# Reyee Mesh Routers
# Web-based Configuration Guide

## ReyeeOS 1.77.1321



Document Version: V1.0
Date: 2022-02-16

# Contents


Preface ..... 6

1 Fast Internet Access ..... 8

1.1 Connecting to the Router ..... 8

1.2 Logging in ..... 8

1.3 Internet Access Mode ..... 9

1.4 Primary Router Mode ..... 9

1.4.1 Getting Started ..... 9

1.4.2 Configuration Steps ..... 10

1.4.3 Verification and Testing ..... 12

1.4.4 Forgetting the PPPoE Account ..... 13

1.5 Secondary Router Mode ..... 13

1.5.1 Getting Started ..... 13

1.5.2 Configuration Steps ..... 13

1.5.3 Verification and Testing ..... 15

1.6 Mesh Pairing ..... 15

1.6.1 Performing Mesh Pairing through the Mesh Button ..... 15

1.6.2 Configuring Mesh Pairing on the Management Page ..... 16

1.6.3 Managing Secondary Router ..... 17

1.6.4 Enabling Reyee Mesh ..... 18

1.6.5 Troubleshooting ..... 18

2 Wi-Fi Network Settings ..... 20

2.1 Changing the SSID and Password ..... 20

2.2 Hiding the SSID ..... 20

2.2.1 Overview ..... 20
2.2.2 Getting Started ..... 20
2.2.3 Configuration Steps ..... 20
2.3 Enabling Band Steering ..... 21
2.4 Adding a Wi-Fi Network ..... 22
2.4.1 Overview ..... 22
2.4.2 Configuration Steps ..... 23
2.4.3 Verification and Testing ..... 23
2.5 Configuring the Wi-Fi Blacklist or Whitelist ..... 23
2.5.1 Overview ..... 23
2.5.2 Configuration Steps ..... 24
2.6 Enabling Smart Optimization ..... 25
2.7 Optimizing the Wi-Fi Network ..... 27
2.7.1 Overview ..... 27
2.7.2 Getting Started ..... 27
2.7.3 Configuration Steps ..... 27
2.8 Configuring the Healthy Mode ..... 30
3 Networks Settings ..... 32
3.1 Configuring Internet Connection Type ..... 32
3.2 Changing the Address of a LAN Port ..... 32
3.3 Changing the MAC Address ..... 32
3.4 Changing the MTU ..... 33
3.5 Configuring the Repeater Mode ..... 34
3.5.1 Wired Repeater ..... 34

3.5.2 Wireless Repeater ..... 35
3.6 Configuring IPv6 Address ..... 36
3.6.1 Configuring the IPv6 Address of the WAN Port ..... 36
3.6.2 Configuring the IPv6 Address of the LAN Port ..... 37
3.7 Enabling Parental Control ..... 39
3.8 Configuring XPress ..... 39
3.9 Configuring Port Mapping ..... 40
3.9.1 Overview ..... 40
3.9.2 Getting Started ..... 41
3.9.3 Configuration Steps ..... 41
3.9.4 Verification and Testing ..... 42
3.9.5 Solution to a Test Failure ..... 42
3.9.6 DMZ Configuration Steps ..... 42
3.10 Configuring DHCP Server ..... 42
3.10.1 Overview ..... 42
3.10.2 Configuration Steps ..... 43
3.11 Configuring DNS ..... 45
3.12 Configuring DDNS ..... 46
3.12.1 Overview ..... 46
3.12.2 Getting Started ..... 46
3.12.3 Configuration Steps ..... 46
3.13 Configuring APR Binding and Guard ..... 47
3.13.1 Overview ..... 47
3.13.2 Configuration Steps ..... 47

