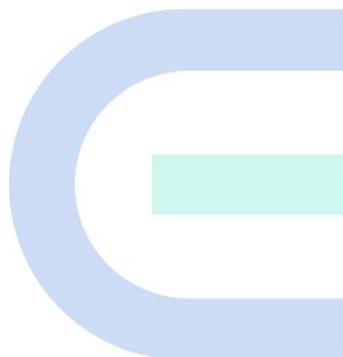


# Ruijie Reyee RG-EW7200BE PRO Wi-Fi Router

ReyeeOS 1.309 Configuration Guide



## Copyright

Copyright © 2024 Ruijie Networks

All rights are reserved in this document and this statement.

Any reproduction, excerpt, 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

- Official website of Ruijie Reyee: <https://reyee.ruijie.com>
- Technical Support Website: <https://reyee.ruijie.com/en-global/support>
- Case Portal: <https://www.ruijenetworks.com/support/caseportal>
- Community: <https://community.ruijenetworks.com>
- Technical Support Email: [service\\_rj@ruijenetworks.com](mailto:service_rj@ruijenetworks.com)
- Online Robot/Live Chat: <https://reyee.ruijie.com/en-global/rita>

## Conventions

### 1. GUI Symbols

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

### 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 .....	1
1 Quick Setup (As a Primary Router).....	1
1.1 Getting Started.....	1
1.2 Connecting to the Router.....	1
1.3 Logging In .....	2
1.4 Configuration Steps .....	3
1.4.1 Configuring the Internet Connection Type.....	3
1.4.2 Configuring a Wi-Fi Network.....	5
1.4.3 Configuring IoT Wi-Fi .....	8
2 Quick Setup (As a Secondary Router).....	11
2.1 Getting Started.....	11
2.2 Connecting to Primary Router .....	11
2.2.1 Wired Connection .....	11
2.2.2 Wireless Connection .....	12
2.3 Verification and Testing .....	17
2.4 Manage the Device After Successful Setup.....	17
3 Wi-Fi Network Settings.....	19
3.1 Adding Wi-Fi Networks .....	19
3.1.1 Adding Game Wi-Fi Network .....	19
3.1.2 Adding Other Types of Wi-Fi Networks.....	19
3.2 Changing the SSID and Password.....	20
3.3 Enabling Band Steering .....	21
3.4 Hiding the SSID .....	22

3.4.1 Overview .....	22
3.4.2 Getting Started.....	22
3.4.3 Configuration Steps .....	22
3.5 Wi-Fi Advanced Settings .....	23
3.6 Configuring the Wi-Fi Blocklist or Allowlist .....	25
3.6.1 Overview .....	25
3.6.2 Configuration Steps .....	25
3.7 Configuring the Radio Frequency.....	27
3.7.1 Overview .....	27
3.7.2 Getting Started.....	27
3.7.3 Configuration Steps .....	27
3.8 Configuring the Healthy Mode .....	30
3.9 Enabling Roaming Optimization .....	31
3.10 Configuring Wi-Fi/IGMP.....	31
3.10.1 Overview .....	31
3.10.2 Configuration Steps .....	32
3.11 Configuring Preamble Puncturing.....	32
4 Configuring Work Mode .....	33
4.1 Access Point .....	33
4.2 Wireless Repeater .....	34
5 Configuring Network Settings .....	36
5.1 Configuring Internet Connection Types.....	36
5.2 Configuring WAN Settings .....	37
5.2.1 Configuring Internet connection types .....	37

5.2.2 Changing the MAC Address .....	38
5.2.3 Modifying MTU .....	39
5.2.4 Configuring a Private Line .....	39
5.2.5 Configuring the VLAN Tag .....	40
5.2.6 Configuring Load Balancing Settings .....	40
5.3 Changing the Address of a LAN Port .....	41
5.4 Connecting to IPTV.....	42
5.4.1 Getting Started.....	42
5.4.2 IPTV Configuration Steps (VLAN Type) .....	42
5.5 Configuring IPv6 .....	43
5.5.1 Configuring the IPv6 of the WAN Port .....	43
5.5.2 Configuring the IPv6 of the LAN Port .....	44
5.6 Configuring Auto Bandwidth Control .....	45
5.7 Client Management.....	48
5.7.1 Setting Blocking Schedules .....	48
5.7.2 Viewing Number of Connections for Clients .....	49
5.8 Configuring DHCP Server.....	50
5.8.1 Overview .....	50
5.8.2 Configuration Steps .....	51
5.9 Configuring DNS Server .....	53
5.9.1 Local DNS Server .....	53
5.9.2 Configuring DNS Proxy.....	53
5.10 Configuring Port Mapping .....	54
5.10.1 Overview .....	54

5.10.2 Getting Started.....	54
5.10.3 Configuration Steps .....	54
5.10.4 Verification and Testing.....	55
5.10.5 Solution to a Test Failure .....	55
5.10.6 DMZ Configuration Steps .....	56
5.11 Configuring DDNS .....	56
5.11.1 Overview .....	56
5.11.2 Getting Started .....	56
5.11.3 Configuration Steps.....	56
5.12 Configuring Connectivity Detection .....	57
5.13 Enabling CWMP.....	58
5.14 Configuring APR Binding .....	59
5.14.1 Overview .....	59
5.14.2 Configuration Steps .....	59
5.15 Link Aggregation .....	60
5.16 Configuring Static Routing .....	60
5.17 Policy-based Routing.....	62
5.18 Configuring Game Port Guarantee.....	64
5.19 Enabling Smart Flow Control .....	65
5.19.1 Enabling Smart Flow Control.....	65
5.19.2 Custom Policy .....	66
5.20 Enabling Port-Based Flow Control .....	67
5.21 Enabling Hardware Acceleration .....	67
5.22 Enabling Reyee Mesh.....	68

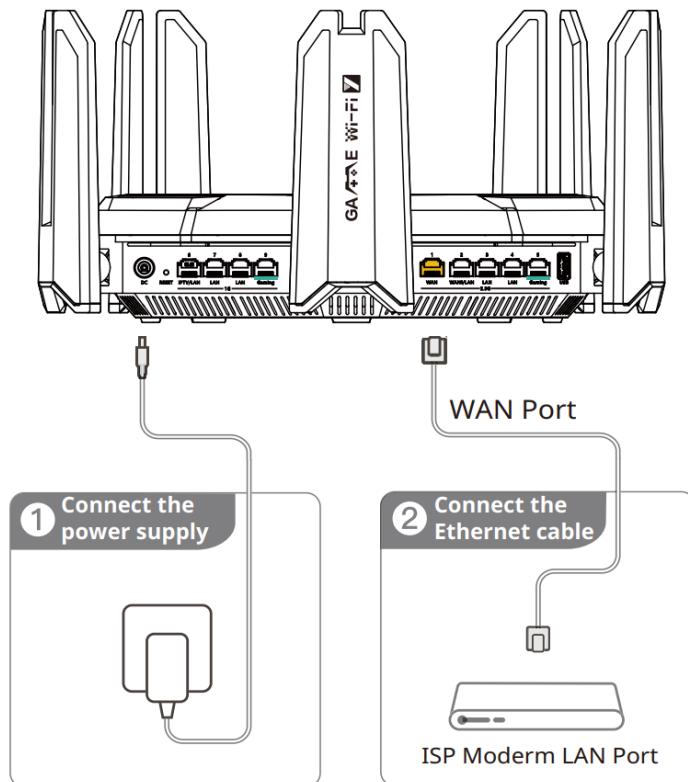
5.23 Configuring UpnP.....	68
5.23.1 Overview .....	68
5.23.2 Configuration Steps .....	68
5.24 Enabling Wi-Fi Switch.....	69
5.25 Configuring Reyee Mesh 3.0 .....	69
5.25.1 Configuration Steps .....	69
5.26 Switching to AP Mode.....	73
5.27 Other Settings .....	74
6 Storage Management.....	75
6.1 Enabling Samba.....	75
6.2 Accessing Samba Shared Files on a Windows Client .....	76
6.3 Accessing Samba Shared Files on an iOS Client .....	77
6.4 Accessing Samba Shared Files on a Linux Client .....	79
7 System Settings .....	81
7.1 Switching to PC View.....	81
7.2 Configuring the Login Password.....	81
7.3 Configuring Session Timeout Duration.....	82
7.4 Remote Access.....	82
7.5 Restoring Factory Settings .....	83
7.6 Configuring Config Backup and Import.....	84
7.7 Configuring System Time .....	84
7.8 Configuring Scheduled Reboot.....	85
7.8.1 Getting Started.....	85
7.8.2 Configuration Steps .....	85

7.9 Performing Online Upgrade and Displaying the System Version .....	86
7.10 Turning On/Off the Indicator .....	87
7.11 Switching System Language .....	87
7.12 Configuring Diagnostics.....	88
7.12.1 Network Check.....	88
7.12.2 Alerts .....	89
7.12.3 Network Diagnosis Tools.....	90
8 FAQs.....	93
8.1 How Do I Restore the Router to Factory Settings? .....	93
8.2 What Should I Do If I Forgot the Password? .....	93
8.3 How Do I Manage the Router When Used As a Range Extender After Installation is Successful? .....	93
8.4 What Should I Do If the System LED Keeps Flashing After the Router is Powered On? .....	93

# 1 Quick Setup (As a Primary Router)

## 1.1 Getting Started

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



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

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

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

## 1.2 Connecting to the Router

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.

- **Wired Connection**

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

- Wireless Connection

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

## 1.3 Logging In

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 device IP address in the address bar of the browser to navigate to the login page, and then enter the password to log in.

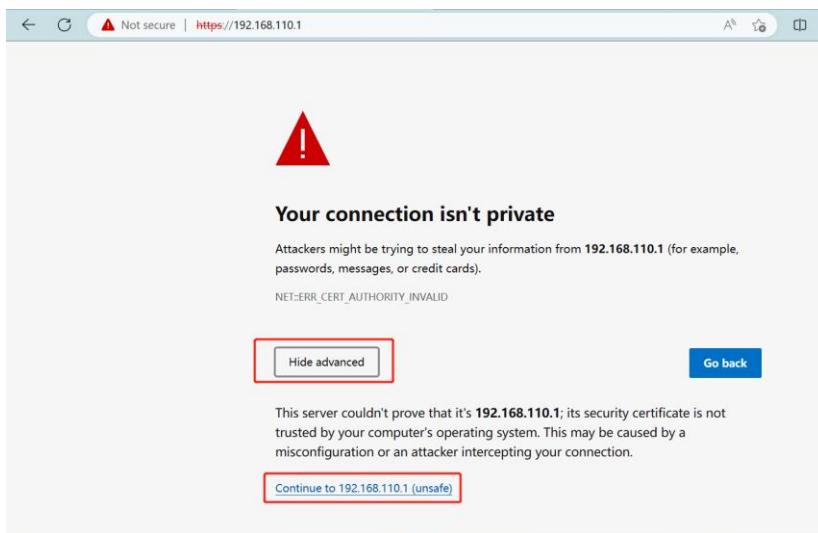
**Table 1-1 Default Configuration**

Item	Default Value
Device IP address (http or https)	192.168.110.1
Password	Password is not required at your first login. You can configure the router directly.

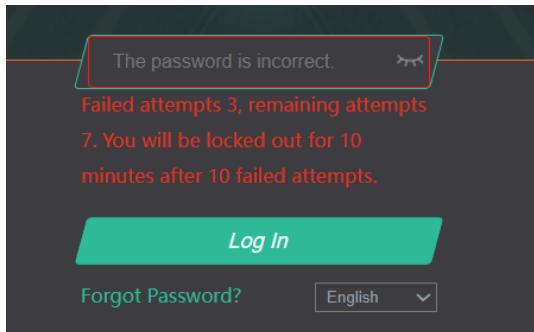
Enter the IP address of the router (default: 192.168.110.1) or <https://192.168.110.1> in the address bar of your browser, and press **Enter**. The login page is displayed.

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

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



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



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

### ⚠ Caution

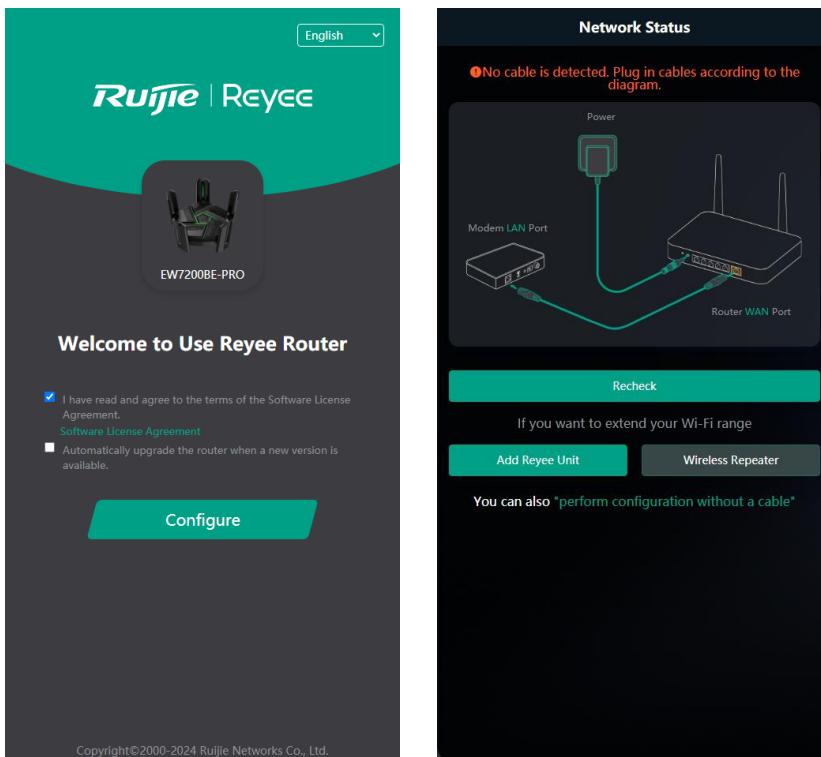
- Restoring factory settings will delete existing configuration. You will be required to configure Internet access again at your next login. Therefore, exercise caution when performing this operation.
- If you choose to retain the configuration while restoring the router to its factory settings, the router will be reset to its default configurations while retaining the network settings, Wi-Fi parameters, and time zone configuration.

## 1.4 Configuration Steps

### 1.4.1 Configuring the Internet Connection Type

Click **Configure** and select the Internet connection type confirmed by your local ISP.

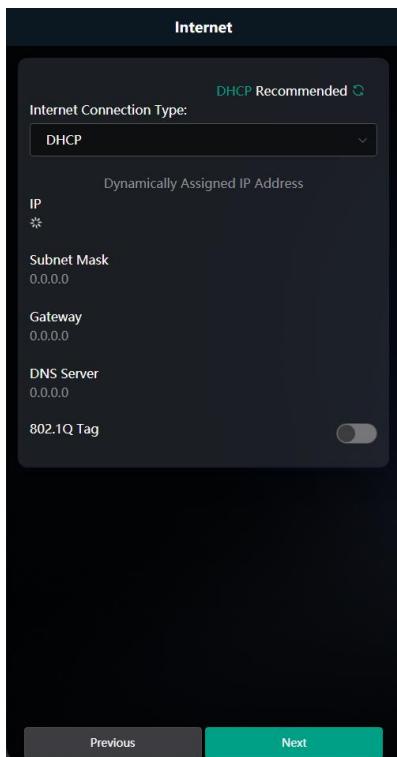
If the Ethernet cable is unplugged, you will be prompted to connect the Ethernet cable first. Click **perform configuration without a cable** below to connect the Ethernet cable.



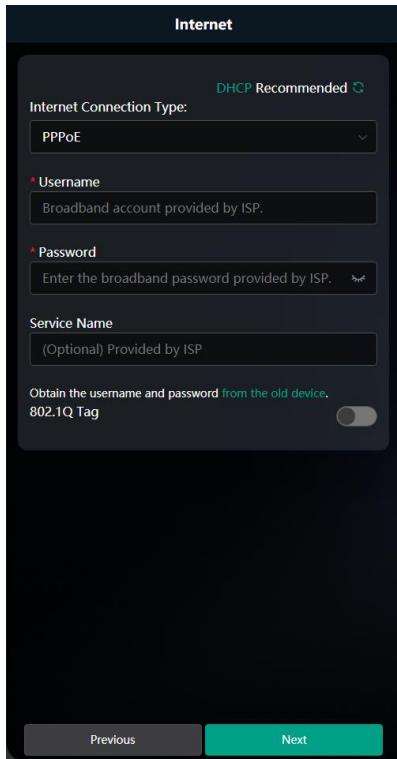
**⚠ Caution**

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.

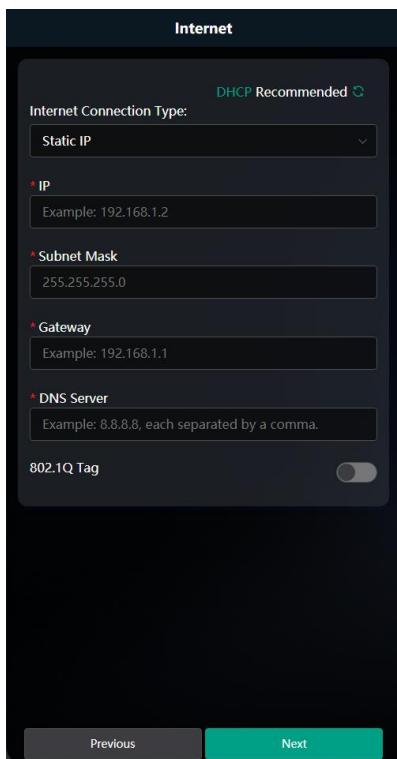
- **DHCP:** The router detects whether it can obtain an IP address from a DHCP server by default. If the router connects to the Internet successfully, you can click **Next** without entering an account.



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

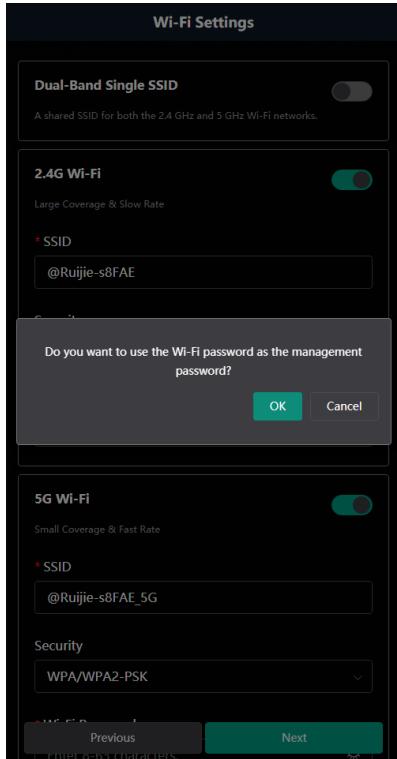


- **Static IP:** Enter the IP address, subnet mask, gateway, and DNS server, and click **Next**.

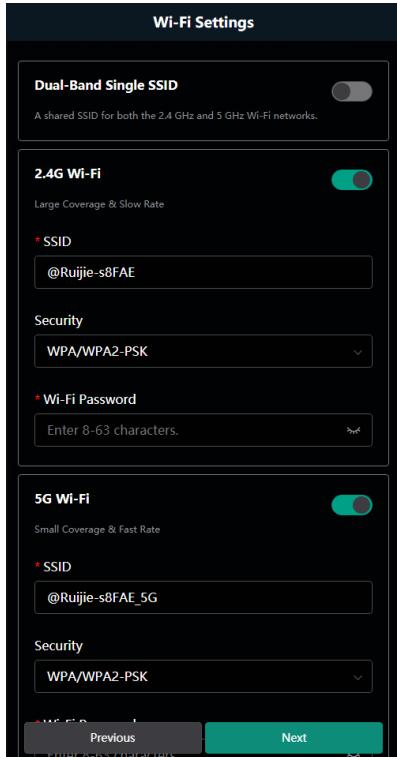


### 1.4.2 Configuring a Wi-Fi Network

- (1) Click **OK** to set the management password same as the Wi-Fi Password. Click **Cancel** to set a new management password on the **Wi-Fi Settings** page.



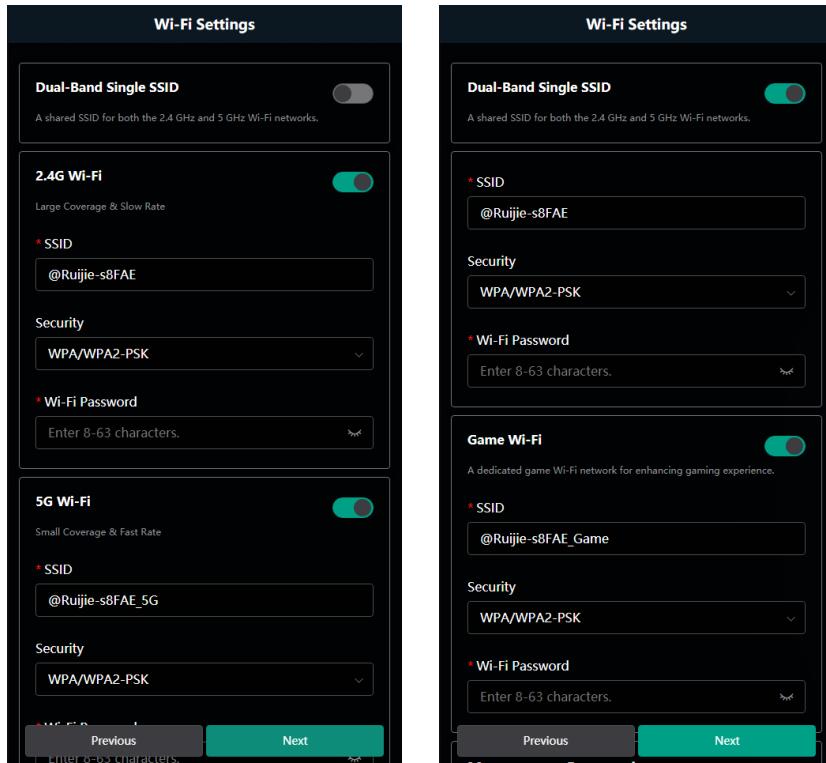
(2) On the **Wi-Fi Settings** page, you can set the network name and password for the host Wi-Fi network and Game Wi-Fi network.



- **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.

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.

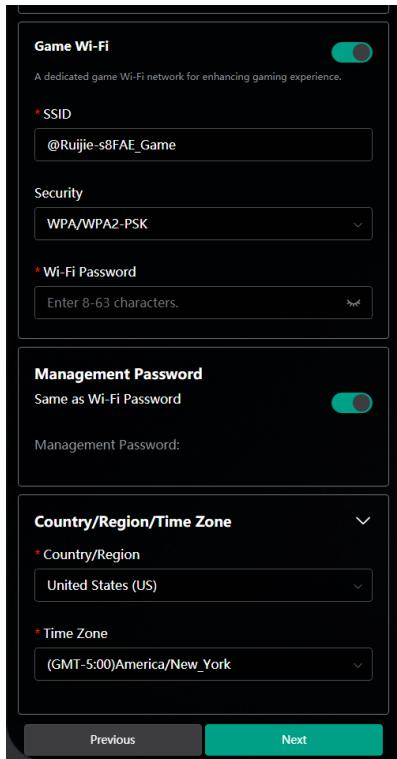
You can also enable **Dual-Band Single SSID**. The 5G-capable client will access 5G radio preferentially after the feature is enabled.



### 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.

- **Setting the SSID and Wi-Fi password:** The router has no Wi-Fi password by default, indicating that the Wi-Fi network is an open network. You are advised to configure a complex password to enhance the network security. The password must be a string of 8 to 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. The SSID (5G) is the name of the 5G radio. If **Dual-Band Single SSID** is enabled, set only one SSID.
- **Management Password:** Click **Same as Wi-Fi Password** to set the Management Password same as the Wi-Fi Password.
- **Setting the country or region:** The Wi-Fi channel may vary from country to country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.
- **Setting time zone:** Set the system time. The network time server is enabled by default to provide the time service. You are advised to select the actual time zone.



(3) Click **Next**.

### 1.4.3 Configuring IoT Wi-Fi

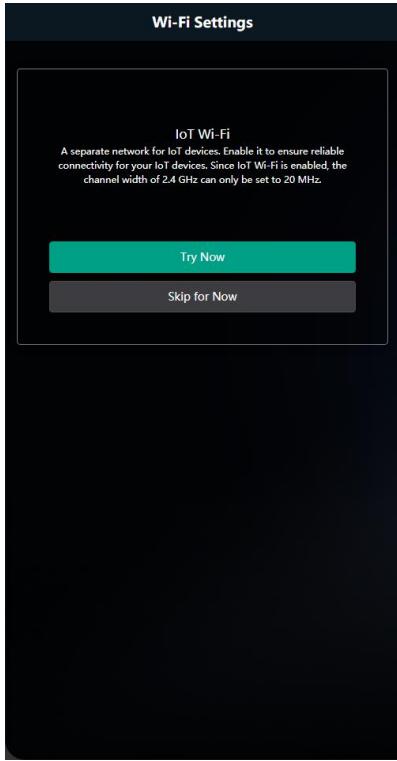
---

#### Note

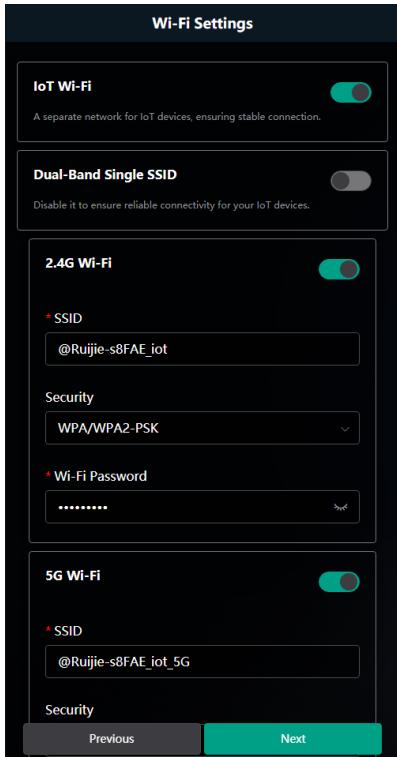
Only smart home devices supporting IEEE 802.11b/g standards can connect to the IoT Wi-Fi.

---

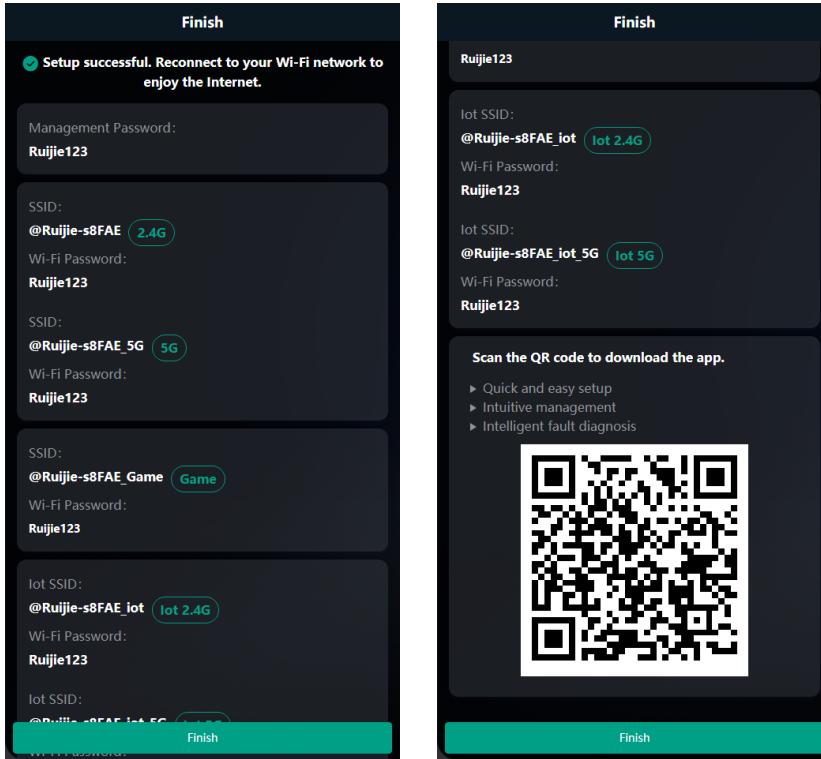
If IoT devices exist on the network, click **Try Now** to create a separate Wi-Fi network for IoT devices to ensure reliability of network connection. For details about Wi-Fi configuration, see [1.4.2 Configuring a Wi-Fi Network](#).



