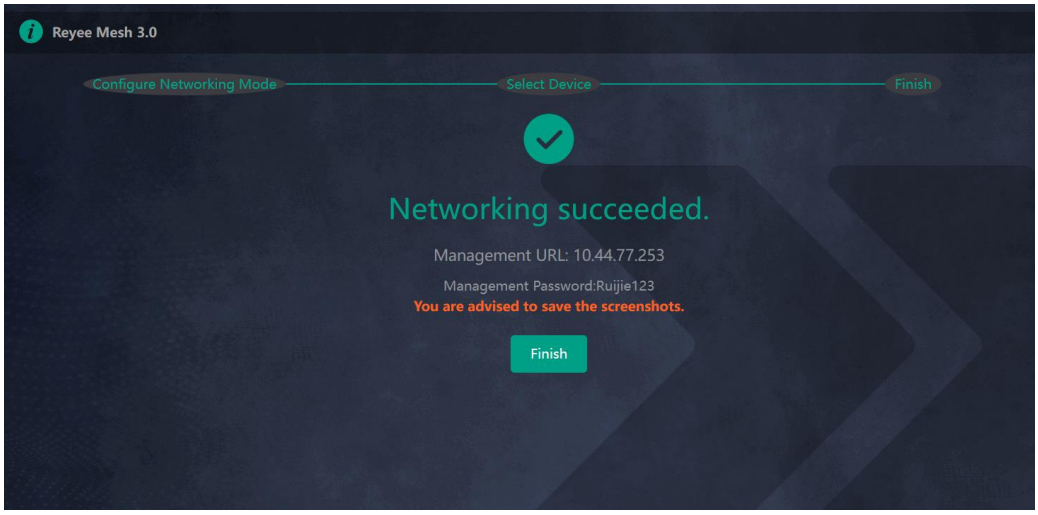
(2) Choose Parallel Networking, and click **Next**.



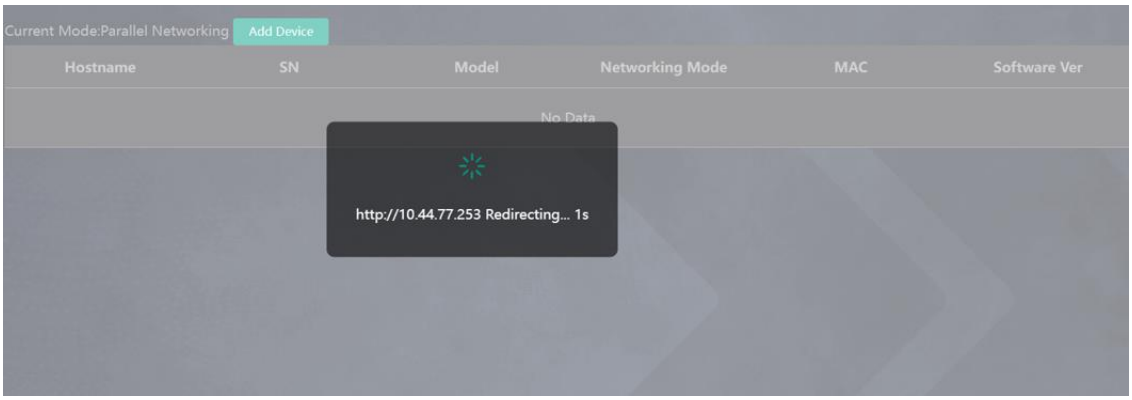
(3) Check routers for the networking.



(4) Click **Next**.



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

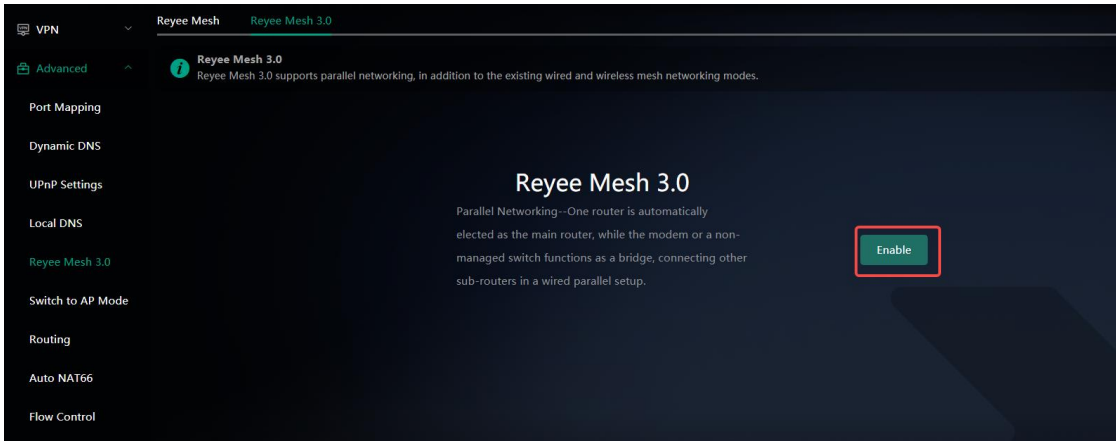


(6) On the master router page that is displayed, enter the password to log in.

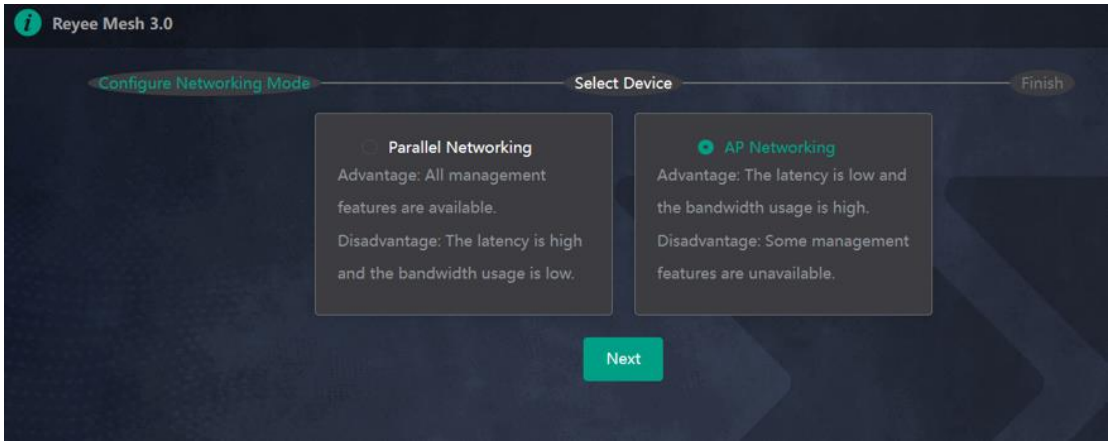
6.19.2 AP Networking

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

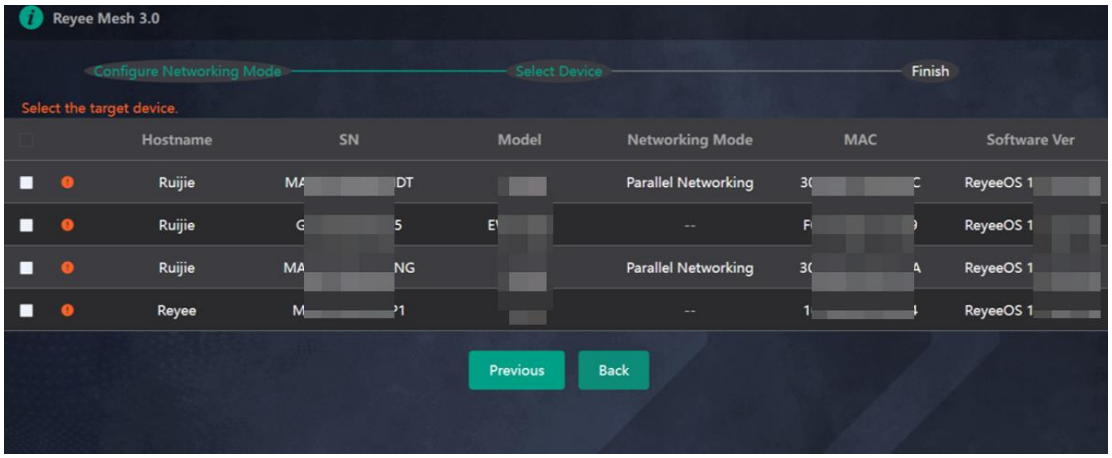
(1) Click **Enable** to enable Reyee Mesh 3.0.



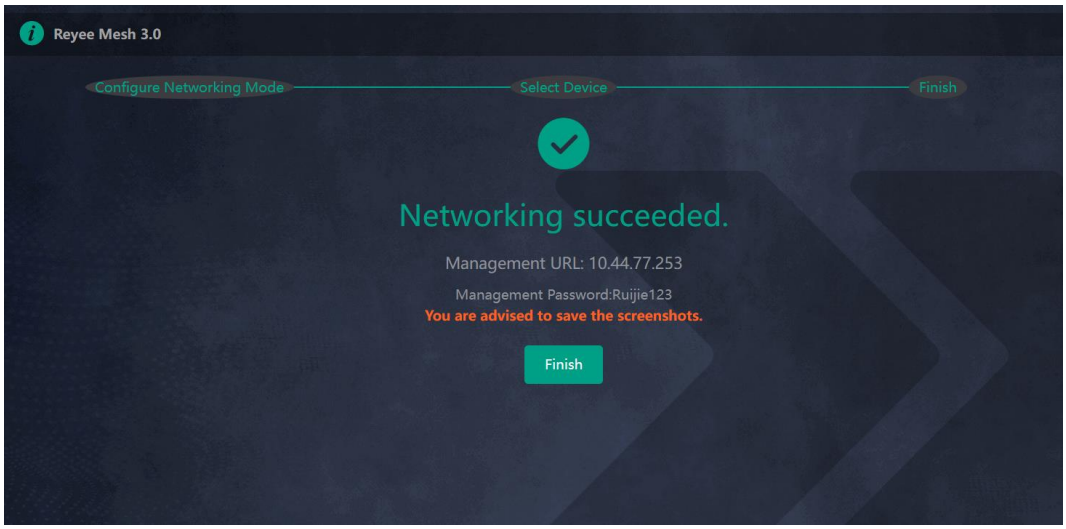
(2) Choose **AP networking**, and click **Next**.

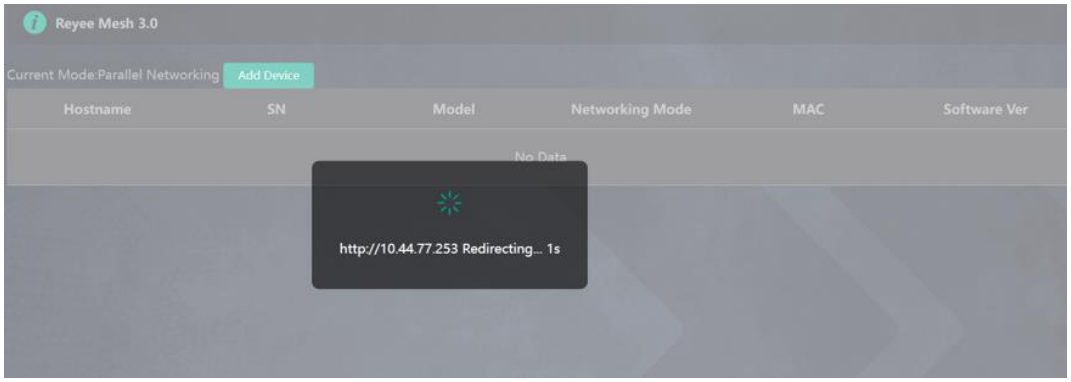


(3) Check routers for AP networking, and click **Next**.



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





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

6.20 Configuring UPnP

Caution

This feature is supported in router mode.

6.20.1 Overview

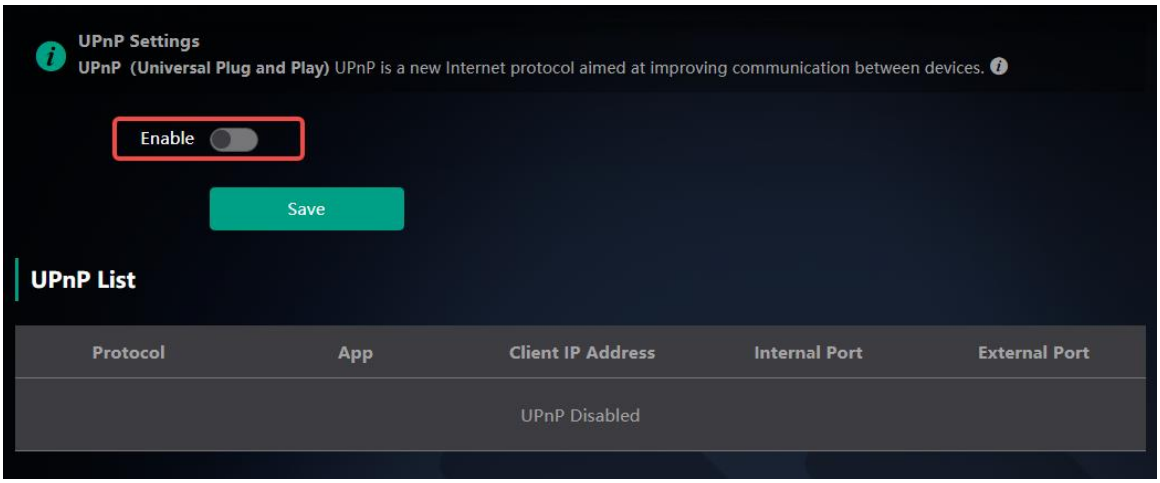
The universal plug and play (UPnP) function can map the port used by a client for Internet access according to the client's request so that related applications run faster or more stably. Common applications that support UPnP include MSN Messenger.