3.14 Connecting to IPTV ..... 48
3.14.1 Getting Started ..... 48
3.14.2 IPTV Configuration Steps (VLAN Type) ..... 48
3.14.3 IPTV Configuration Steps (IGMP Type) ..... 49
3.15 Enabling Hardware Acceleration ..... 49
3.16 Enabling Smart Flow Control ..... 50
3.17 Enabling Port-Based Flow Control ..... 51
3.18 Performing Advanced Network Settings ..... 51
3.19 Configuring UPnP ..... 52
3.19.1 Overview ..... 52
3.19.2 Configuration Steps ..... 52
3.20 Configuring PPTP VPN ..... 53
3.20.1 Overview ..... 53
3.20.2 Configuring PPTP Server ..... 53
3.20.3 Configuring PPTP Client ..... 54
4 System Settings ..... 55
4.1 Switching to PC View ..... 55
4.2 Configuring the Login Password ..... 56
4.3 Restoring Factory Settings ..... 57
4.4 Configuring System Time ..... 58
4.5 Configuring Scheduled Reboot ..... 58
4.5.1 Getting Started ..... 58
4.5.2 Configuration Steps ..... 58
4.6 Performing Online Upgrade and Displaying the System Version ..... 59

4.7 Turning On/Off the Indicator ..... 60

4.8 Switching System Language ..... 60

4.9 Enabling Alarms ..... 61

4.10 Diagnosing Network Problems ..... 63

4.11 Network Diagnosis Tools ..... 64

4.12 Configuring Config Backup and Import ..... 65

4.13 Configuring Session Timeout Duration ..... 66

# Preface

## Intended Audience

This document is intended for:

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

## Technical Support

- The official website of Reyee: https://www.ireyee.com/

## Conventions

### 1. GUI Symbols

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

### 2. Signs

The signs used in this document are described as follows:

**Danger**

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

**Warning**

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

**Caution**

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

**Note**

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

**Specification**

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

### 3. Note

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

# 1 Fast Internet Access

## 1.1 Connecting to the Router

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

- Wired Connection

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

- Wireless Connection

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

## 1.2 Logging in

After a PC connects to a router in the initial state, the configuration wizard page pops up. If the configuration page does not pop up, enter the device IP address into the address bar of the browser to navigate to the login page, and then enter the password for login.

**Table 1-1 Default Configuration**

| Item | Default Value |
| --- | --- |
| Device IP address | 192.168.110.1 |
| Username/Password | No username and password are required at your first login and you can configure the router directly. |

If you forget the IP address or password, hold down the **Reset** button for more than 3 seconds to restore factory settings. After restoration, you can use the default IP address and password to log in.

**Caution**

Restoring factory settings will delete existing configuration and you are required to configure Internet access again at your next login. Therefore, exercise caution when performing this operation.

If the router in the initial state detects that the IP address of the primary router is 192.168.110.1, the router automatically changes its own IP address to 192.168.111.1 to avoid an IP address conflict. You may fail to log in to the router during the IP address change, but can reconnect to the Wi-Fi network and complete configuration one minute later.

# 1.3 Internet Access Mode

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

**Primary Router Mode**: This mode is suitable for network creation. The router connects to the Internet through wired connection, and can manage secondary routers. You are advised to select the device with the best performance as the primary router. The primary router can work in PPPoE mode, Dynamic Host Configuration Protocol (DHCP) mode, and static IP address mode.

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

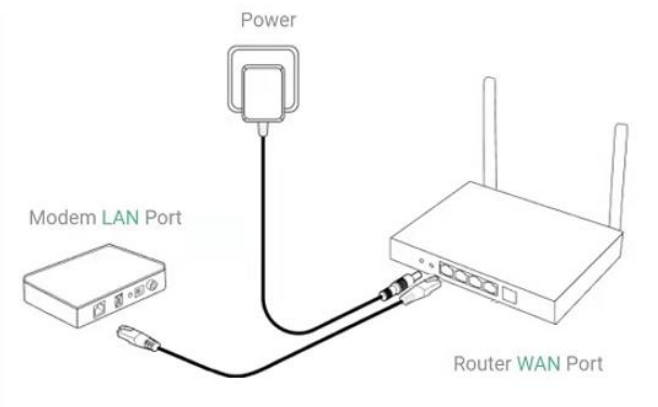
**Note**

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

# 1.4 Primary Router Mode

## 1.4.1 Getting Started

Connect the router to a power supply and connect the LAN port of a modem to the WAN port of the router. The yellow port is the WAN port, and other network ports are LAN ports.