**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.



Click **Next**. Wait for a certain period of time for the settings to apply.



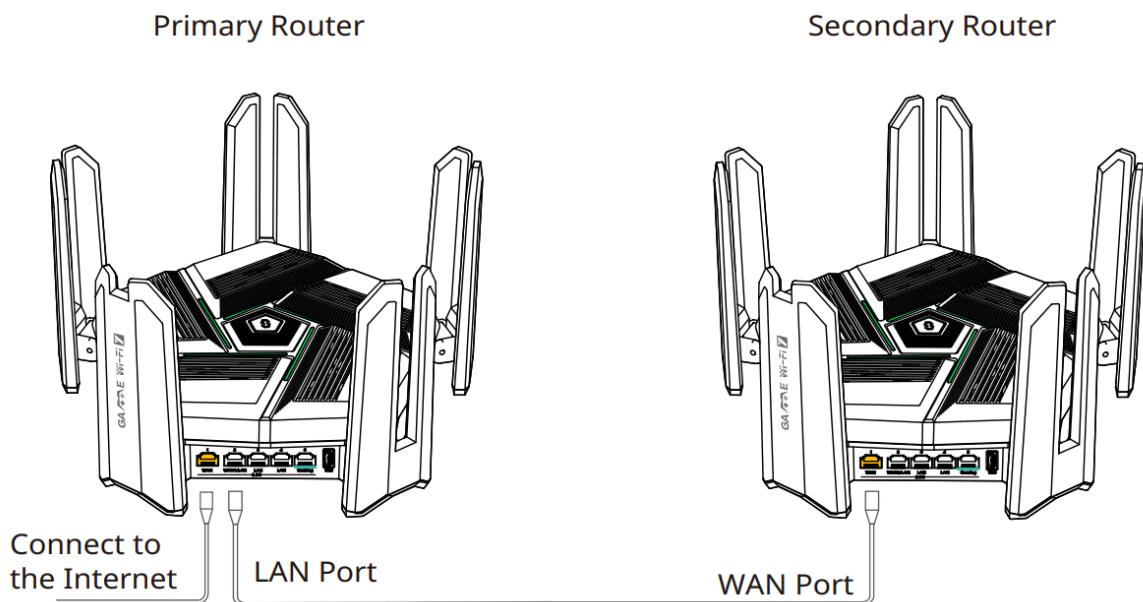
# 2 Quick Setup (As a Secondary Router)

## 2.1 Getting Started

- Before configuring this router as a secondary router, configure the primary router and verify that the primary router can access the Internet.
- The router supports both wireless and wired connection. If an Ethernet cable is available, you are advised to connect the secondary router to the primary router through wired connection.
- If no Ethernet cable is available, place the secondary router in a place where it can scan at least two-bar Wi-Fi signal of the primary router.

## 2.2 Connecting to Primary Router

### 2.2.1 Wired Connection



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

---

#### **i** Note

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

---

## 2.2.2 Wireless Connection

To use this router to wirelessly extend the Wi-Fi range of the primary router, simply connect this router to a power source.

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

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.

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

#### Caution

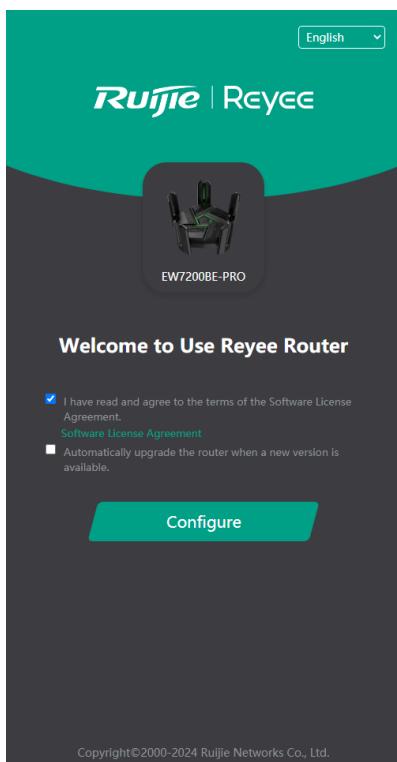
No Ethernet cable is required in the wireless repeater mode. The wireless network stability can be affected by many factors. Therefore, the wired connection is recommended.

### 2. Wireless Connection by Web configuration

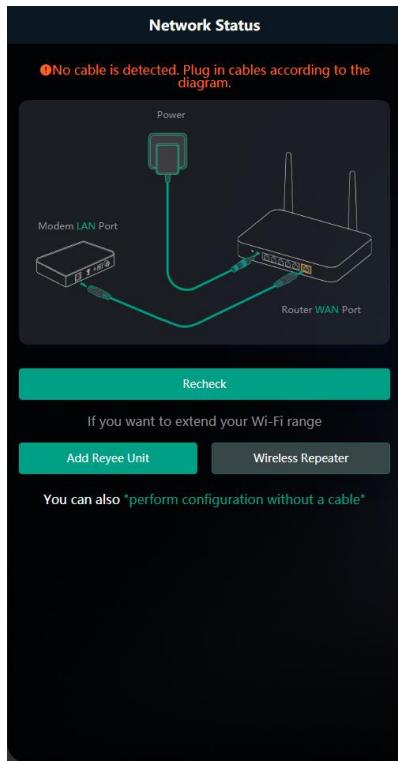
When the primary router is a non-Reyee Home Wi-Fi router, to wireless connect this router to the primary router, you can log in to its web interface and connect this router to the Wi-Fi network of the primary router.

Connect the router to a power source and log in to the web interface. For details, see [1.2 Connecting to the Router](#) and [1.3 Logging In](#).

- (1) Click **Configure**.

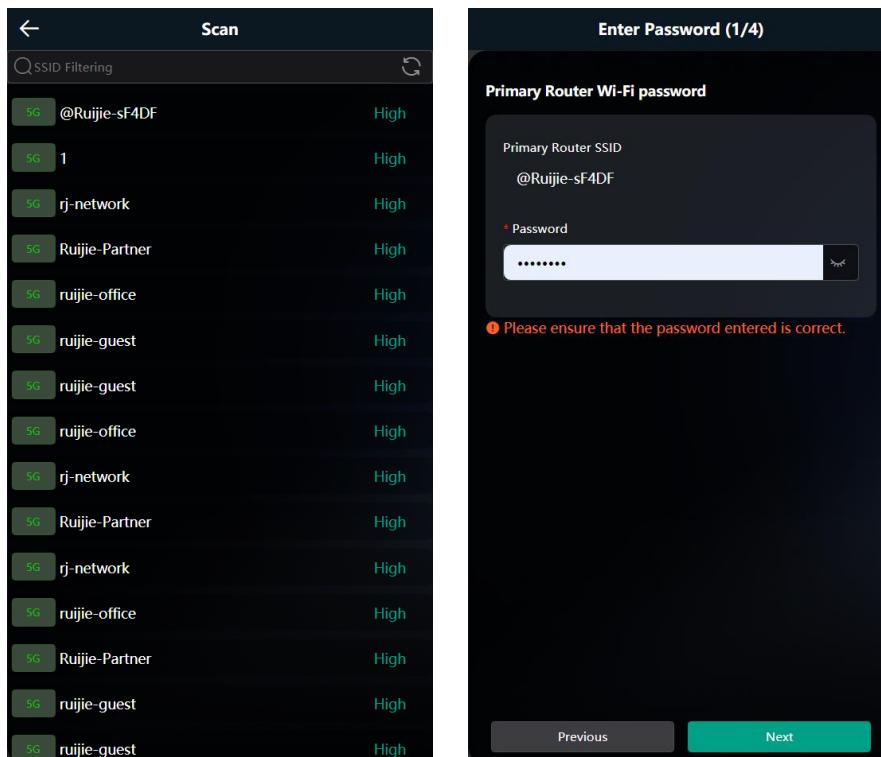


## (2) Select Wireless Repeater.

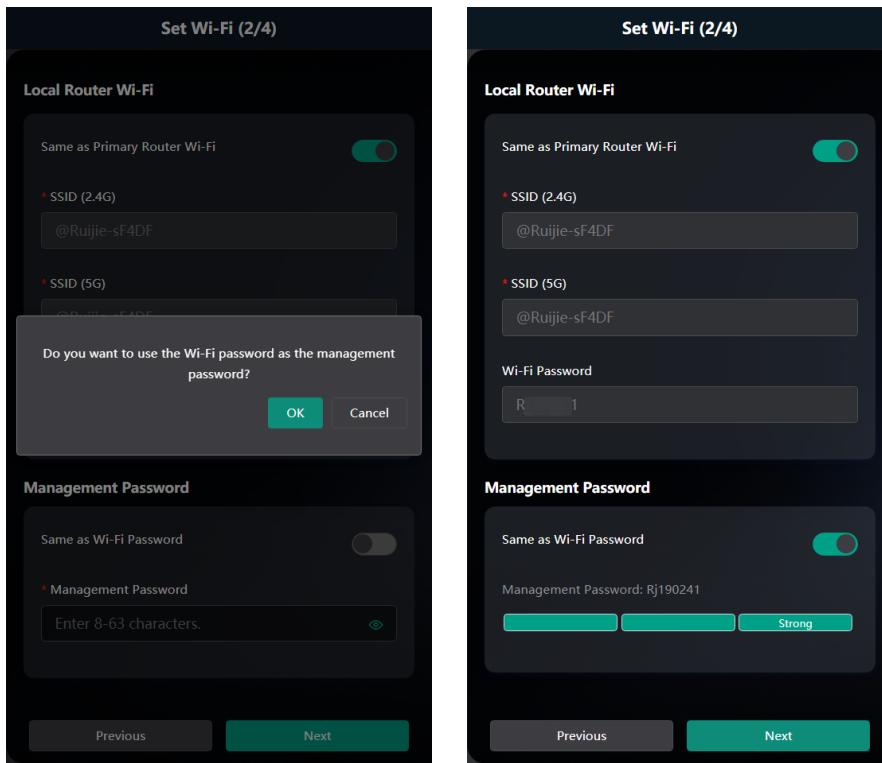


## (3) Select the SSID of the primary router, and enter the Wi-Fi password to connect to the primary router.

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

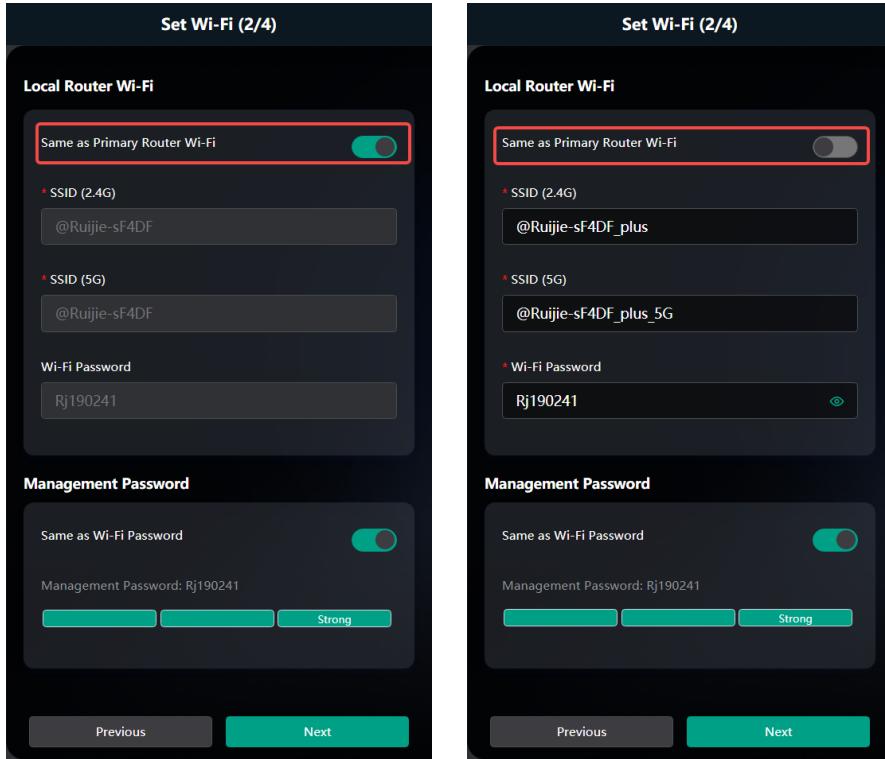


(4) Click **Next**. Click **OK** to set the management password same as the Wi-Fi Password. Click **Cancel** to set a new management password on the **Wi-Fi Settings** page.



(5) On the **Set Wi-Fi** page that opens, enter the Wi-Fi SSID and password:

- o You can toggle on **Same as Primary Router Wi-Fi**, in which the SSID and password will be same as the primary router Wi-Fi. If the primary router Wi-Fi is an open network, a separate management password should be set for the extender.
- o You can toggle off **Same as Primary Router Wi-Fi** to set a new Wi-Fi SSID and password for the extender.



## (6) Configuring IoT Wi-Fi

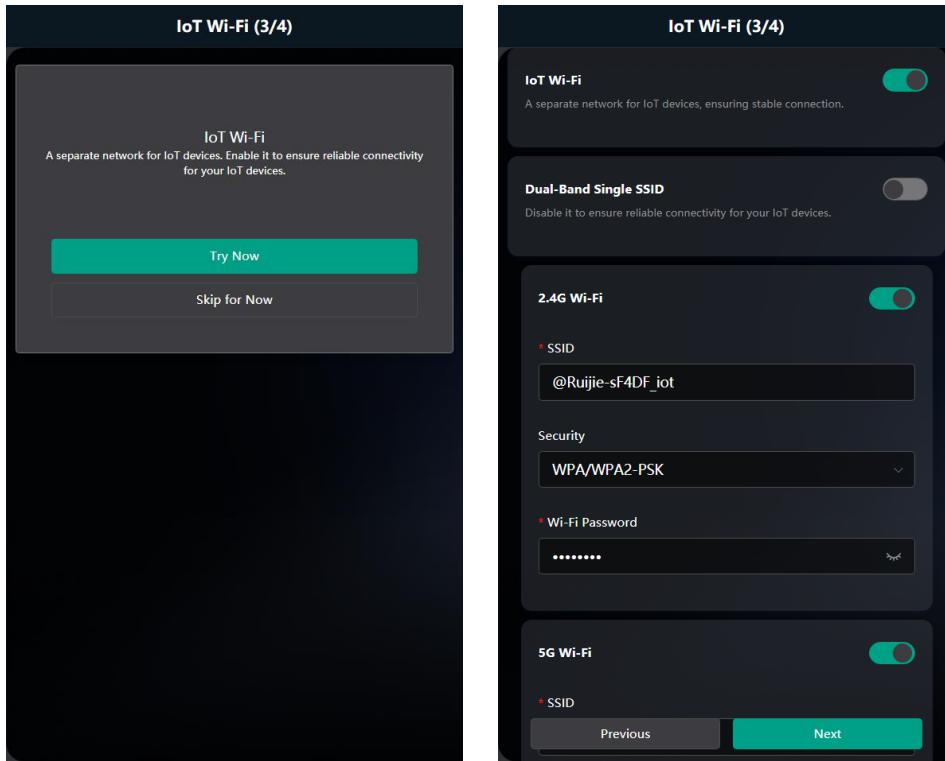
A separate network for IoT devices. Enable it to ensure reliable connectivity for your IoT devices.

### Note

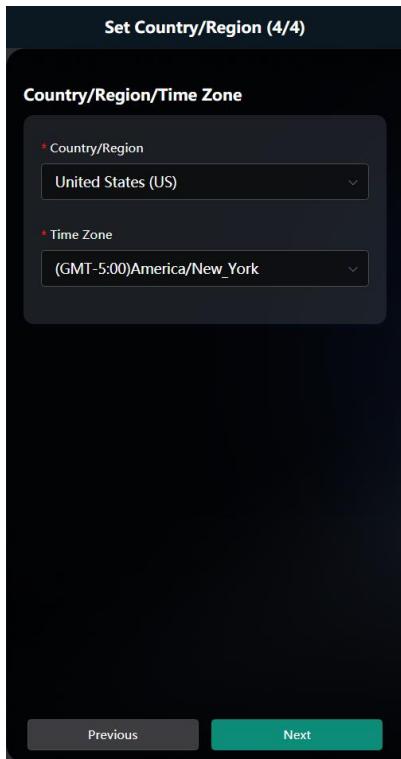
Only smart home devices supporting IEEE 802.11b/g standards can connect to the IoT Wi-Fi.

**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.

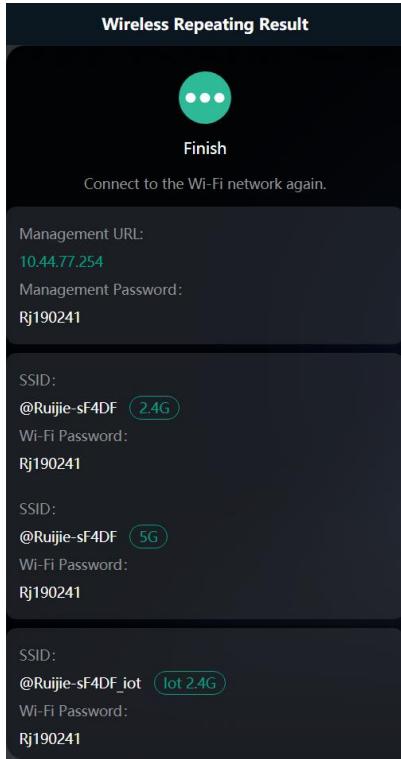
Click **Next**. Wait for a certain period of time for the settings to apply.



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



(8) Click **Next**.



## 2.3 Verification and Testing

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

## 2.4 Manage the Device After Successful Setup

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

### 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.

### 2. Logging In to the Web Interface

- Login using the default IP address

Enter the default IP address ([192.168.110.1](http://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:

- a Log in to the web interface of the primary router to find the current IP address of the router.

- b 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 [www.ireyee.com](http://www.ireyee.com) or reach out to customer service by emailing [service\\_rj@ruijienetworks.com](mailto:service_rj@ruijienetworks.com).

# 3 Wi-Fi Network Settings

## 3.1 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.

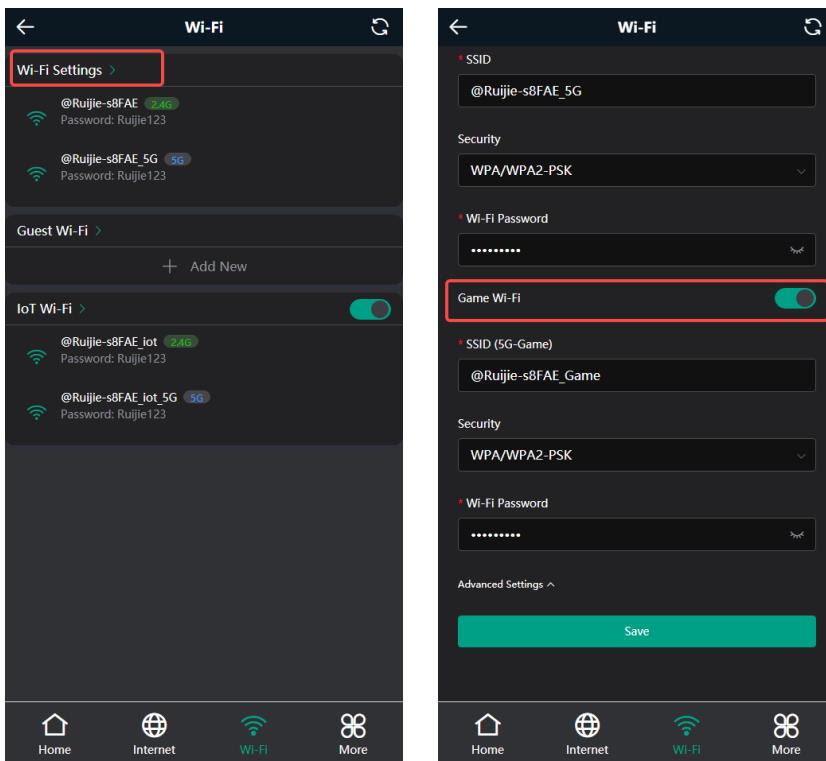
Smartphone View: Choose **Wi-Fi > Wi-Fi Settings**.

Click the target Wi-Fi network.

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

### 3.1.1 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.



### 3.1.2 Adding Other Types of Wi-Fi Networks

#### 1. Overview

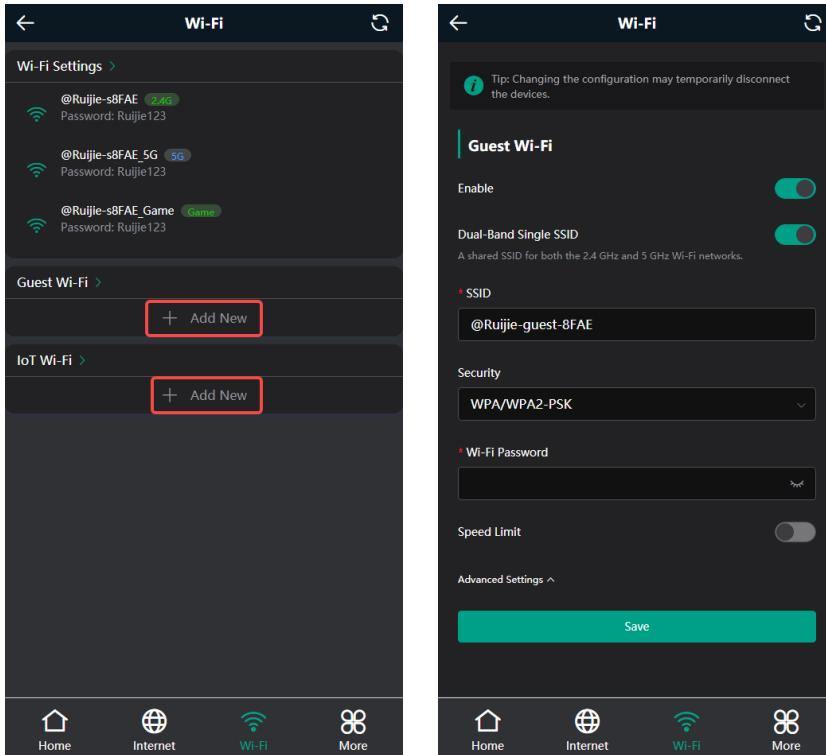
In addition to the Game Wi-Fi network, this router also supports other three types of Wi-Fi networks: primary Wi-Fi network, guest Wi-Fi network, and IoT Wi-Fi network. Only one Wi-Fi network can be configured for each type.

- **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 function is enabled, the 2.4G SSID will be consistent with the 5G SSID. For the host Wi-Fi network, 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.
- **Effective Time:** Options include Weekdays, Weekends, Always and Custom. When Custom is selected, you can select a custom effective time. This Wi-Fi can only be used during the effective period.
- **Client Isolation/Guest Isolation:** This feature is supported by **Wi-Fi Settings** and **Guest Wi-Fi**. You can enable **Client Isolation** in **Wi-Fi Settings** to prevent wireless clients of this Wi-Fi from communicating with each other. You can enable **Guest Isolation** in **Guest Wi-Fi** to enable wireless clients on the Guest Wi-Fi to access the Internet, and to prevent them from accessing the intranet and from communicating with each other.
- **Speed Limit:** You can set a rate limit for the Guest Wi-Fi. You can enable **Speed Limit**, and set the **Maximum Up Rate** and **Maximum Down Rate**.

## 3.2 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**.

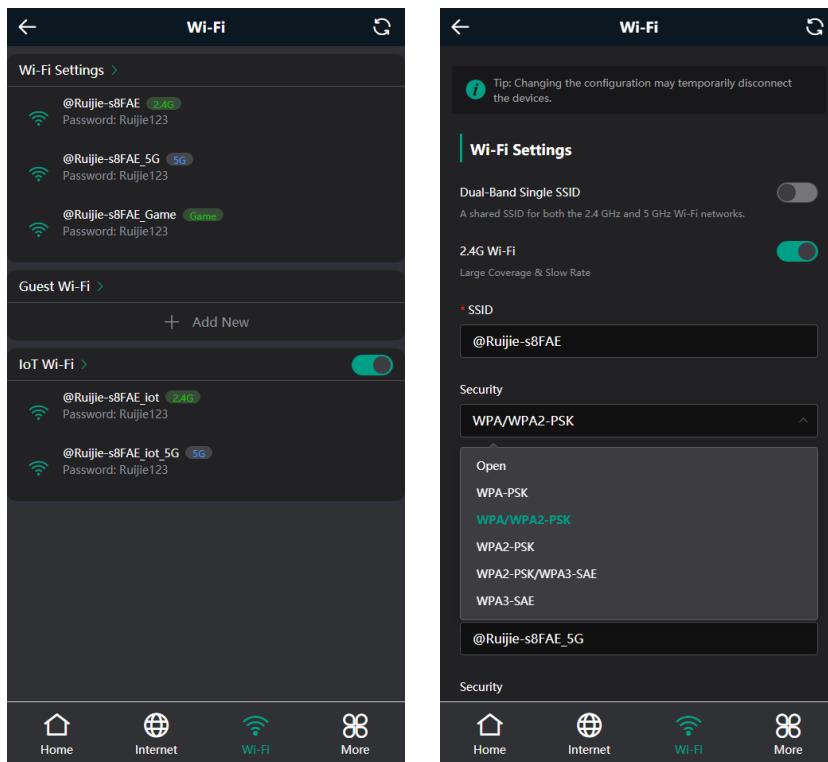
### ⚠️ Caution

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 2.4G Wi-Fi, 5G Wi-Fi, Game Wi-Fi, Guest Wi-Fi and IoT 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.



## 3.3 Enabling Band Steering

### ⚠️ Caution

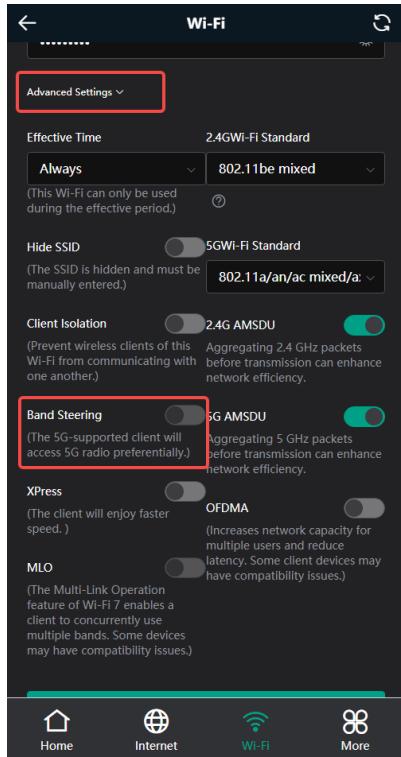
Before enabling the band steering, you must enable the dual-band integration. Because the client can automatically choose to steer to either band only when the 2.4G and 5G bands use the same SSID.

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 5G-capable client will access 5G radio preferentially after this function is enabled.