6.20.2 Configuration Steps

Smartphone 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.

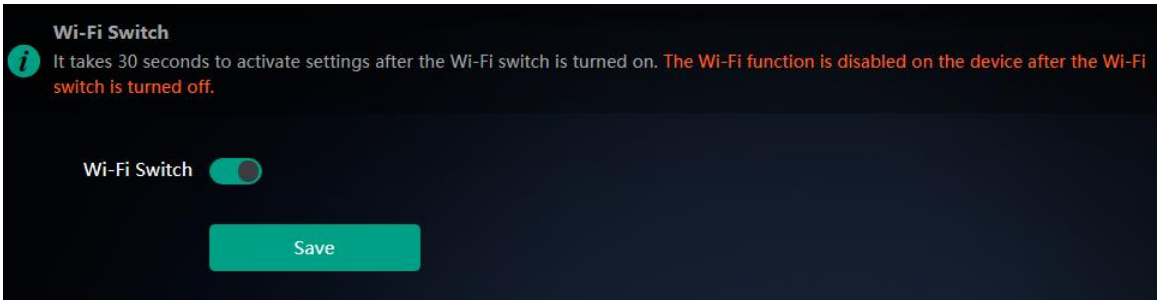


6.21 Enabling Wi-Fi Switch

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

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

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



6.22 Switching to AP Mode

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

PC View: Choose More > Advanced > Switch to AP Mode

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



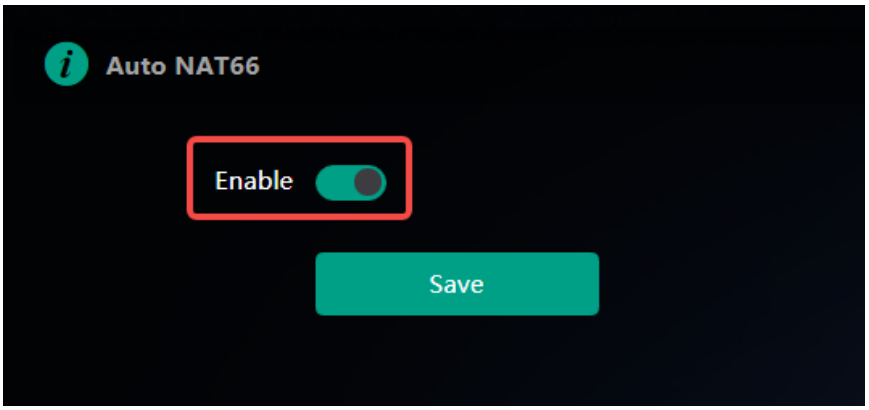
6.23 Configuring Auto NAT66

Smartphone View: Choose More > Switch to PC view > More > Advanced > Auto NAT66.

PC View: Choose **More** > **Advanced** > **Auto NAT66**.

In a home network, there is often a need to connect multiple devices to the Internet, but IPv6 addresses can be limited. By using auto NAT66, a single IPv6 address can be shared by multiple devices on a home network for Internet access.

Toggle on **Enable** to enable **Auto NAT66**. Once this feature is enabled, automatic address translation for the IPv6 network can be achieved.



6.24 Configuring PPTP VPN

6.24.1 Overview

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

6.24.2 Configuring PPTP Server

Smartphone View: Choose More > Switch to PC view > More > VPN > PPTP > PPTP.

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

1. Configuring PPTP Server

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

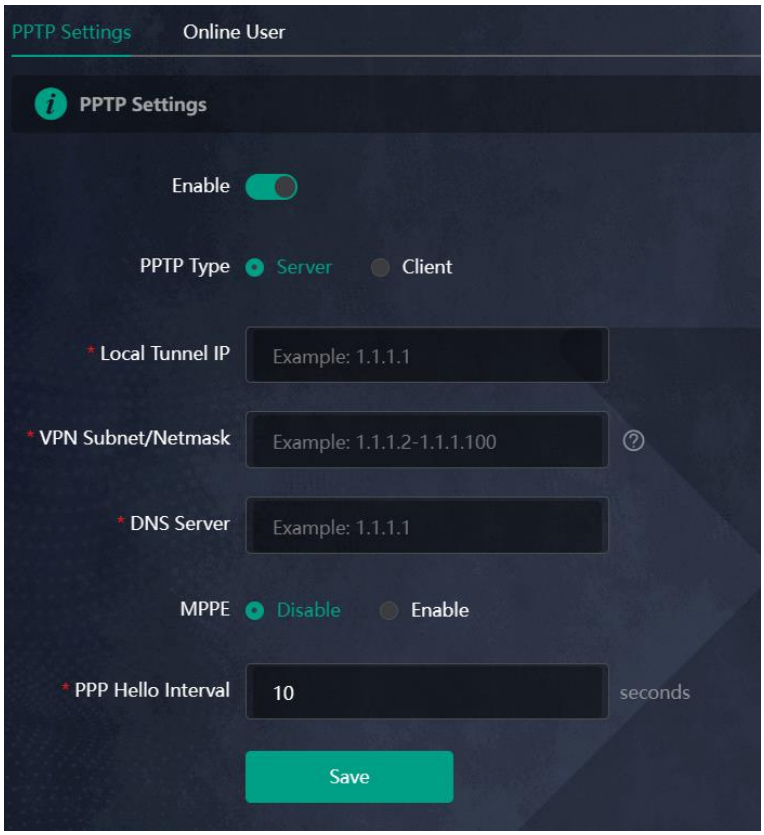
Local Tunnel IP: Enter the local address. It is used as the local virtual IP address of the VPN tunnel for the client to access the server after dialing in.

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

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

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

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



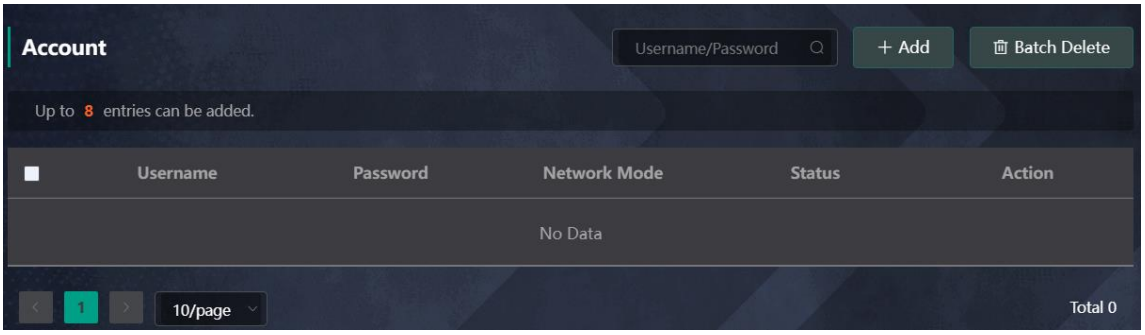
(2) Click **Save** and the device will receive and process the VPN request.

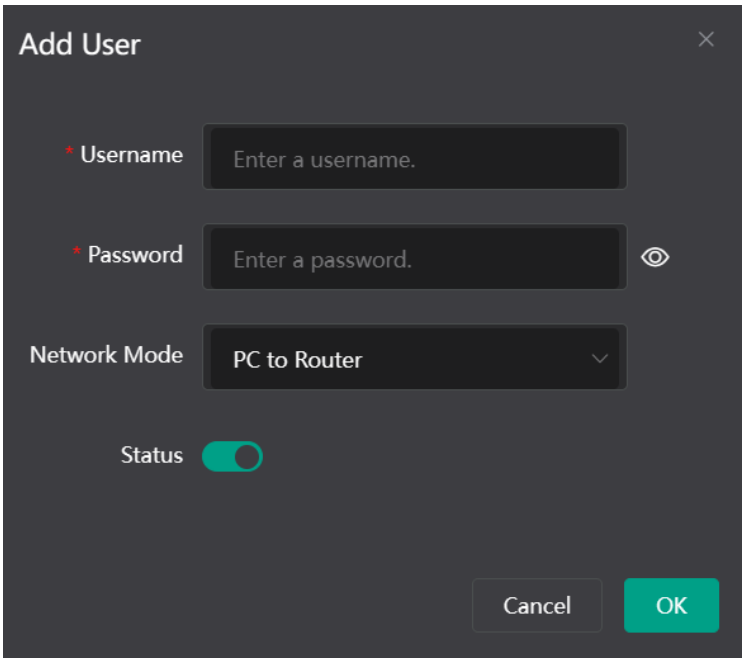
2. Add the PPTP user

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

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

Enable **Status** and click OK.





6.24.3 Configuring PPTP Client

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

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

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

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

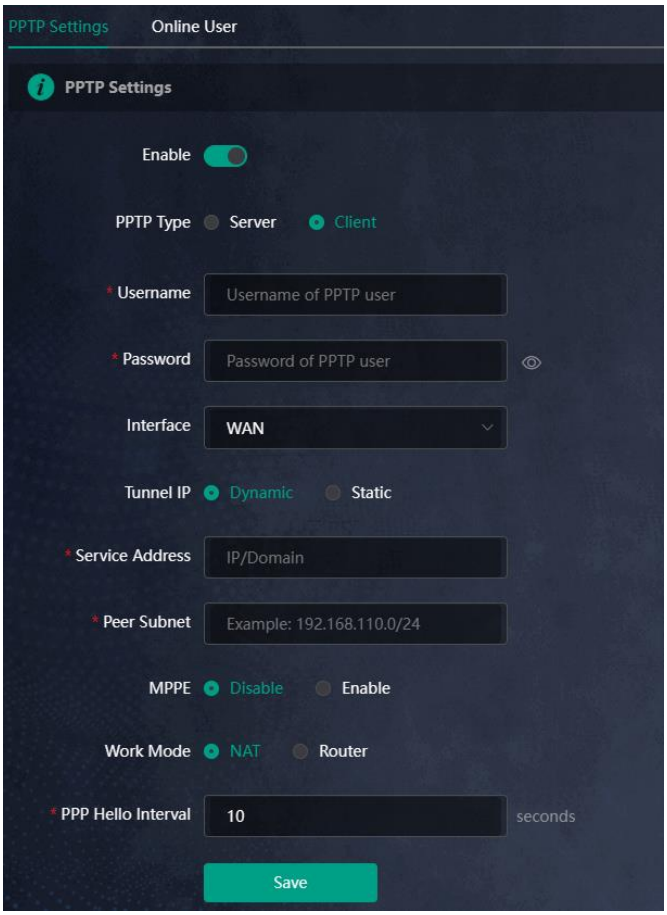
Server Address: Enter the WAN port IP address (the public IP is required) or the domain name of the server.

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

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

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

Click **Save** and the device will send the VPN tunnel request to the WAN port.



6.25 Configuring OpenVPN

6.25.1 Overview

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

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

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

6.25.2 Configuring OpenVPN (Server Mode)

Smartphone View: Choose More > Switch to PC view> More> VPN> OpenVPN.

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

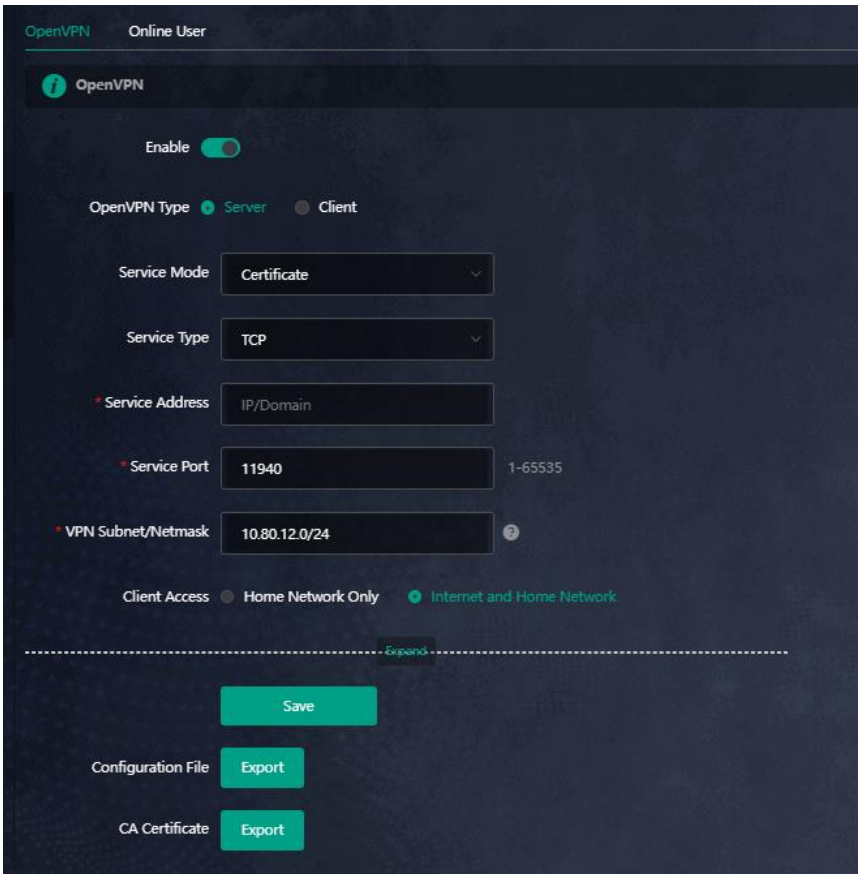
1. Configuring OpenVPN

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

(2) Select Server for the OpenVPN Type.