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

- Figure out whether the Internet connection type is PPPoE, DHCP mode, or static IP address mode.
- In the PPPoE mode, a username, a password, and possibly a service name are needed.
- In the static IP address mode, an IP address, a subnet mask, a gateway, and a DNS server need to be configured.

## 1.4.2 Configuration Steps

### 1. Configuring the Internet Connection Type

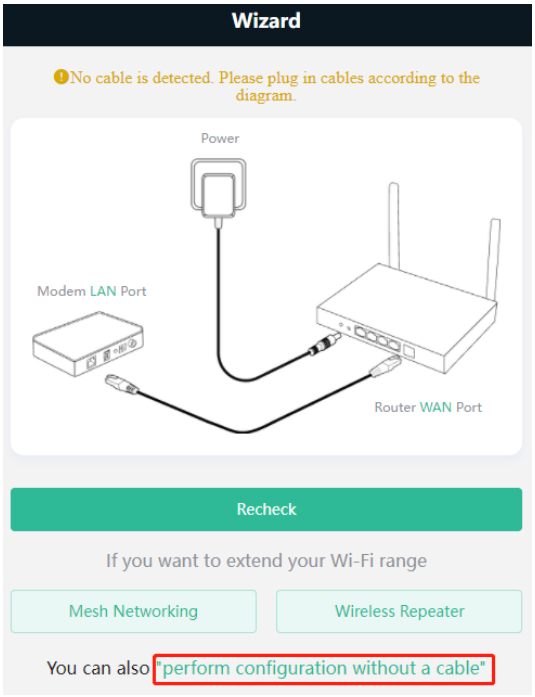
Click **Configure** and select the Internet connection type confirmed by the carrier.

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

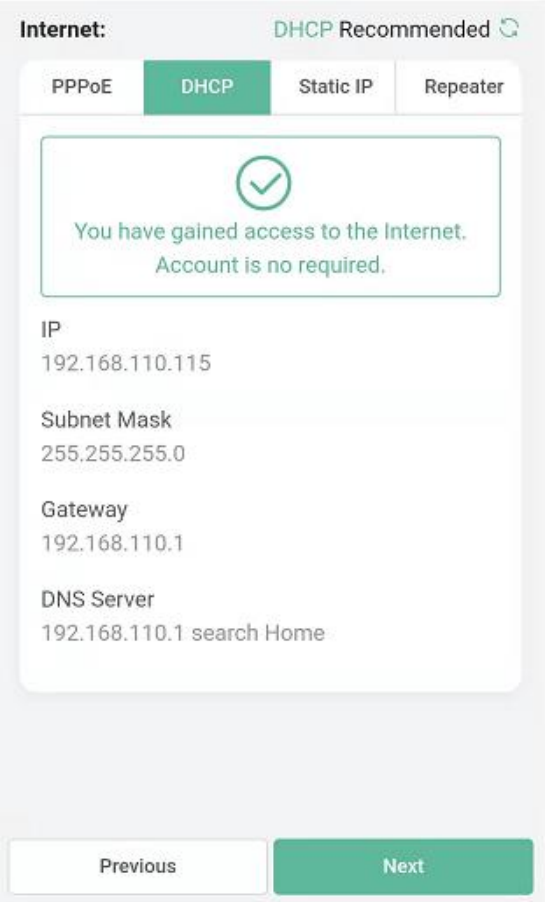
**Caution**

- If the IP address delivered by the primary router is also 192.168.110.0, the router automatically changes the IP address of its LAN interface to 192.168.111.1 to avoid conflicts. Do not change the configuration of the primary router by mistake. You can differentiate routers by checking the router model and Wi-Fi information on the home page.