## 3.4 Hiding the SSID

### 3.4.1 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.

### 3.4.2 Getting Started

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

### 3.4.3 Configuration Steps

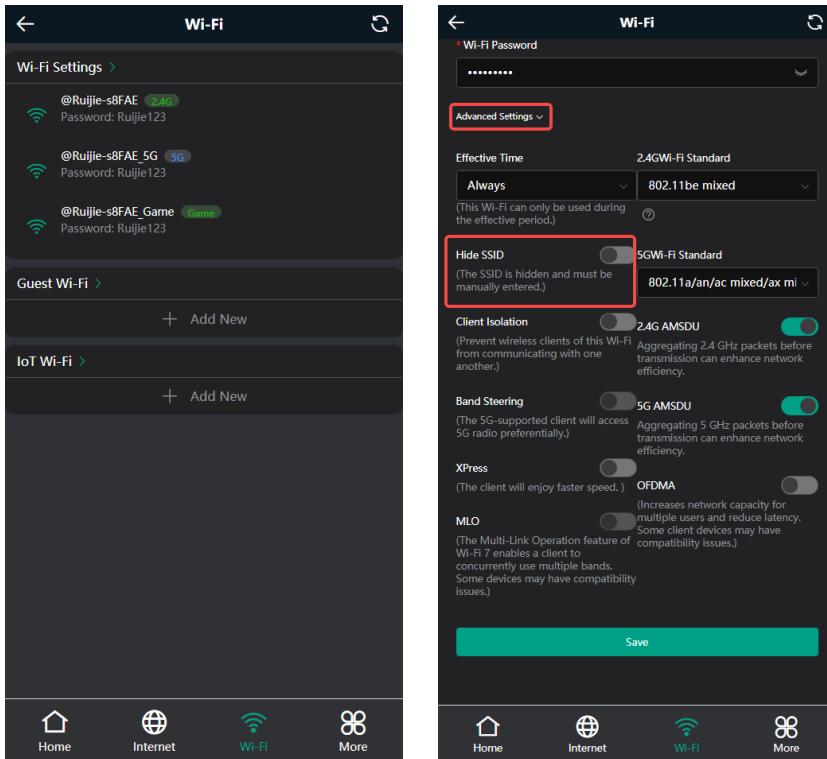
Smartphone View: Choose **Wi-Fi > Wi-Fi Settings**

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**. 2.4G Wi-Fi, 5G 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

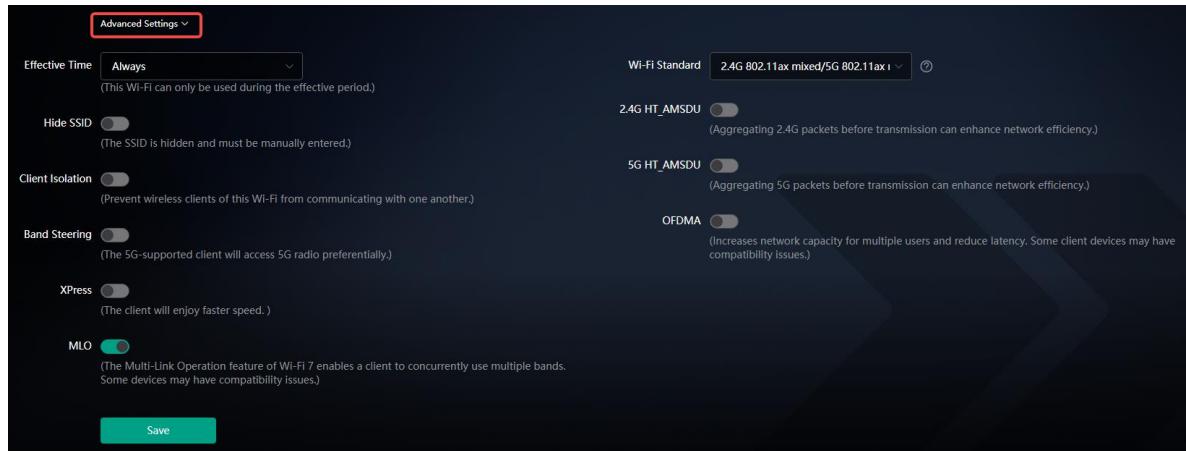
Users need to manually enter the SSID and password each time they connect to a hidden Wi-Fi network. Take an Android-based device as an example: To connect it to a hidden Wi-Fi network, choose **WLAN > Add network > Network name**, enter the Wi-Fi name, select **WPA/WPA2** from the **Security** dropdown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

## 3.5 Wi-Fi Advanced Settings

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

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

Click **Advanced Settings** and configure relevant parameters. For details, see [Table 3-1 Parameters of Wi-Fi Network Advanced Settings](#).



**Table 3-1 Parameters of Wi-Fi Network Advanced Settings**

Parameter	Description
Effective Time	Options include Weekdays, Weekends, Always and Custom. When Custom is selected, you can select a custom effective time. This Wi-Fi can only be used during the effective period.
Hide SSID	Enabling <b>Hide SSID</b> can prevent unauthorized user access to Wi-Fi, improving security. However, mobile phones or computers cannot find the SSID after this function is enabled. You must manually enter the correct name and password to connect to Wi-Fi. Record the current SSID before you enable this function.
Client Isolation	When enabled, clients connected to the Wi-Fi network are isolated from each other, thereby enhancing security. Note: Client Isolation is not supported by the IoT Wi-Fi network.
Band Steering	When enabled, 5G-capable clients connect to the 5 GHz Wi-Fi network preferentially. You can enable this function only when <b>Dual-Band Single SSID</b> is enabled.
XPress	When enabled, the device sends game packets preferentially, providing more stable wireless network for games.
MLO	Multi-Link Operation (MLO) is a feature of Wi-Fi 7 that enhances data transmission performance and coverage by utilizing multiple wireless channels simultaneously, allowing devices to connect to multiple frequency bands. Note: Enabling MLO could result in compatibility issues if the connected devices do not support Wi-Fi 7.
(2.4G/ 5G) Wi-Fi Standard	Set the wireless mode for the 2.4 GHz or 5 GHz Wi-Fi network. When the wireless mode is 802.11bg/b/g, the channel width for the 2.4 GHz band can only be set to 20 MHz. Unless otherwise required, keep the default settings.

Parameter	Description
(2.4G/ 5G) Encryption	<p>Set the encryption algorithm for the 2.4 GHz or 5 GHz Wi-Fi network. Unless otherwise required, keep the default settings.</p> <ul style="list-style-type: none"> <li>When the encryption type is set to "WPA-PSK", "WPA/WPA2-PSK", or "WPA2-PSK", the default encryption algorithm is "TKIP/AES".</li> <li>When the encryption type is set to "WPA2-PSK/WPA3-SAE" or "WPA3-SAE", the default encryption algorithm is "AES".</li> </ul> <p>Note: This parameter is only supported by the IoT Wi-Fi network.</p>
2.4G HT_AMSDU	When enabled, 2.4 GHz data packets are aggregated before transmission, thereby improving network efficiency.
5G HT_AMSDU	When enabled, 5 GHz data packets are aggregated before transmission, thereby improving network efficiency.
OFDMA	When enabled, it allows multiple users to simultaneously transmit and receive data over the same frequency band, enhancing multi-user transmission capacity and reducing latency. However, some clients may experience compatibility issues.

## 3.6 Configuring the Wi-Fi Blocklist or Allowlist

### 3.6.1 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.

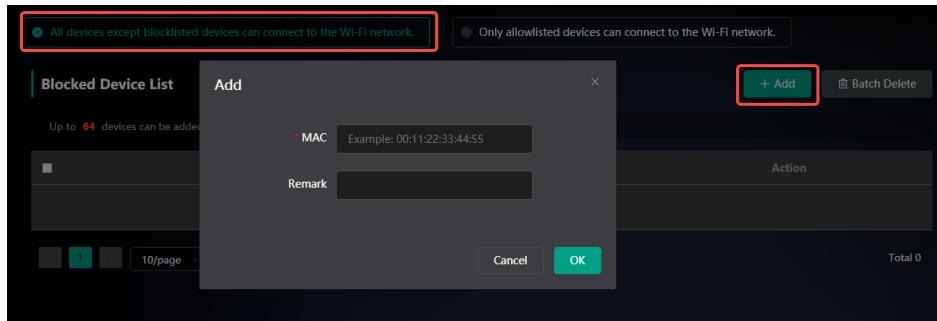
### 3.6.2 Configuration Steps

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.

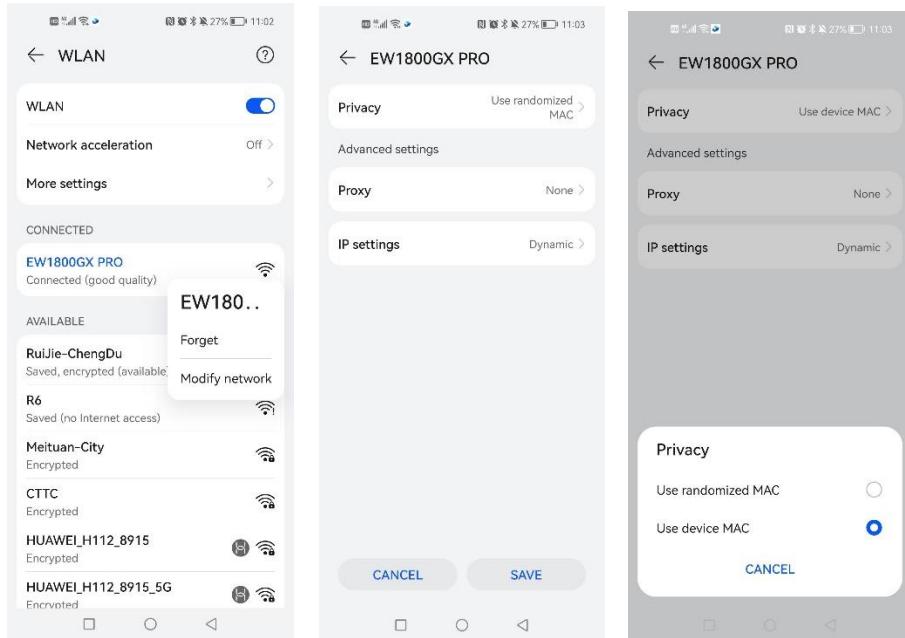
### Caution

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.

Blocked Device List		<b>+ Add</b>	<b>Batch Delete</b>
		Up to <b>64</b> devices can be added.	
MAC	Remark	Action	
00:11:22:33:44:55		<b>Edit</b>	<b>Delete</b>
<b>1</b>	10/page	Total 1	

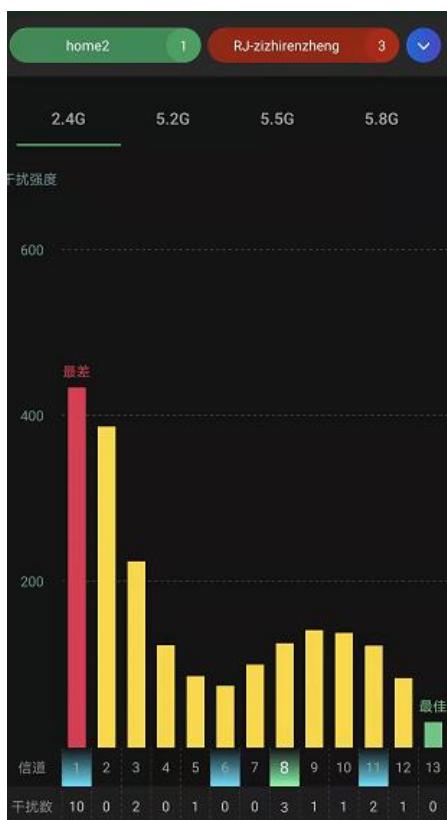
## 3.7 Configuring the Radio Frequency

### 3.7.1 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 [7.8 Configuring Scheduled Reboot](#). You can also analyze the wireless environment around the router and select appropriate parameters.

### 3.7.2 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.



### 3.7.3 Configuration Steps

#### 1. Optimizing the radio channel

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

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

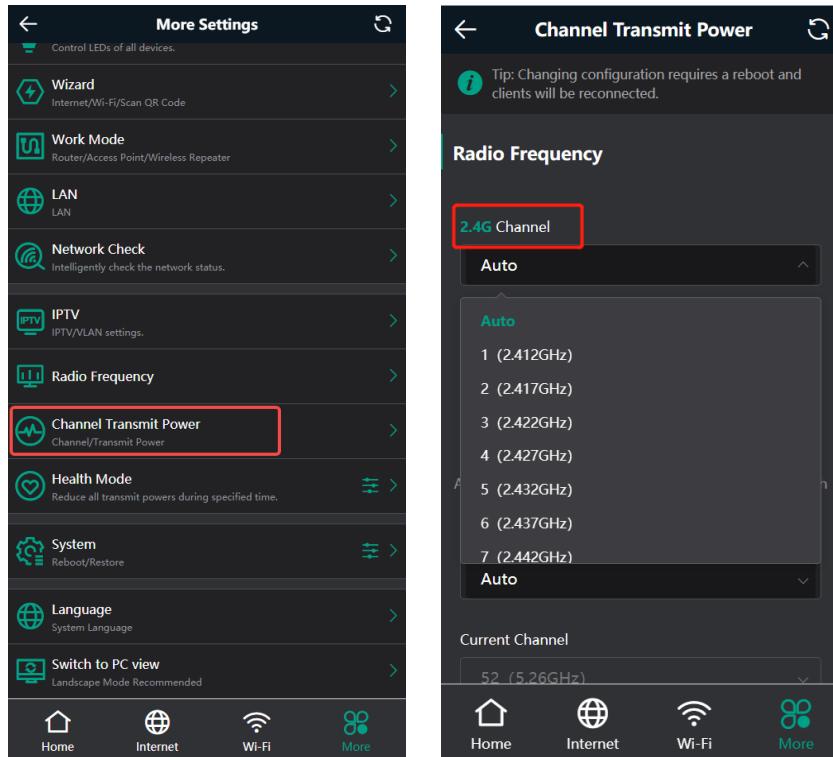
Choose the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. Excess clients connected to a channel can bring stronger wireless interference.

### 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.



## 2. 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.

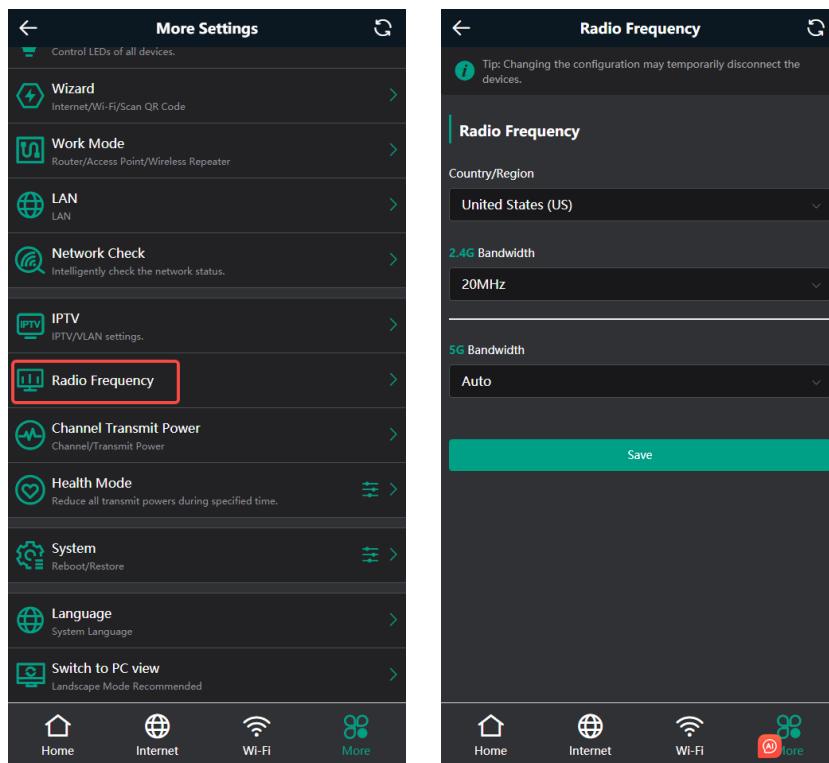
You can select 20MHz and 40MHz bandwidths for the 2.4GHz band, or 20MHz, 40MHz, 80MHz and 160MHz for the 5GHz band. The default value is "Auto", indicating that the bandwidth will be automatically selected based on the wireless environment.

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

After changing the channel bandwidth, click **Save** to make the configuration take effect immediately.

### Caution

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



### 3. Optimizing the transmit power

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

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

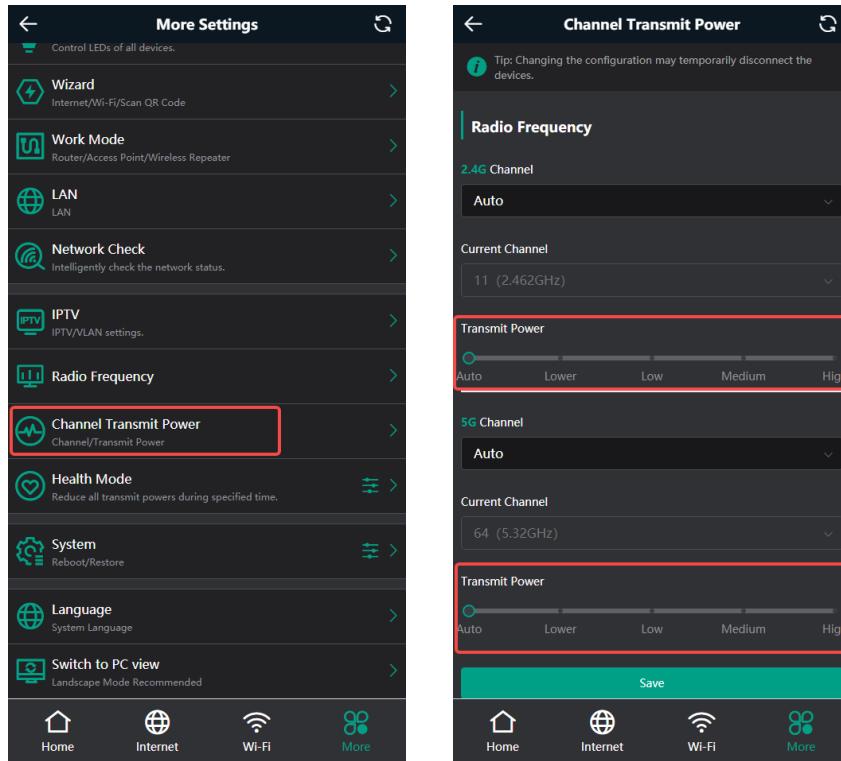
A greater transmit power indicates a larger coverage and brings stronger interference to surrounding wireless routers. The default value is **Auto**, indicating automatic adjustment of the transmit power. In a scenario in which routers are installed densely, a lower transmit power is recommended.

---

#### Caution

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

---



## 3.8 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.

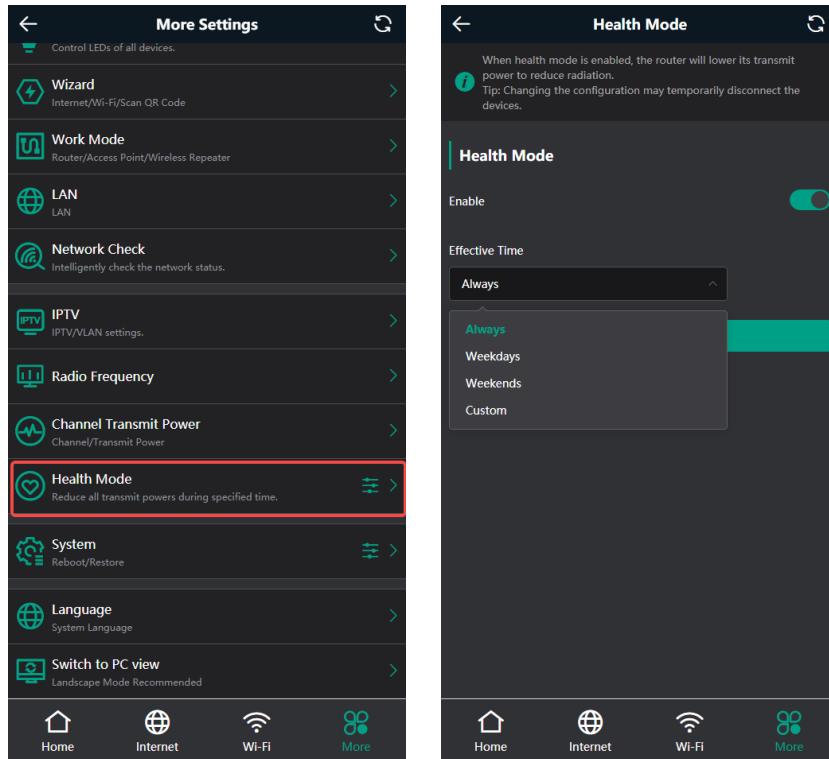
After the healthy mode is enabled, the transmit power and the Wi-Fi coverage area will decrease. The healthy mode may reduce signal strength and cause network stalling. You are advised to disable it.

---

### **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.

---

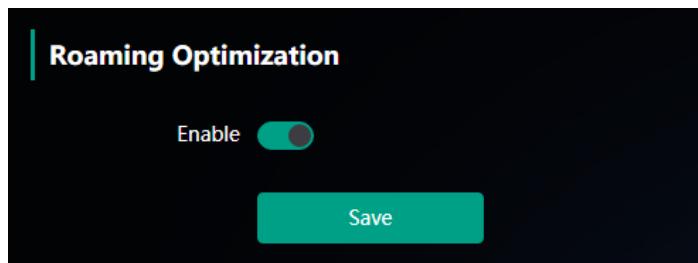


## 3.9 Enabling Roaming Optimization

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

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

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



## 3.10 Configuring Wi-Fi/IGMP

### 3.10.1 Overview

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

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

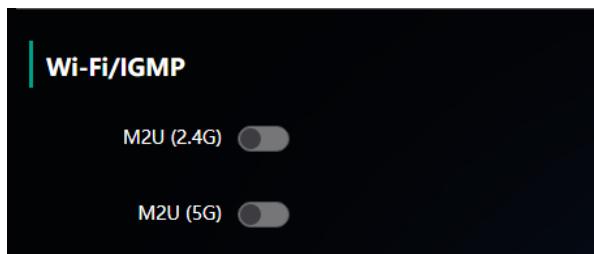
### 3.10.2 Configuration Steps

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

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

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

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



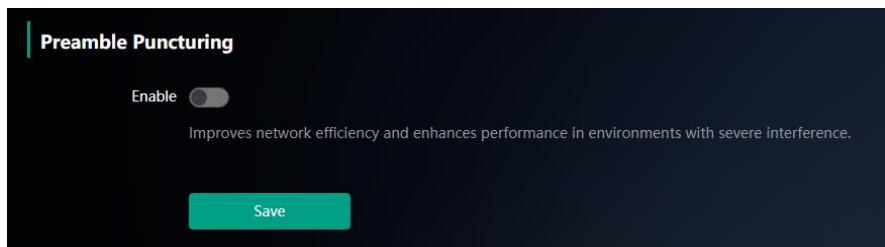
## 3.11 Configuring Preamble Puncturing

Smartphone View: Choose **More** > **Switch to PC view** > **More** > **WLAN** > **Wi-Fi** > **More Settings** > **Preamble Puncturing**.

PC View: Choose **More** > **WLAN** > **Wi-Fi** > **More Settings** > **Preamble Puncturing**.

Preamble Puncturing is a signal processing technique that enhances network transmission efficiency and improves performance in interference-prone environments. This feature is disabled by default.

Toggle on **Enable**, and then click **Save** to enable the Preamble Puncturing feature.



# 4 Configuring Work Mode

Smartphone View: Choose **More** > **Switch to PC view** > **More** > **Work Mode**.

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

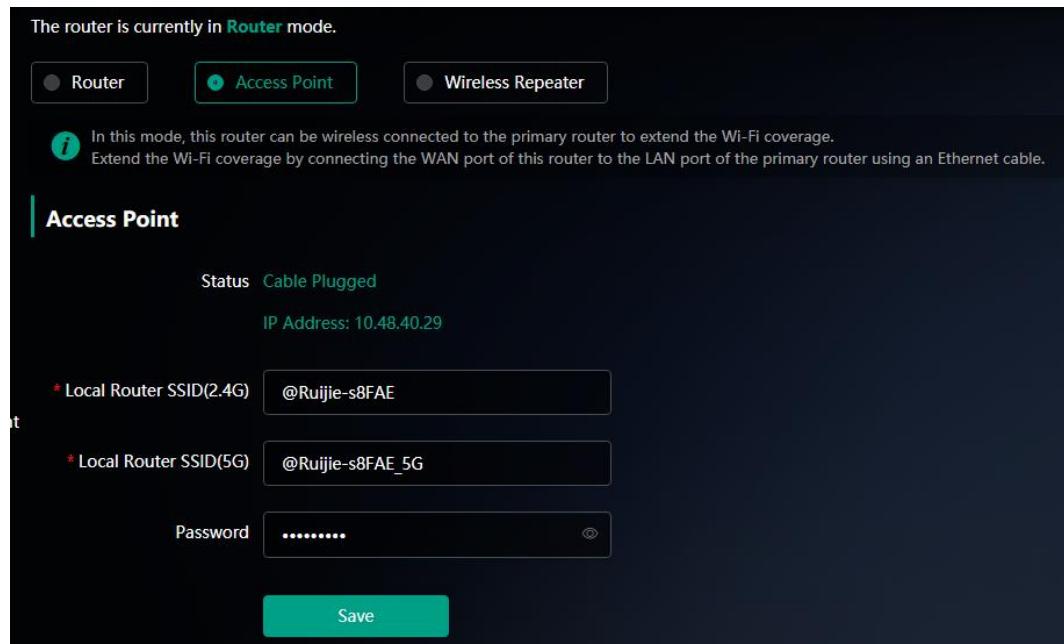
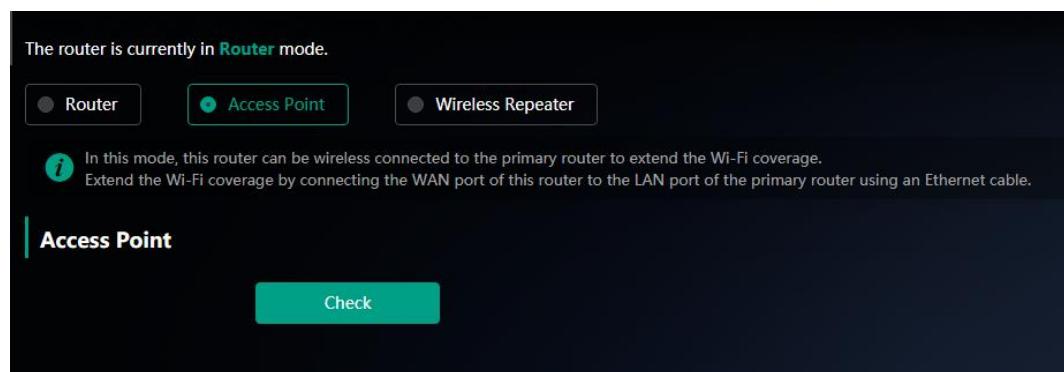
## 4.1 Access Point

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.