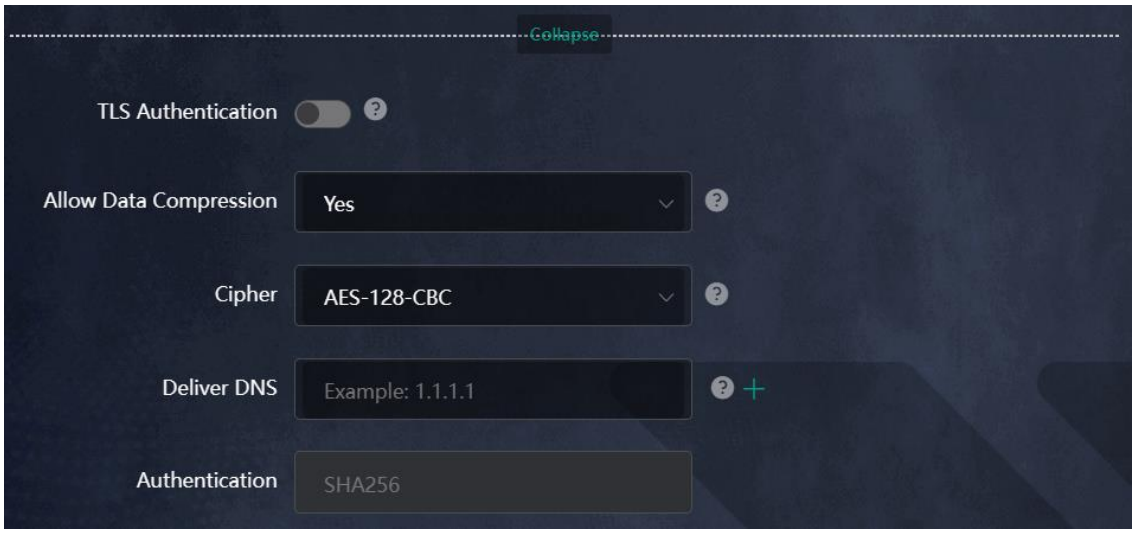
(3) Select the protocol, and enter the server address, port number and other information.

Figure6-1 Configuring OpenVPN Server



(4) (Optional) Advanced settings.

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



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

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

Table6-4 Configuration Items of OpenVPN Server Mode

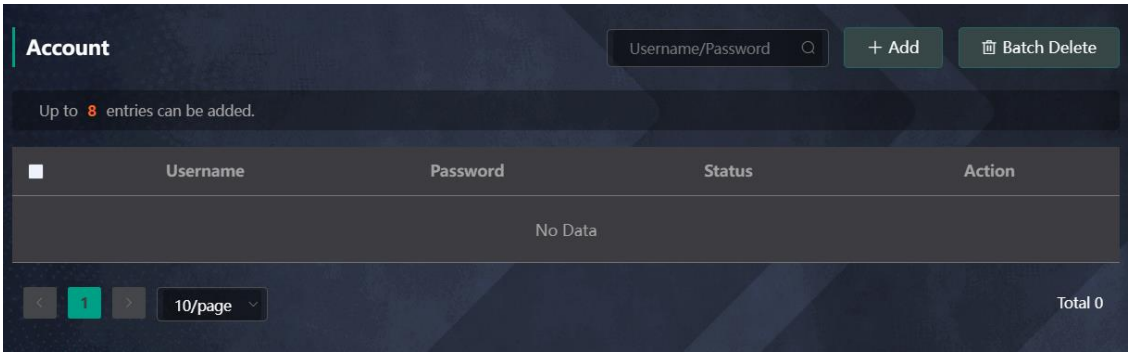
Item	Description
Server Mode	The device supports Account, Certificate and Account & Certificate authentication modes: ● Account mode: The correct account name, password, and CA certificate are required to connect to the server. The configuration is simple. ● Certificate mode: The client needs the correct CA certificate, client certificate, and pre-shared key to connect to the server. ● Account & Certificate mode: The client needs the correct account name, password, CA certificate, client certificate, and pre-shared key to connect to the server. This mode is suitable for scenarios with high security requirements.
Service Type	All communication on OpenVPN is based on a single IP port, using **UDP** or **TCP** protocols. The default value is UDP. You can select TCP for higher performance. TCP protocol can be used to improve the stability of VPN channels in high latency or unstable network conditions.
Service Address	The server address used for client docking, which can be a domain name.
Service Port	The port used by the OpenVPN service process. The official port assigned to OpenVPN is 1194. If the port is occupied or disabled on the local network, the server log will prompt a log indicating port binding failure. In this case, the port number needs to be changed.
VPN Subnet/Netmask	The IP address pool delivered to VPN clients, in the form of a network segment. The first address in that segment is reserved by the server. For example, if 10.80.12.0/24 is set, then the VPN server address is 10.80.12.1.
Client Access	You can choose **Home Network Only** or **Internet and Home Network** ● **Home Network Only**: The client can only access the LAN segment on the

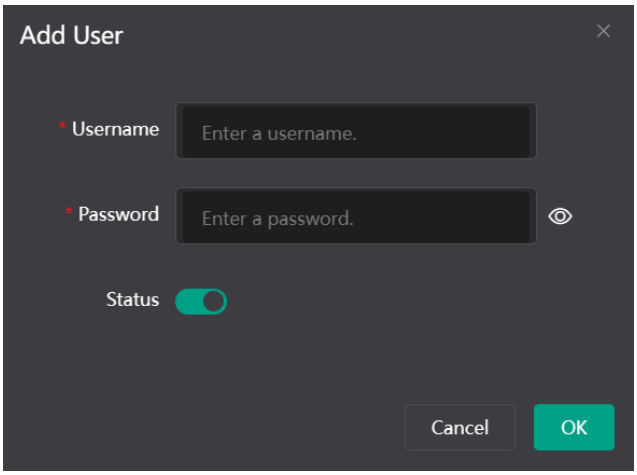
Item	Description
	server. ● **Internet and Home Network**: The client can access the LAN and WAN segments on the server. In this mode, all traffic from the client will be forwarded to the server.
TLS Authentication	TLS Authentication can enhance the security of OpenVPN. Once enabled, the client must import the TLS key. (The version of the peer OpenVPN client must be later than 2.40.)
Allow Data Compression	Once enabled, the device will compress the transmitted data to save bandwidth, but it will occupy a certain amount of CPU resources. This configuration must be consistent on the client and the server to avoid any potential connection failures.
Cipher	Encrypts the data to prevent it from being intercepted midway. The default encryption standard is AES-128-CBC. If the server is configured in auto mode, the client can be configured with any data encryption algorithm, which will be automatically matched by the server. If a specific encryption method is configured on the server, the client must be configured with the same encryption method. Otherwise, the connection between the server and the client cannot be established.
Deliver DNS	The information pushed by the server to the client's DNS. Currently only Windows clients are supported.
Authentication	The digest algorithm informed by the server to the client. The default value is SHA256.

2. Adding OpenVPN clients

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

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





6.25.3 Configuring OpenVPN (Client Mode)

Smartphone View: Choose More > Switch to PC view> More> VPN > OpenVPN.

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

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

(1) Click **Enable** to enable the **OpenVPN** function. Configure **OpenVPN Type** as **Client.**

(2) Configure the Server Mode, and click **Browse** to import the client configuration file. Click **Save** to save the configuration.

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

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

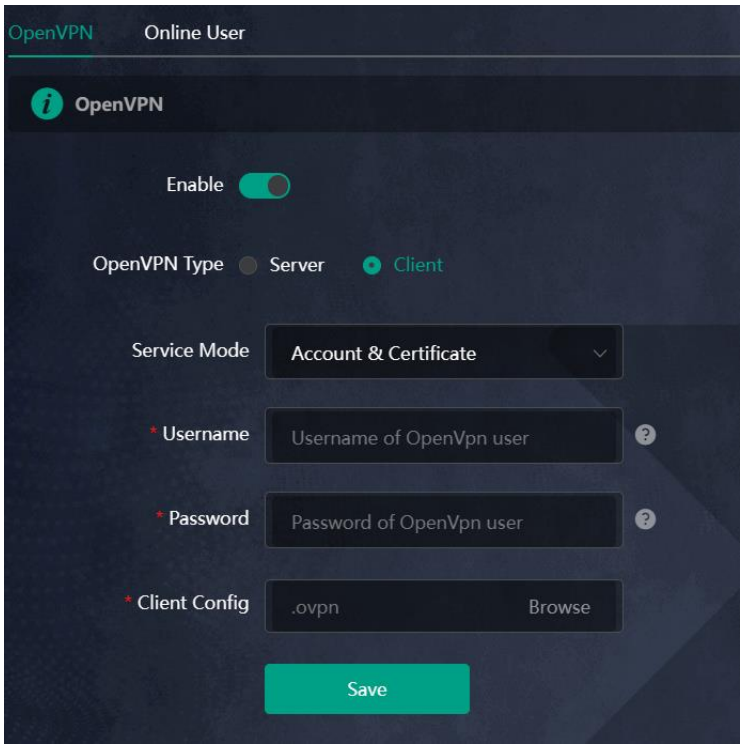


Table6-5 Configuration Items of OpenVPN Client Web Setting Configuration Mode

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

6.25.4 Typical Configuration Example

1. Requirements

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

2. Topology



3. Notes

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

4. Configuring OpenVPN Server (Device A)

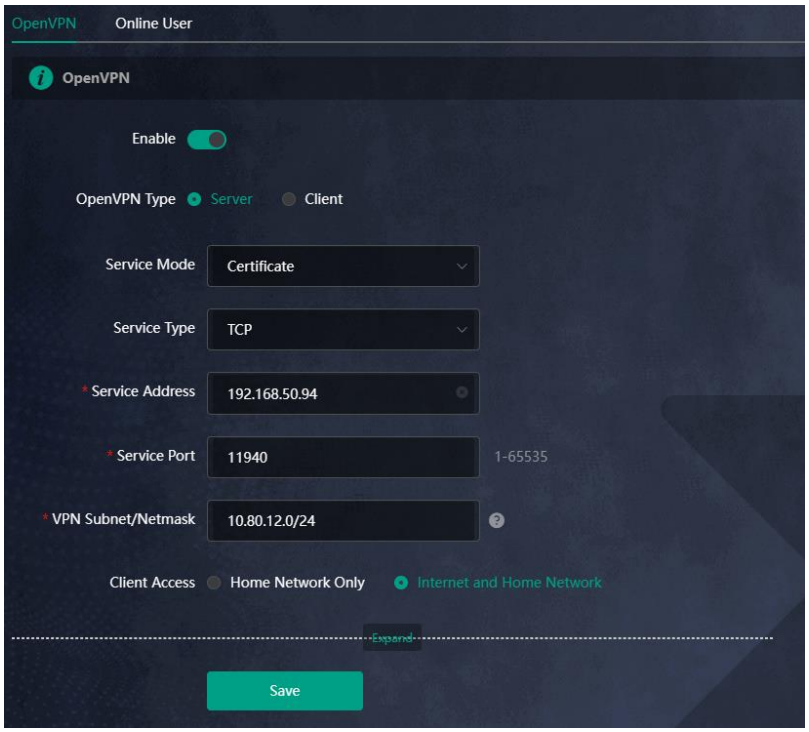
(1) Log in to the web interface of the router, and choose **VPN** > **OpenVPN**. Then, flip on the toggle switch next to **Enable** to enable the OpenVPN function. On the page that is displayed, enter the IP address of the WAN port as the service address, as well as other required parameters.

Use the default settings unless there are specific requirements.

Note

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

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

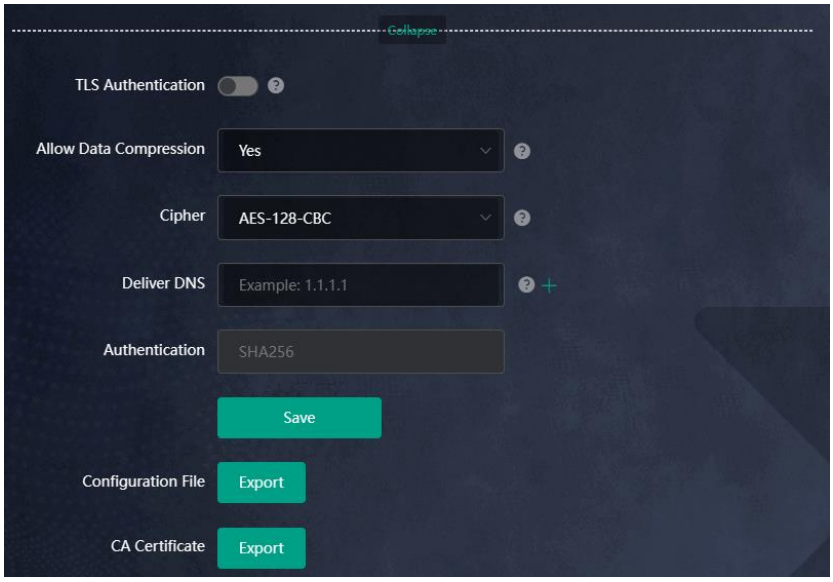


(2) Click **Save**. The OpenVPN settings are saved.