- If the Ethernet cable is unplugged, you are prompted to connect the Ethernet cable first. Click **perform configuration without a cable** below to configure and connect the Ethernet cable.




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




## 2. Configuring a Wi-Fi Network

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

**Note**

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

(2) **Setting the SSID and Wi-Fi password**: The device has no Wi-Fi password by default, indicating that the Wi-Fi network is an open network. You are advised to configure a complex password to enhance the network security. The password must be a string of 8 to 31 characters, which can contain uppercase and lowercase letters, digits, and English characters but cannot contain special characters such as single quotation marks ('), double quotation marks ("), or spaces. The SSID (5G) is the name of the 5G radio. If the dual-band integration is enabled, set only one SSID.

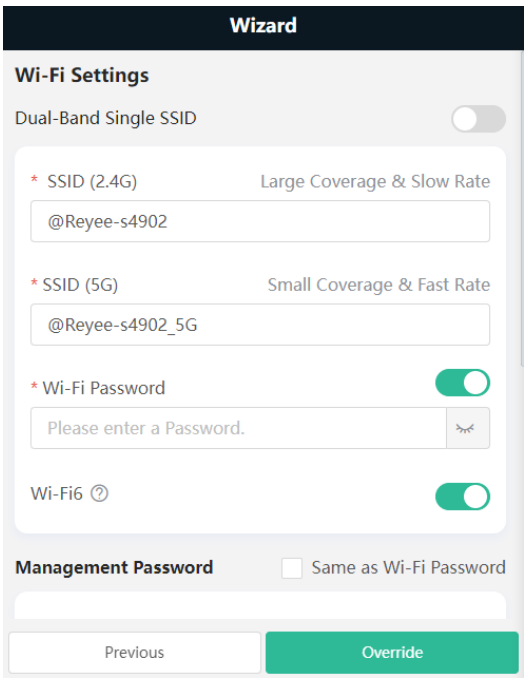
(3) **Setting the management password**: The password is used for logging in to the management page. The management password must be a string of 8 to 31 characters that contain at least three types among uppercase letters, lowercase letters, digits, and English characters but cannot contain **admin**, Chinese characters, spaces, or question marks (?). You can select **Same as Wi-Fi Password**.

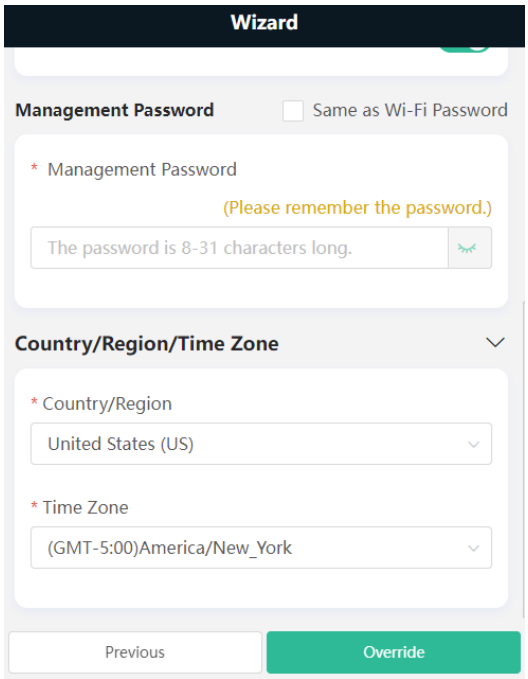
(4) **Enabling the Wi-Fi 6**: The Wi-Fi 6 can provide a faster and more stable network for Wi-Fi 6-capable clients. You are advised to enable this function.

(5) **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.

(6) **Setting time**: 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.

(7) **Overriding the configuration**: Click **Override**. The Wi-Fi network will be restarted. You need to enter the new Wi-Fi password to connect to the new Wi-Fi network.