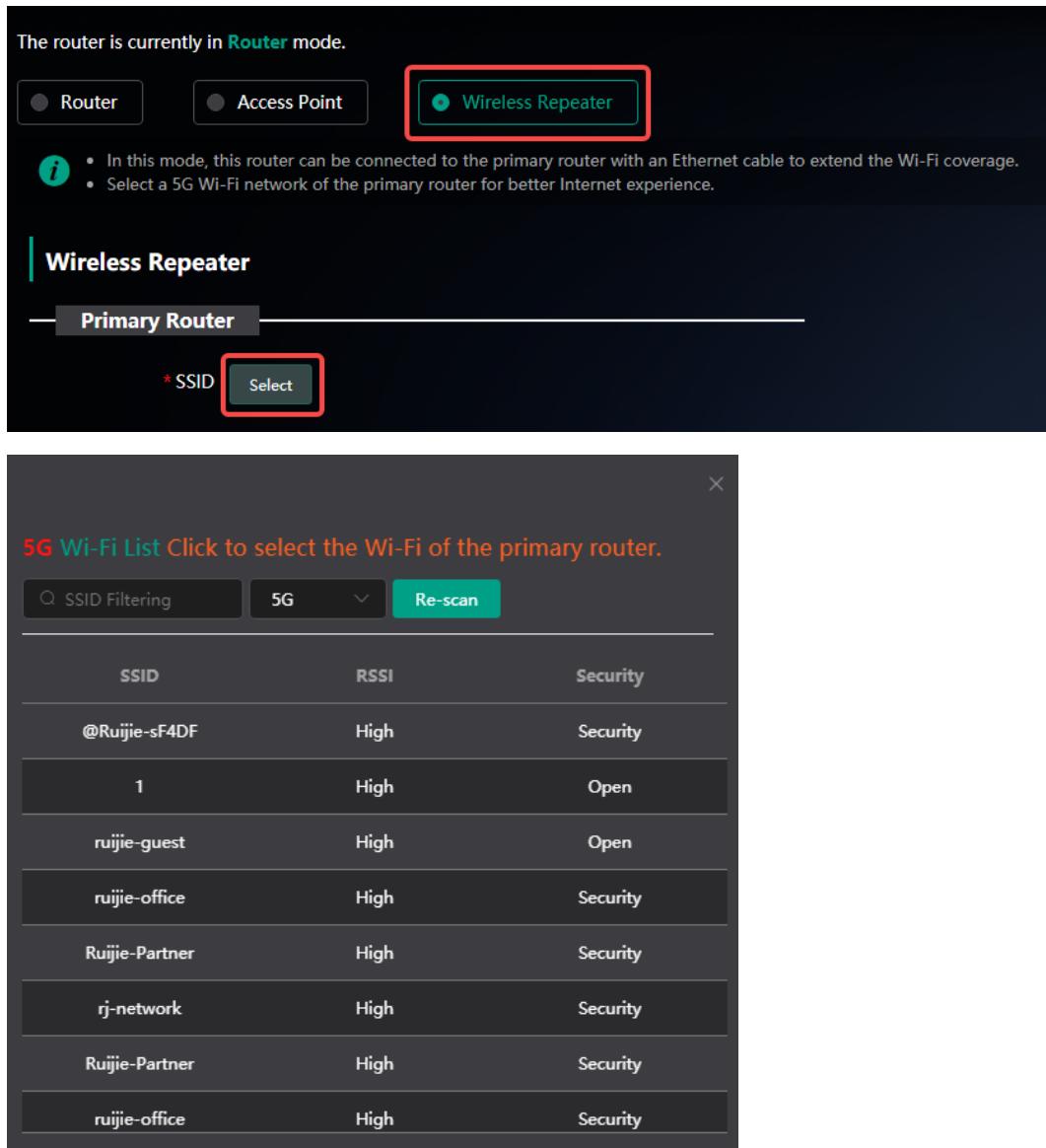


## 4.2 Wireless Repeater

### **i** Note

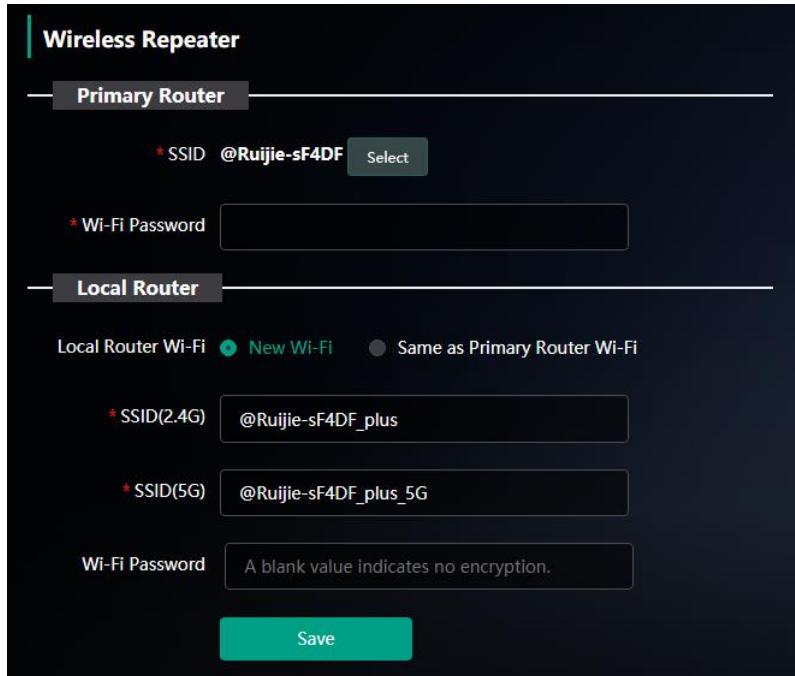
- For wireless repeater, first unplug the Ethernet cable from the router.
- Before configuring wireless repeater, obtain the Wi-Fi network name and password of the primary router.

- 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 **5G** drop-down box and select **2.4G**. You are advised to select a 5 GHz Wi-Fi network of the primary router for better internet experience.



- 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.
- 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 Configuring Network Settings

## 5.1 Configuring Internet Connection Types

### ⚠ Caution

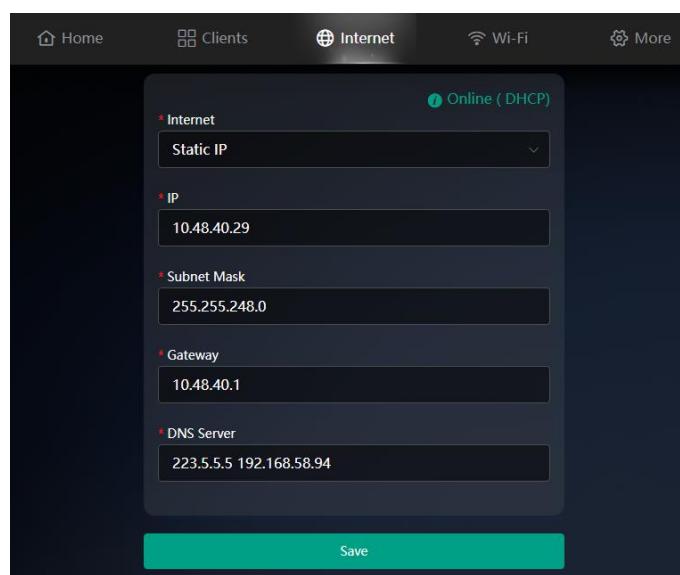
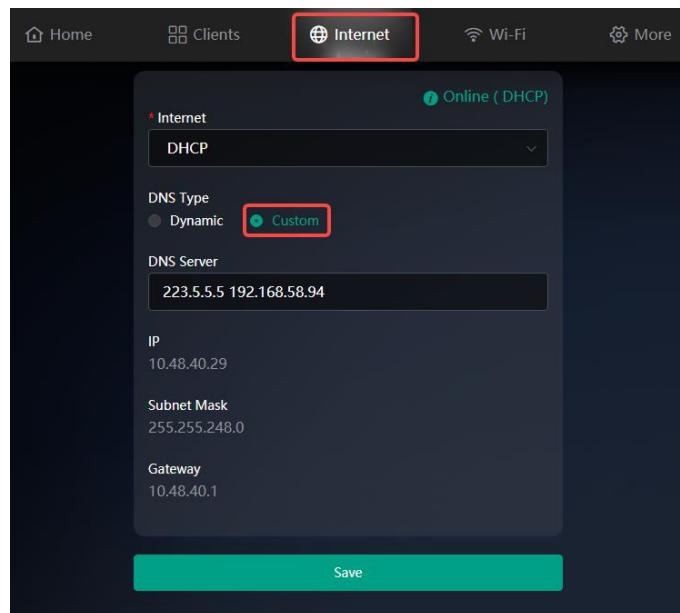
This feature is supported in router mode.

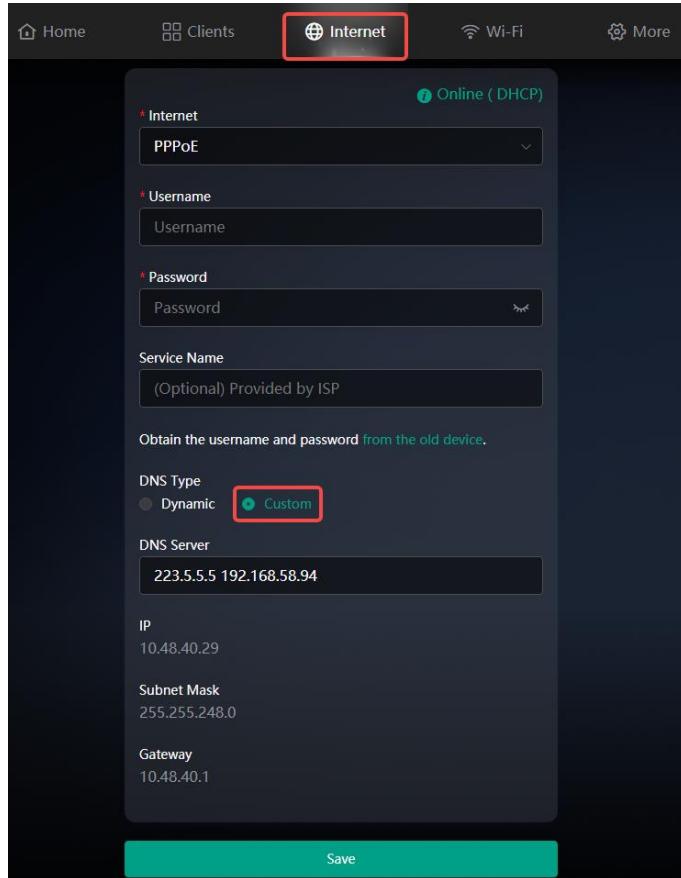
Smartphone View: Choose **Internet**.

PC View: Choose **Internet**.

The router supports three Internet connection types: PPPoE, DHCP, and static IP. For details, see [1.4.1 Configuring the Internet Connection Type](#)

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





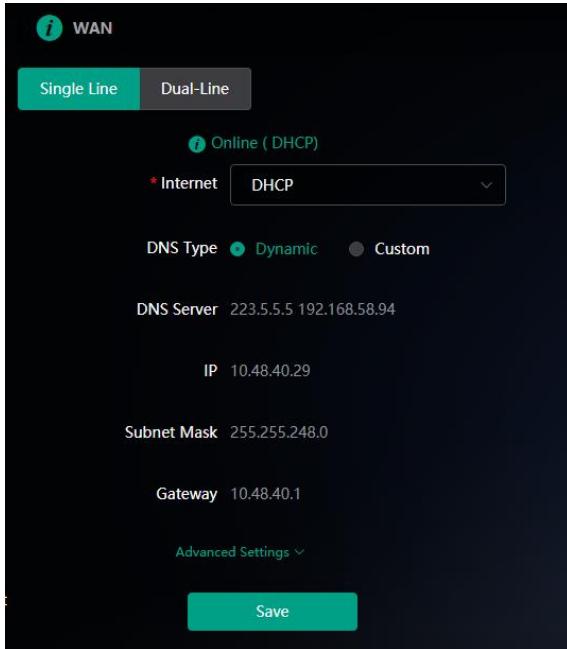
## 5.2 Configuring WAN Settings

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

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

### 5.2.1 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.



## 5.2.2 Changing the MAC Address

### ⚠️ Caution

Changing the MAC address of the WAN port is only supported when the router is in router mode.

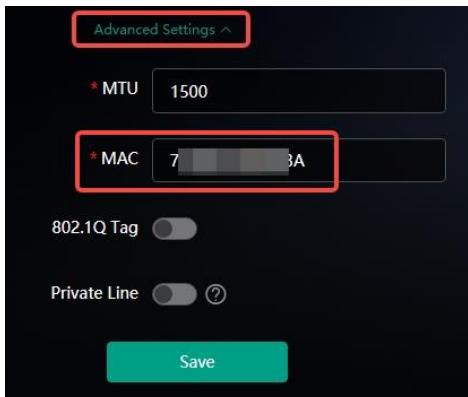
The ISP may restrict the access of devices with unknown MAC addresses to the Internet for the sake of security. In this case, you can change the MAC address of the WAN port to another address. You are advised to use the MAC address of an old router that is allowed to access the Internet (the MAC address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

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.



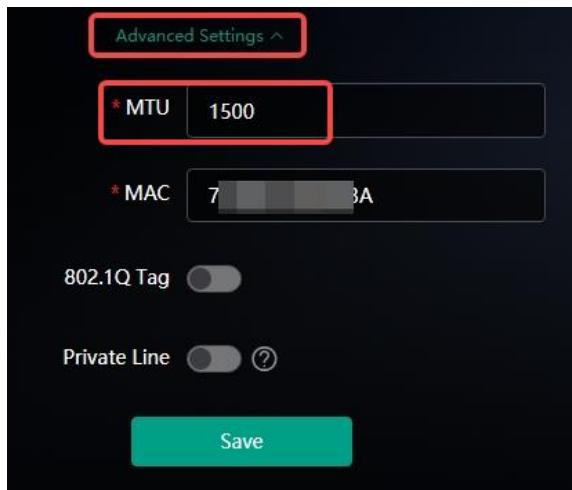
### 5.2.3 Modifying MTU

#### ⚠ Caution

This feature is supported in router mode.

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

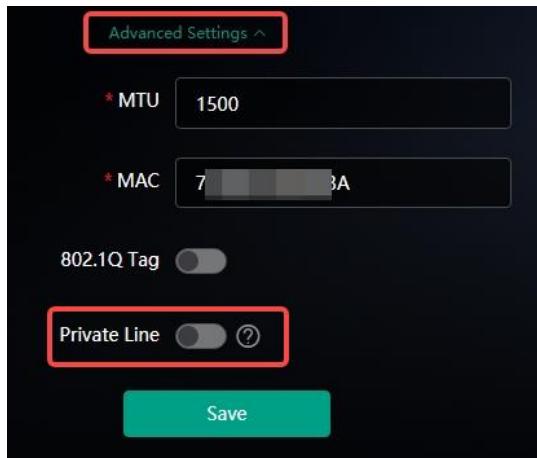
Click **Advanced Settings**. The default MTU value is 1500, which is the maximum MTU size. You are advised to gradually adjust the value to 1492, 1400, or even smaller if necessary.



### 5.2.4 Configuring a Private Line

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.



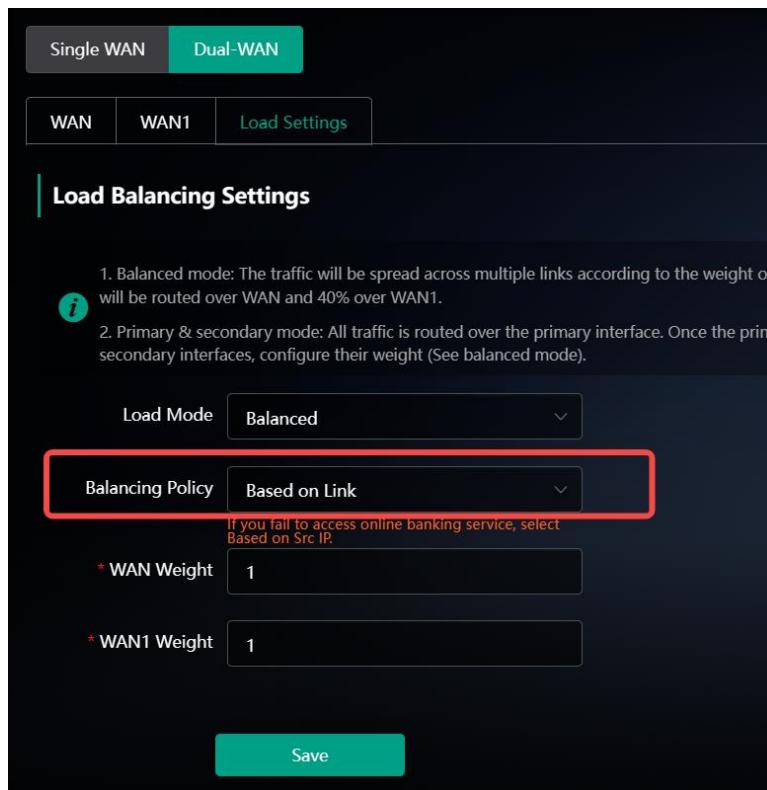
### 5.2.5 Configuring the VLAN Tag

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 interface. By default, the VLAN tag function is disabled. You are advised to keep the VLAN tag function disabled unless otherwise specified.



### 5.2.6 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.



**Table 5-1 Description of Load-balancing Mode**

Load Mode	Description
Balanced	<p>Traffic is allocated in proportion to the weight of each WAN port. The higher the weight is, the more traffic is allocated.</p> <p>The weight of each WAN port must be specified in this mode.</p> <p>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.</p>
Primary & Secondary	<p>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.</p> <p>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).</p>

## 5.3 Changing the Address of a LAN Port

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

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

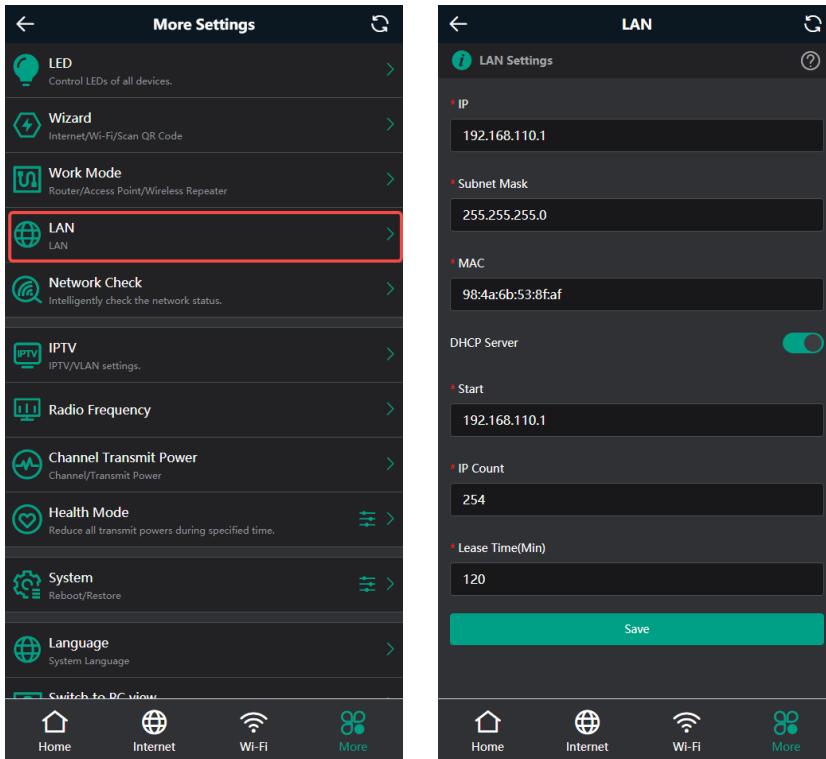
Change the IP address and subnet mask, and click **Save**. After the IP address of a LAN port is changed, you need to log in to the web interface by using the new IP address of the LAN port.

---

 **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.

---



## 5.4 Connecting to IPTV

### ⚠ Caution

This feature is supported in router mode.

IPTV is an Internet television service provided by ISP.

### 5.4.1 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.

### 5.4.2 IPTV Configuration Steps (VLAN Type)

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

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

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

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

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

### ⚠️ Caution

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



## 5.5 Configuring IPv6

### ⚠️ Caution

This feature is supported in router mode.

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

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

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

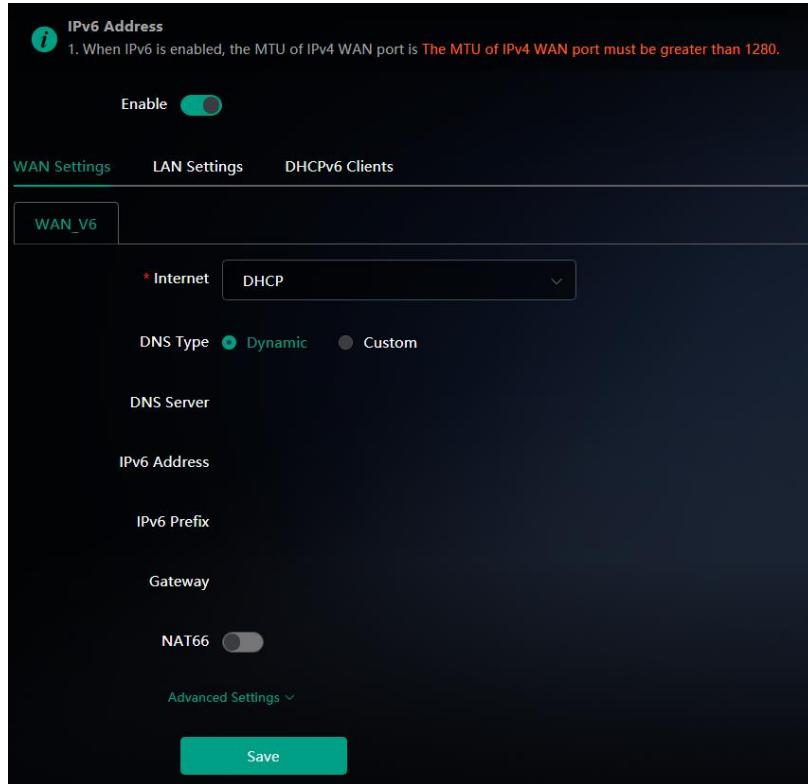
### 5.5.1 Configuring the IPv6 of the WAN Port

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

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

### ⚠️ Caution

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



### 5.5.2 Configuring the IPv6 of the LAN Port

Click **LAN Settings**.

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

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

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

WAN Settings   LAN Settings   DHCPv6 Clients

IPv6 Assignment: Auto

IPv6 Address/Prefix: 2000:0::2

Length: 64

Subnet Prefix Name: Default

Subnet Prefix Length: 64

Subnet ID: 0

\* Lease Time(Min): 120

DNS Server: Example: 2000:0::2, each separated by a comma

Save

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

WAN Settings   LAN Settings   DHCPv6 Clients

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

**DHCPv6 Clients**

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

No Data

10/page Total 0

## 5.6 Configuring Auto Bandwidth Control

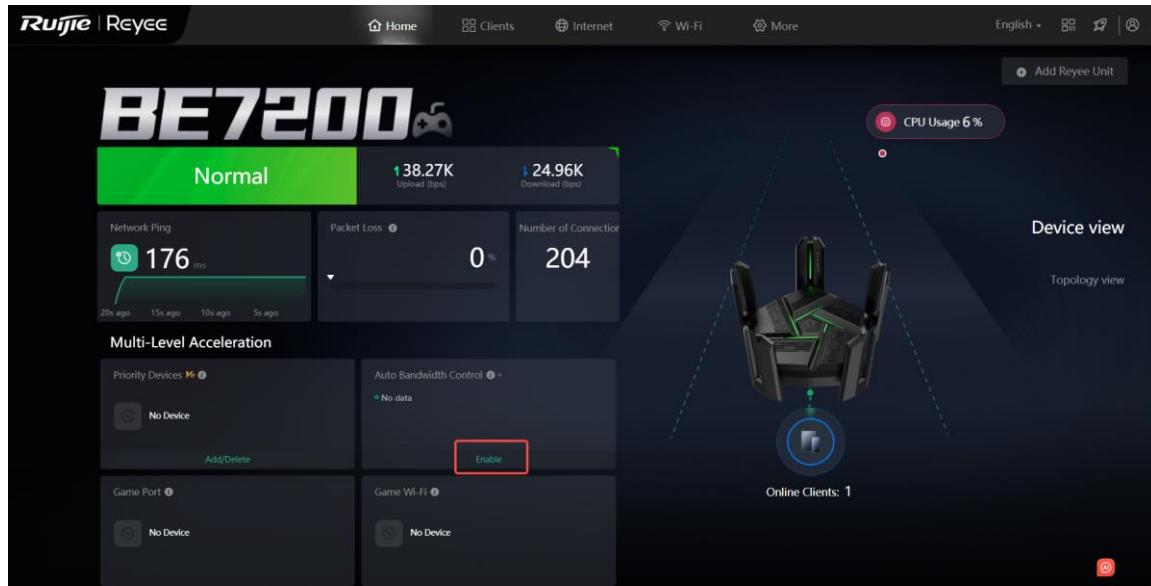
### ⚠️ Caution

This feature is supported in router mode.

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

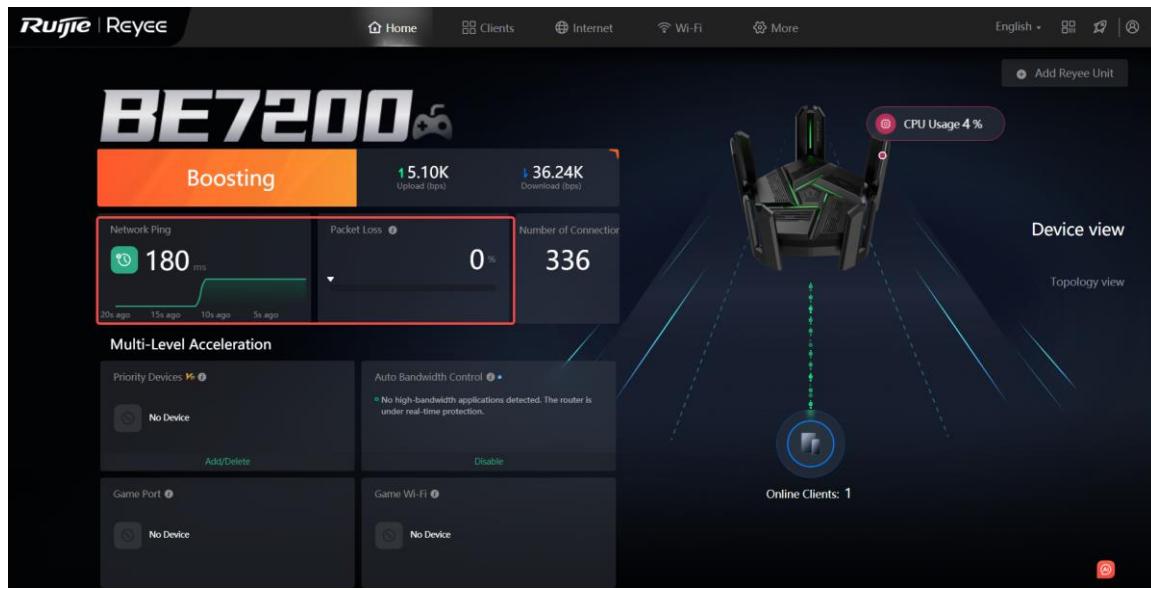
PC View: **Home page > Auto Bandwidth Control**

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



## 1. Viewing Network Latency

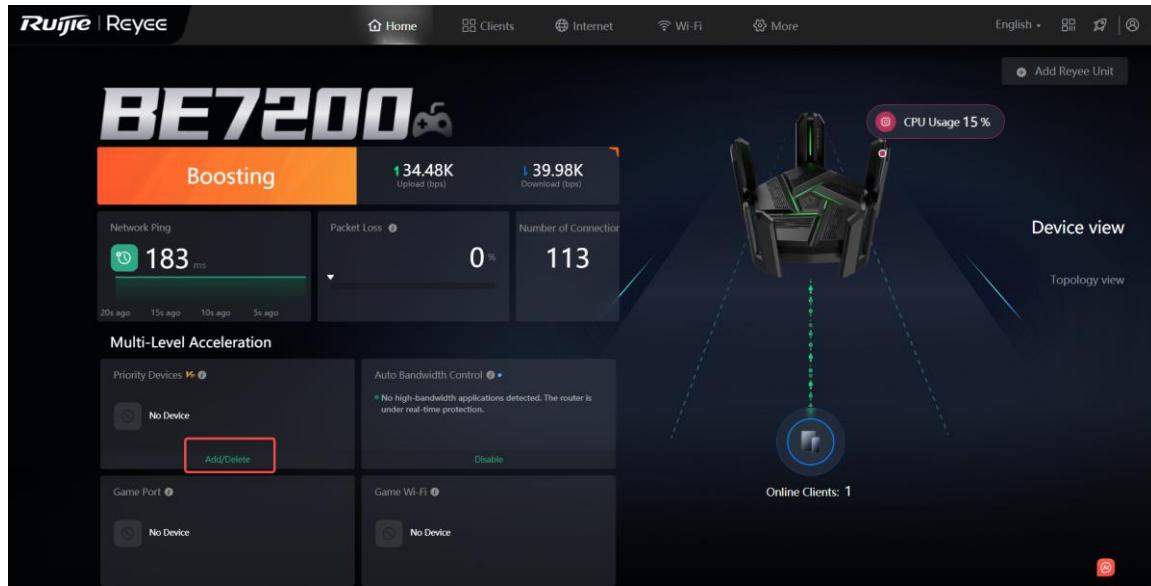
After **Auto Bandwidth Control** is enabled, you can view details such as network latency and packet loss rate of the router.