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

Parameter	Description
Service Mode	● Account: Authentication based on password. ● Certificate: Authentication based on client certificate. ● Account & Certificate: Authentication based on password and client certificate.
Service Type	Use the default value unless there are specific requirements. Both **UDP** and **TCP** are supported. If the network connection between the two ends of an encrypted tunnel is poor, for example due to high latency or heavy packet loss, then select **TCP**.
Service Address	The IP address of the WAN port is automatically populated.
Service Port	Indicates the port for OpenVPN service. Use the default value unless there are specific requirements.
VPN Subnet/Netmask	Indicates the network segment of the OpenVPN address pool. The first available IP address in the address pool is reserved for the server, while other addresses can be allocated to clients. For example, if this parameter is set to **10.80.12.0/24**, then the virtual IP address of the VPN server is 10.80.12.1.
Client Access	● **Home Network Only**: If this access mode is selected, then the client can only access resources on the server's internal network, but is unable to access the Internet through the server's network proxy. ● **Internet and Home Network**: If this access mode is selected, then the client not only can access resources on the server's internal network, but also can access the Internet through the server's network proxy.

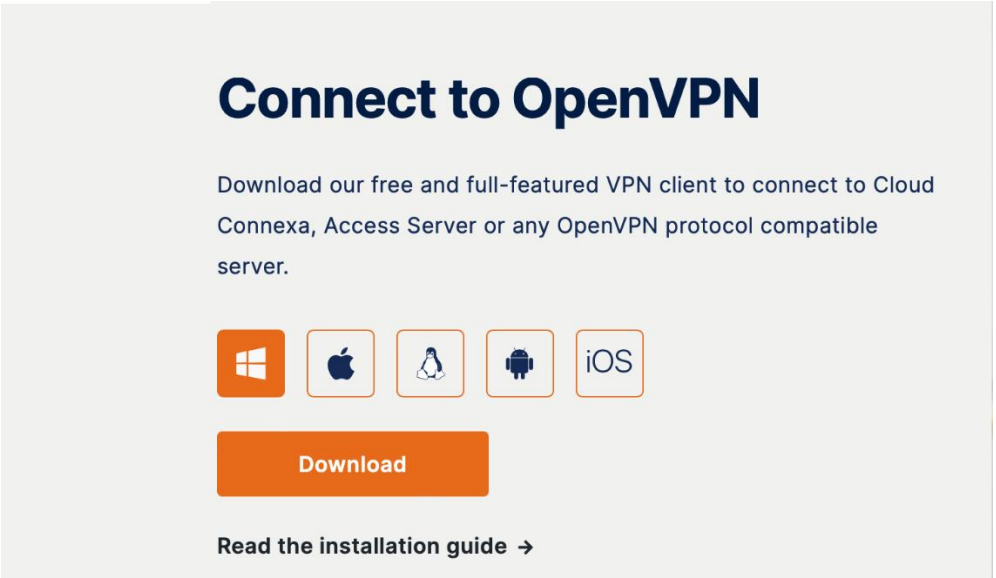
(4) Click **Expand** to show advanced settings. Use the default values unless there are specific requirements.



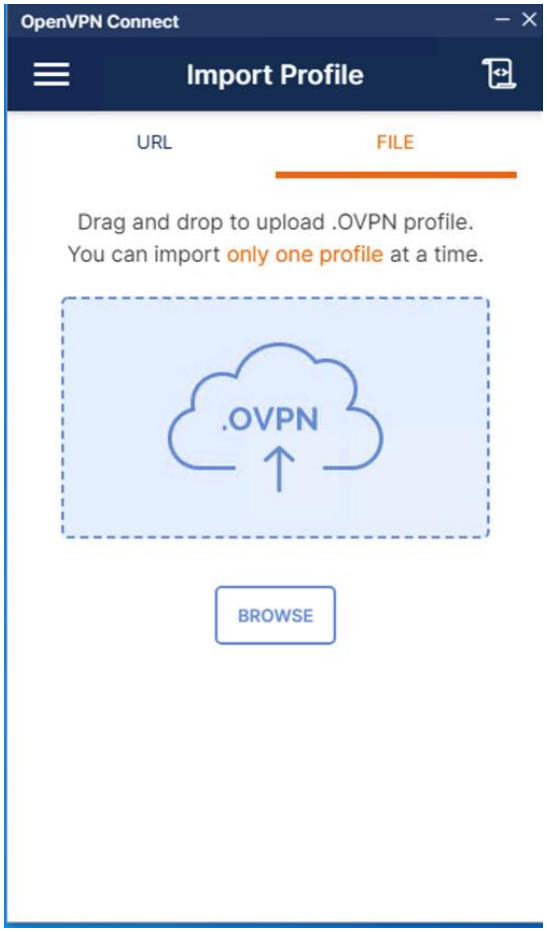
(5) Click **Export** next to **Configuration File** to export the .ovpn file which can be imported on the client side. Unless there are specific requirements, you do not need to export the CA certificate.

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

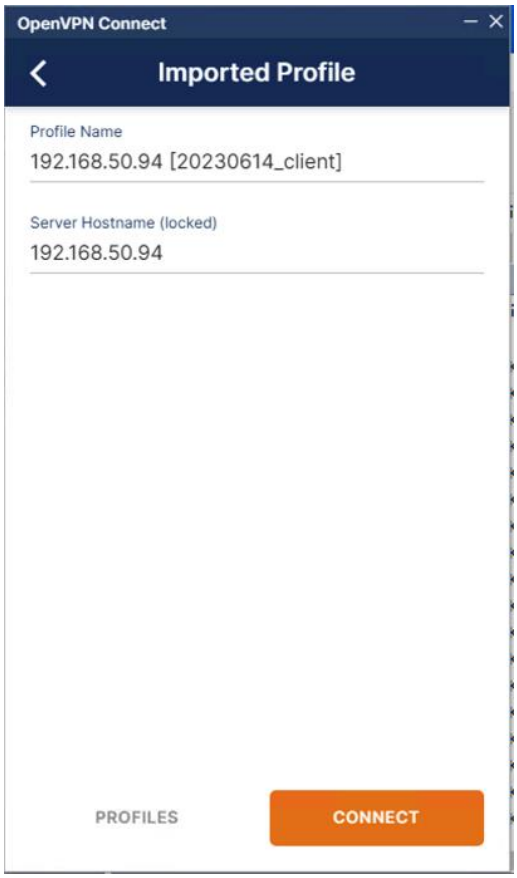
(1) Download the OpenVPN client (https://openvpn.net).



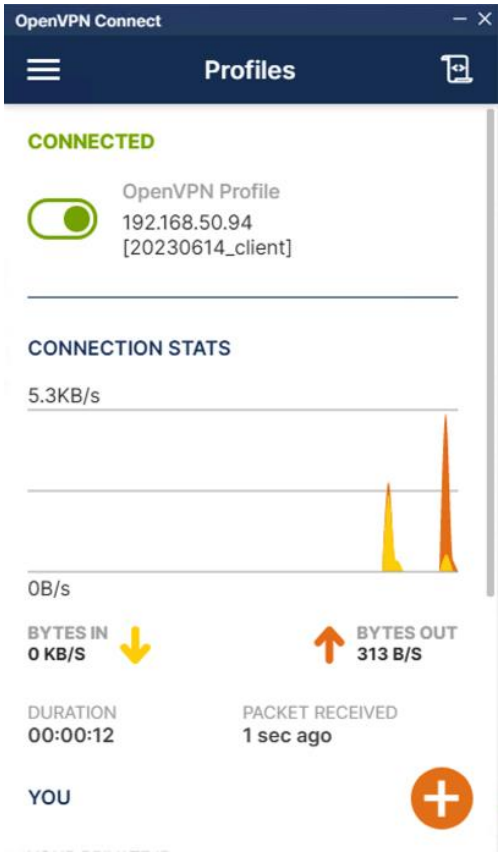
(2) Open the Windows OpenVPN client and choose the **File** tab.



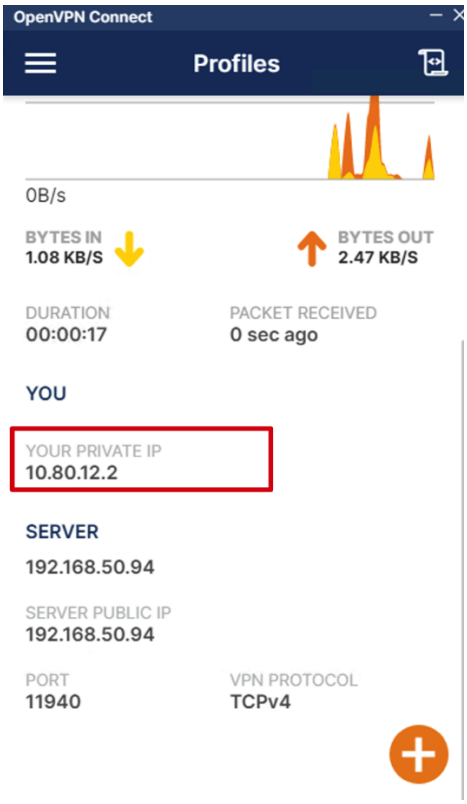
(3) Click **BROWSE** and select the .ovpn file exported from the server side.



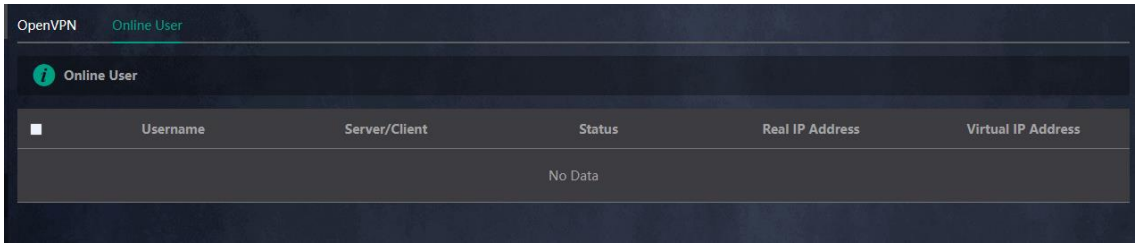
(4) Click **CONNECT** to connect to the OpenVPN server.



(5) Check the obtained virtual IP addresses.



(6) Log in to the web interface of the router, and choose **More** > **VPN > OpenVPN** > **Online User** to find the connected client.



6.26 Other Settings

Caution

This feature is supported in router mode.

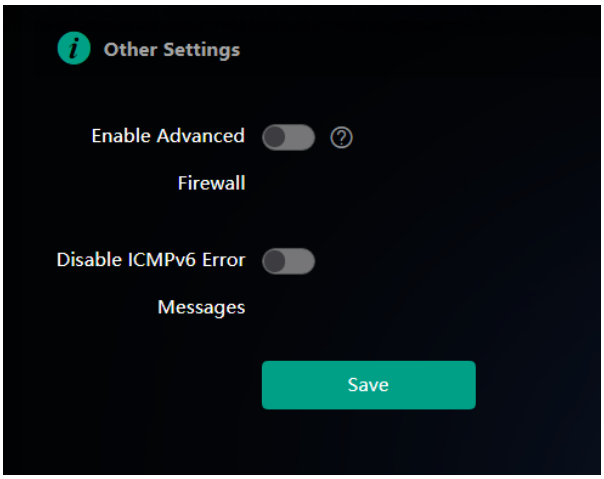
Smartphone View: Choose More > Switch to PC view > More > Advanced > Other Settings.

PC View: Choose More > Advanced > Other Settings.

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

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

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


Other Settings
Enable Advanced Firewall
Disable ICMPv6 Error Messages
Save

7 Configuring Diagnostics

Caution

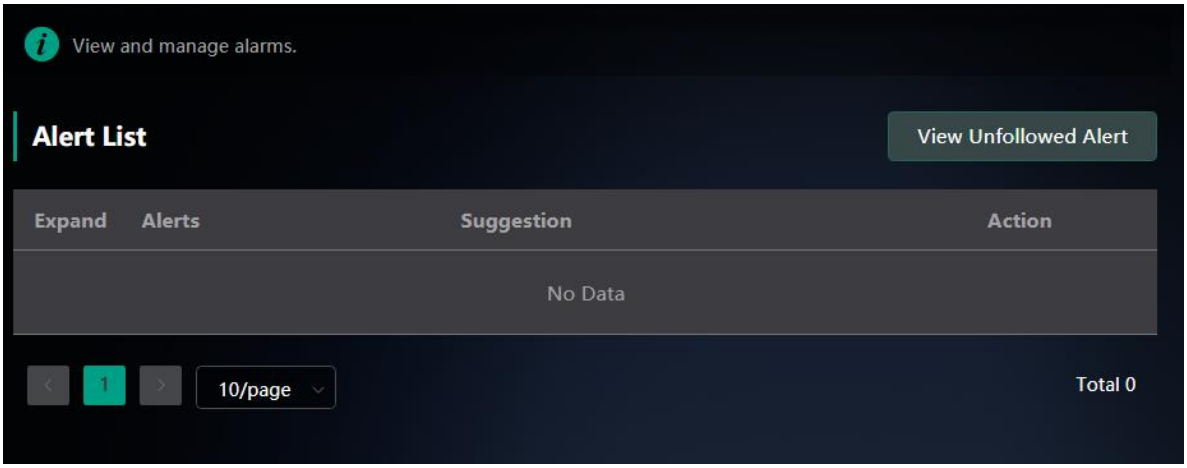
If the issue persists despite following the troubleshooting methods provided in this section, you may require remote support from a technician who will enable developer mode to resolve the issue. We will ensure your data is protected during this process.