## 1.4.3 Verification and Testing

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

**Note**

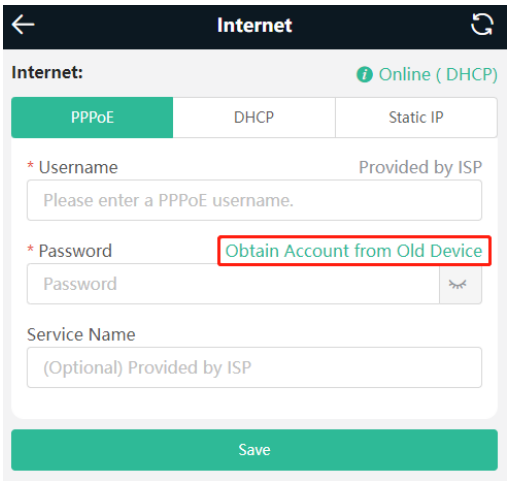
- The mobile phone view of the configuration may not be fully displayed on the vertical screen. You can view the complete network diagram on the horizontal screen.

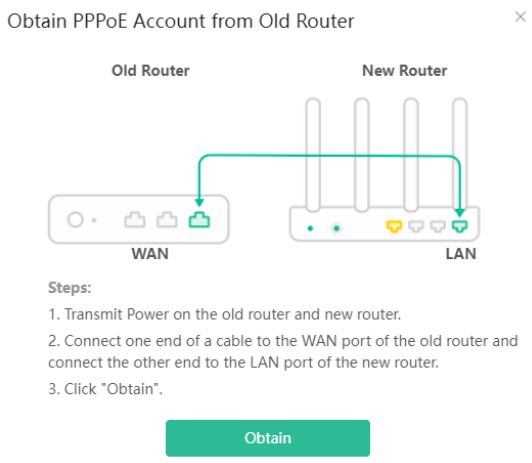



### 1.4.4 Forgetting the PPPoE Account

(1) Consult your local ISP.

(2) If you replace the old router with a new one, click **Obtain Account from Old Device**. Connect the old and new routers to a power supply and start them. Insert one end of an Ethernet cable into the WAN port of the old router and connect the other end to a LAN port of the new router, and click **Obtain**. The new router automatically fetches the PPPoE account of the old router. Click **Save** to make the configuration take effect.




## 1.5 Secondary Router Mode

### 1.5.1 Getting Started

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

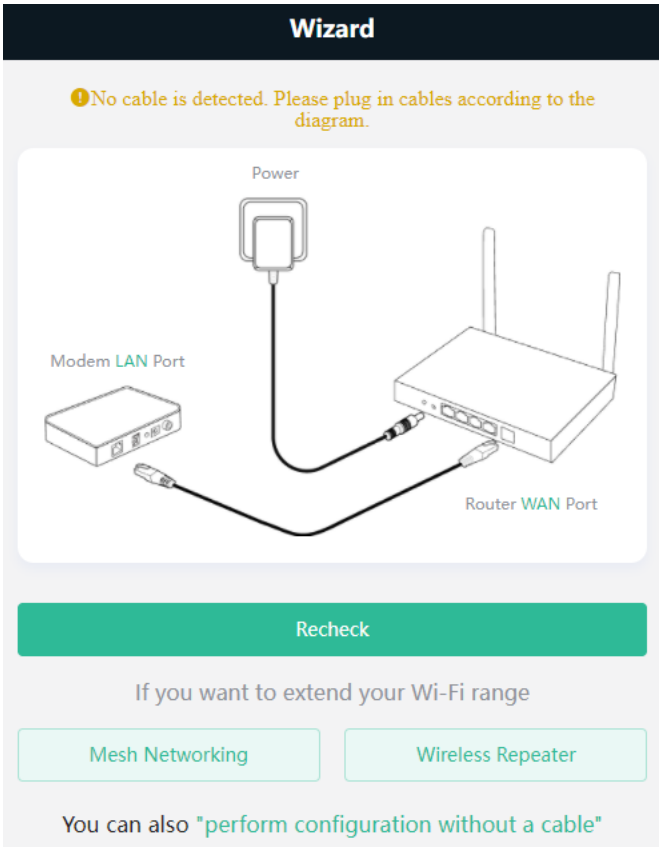
### 1.5.2 Configuration Steps

**Wired Connection**: After plugging in an Ethernet cable, set the Internet connection type to DHCP. For details, see 1.4.2 1.