## 2. Configuring Priority Devices

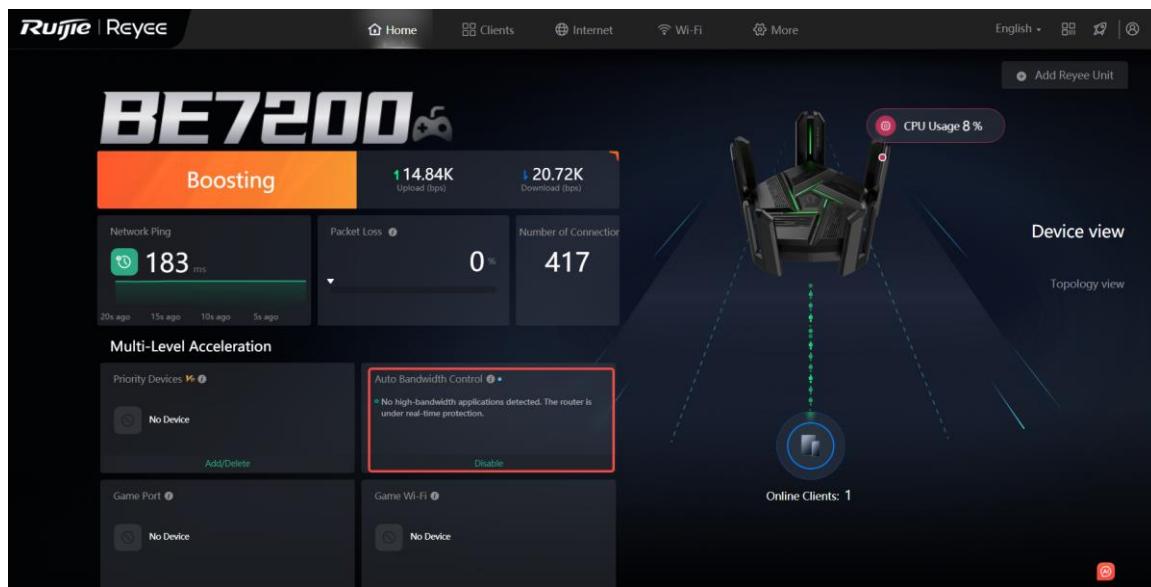
Clients in the designated device list will be prioritized and protected from the interference of other heavy traffic (such as downloading large videos). A maximum of 4 designated devices can be added.

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



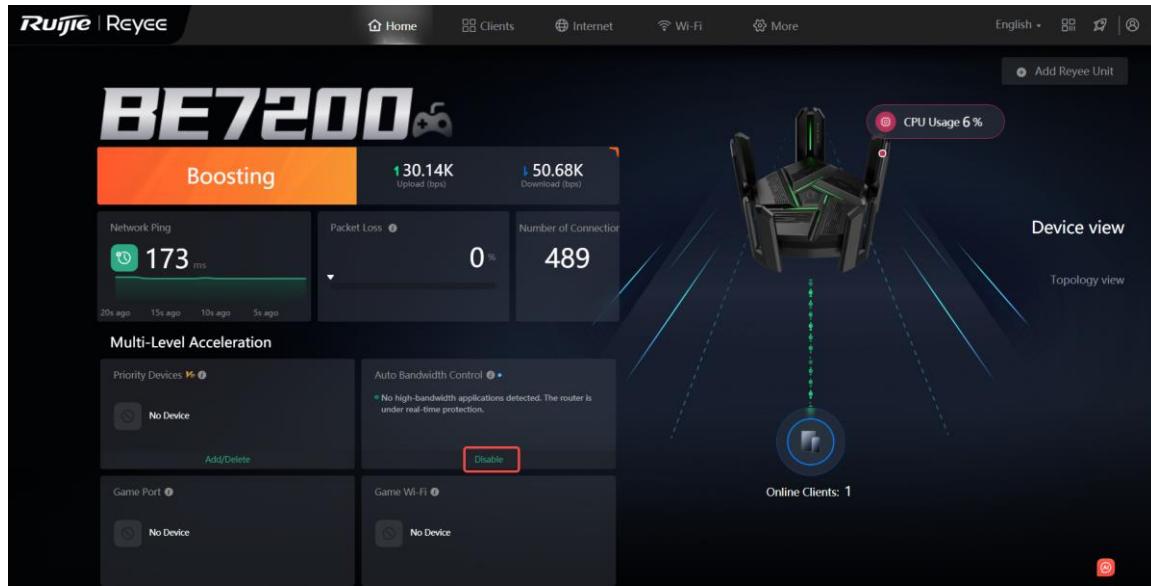
### 3. Viewing Auto Bandwidth Control Device Details

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.



### 4. Disabling Auto Bandwidth Control

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



## 5.7 Client Management

### 5.7.1 Setting Blocking Schedules

Smartphone View: Choose **More > Switch to PC > Client**.

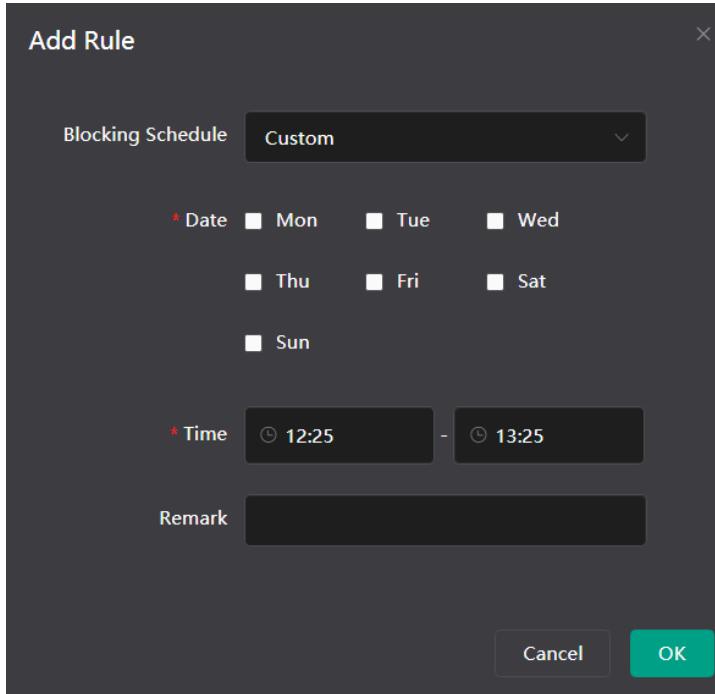
PC View: Choose **Client**.

#### 1. Setting a blocking schedule

- (1) Select a client and click **Add Blocking Schedule**.

Clients						
Clients						
Username/Conn...	IP/MAC	Number of Connections	Current Rate	Blocking Schedule	Action	
Me Wired	192.168.110.3 7a Unbind	48	Up:8.02Kbps Down:6.42Kbps	No schedule (No time is blocked) + Add Blocking Schedule	Wired Client	
2.4G Detail	192.168.110.217 2 Unbind	66	Up:0.00bps Down:0.00bps	No schedule (No time is blocked) + Add Blocking Schedule	Block	
2.4G Detail	192.168.110.85 E Unbind	0	Up:0.00bps Down:0.00bps	No schedule (No time is blocked) + Add Blocking Schedule	Block	

- (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. Click **OK** to save the changes.



## 2. Remove a blocking schedule

Click the  icon next to a blocking schedule to remove it.

Username/Conn...	IP/MAC	Number of Connections	Current Rate	Blocking Schedule	Action
Me	192.168.110.3	74	Up:1.03Kbps Down:0.00bps	12:25-13:25 Sun You have set 1 blocked time. + Add Blocking Schedule	 Wired Client
	192.168.110.217	39	Up:0.00bps Down:0.00bps	No schedule (No time is blocked.) + Add Blocking Schedule	
	192.168.110.85	0	Up:0.00bps Down:0.00bps	No schedule (No time is blocked.) + Add Blocking Schedule	

### 5.7.2 Viewing Number of Connections for Clients

Smartphone View: Choose **More > Switch to PC > Client**.

PC View: Choose **Client**.

On the **Clients** page, you can view the number of connections established for all clients.

The number of connections that the device can handle simultaneously is displayed in real-time on the **Home** page.

## 5.8 Configuring DHCP Server

### ⚠️ Caution

This feature is supported in router mode.

### 5.8.1 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.

## 5.8.2 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.



No.	Hostname	IP	MAC	Remaining Lease Time(min)	Status
1	*	192.168.110.85	ba [REDACTED] 25	116	<a href="#">Convert to Static IP</a>
2	*	192.168.110.217	22 [REDACTED] 2f	116	<a href="#">Convert to Static IP</a>
3	PC-6049ba	192.168.110.3	70 [REDACTED] 5a	102	<a href="#">Convert to Static IP</a>

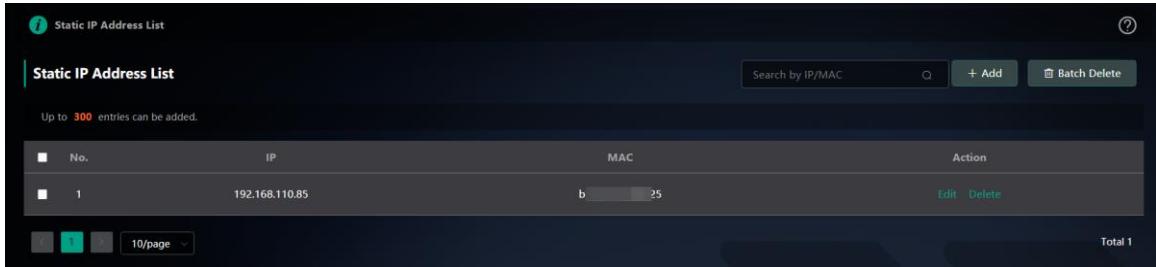
10/page ▾ Total 3

### 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.



No.	IP	MAC	Action
1	192.168.110.85	b [REDACTED] 25	<a href="#">Edit</a> <a href="#">Delete</a>

Up to 300 entries can be added.  
10/page ▾ Total 1

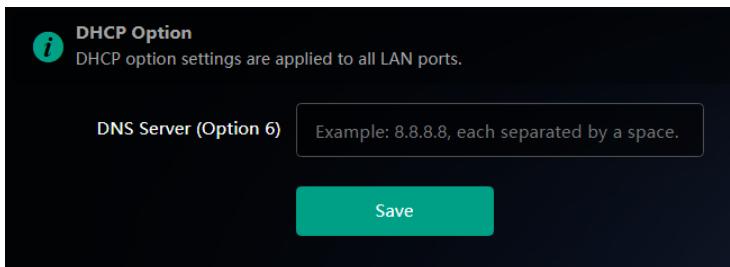
### 4. Configuring DHCP Option

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.



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

DNS Server (Option 6) Example: 8.8.8.8, each separated by a space.

Save

## 5.9 Configuring DNS Server

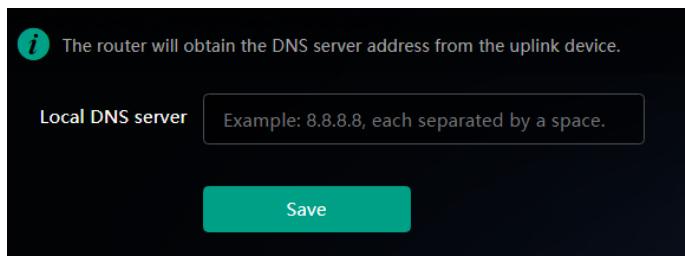
### 5.9.1 Local DNS Server

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.



### 5.9.2 Configuring DNS Proxy

#### ⚠ Caution

This feature is supported in router mode.

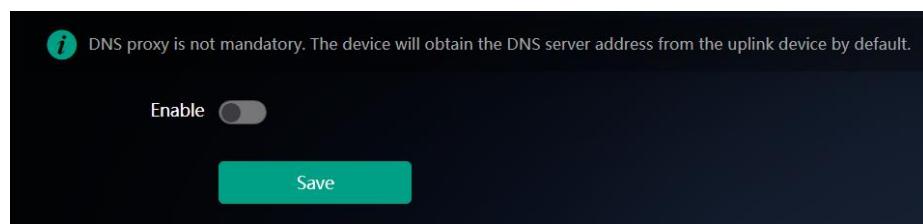
The domain name system (DNS) proxy configuration is not mandatory. The device obtains the DNS server address from the uplink device by default.

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.



## 5.10 Configuring Port Mapping

### ⚠ Caution

This feature is supported in router mode.

### 5.10.1 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.

### 5.10.2 Getting Started

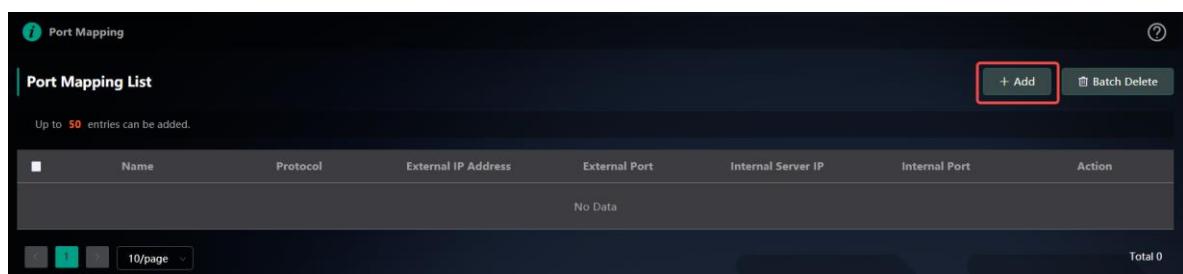
- Confirm the IP address of the target device in the internal network and service port ID.
- Ensure that port mapping is available in the internal network.
- Verify that your router has a public IP address. If the IP address is dynamic, changing it may cause port mapping failure. In this case, you are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

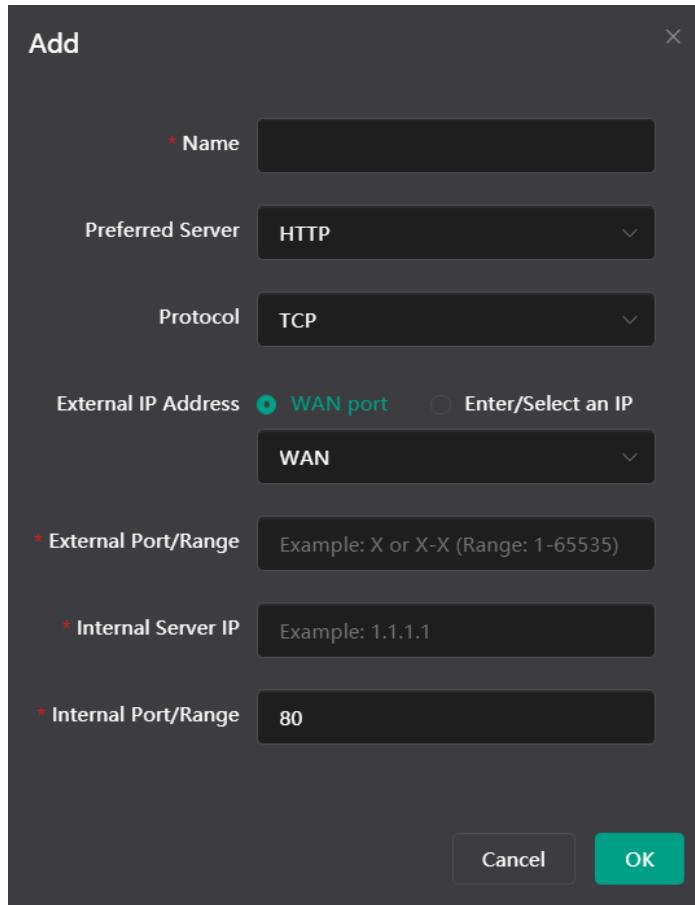
### 5.10.3 Configuration Steps

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

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

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





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

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

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

**External 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.

#### 5.10.4 Verification and Testing

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

#### 5.10.5 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.

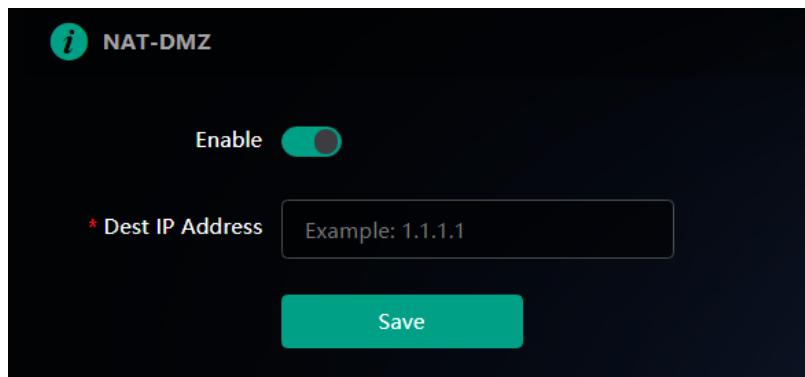
- (2) Enable the remote access permission on the server. The common cause is that remote access is disabled on the server by default. As a result, the internal network access is successful but the access across different network segments fails.
- (3) Enable the DMZ service. For details, see [5.10.6 DMZ Configuration Steps](#). The common cause is that port configuration is incorrect or incomplete.

## 5.10.6 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 IP address of the internal server, and click **Save**.



## 5.11 Configuring DDNS

### 5.11.1 Overview

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

### 5.11.2 Getting Started

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

### 5.11.3 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.

The screenshot shows the 'No-IP DDNS' configuration page. At the top, there are two tabs: 'No-IP DDNS' (which is selected, indicated by a green underline) and 'DynDNS'. The main section is titled 'No-IP DDNS' with an information icon. It contains the following fields:

- \* Service Interface: A dropdown menu set to 'WAN'.
- \* Username: An input field.
- \* Password: An input field.
- Domain Name: An input field with a help icon (question mark) and a 'Delete' button.

Below these fields are two buttons: 'Log In' (in a teal box) and 'Delete'. At the bottom of the page, there are two sections: 'Connection Status' and 'Domain Name'.

## 5.12 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.

Connectivity Detection

\* Keepalive Interval: 120 seconds

\* Probe Interval: 5 seconds

\* URL List:

- http://www.amazon.com Add
- http://www.google.com Delete
- http://www.yahoo.com Delete
- http://wikipedia.org Delete
- http://www.msn.com Delete

Save

## 5.13 Enabling CWMP

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

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

### 1. Overview

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

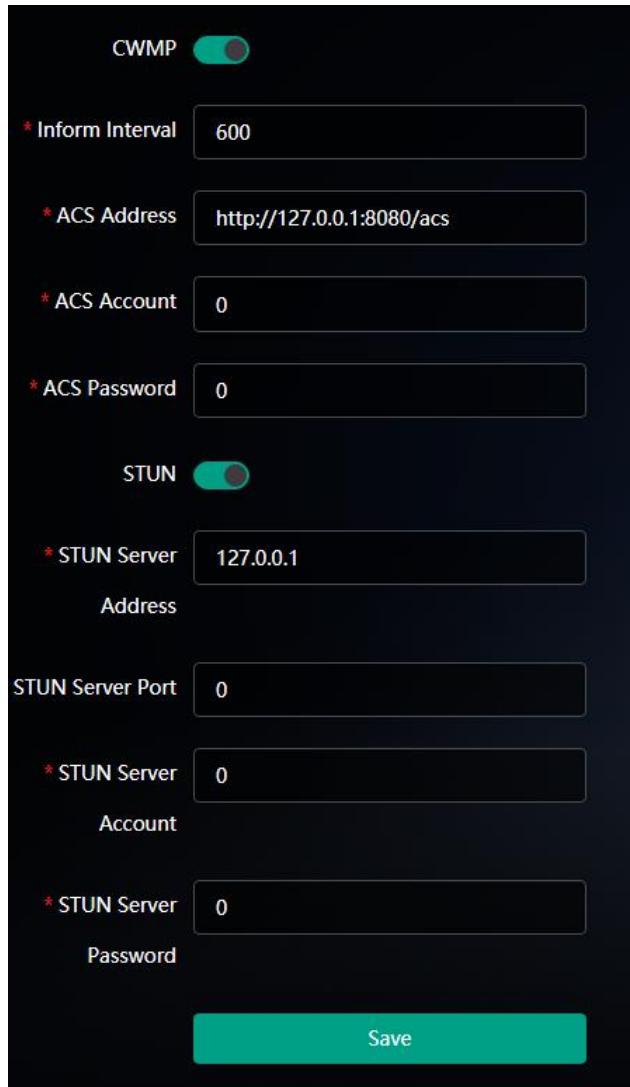
CWMP uses ACS and CPE models to manage devices. With CWMP, CPE can perform mandatory initialization and O&M actions such as service activation, function settings, file upload and download, and system detection.

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

### 2. Configuration Steps

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

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



## 5.14 Configuring APR Binding

---

### ⚠️ Caution

This feature is supported in router mode.

---

### 5.14.1 Overview

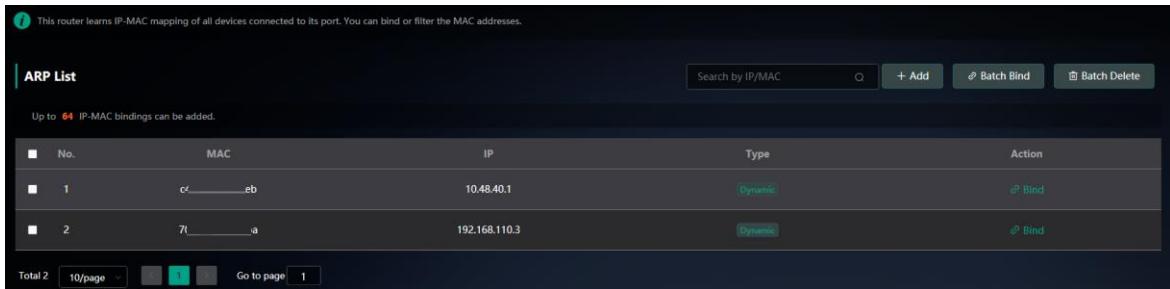
The router learns the ARP table from all devices connected to its ports. You can search for a device by its MAC address, perform ARP binding.

### 5.14.2 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.



No.	MAC	IP	Type	Action
1	c4-eb	10.48.40.1	Dynamic	 Bind
2	71-4a	192.168.110.3	Dynamic	 Bind

## 5.15 Link Aggregation

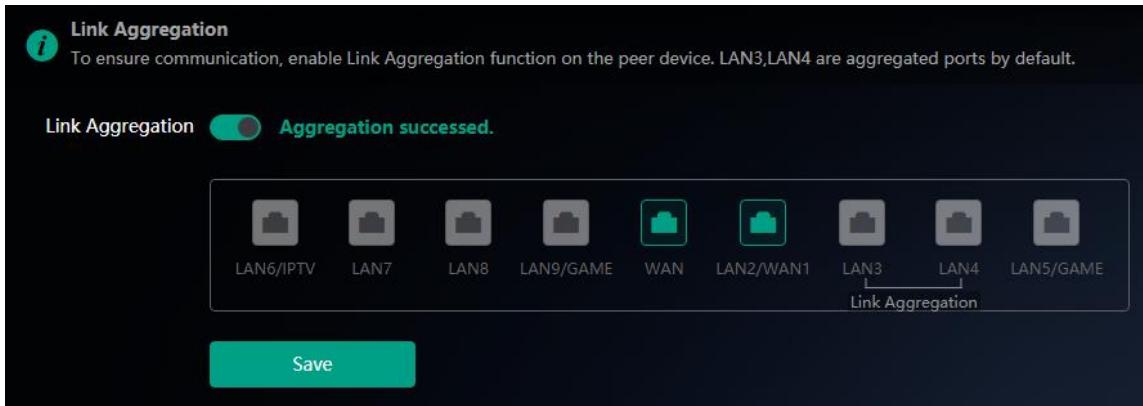
### Note

This feature is mutually exclusive with the Game Port Guarantee feature.

Smartphone View: Choose **More > Switch to PC view > More > Advanced > Link Aggregation**.

PC View: Choose **More > Advanced > Link Aggregation**.

Connect LAN3 and LAN4 ports to the downlink device (e.g., Network Attached Storage (NAS)) with an Ethernet cable, enable the 802.3ad link aggregation mode on the downlink device, and click **Save**.



## 5.16 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.

**Static Routing**  
*i* When a packet arrives at the router, it checks its routing table to find a matching entry for the destination IP address, and then forwards the packet to the corresponding next-hop IP address or outgoing interface. [?](#)

**Static Route List**

Up to 100 entries can be added.

	Dest IP Address	Subnet Mask	Outbound Interface	Next Hop	Reachability	Action
No Data						

10/page [▼](#)

Total 0

**Add**

\* Dest IP Address:

\* Subnet Mask:

\* Outbound Interface:

\* Next Hop:

[Cancel](#) [OK](#)

**Table 5-2 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.

Static Route List					
<input type="checkbox"/>	Dest IP Address	Subnet Mask	Outbound	Next Hop	Reachable
The route is unreachable. Initiate a Ping test from the outbound interface to the next hop.					
<input type="checkbox"/>	192.168.2.0	255.255.255.0	WAN	172.168.1.1	No 
					<a href="#">Edit</a> <a href="#">Delete</a>

Up to **100** entries can be added.