7.1 Enabling Alerts

Smartphone View: Choose More > Switch to PC > More > Diagnostics > Alerts.

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

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



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

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

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

Table7-1 Alerts and Suggested Action

Alerts	Suggested Action
The WAN port has no link.	Please check whether a cable is plugged into the WAN port.

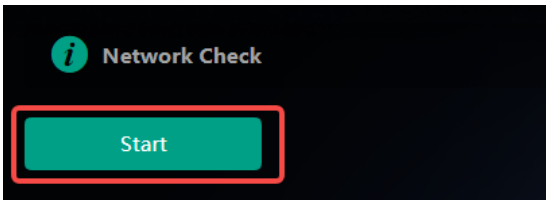
Alerts	Suggested Action
The port is operating at 10Mbps.	Please check the peer port settings, unplug and re-plug the cable, or replace the cable.
There is more than one DHCP server in the LAN network.	Please disable the extra DHCP server in the LAN network.
There is more than one DHCP server in the WAN network.	Please disable the extra DHCP server in the WAN network.
Address pool of DHCP server is full.	Enlarge the DHCP address pool.
WAN & LAN Address Conflict.	Please check the IP addresses of WAN and LAN ports. If the network addresses conflict (including IP address conflict), change the IP of LAN port.
The WAN IP address is already in use.	Please check the WAN IP address. If it is a static IP address, please change the IP address.
The LAN IP address is already in use.	Please check the LAN IP address. If it is a static IP address, please change the IP address.
The IP address of the downlink address is already in use.	Please check the IP address of the downlink device. If it is a static IP address, please change the IP address.
A MAC address conflict or loop error occurs.	Please troubleshoot the MAC address conflict or loop error.
No DNS server address is configured.	Please add a DNS server address, e.g., 114.114.115.115.
DNS failure	Please check the network configuration.
DNS resolution error.	Please check the network configuration.
Cloud service is not running.	Please reboot the device.
Cloud service is not enabled.	Please contact Reyee technical support.
The device is not connected to the Cloud server.	Please reboot the device.
Loops occur.	Please check the network environment.

7.2 Diagnosing Network Problems

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

PC View: Choose More > Diagnostics > Network Check.

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



7.3 Network Diagnosis Tools

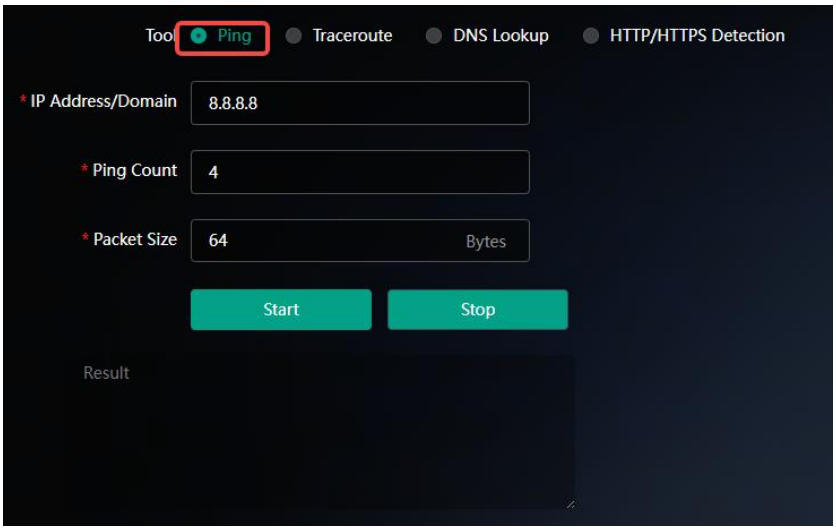
7.3.1 Ping

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.



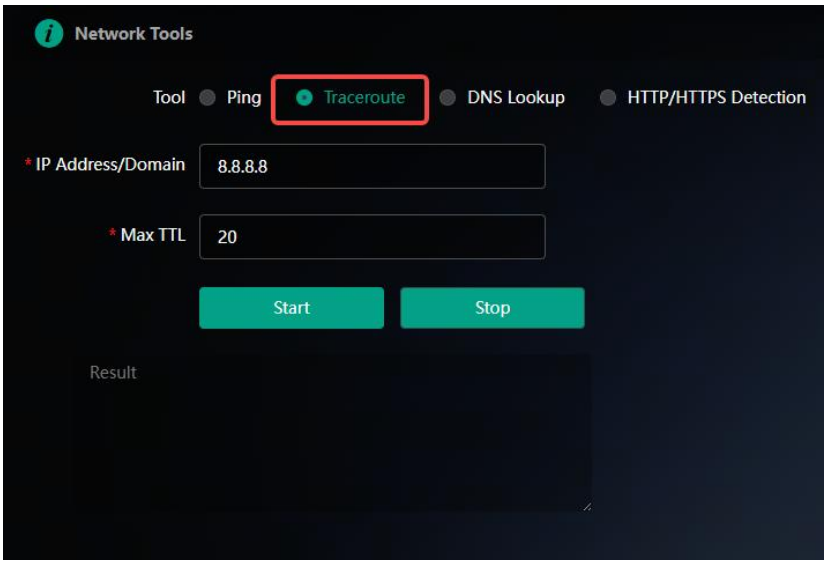
7.3.2 Traceroute

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**.



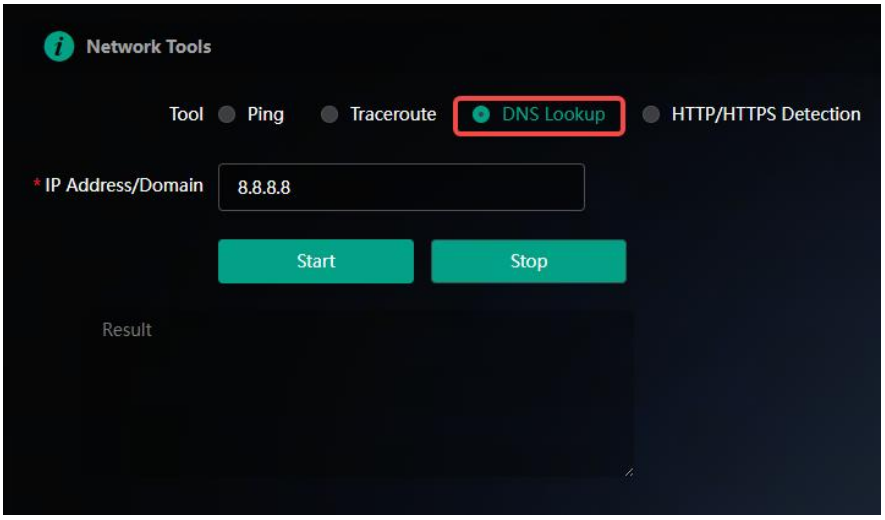
7.3.3 DNS Lookup

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**.



7.3.4 HTTP/HTTPS Detection

Specification

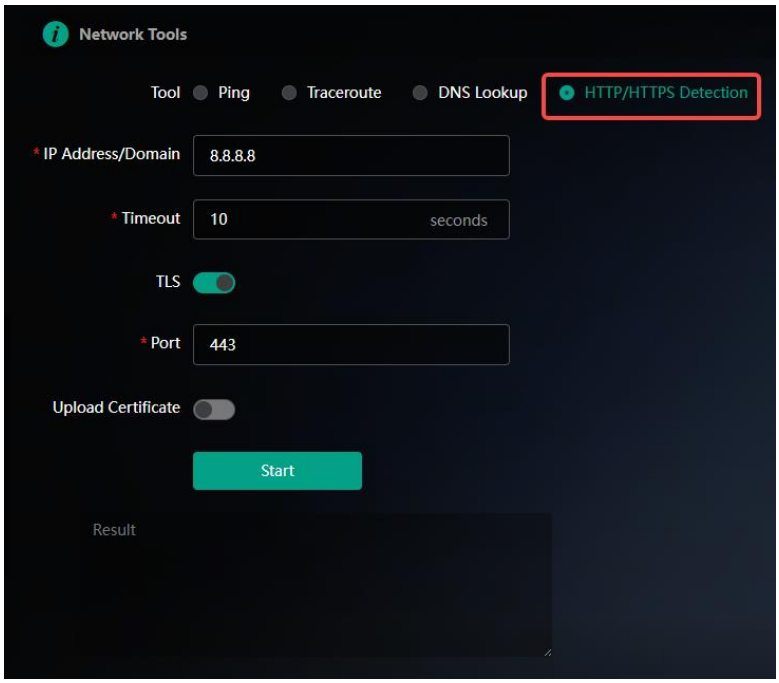
The device running ReyeeOS 1.420 version or later supports this feature.

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**.

Table7-2 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:

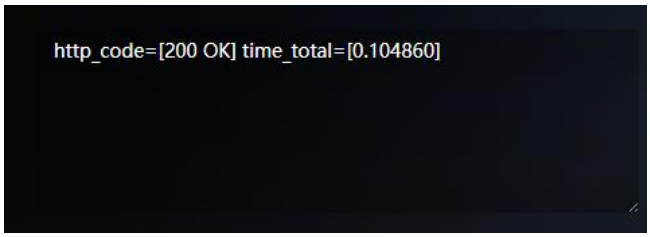


Table7-3 HTTP/HTTPS Detection Results

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.

7.4 Packet Capture Tool

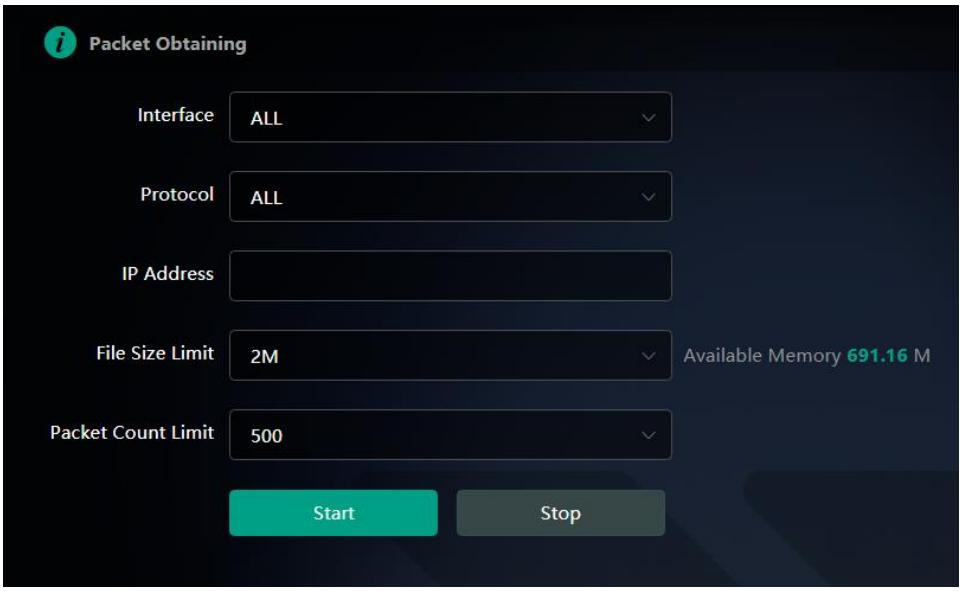
Smartphone View: Choose **More** > **Switch to PC view** > **More** > **Diagnostics** > **Packet Obtaining**.

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.


Packet Obtaining
Interface
ALL
Protocol
ALL
IP Address
File Size Limit
2M
Available Memory 691.16 M
Packet Count Limit
500
Start
Stop

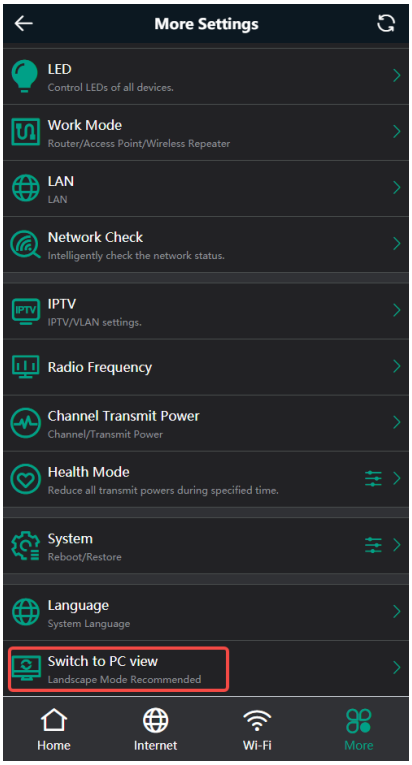
8 System Settings

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 smartphone.