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

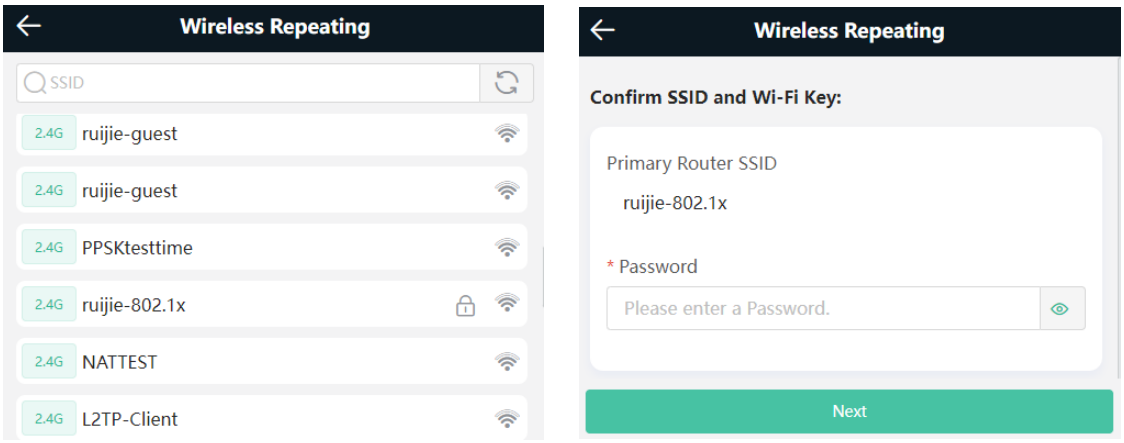
**Caution**

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




(1) Select **Wireless Repeater**.

- Wireless repeater mode: Click **Wireless Repeater**, select the Country/Region and the SSID of the primary router, and enter the Wi-Fi password to connect to the primary router.
- In wireless repeater mode, only Wi-Fi signals are extended and the DHCP function is disabled. The IP addresses of all clients connected to the primary and secondary routers are assigned by the primary router. If the device connects to the primary router in wireless repeater mode, the WAN port of the device keeps unchanged. If WAN cable is plugged in, the device automatically switches to the wired repeater mode.




(2) Set the SSID and password and save the settings. Then, the Wi-Fi network will be restarted.

### 1.5.3 Verification and Testing

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

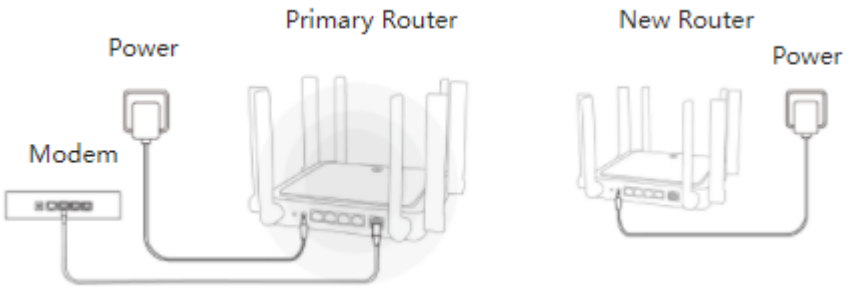
## 1.6 Mesh Pairing

To extend the Wi-Fi coverage, the routers can be connected to the primary router through either wired or wireless connection to build a wireless network that supports seamless roaming. You can press the **Mesh** button to automatically search for new routers around and perform automatic pairing, or log in to the router management page to select a new router for pairing. After the mesh pairing, the secondary router will synchronize the Wi-Fi settings (SSID and password) of the primary router, and the original Wi-Fi (SSID) will disappear. Up to 5 (1+4) routers are supported.

### 1.6.1 Performing Mesh Pairing through the Mesh Button

(1) Make the primary router connect to the Internet.