10/page  Total 1

## 5.17 Policy-based Routing

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

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

### 1. Overview

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

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

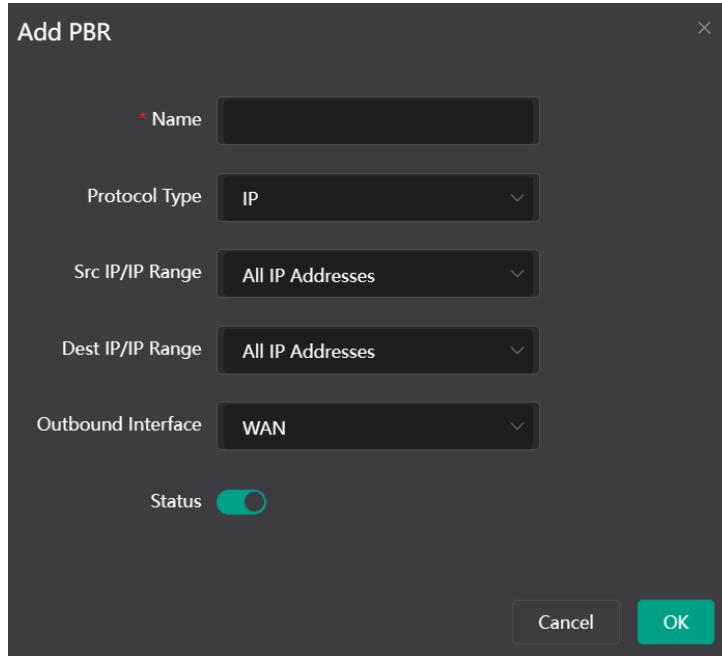
This router supports three routing policies, namely, PBR, ISP routing, and static routing. In case all three routing policies are present, the priority is: policy-based routing > static routing > ISP routing.

### 2. Configuration Steps

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

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

PBR List										
<input type="checkbox"/>	Name	Protocol	Src IP	Dest IP	Src Port Range	Dest Port Range	Outbound Interface	Status	Action	
Up to <b>30</b> entries can be added.										
The route is unreachable. Initiate a Ping test from the outbound interface to the next hop.										
<input type="checkbox"/>									<a href="#">+ Add</a> <a href="#">Batch Delete</a>	
No Data										
									Total 0	



**Table 5-3 Description of Policy-based Routing**

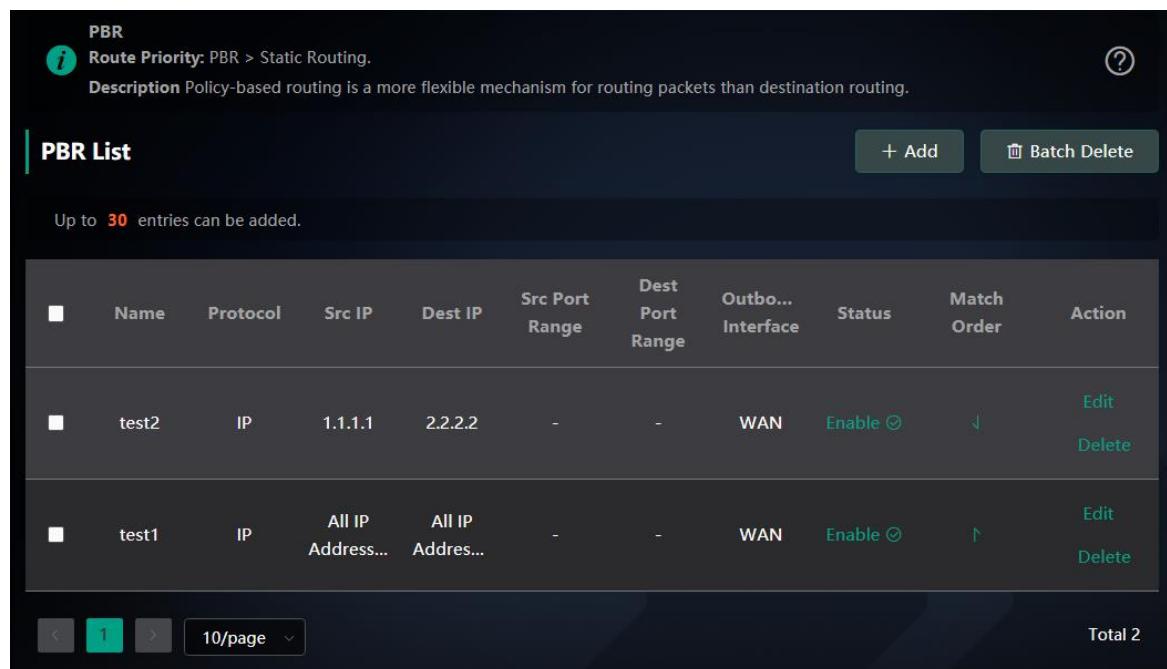
Parameter	Description
Name	The name of the PBR rule, as the identifier of the PBR route. The name must be unique.
Protocol Type	The protocol for the PBR route to take effect, which can be IP, ICMP, UDP, TCP, or a custom protocol type as needed.
Protocol Number	When the protocol type is Custom, the protocol number is required.
Src IP/IP Range	<p>The source IP/IP range to which the PBR rule matches. By default, All IP is selected.</p> <ul style="list-style-type: none"> <li>● All IP: Matches all source IP addresses.</li> <li>● Custom: Matches source IP addresses in the specified range.</li> </ul>
Custom Src IP	The source IP address or range is required when the matching source IP/IP range is Custom.
Dest IP/IP Range	<p>The destination IP/IP range to which the PBR rule matches. By default, All IP is selected.</p> <ul style="list-style-type: none"> <li>● All IP: Matches all destination IP addresses.</li> <li>● Custom: Matches destination IP addresses in the specified range.</li> </ul>
Custom Dest IP	The destination IP address or range is required when the matching destination IP/IP range is 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.

Parameter	Description
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.



	Name	Protocol	Src IP	Dest IP	Src Port Range	Dest Port Range	Outbound Interface	Status	Match Order	Action
<input type="checkbox"/>	test2	IP	1.1.1.1	2.2.2.2	-	-	WAN	Enable 		 
<input type="checkbox"/>	test1	IP	All IP Address...	All IP Address...	-	-	WAN	Enable 		 

## 5.18 Configuring Game Port Guarantee

### Note

This feature is only supported on E6.

Smartphone View: Choose **More > Switch to PC view > More > Advanced > Game Port Guarantee**.

PC View: Choose **More > Advanced > Game Port Guarantee**.

## 1. Overview

In a home network, it is often the case that one client occupies a large amount of bandwidth when downloading resources, causing slow Internet connection for other clients. In order to protect the Internet experience (especially gaming experience) of other clients in this situation, you can connect a specific client to the GAME port (LAN4) of the router using an Ethernet cable and enable **Game Port Guarantee** on the router. This can ensure a smooth gaming experience even when other clients are consuming large amounts of bandwidth.

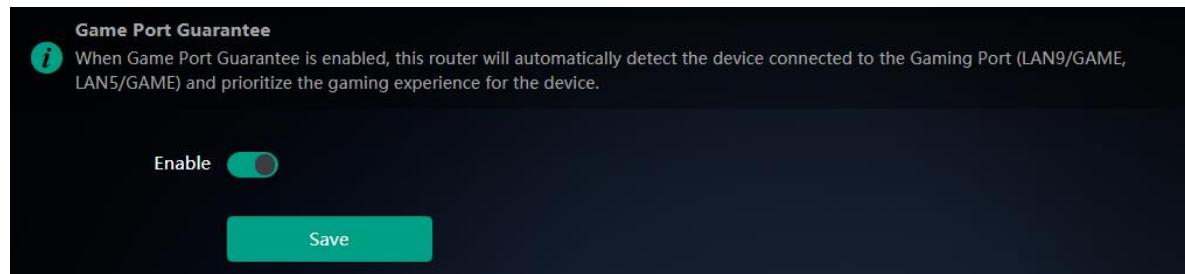
If the basic average latency of the Internet is lower than 25 ms, even if other clients or gaming clients connected to the GAME port are performing heavy traffic downloads, the gaming latency of the gaming client connected to the GAME port can be guaranteed to be 40 ms or lower.

## 2. Configuring Steps

First, connect the client to the GAME port of the router using an Ethernet cable. Then, access the router's web interface and enable **Game Port Guarantee** by choosing **More > Advanced > Game Port Guarantee**. Next, click **Save**.

### Note

**Game Port Guarantee** is automatically disabled if **Link Aggregation** or **IPTV** is configured on the GAME port.



## 5.19 Enabling Smart Flow Control

### 5.19.1 Enabling Smart Flow Control

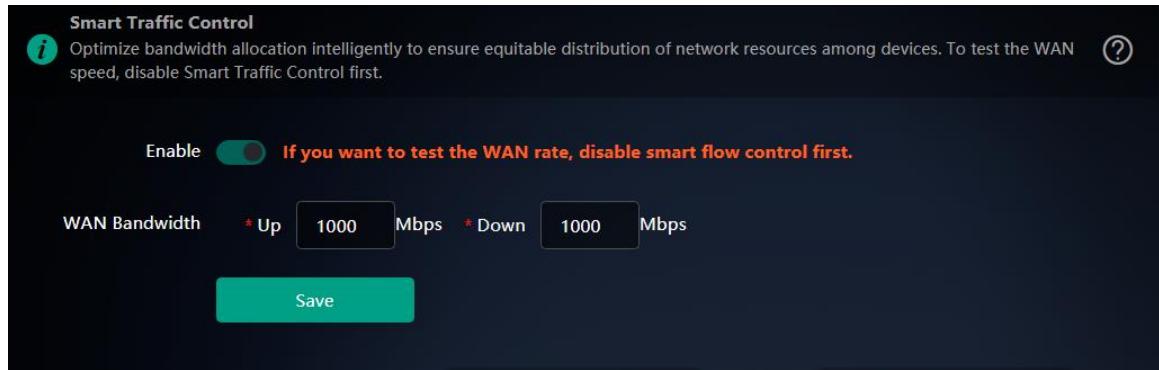
Smartphone View: Choose **More > Switch to PC view > More > Advanced > Flow Control > Smart Flow Control**.

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

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

### Caution

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

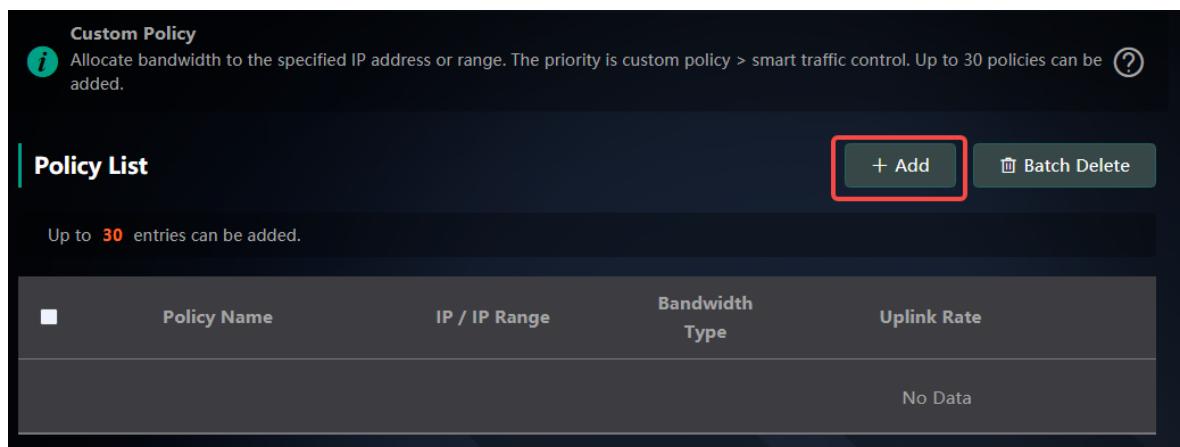


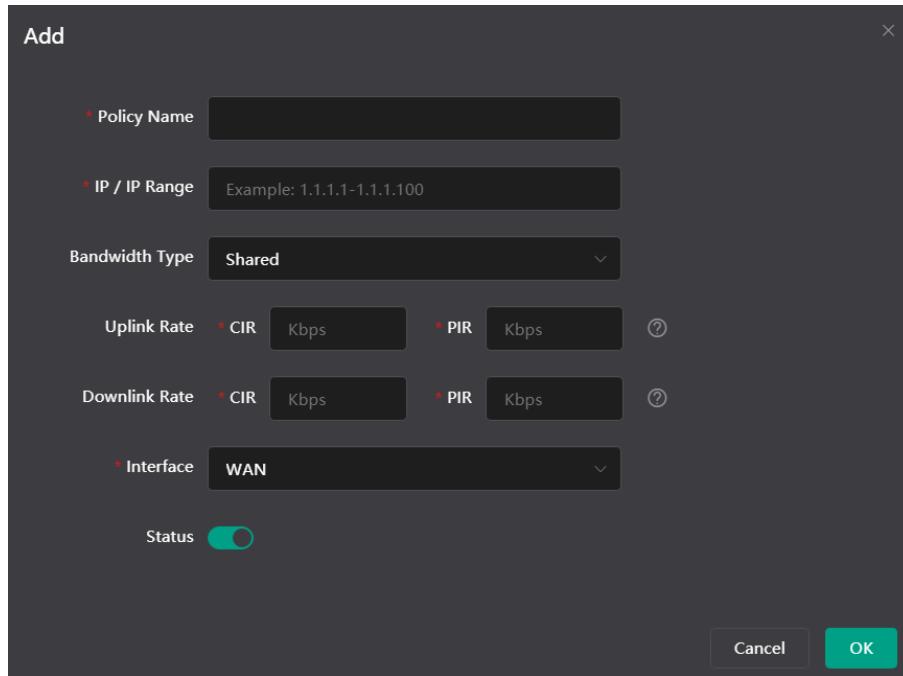
## 5.19.2 Custom Policy

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

PC View: Choose **More > Advanced > Flow Control > Custom Policy**.

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



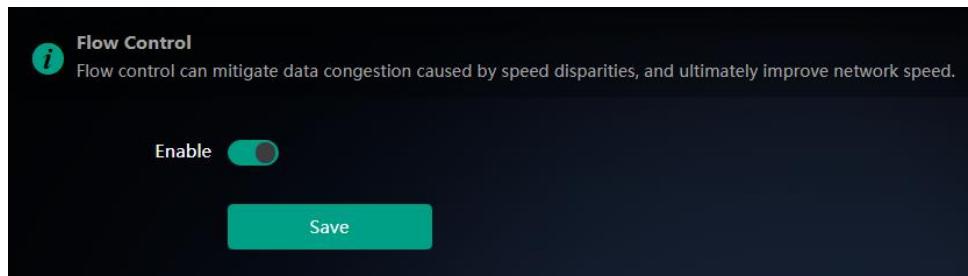


## 5.20 Enabling Port-Based Flow Control

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.



## 5.21 Enabling Hardware Acceleration

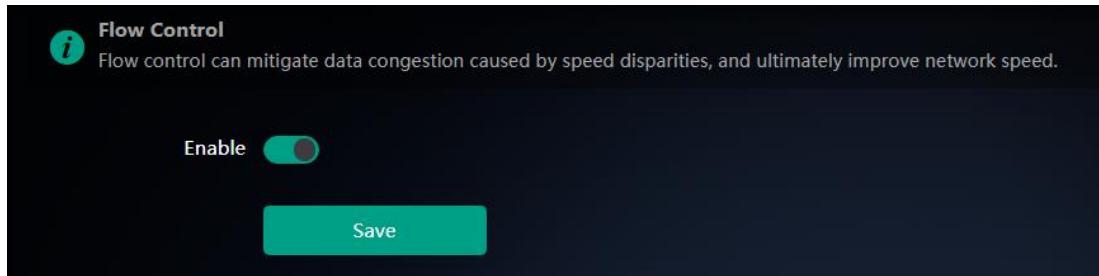
### ⚠ Caution

- This feature is supported in router mode.
- 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.



## 5.22 Enabling Reyee Mesh

---

### **i** Note

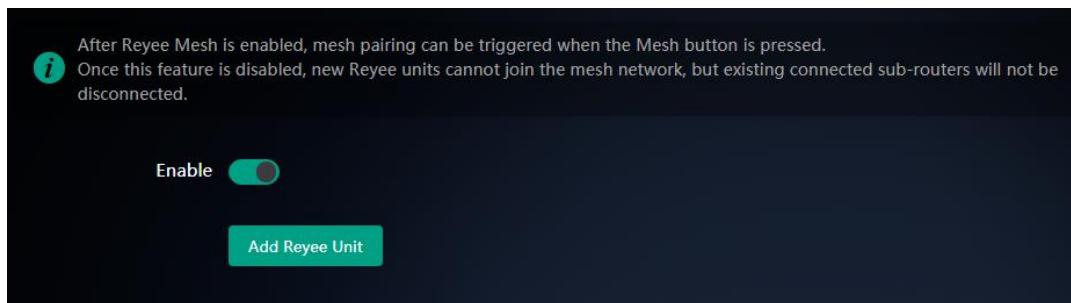
When Reyee Mesh is disabled, bridged mesh repeaters will not be disconnected.

---

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 **Add Reyee Unit** button to start mesh pairing. When Reyee Mesh is disabled, no action will be triggered by pressing the **Add Reyee Unit** button.



## 5.23 Configuring UPnP

---

### **⚠ Caution**

This feature is supported in router mode.

---

### 5.23.1 Overview

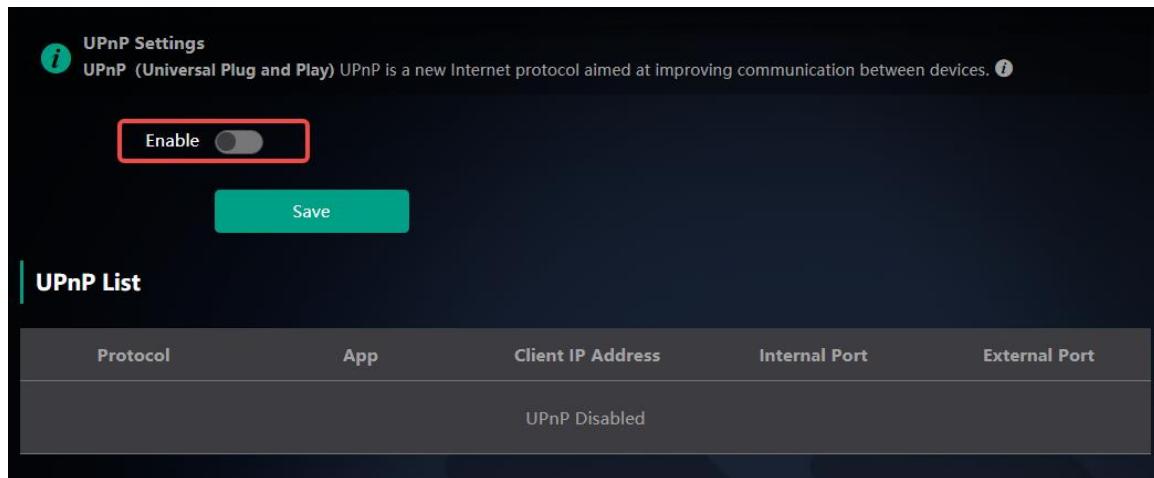
The universal plug and play (UPnP) function can map the port used by a client for Internet access according to the client's request so that related applications run faster or more stably. Common applications that support UPnP include MSN Messenger.

### 5.23.2 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.

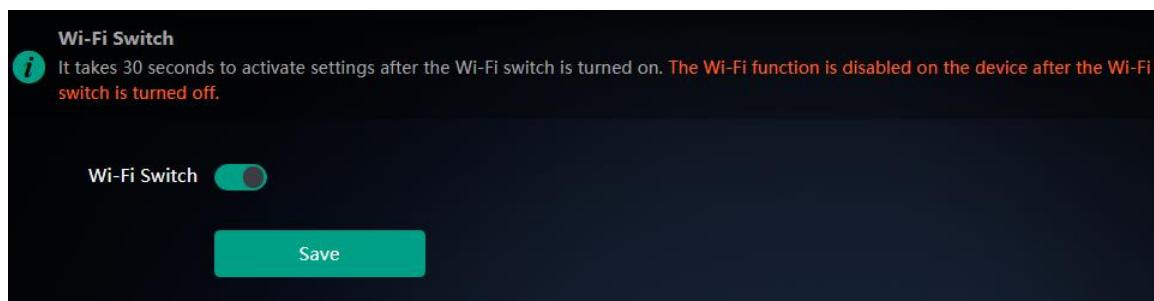


## 5.24 Enabling Wi-Fi Switch

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

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

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



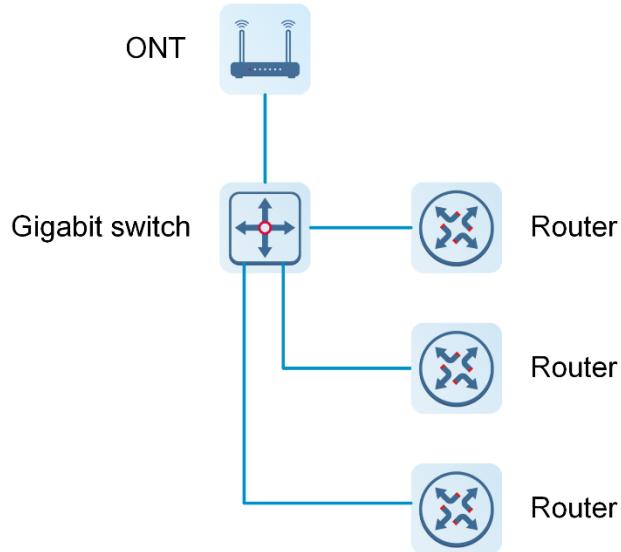
## 5.25 Configuring Reyee Mesh 3.0

### 5.25.1 Configuration Steps

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

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

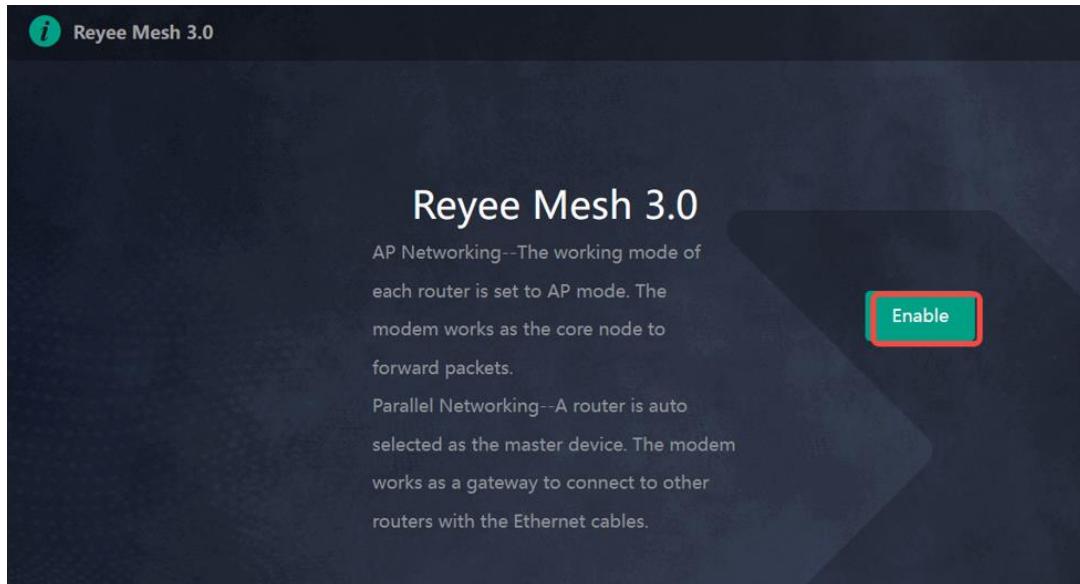
Connect the routers as indicated in the following figure:



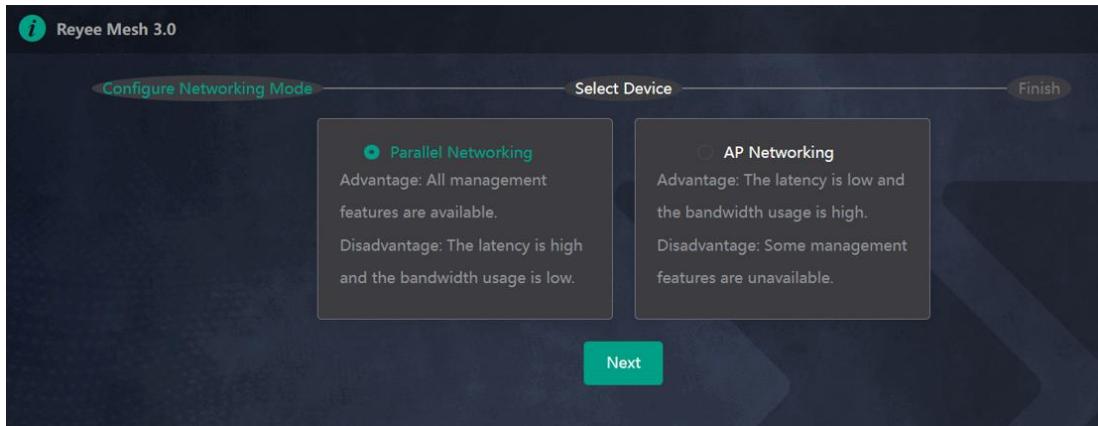
### 1. Parallel Networking

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

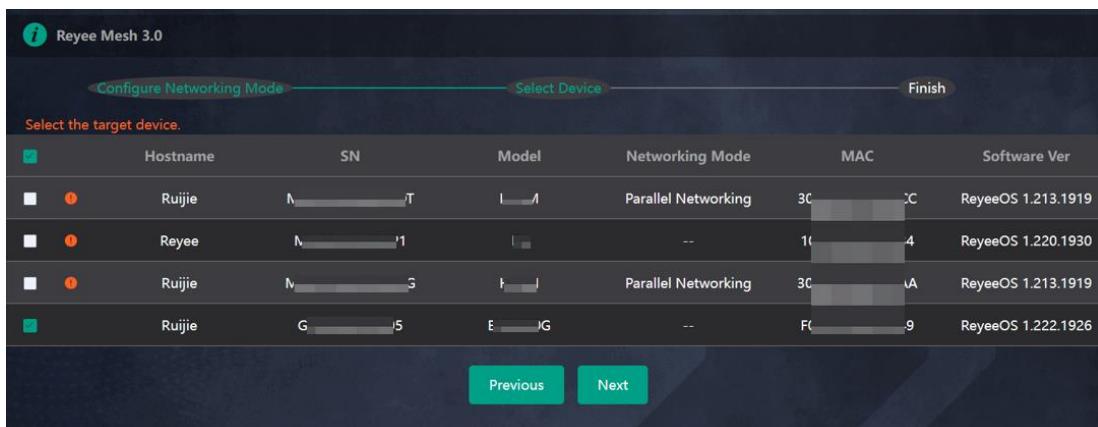
- (1) Click **Enable** to enable Reyee Mesh 3.0.



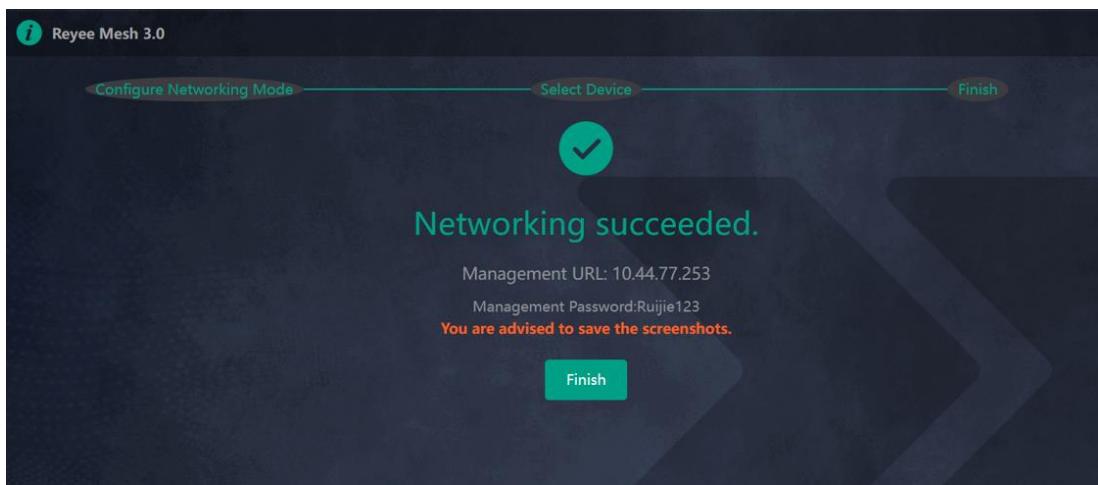
- (2) Choose Parallel Networking, and click **Next**.