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 System Logs

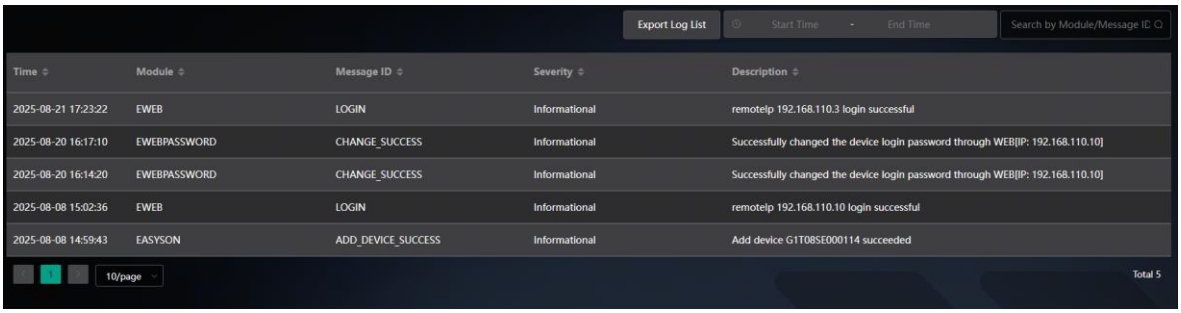
For medium to large-scale network projects, network administrators often use third-party software to interface with all devices, monitoring system metrics and identifying any abnormal behavior to ensure system health and security. Devices usually support network management protocols such as SNMP and Syslog for seamless integration.

8.2.1 Viewing System Logs

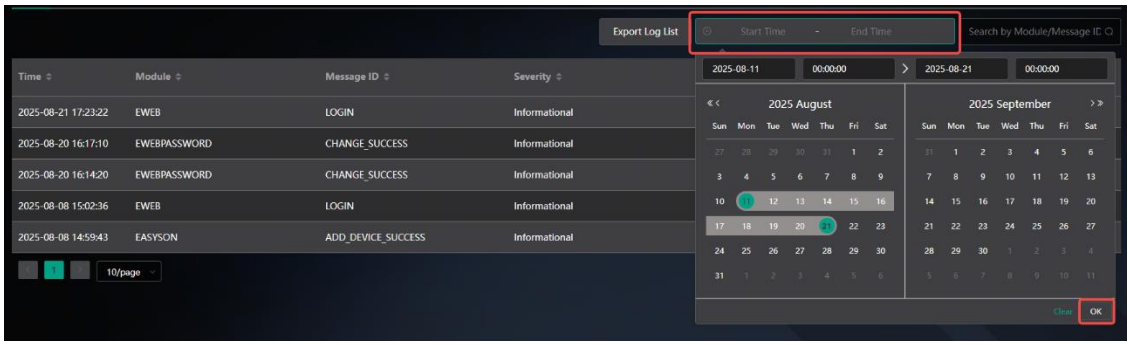
Smartphone View: Choose More > Switching to PC View > More > System > Syslog > View Log.

PC View: Choose More > System > Syslog > View Log.

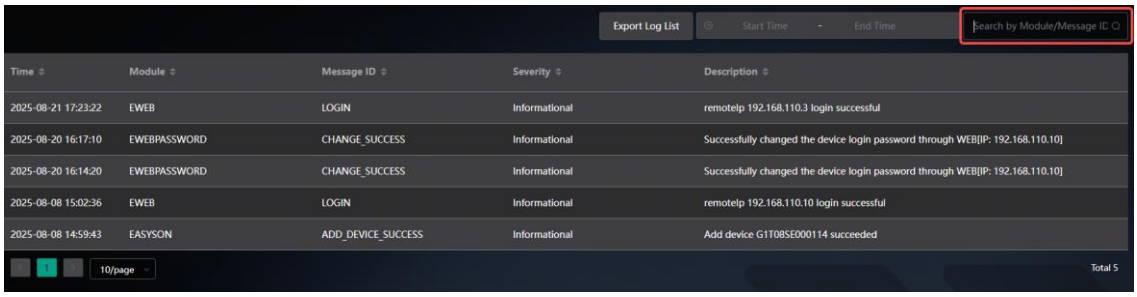
The **Log List** displays the operation logs of the local device. You can filter the logs by specific dates or modules on the **View Log** page. You can also export the log list and log files to your local system for storage, viewing, or backup.



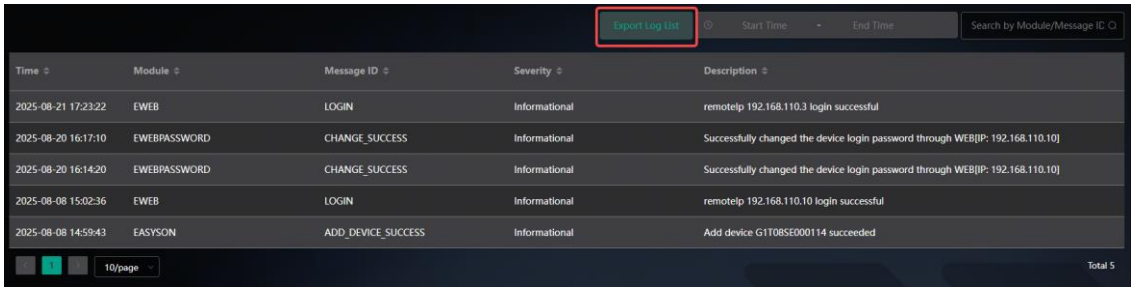
- To view logs for a specific date, click **Start Time**, select the start and end time, and then click **OK** to filter the logs accordingly.



- To view the logs of a specific module, enter the module name in the search box to access its operation logs.



- To export the log list, click **Export Log List** to download the log list in .csv format for viewing on your computer.



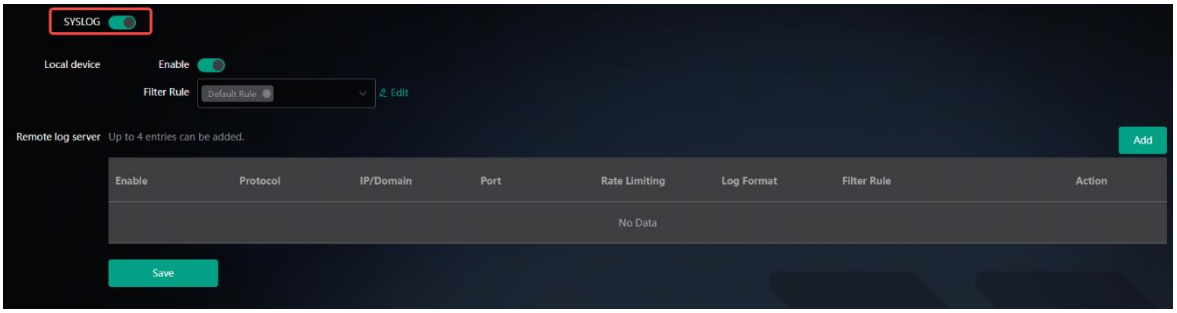
8.2.2 Configuring System Logs

Smartphone View: Choose More > Switching to PC View > More > System > Syslog > View Log.

PC View: Choose More > System > Syslog > View Log.

1. Enabling Syslog

Toggle on **SYSLOG** to enable the SYSLOG protocol. When enabled, the device can connect with a remote log server to send log information over the network.

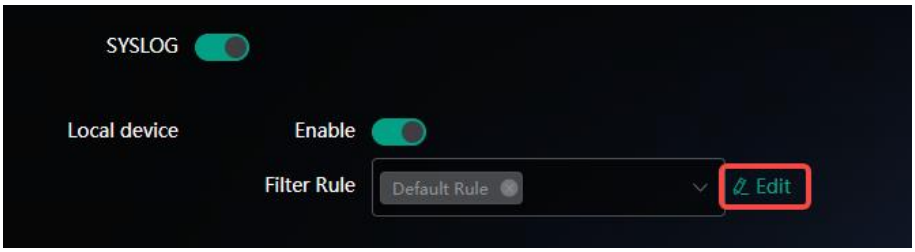


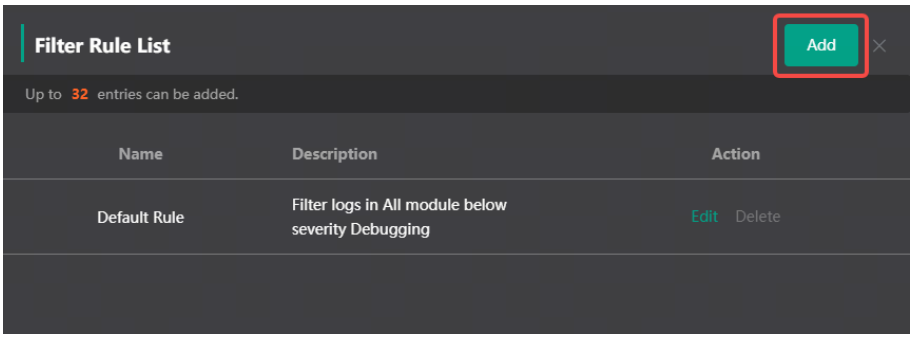
2. Configuring Local Logs

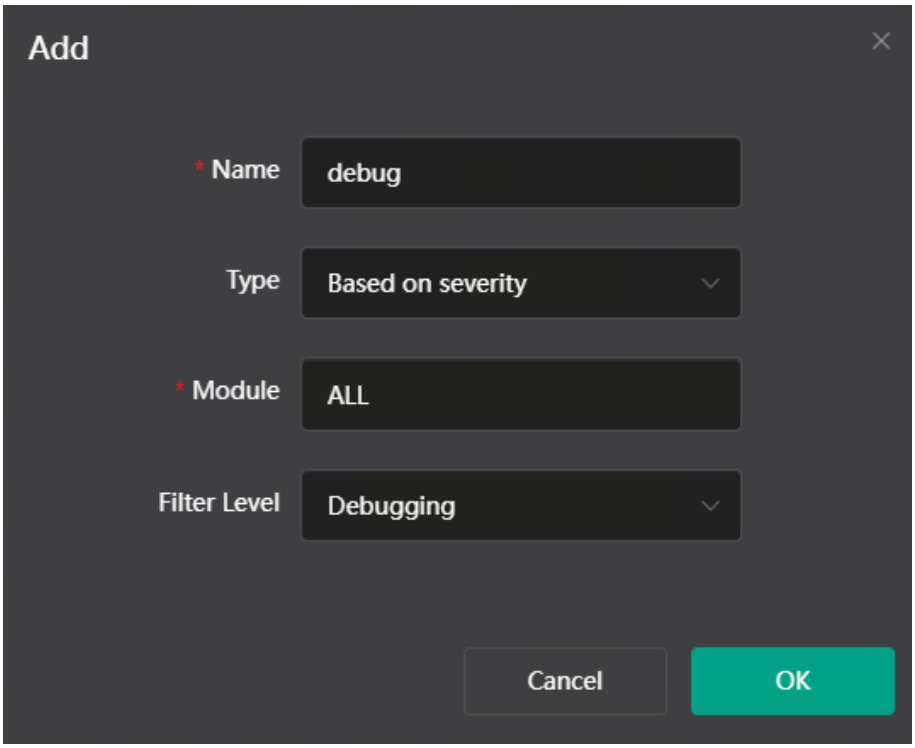
Local log saving is enabled by default. Click **Edit**, and then **Add** to create filtering rules for device operation logs, allowing you to exclude certain operation logs (like debug messages from all modules) from being displayed in the log list.

Caution

When local log saving is disabled, all actions performed on the device will no longer be displayed in the log list. Please exercise caution.

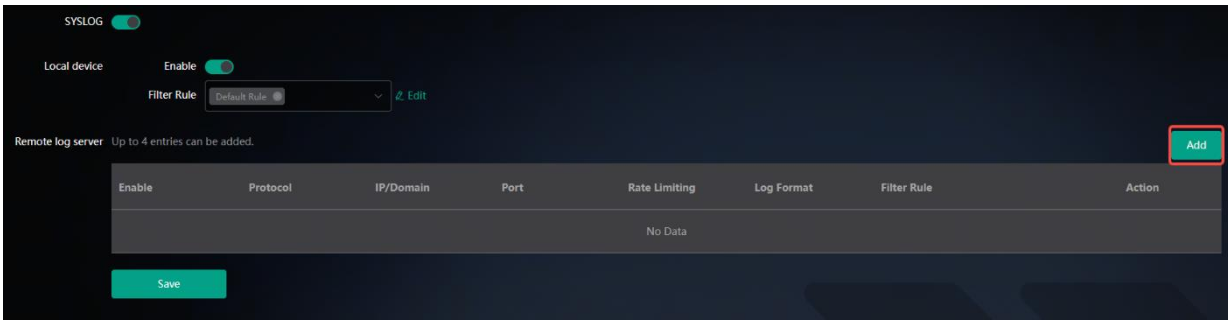






3. Configuring Remote Log Server

Click **Add** next to the **Remote log server** to add basic information of the remote log server.