(2) Place the new router 2 meters (around 6.5ft) away from the primary router and power on the new router. The system LED of the new router starts to blink. Wait for 2 to 3 minutes until the LED turns solid on.




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

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

(4) Place the secondary router in an area where the Wi-Fi signal is weak or nonexistent, and power it on again

Wait for 3 to 5 minutes until the Reyee Mesh indicator on the secondary router turns solid on. The original SSID of the secondary router (@Reyee-sXXXX) will disappear and both routers will broadcast the same SSID, indicating that Mesh networking succeeds.

### 1.6.2 Configuring Mesh Pairing on the Management Page

Mobile Phone View: Choose **Home** > **+add** > **next**.

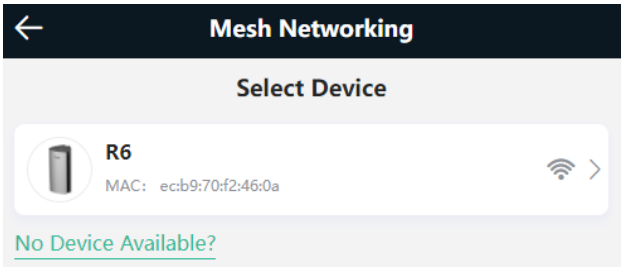
PC View: Choose **Home** > **+add** > **next** > **next**.

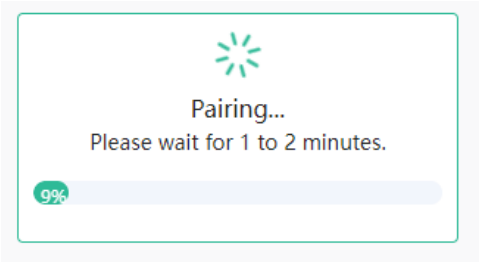
You can set up a wireless network that supports seamless roaming by mesh networking.

1. For quick pairing, please place the new router about 2 meters away from the primary router and connect the new router to the power supply. After pairing, place the new router where the Wi-Fi coverage is needed.

2. The system LED of the new router starts to blink. Wait for 2 to 3 minutes until the LED turns solid on.

3. After the new router is started, click **next** for the primary router to search for devices that can be paired. It takes one or two minutes to select the target device and perform the pairing.




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

**Caution**

- Make sure that the new router is around the primary router and there are not too many obstacles between them.
- If there are 3 or more routers, repeat the above steps. Up to 5 (1+4) routers are supported.




### 1.6.3 Managing Secondary Router

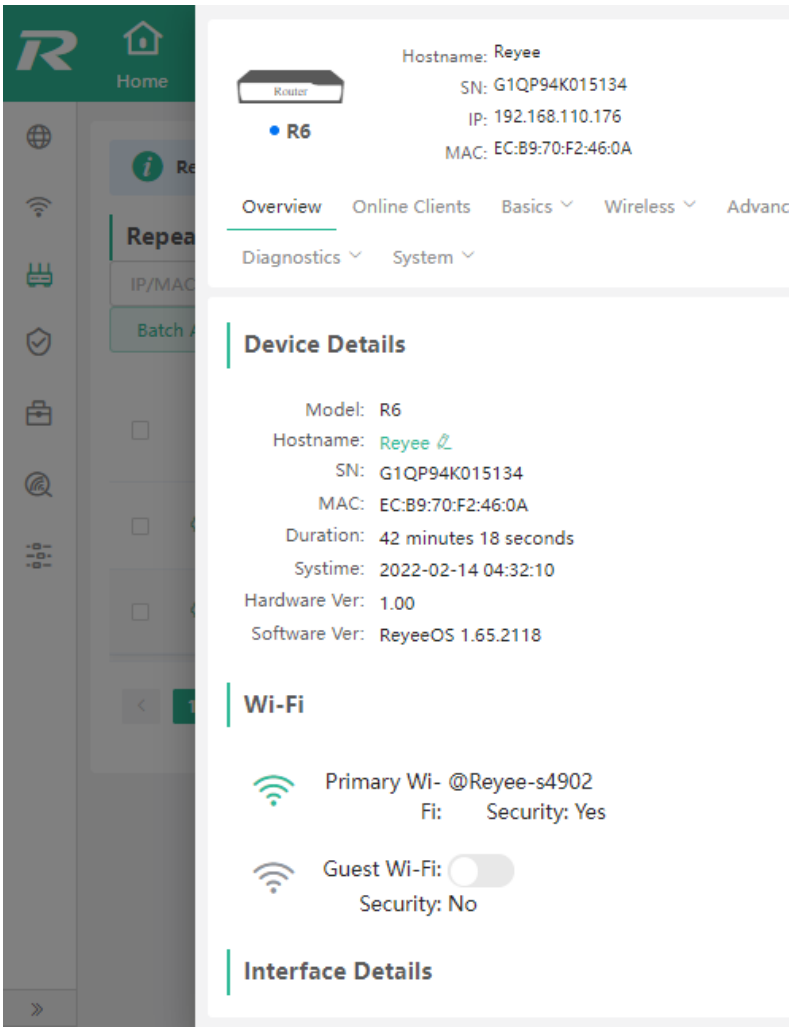
Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Repeaters**.