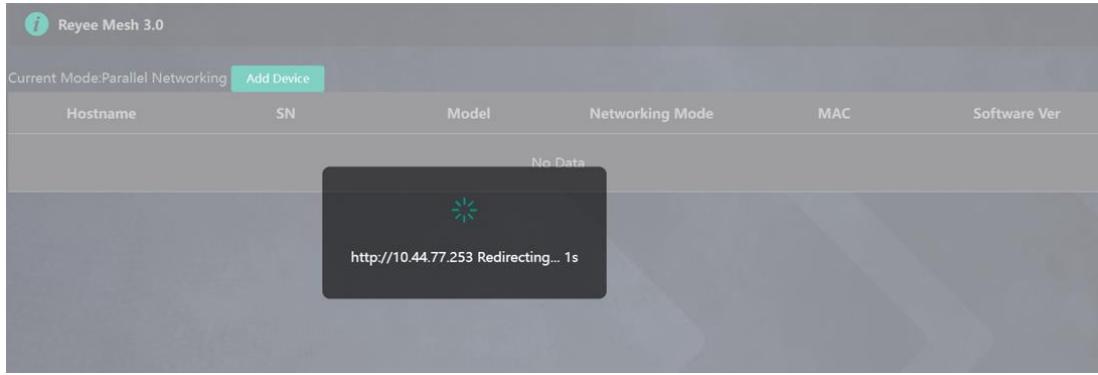
(3) Check routers for the networking.



(4) Click **Next**.



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

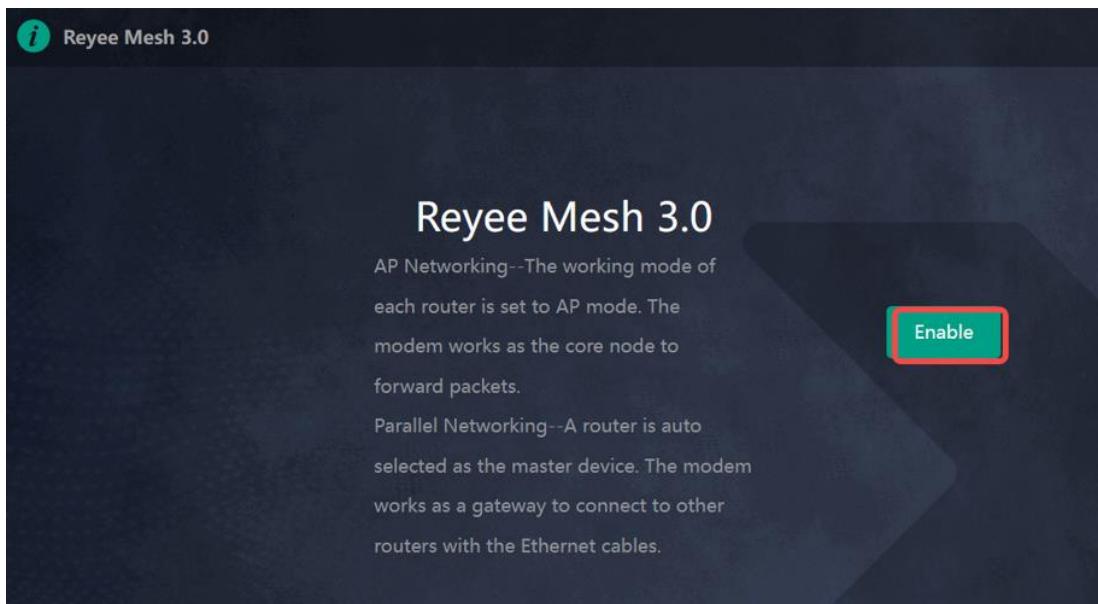


(6) On the master router page that is displayed, enter the password to log in.

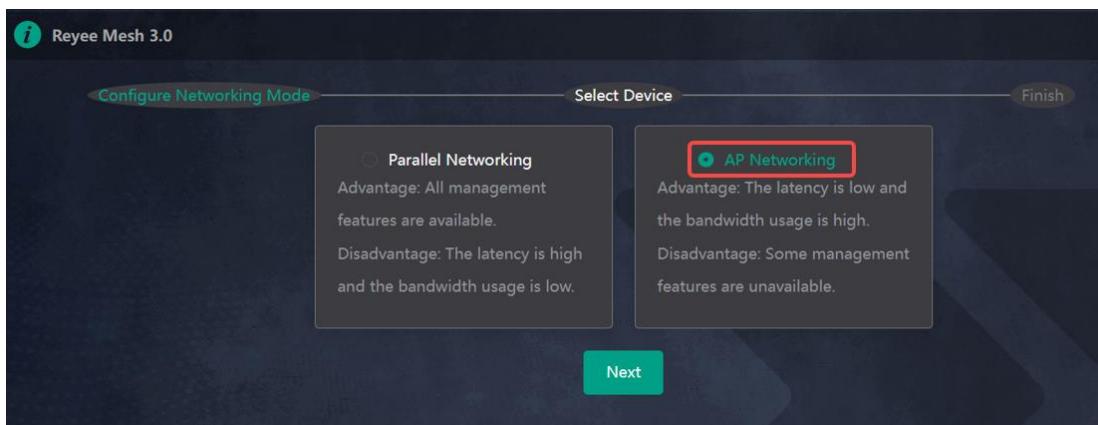
## 2. AP Networking

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

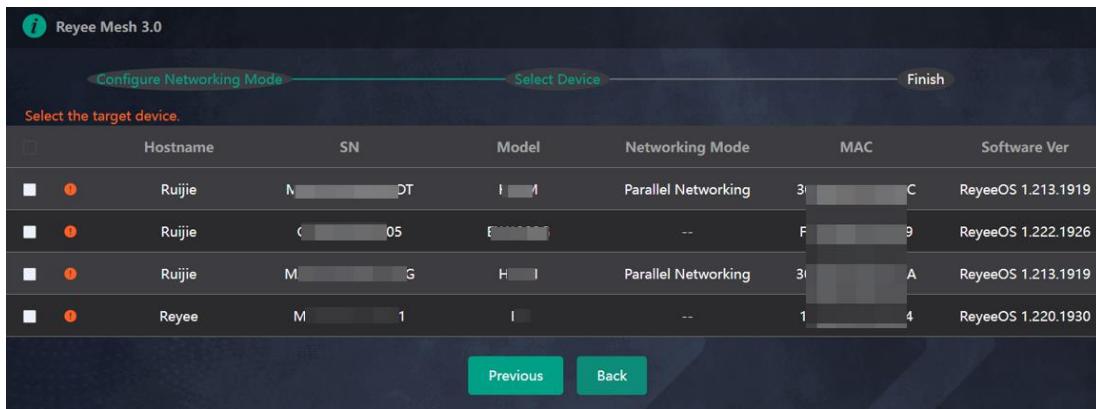
(1) Click **Enable** to enable Reyee Mesh 3.0.



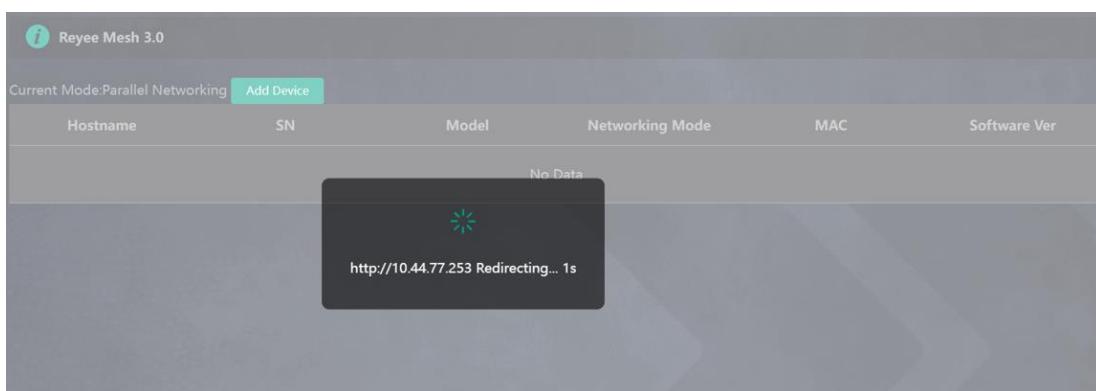
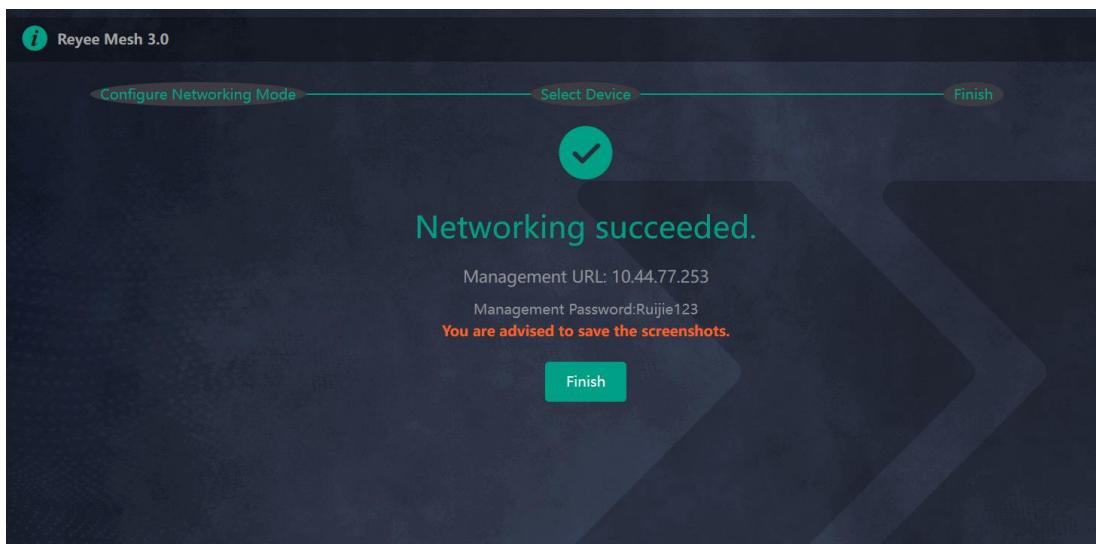
(2) Choose **AP networking**, and click **Next**.



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



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



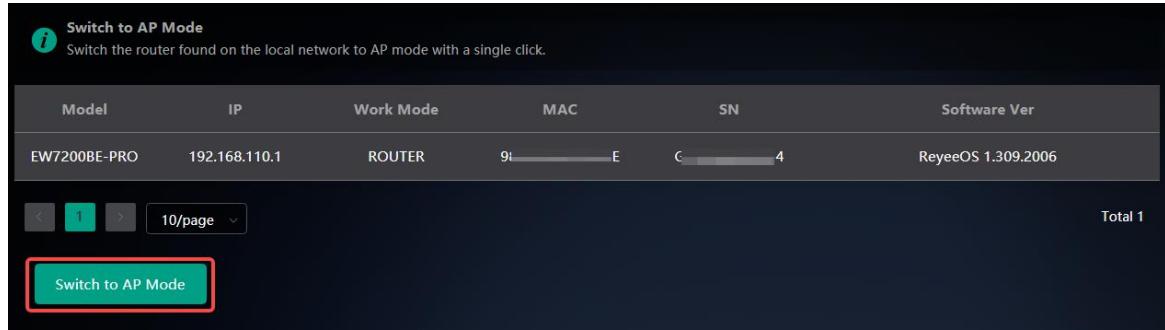
(5) On the master router page that is displayed, enter the password to log in.

## 5.26 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.



## 5.27 Other Settings

### ⚠ Caution

This feature is supported in router mode.

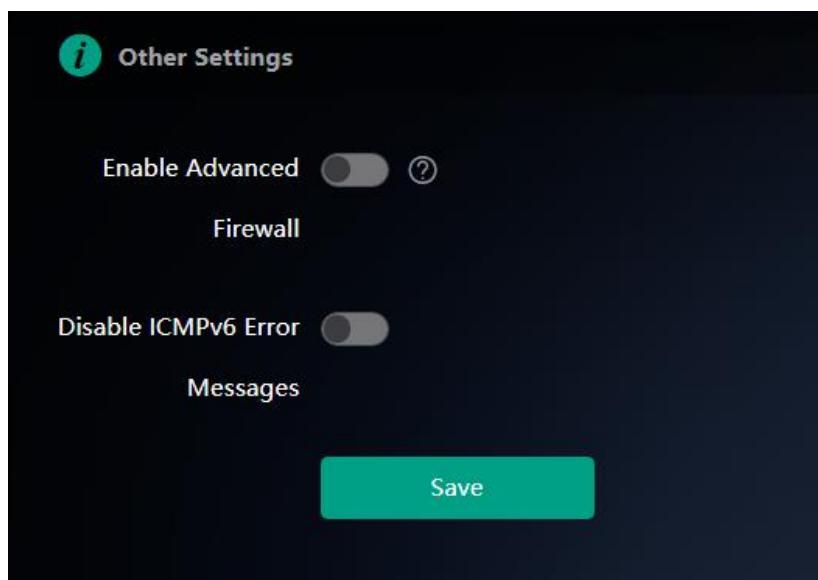
Smartphone View: Choose **More > Switch to PC view > More > Advanced > Other Settings**.

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.



# 6 Storage Management

## ⚠ Caution

- Supported file systems include FAT32, exFAT, EXT4, and NTFS. Using USB 3.0 mode may affect the performance of the 2.4 GHz Wi-Fi network.
- To access files on the storage device, ensure that the client is connected to the router's network first.
- After enabling the Samba service, do not unplug the hard drive directly to avoid data loss. To safely remove the hard drive, ensure that the Samba service is disabled first.

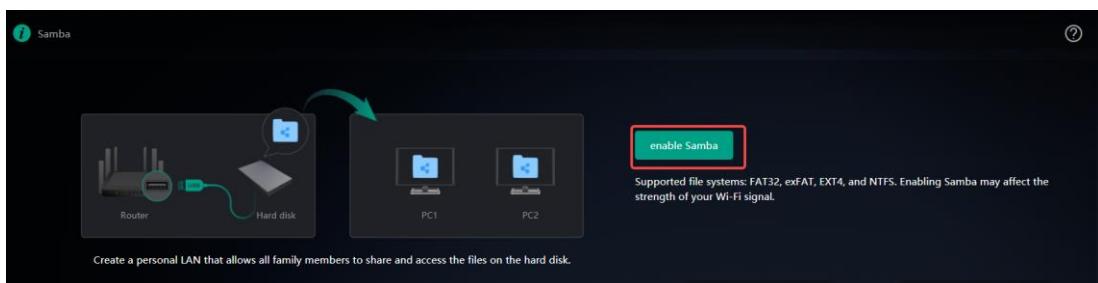
## 6.1 Enabling Samba

Smartphone View: Choose **More > Switch to PC view > More > Storage Management**.

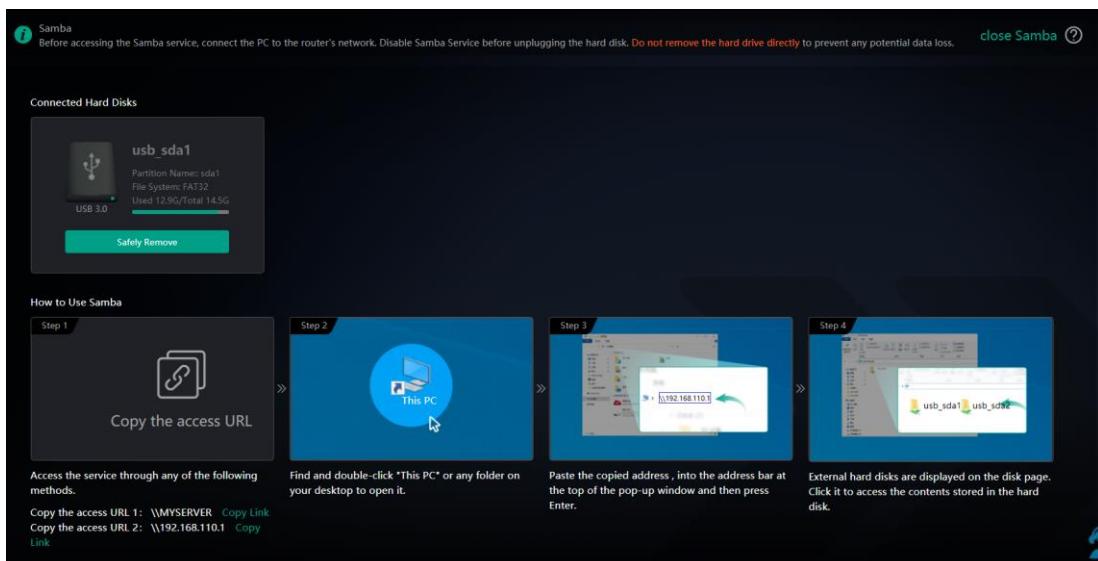
PC View: Choose **More > Storage Management**.

When **Samba** is enabled, clients on the same local area network can share files stored on the hard drive.

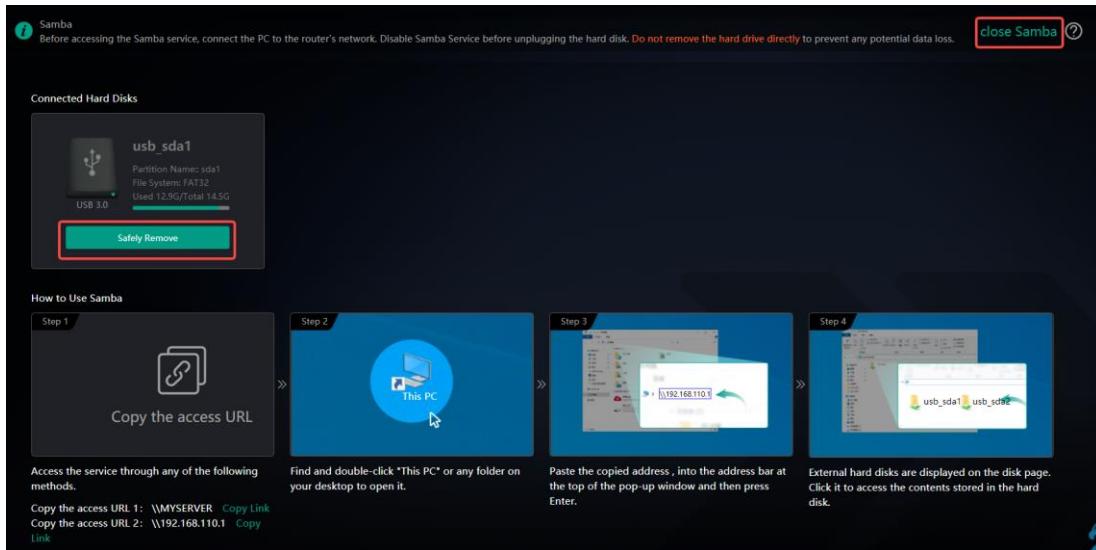
- Insert the storage device into the USB port of the BE72 PRO, and then click **enable Samba**.



- You will see the connected USB device on the page, as well as usage instructions for the Windows system.

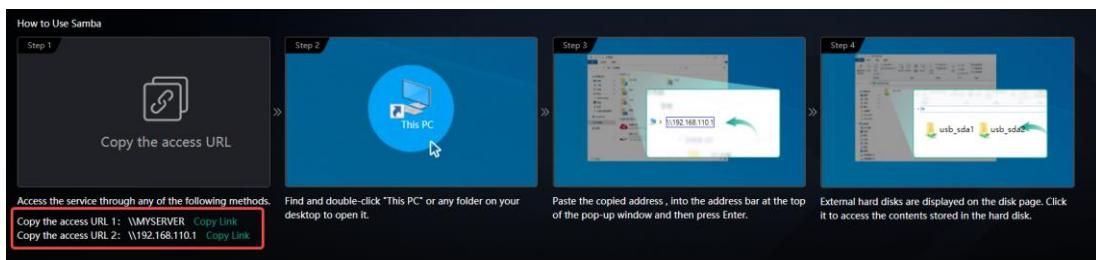


- Click **Safely Remove** to disconnect the current USB device. All devices will be automatically removed if you click **close Samba**.

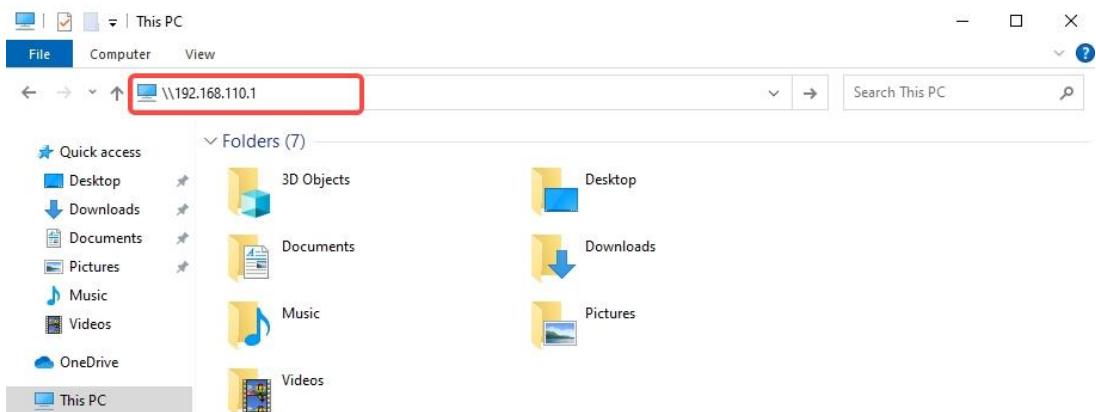


## 6.2 Accessing Samba Shared Files on a Windows Client

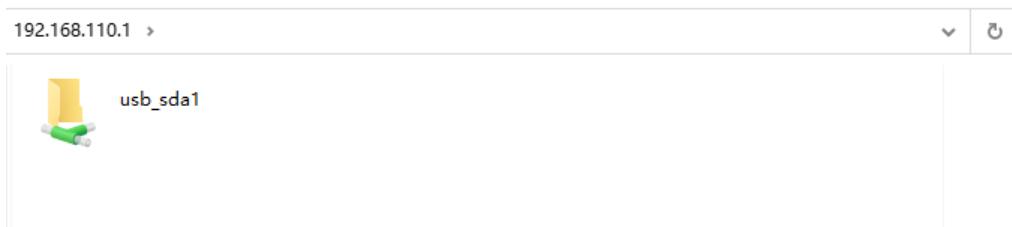
- After enabling the Samba service, click **Copy Link** to copy the access URL.



- Go back to the desktop, double-click **This PC** or any folder, paste the copied address in the address bar, and then press **Enter**.

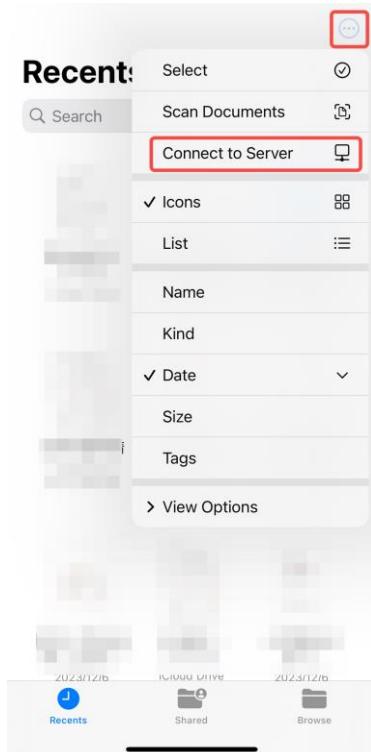


- Click the designated drive to access the files in the hard disk drive.

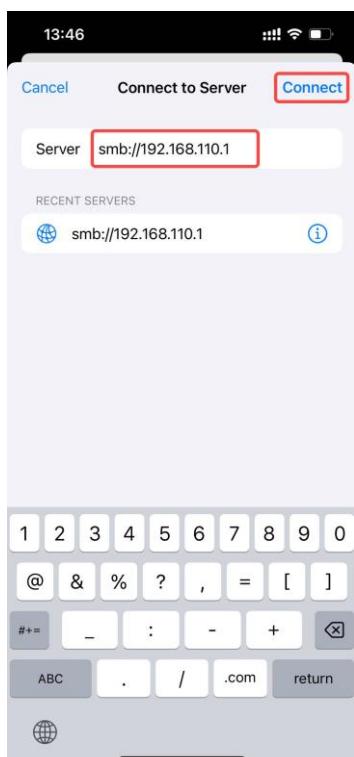


## 6.3 Accessing Samba Shared Files on an iOS Client

- (1) Open the **Files** app on your iOS device, tap the More icon in the top right corner, and select **Connect to Server**.



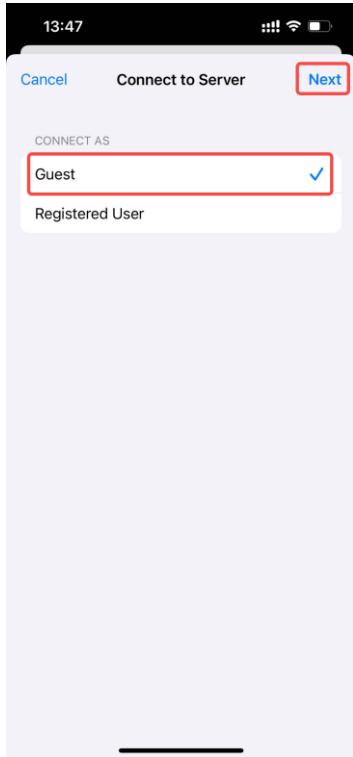
- (2) Enter **smb://192.168.110.1** in the **Server** field and click **Connect**.



**Note**

The IP address entered in the **Server** field is the router's management address, using the default address 192.168.110.1 as an example. If the management address changes, enter the updated management address.

(3) Select **Guest** and click **Next**.



(4) Tap the designated drive to access the files in the hard disk drive.