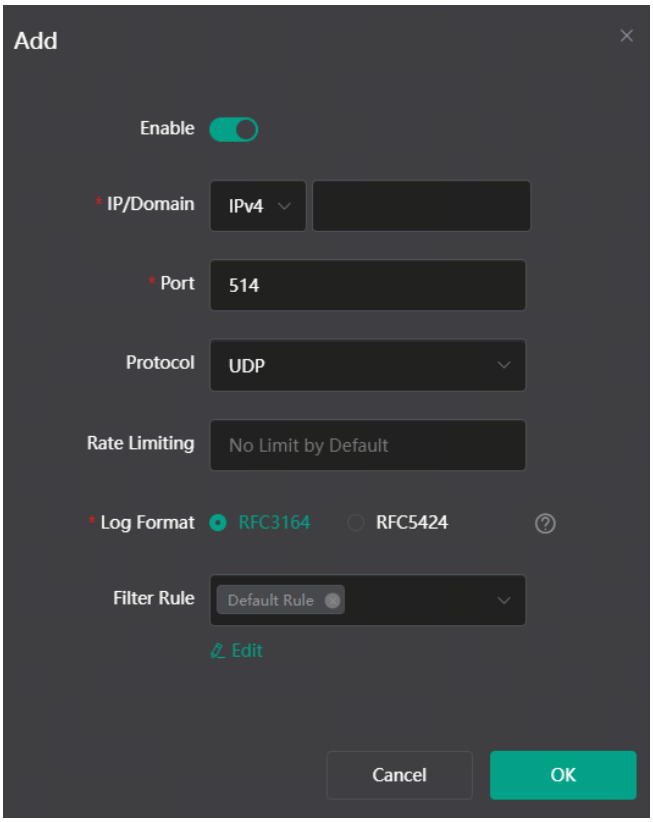


Table8-1 Remote Log Server Configuration Parameters

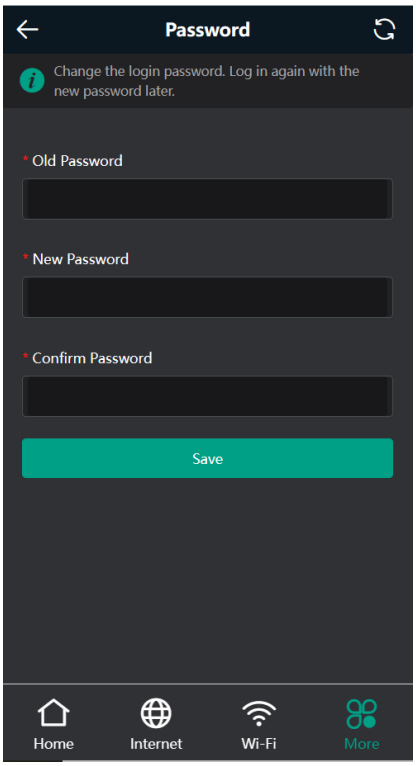
Parameter	Description	Default Value
Enable	Enable or disable the remote log server. When enabled, the device will send its operation logs to the remote log server.	Enabled
IP/Domain	IP address or domain name of the remote log server. The IP address can be an IPv4 or IPv6 address.	N/A
Port	Port number of the remote log server.	514
Protocol	Protocol for communication between the device and the remote log server. Currently only UDP is supported.	UDP
Rate Limiting	The highest rate at which the device can send log data to the remote log server.	No limit
Log Format	The format of logs sent to the remote log server. RFC3164: <Priority> second-level local time Hostname Module Name % Message Identifier: Log Message. RFC5424: <Priority> microsecond-level UTC time Hostname Module % Process ID Message Identifier - Log Message.	RFC3164
Filter Rule	Rules for filtering device operation logs. Any logs that are filtered out will not be sent to the remote log server.	default is selected.

8.3 Configuring the Login Password

Smartphone View: Choose **More** > **System** > **Password**.

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

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

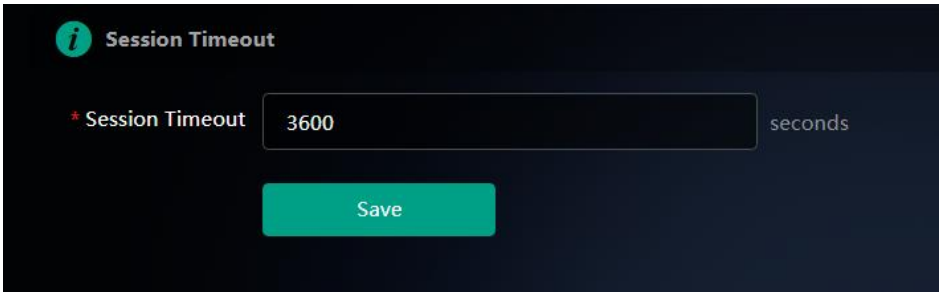


8.4 Configuring Session Timeout Duration

Smartphone 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.



8.5 Remote Access

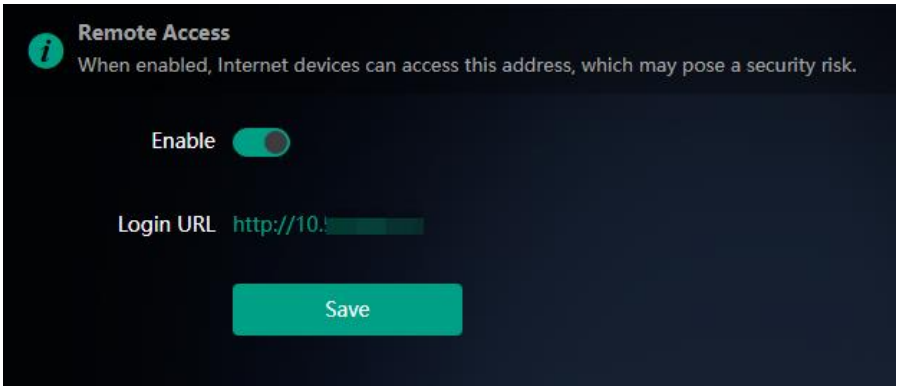
Smartphone View: Choose **More** > **Switching to PC View** > **More** > **System** > **Login** > **Remote Access**.

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

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

Caution

- This 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 8.3 Configuring the Login Password to configure a strong and secure device management password.



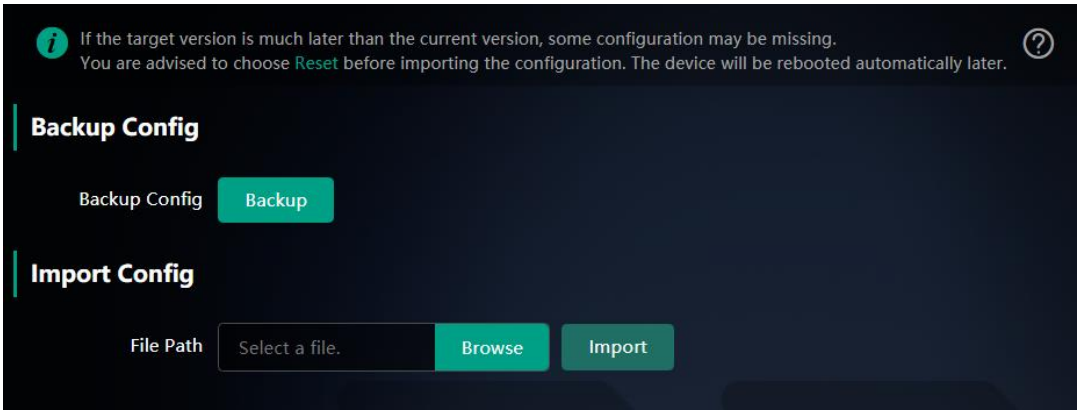
8.6 Configuring Backup and Import

Smartphone 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.



8.7 Restoring Factory Settings

Smartphone 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.

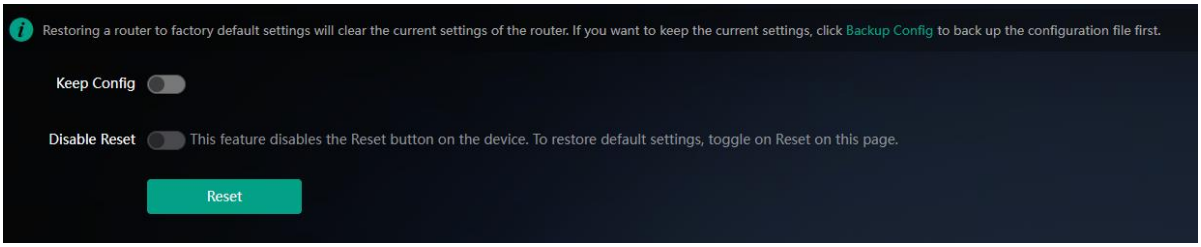
Click **Reset** to restore factory settings.

Caution

- If the **Disable 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, it is possible that the SSID of the primary router is restored to factory defaults (the default SSID can be found on the bottom label of the router), while the SSID of the secondary router is not restored to factory defaults. You can hold down the Reset button of the secondary router for more than 10 seconds to restore it to factory defaults.

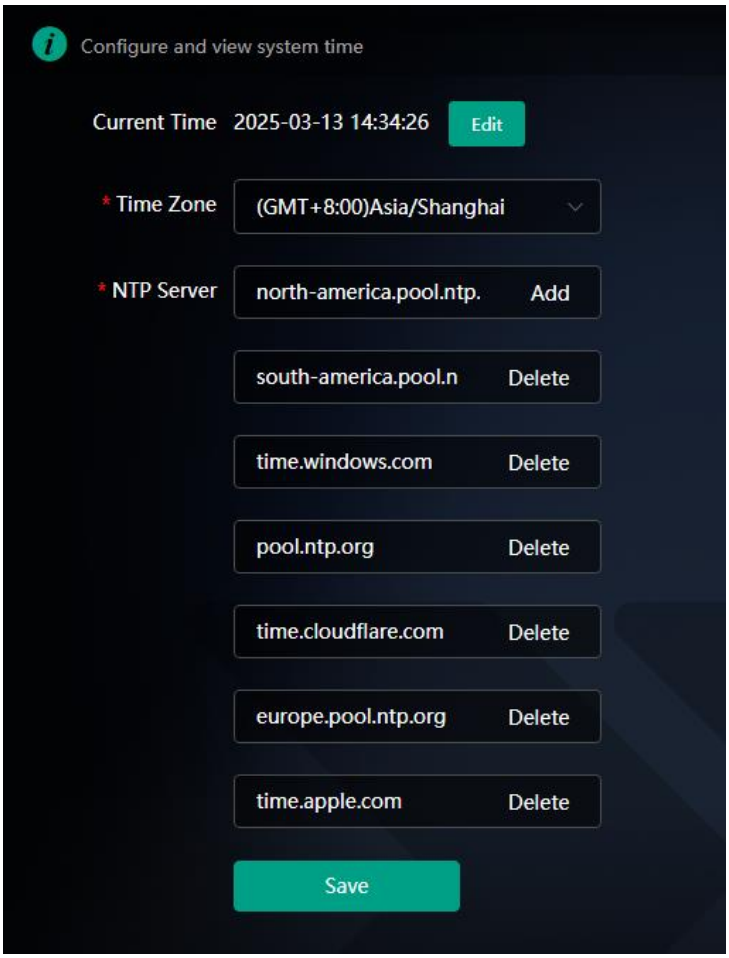


8.8 Configuring System Time

Smartphone 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.

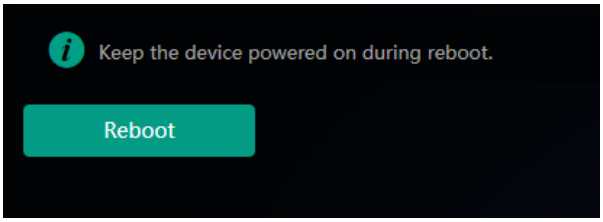


8.9 Configuring Reboot

Smartphone View: Choose **More** > **System** > **Reboot** > **Reboot**.

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

Click **Reboot**, and the device will be restarted. Please do not refresh or close the page during the reboot process. After the device is rebooted, the browser will be redirected to the login page.



8.10 Configuring Scheduled Reboot

8.10.1 Getting Started

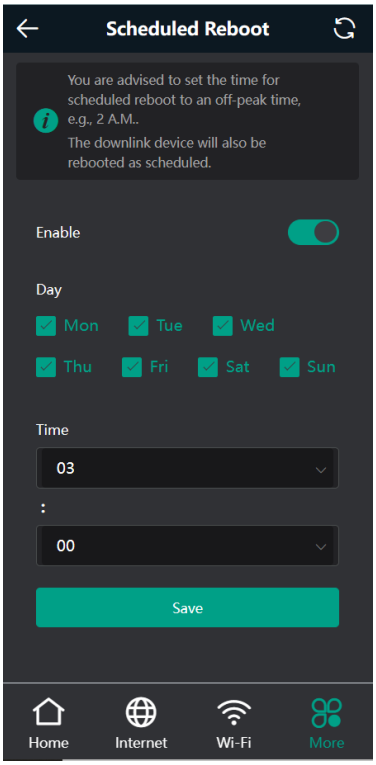
Confirm that the system time is accurate to avoid network interruption caused by device reboot at the wrong time. For details, see 8.8 Configuring System Time.