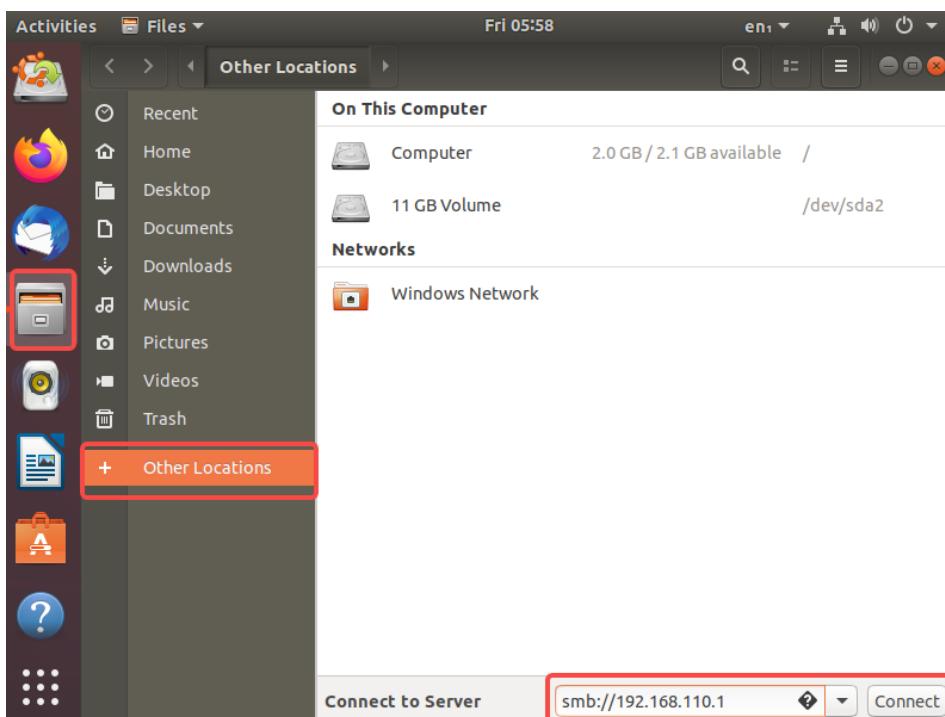


## 6.4 Accessing Samba Shared Files on a Linux Client

Before using this feature on a Linux client, you need to install `smbclient`. Open the CLI and enter the following command:

```
sudo apt-get install smbclient
```

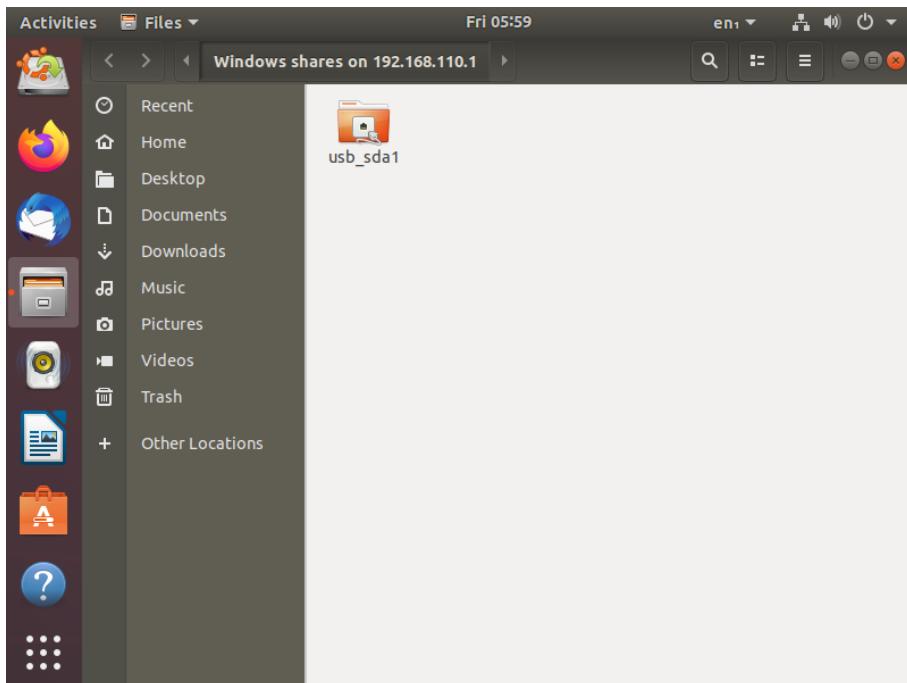
- (1) Open the file, click **Other Locations**. In the **Connect to Server** field, enter `smb://192.168.110.1` or `smb://MYSERVER`, and then click **Connect**.



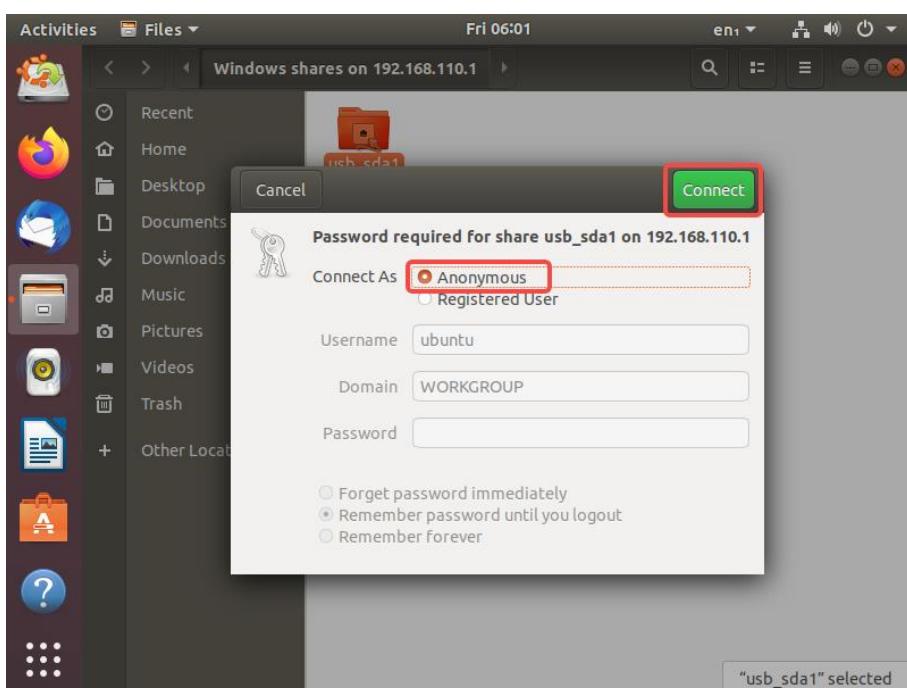
**Note**

The IP address entered in the **Server** field is the router's management address, using the default address 192.168.110.1 as an example. If the management address changes, enter the updated management address.

(2) Upon successful connection, the shared folder will be displayed.



(3) Click the shared folder, select **Anonymous**, and then click **Connect** to access the shared files.



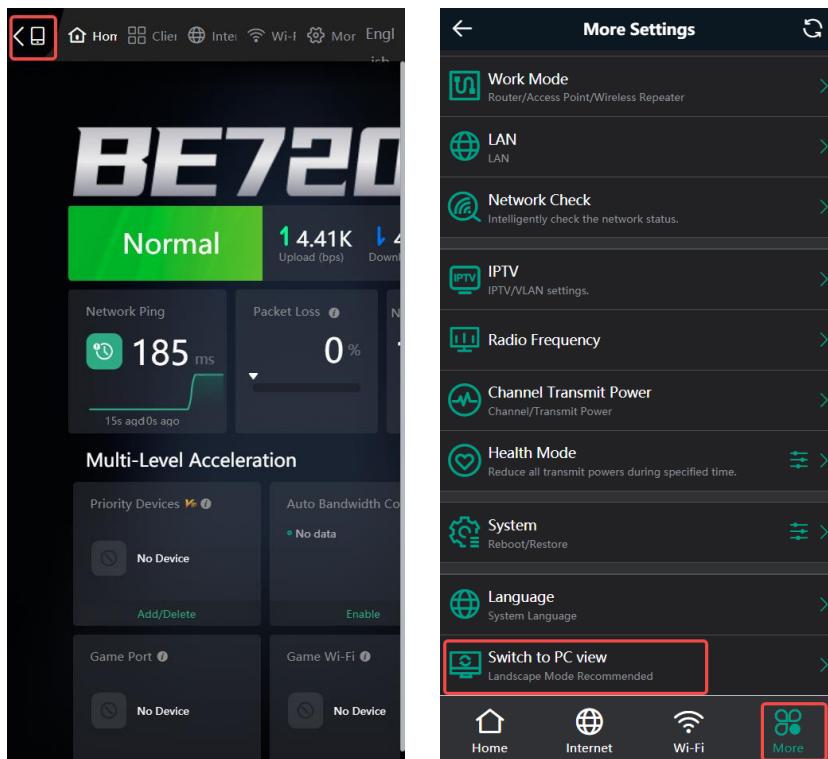
# 7 System Settings

## 7.1 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).

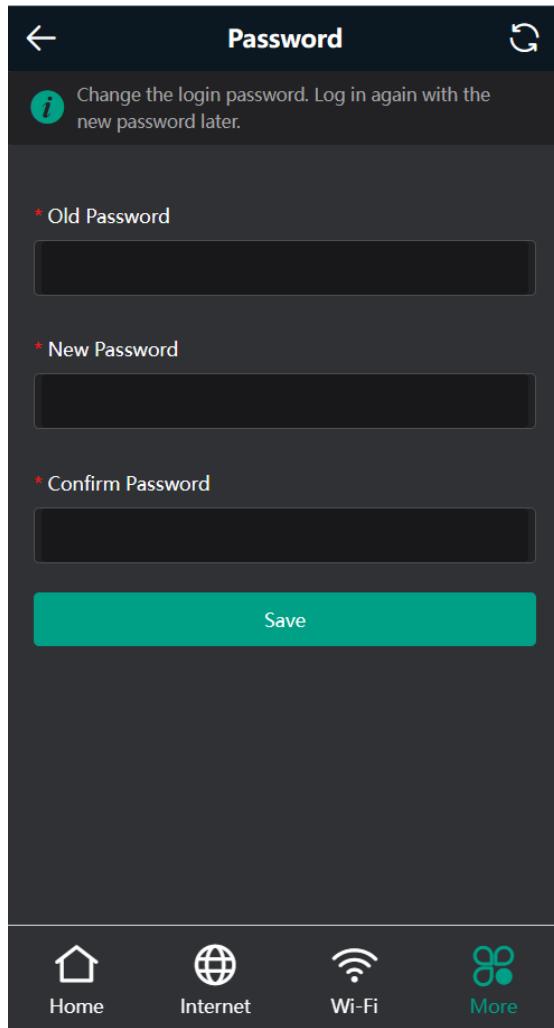


## 7.2 Configuring the Login Password

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

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

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

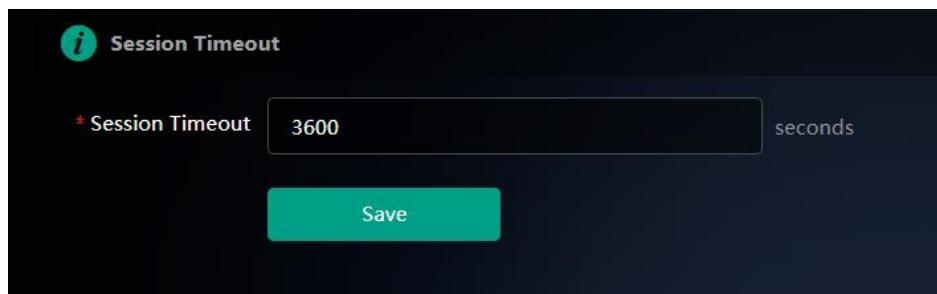


### 7.3 Configuring Session Timeout Duration

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.



**Remote Access**

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

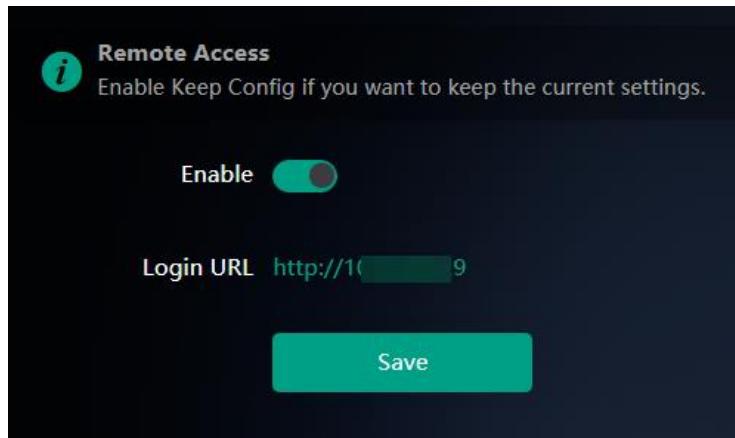
PC View: Choose **More > System > Login > Remote Access**.

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

#### **Caution**

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

This function cannot be enabled if the device management password has a weak security strength, such as being purely numerical or alphabetical. See [7.2 Configuring the Login Password](#) to configure a strong and secure device management password.



## 7.5 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.

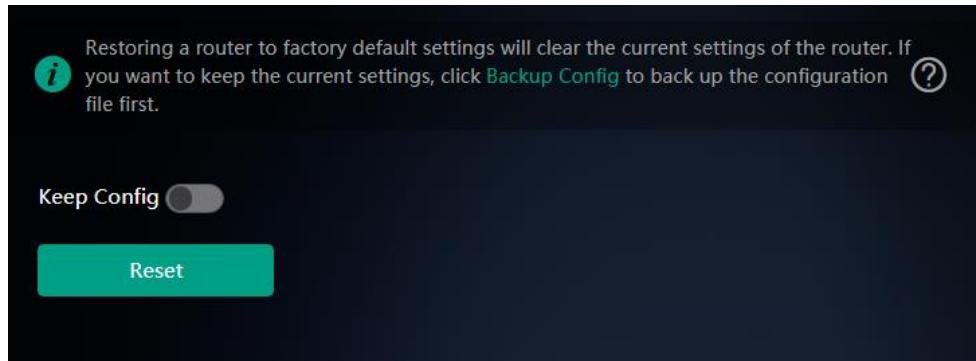
Click **Reset** to restore factory settings.

#### **Caution**

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.



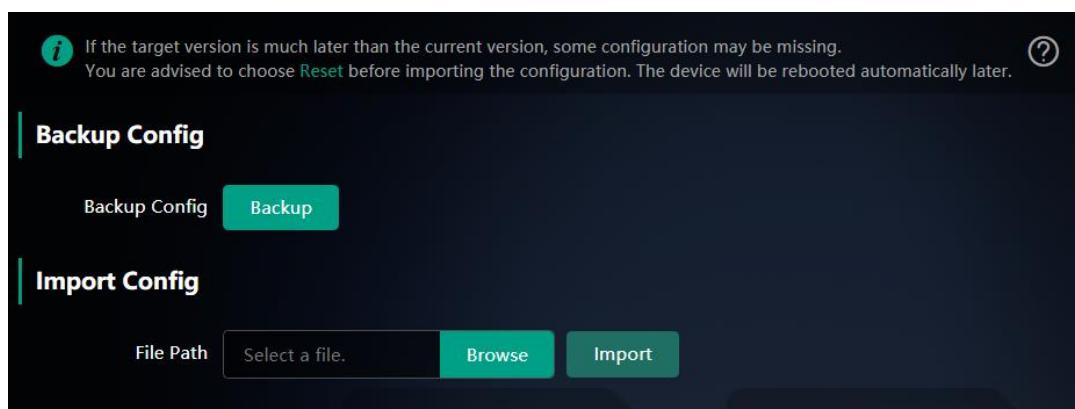
## 7.6 Configuring Config Backup and Import

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.

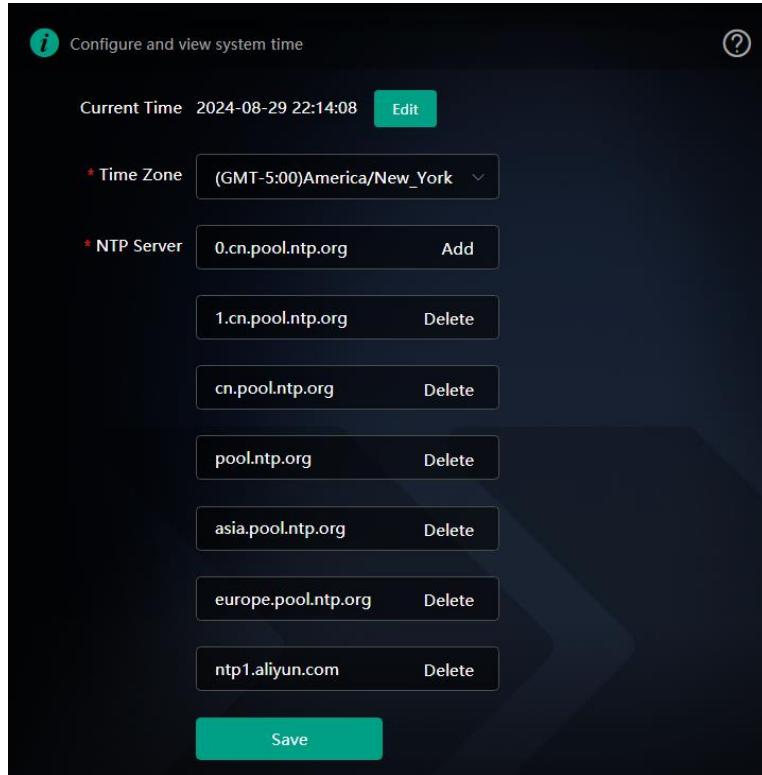


## 7.7 Configuring System Time

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.



## 7.8 Configuring Scheduled Reboot

### 7.8.1 Getting Started

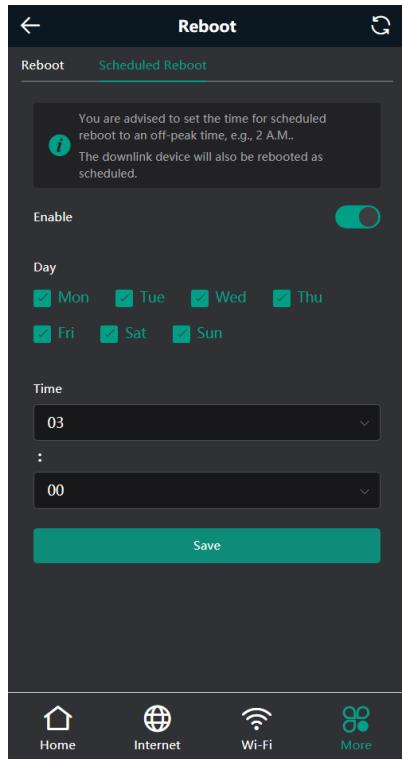
Confirm that the system time is accurate to avoid network interruption caused by device reboot at the wrong time. For details, see [7.6 Configuring Config Backup and Import](#).

### 7.8.2 Configuration Steps

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



## 7.9 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.

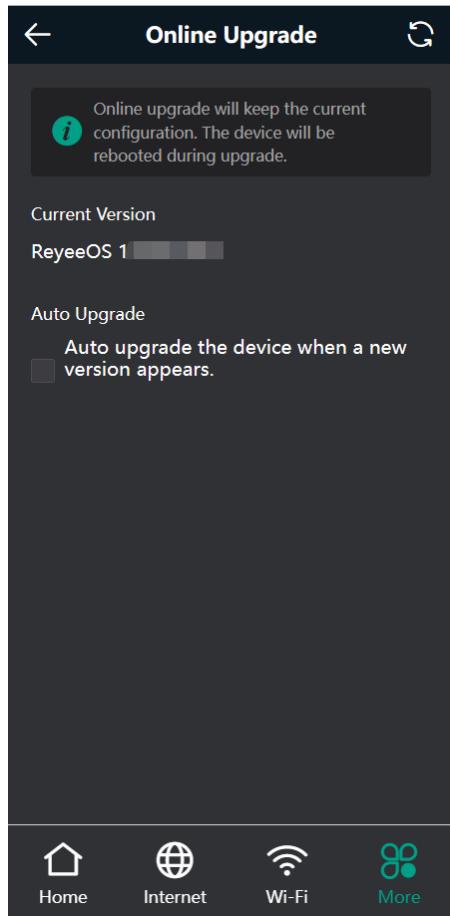
---

### 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.

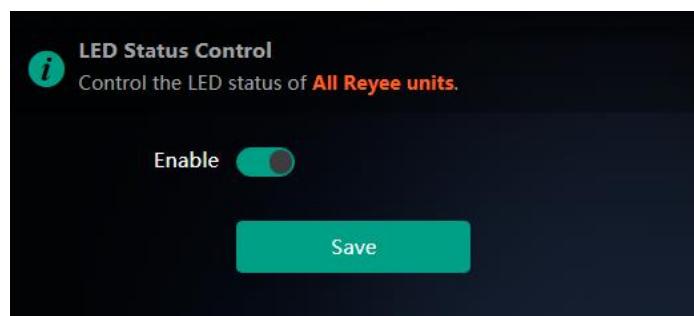
---



## 7.10 Turning On/Off the Indicator

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

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



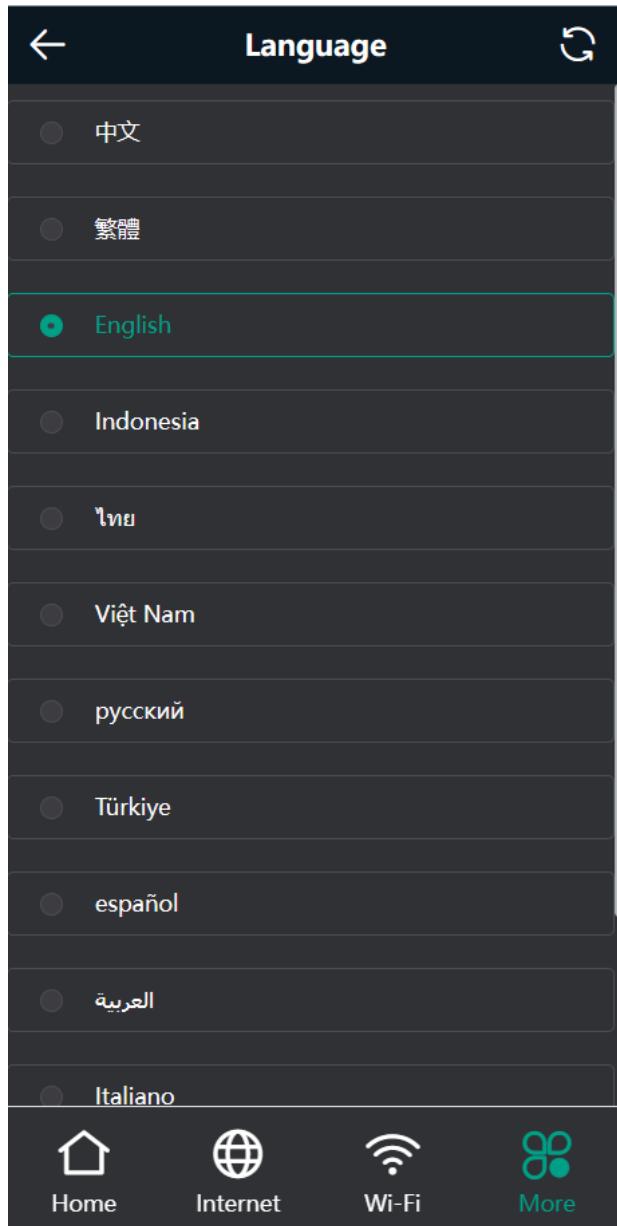
## 7.11 Switching System Language

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

English ▾

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

Click a required language to switch the system language.



## 7.12 Configuring Diagnostics

### **⚠ Caution**

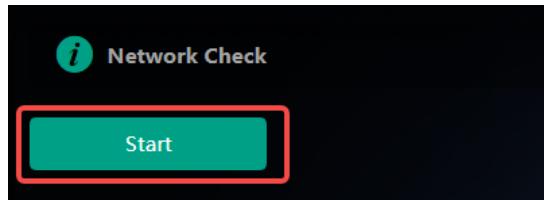
If the issue persists despite following the troubleshooting methods provided in this section, you may require remote support from a technician who will enable developer mode to resolve the issue. We will ensure your data is protected during this process.

### 7.12.1 Network Check

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.

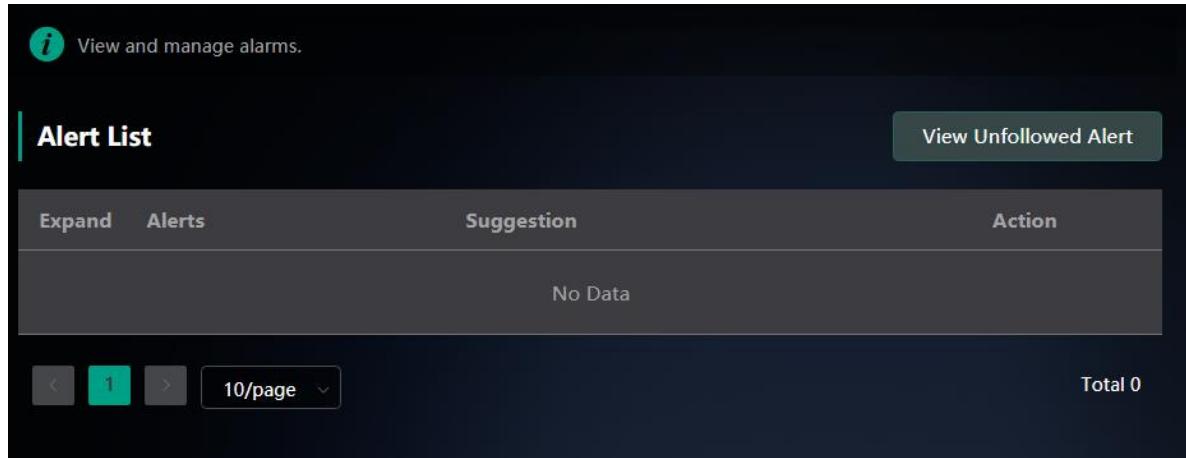


### 7.12.2 Alerts

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.

**Table 7-1 Alerts and Suggested Action**

Alerts	Suggested Action
The WAN port has no link.	Please check whether a cable is plugged into the WAN port.
The port is operating at 10Mbps.	Please check the peer port settings, unplug and re-plug the cable, or replace the cable.

Alerts	Suggested Action
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.

### 7.12.3 Network Diagnosis Tools

#### 1. Network Test Tool

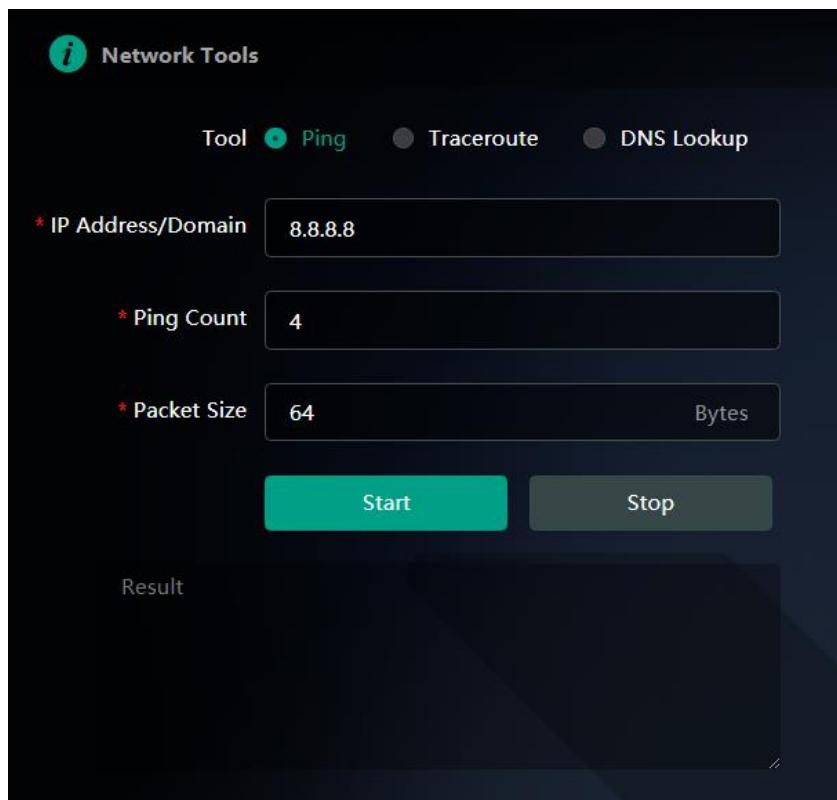
Smartphone View: Choose **More > System > Network Tools**.

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

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

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

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



## 2. 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 FAQs

## 8.1 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.

## 8.2 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 Ruijie Reyee App.
  - If the fault persists, restore the router to factory settings. The management password will also be restored to the default Wi-Fi password.

## 8.3 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 [2.4 Manage the Device After Successful Setup](#).

## 8.4 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, please email us at [service\\_rj@ruijenetworks.com](mailto:service_rj@ruijenetworks.com).