8.10.2 Configuration Steps

Smartphone 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.



8.11 Performing Online Upgrade and Displaying the System Version

Smartphone View: Choose **More** > **System** >**Online Upgrade**.

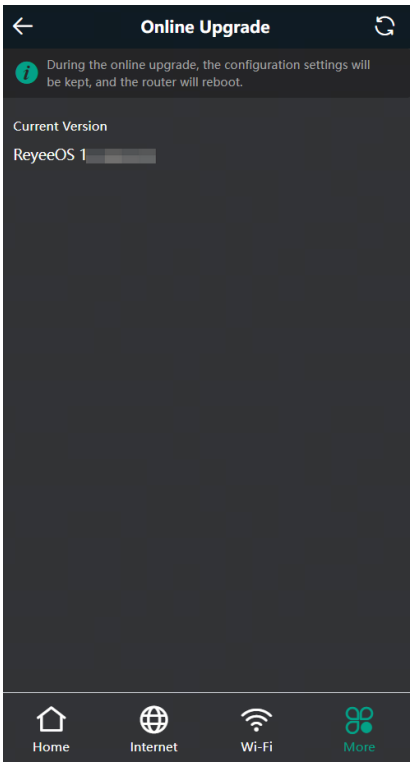
PC View: Choose More > System > Upgrade > Online Upgrade.

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.

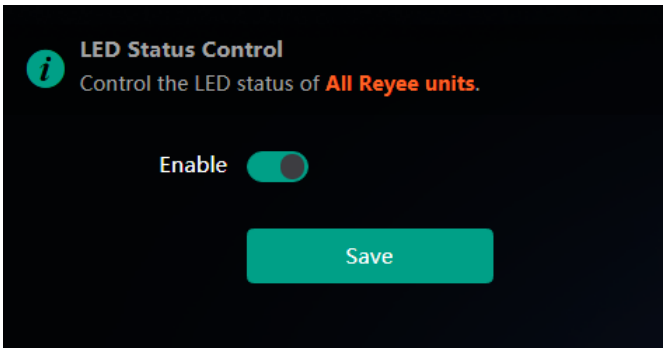
If no new version is detected and online upgrade cannot be performed, check whether the DNS is correctly obtained or go to **More** > **Advanced** > **Local DNS** to set the DNS server for the router.



8.12 Turning On/Off the Indicator

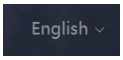
Smartphone View: Choose **More** > **LED**

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

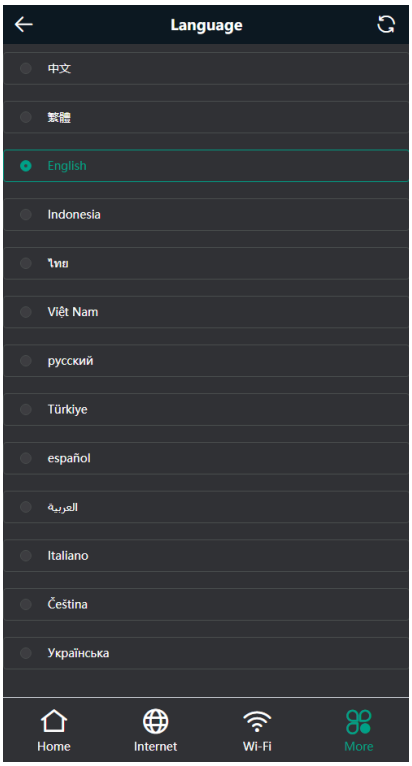


8.13 Switching System Language

Smartphone View: Choose **More** > **Language**.

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

Click a required language to switch the system language.



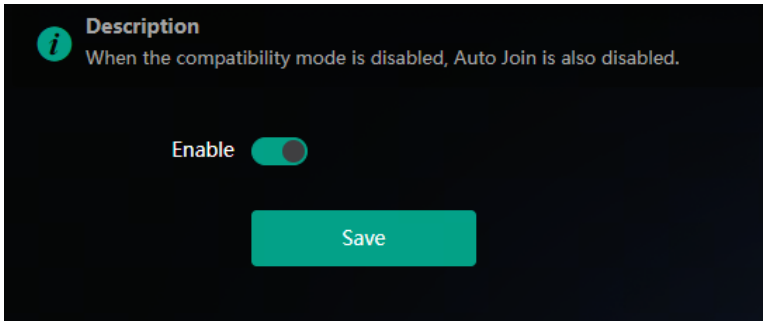
8.14 Configuring the Compatibility Mode

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

PC View: Choose More > System > Compatibility Mode.

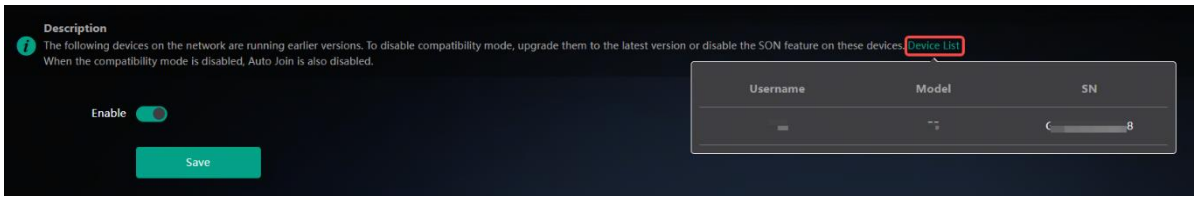
Enabling compatibility mode can improve interoperability between devices running the early and latest versions during networking. If the compatibility mode is disabled, **Auto Join** will be disabled as well.

- 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 8.11 Performing Online Upgrade and Displaying the System Version.



8.15 Configuring Cloud Service

8.15.1 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.

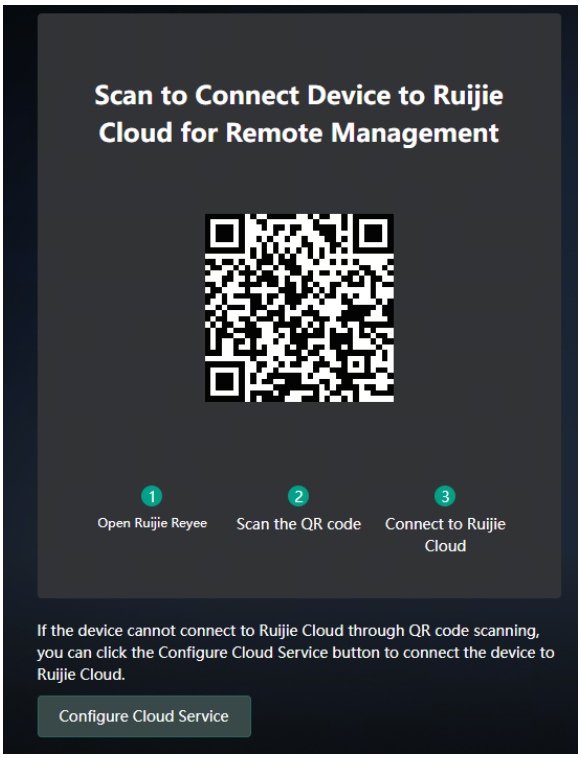
By configuring Cloud Service, you can conveniently mange networks through Ruijie Cloud or the Ruijie Reyee app.

8.15.2 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.

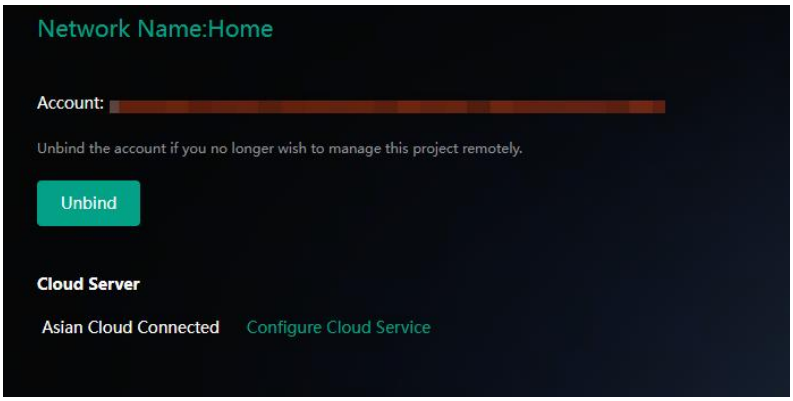


If the device cannot connect to Ruijie Cloud through QR code scanning you can click the **Configure Cloud Service** button to connect the device to Ruijie Cloud.

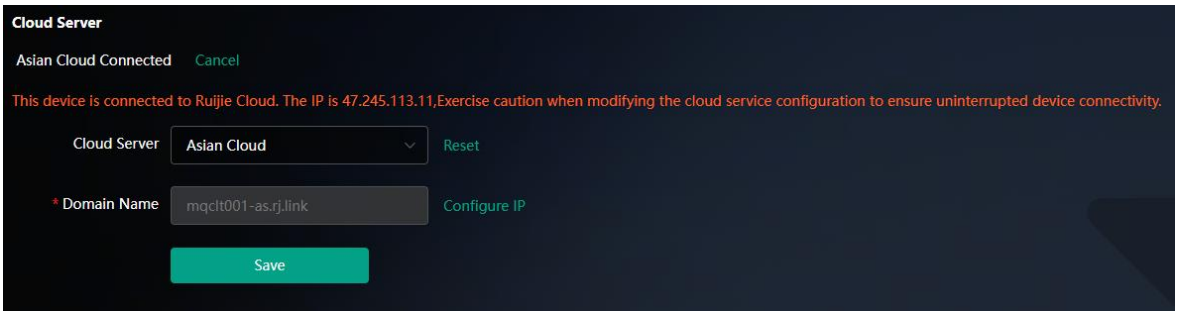
Once the device is associated with a cloud account, it will automatically be bound to a cloud server based on its geographic location.

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**.

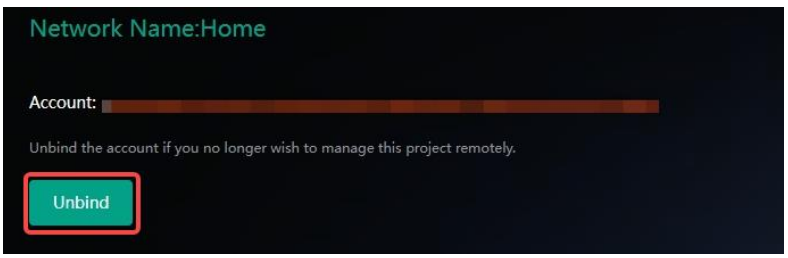


8.15.3 Unbinding Cloud Service

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.



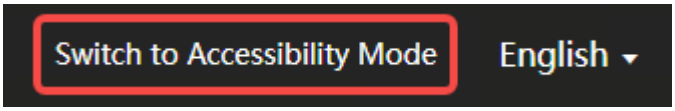
8.16 Switching to Accessibility Mode

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.



8.17 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.

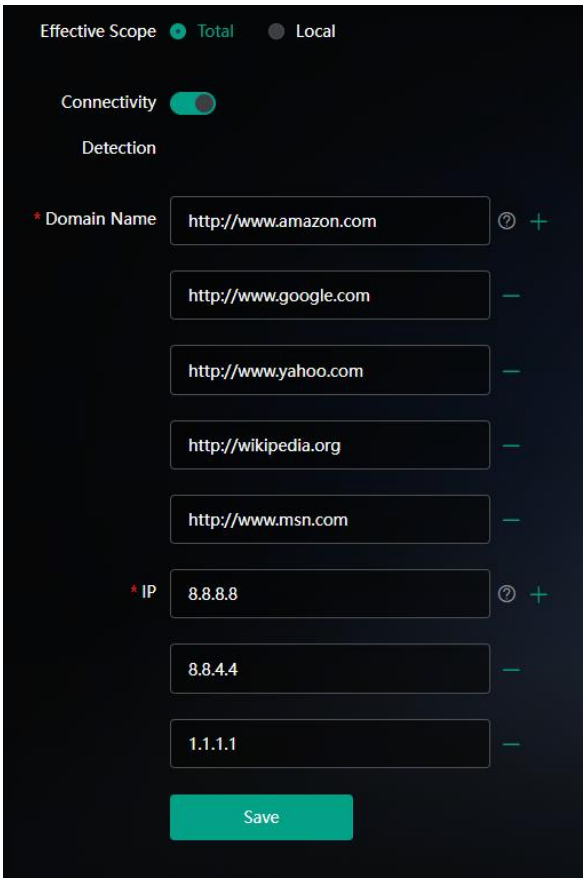


Table8-2 Connectivity Detection Configuration

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 FAQs

9.1 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.

9.2 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.

9.3 How Do I Manage the Router When Used As a Range Extender After Installation is Successful?

You are advised to connect your PC or smartphone to the device's Wi-Fi network. Then, open a browser and enter **192.168.110.1** in the address bar to access the router's web interface.

If you are unable to access the router's web interface using the default IP address, you can use the alternative methods specified in 3.5 Managing the Device After Successful Setup.

9.4 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

10 Appendix

10.1 User Ports

Table10-1 Default Open Port Information

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

10.2 User Privacy Log

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