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

**Caution**

This menu is only displayed when the secondary router is online.

Click **Manage**, and the secondary router management page will pop up. You can make detailed settings for the secondary router. Click on the gray area on the right to close the page. To ensure the effect of seamless roaming, the Wi-Fi configuration of the secondary router must be consistent with that of the primary router and cannot be modified independently.




### 1.6.4 Enabling Reyee Mesh

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

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

Reyee Mesh is enabled on the device by default. You are advised to enable the function. After Reyee Mesh is enabled, the new router joins the network automatically when connected to the LAN port of the device. Then you can press the key for Reyee Mesh pairing.

**Note**

- After Reyee Mesh is disabled, the secondary router will still be connected.

### 1.6.5 Troubleshooting

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

- Press the **Reset** button for at least 3 seconds. Try again after the system LED turns solid on.
- Please make sure that Reyee Mesh is enabled on the primary router. (This function is enabled by default.)

# 2 Wi-Fi Network Settings

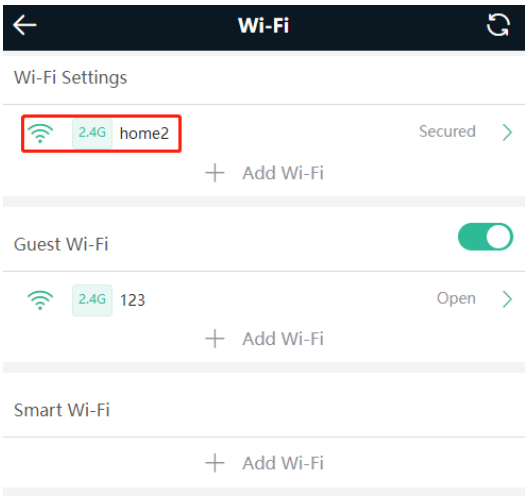
## 2.1 Changing the SSID and Password

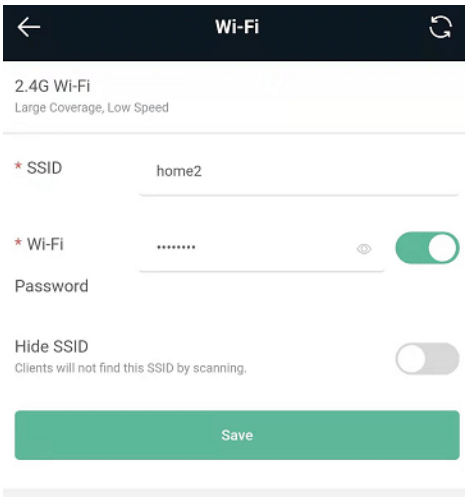
Choose **Wi-Fi** > **Wi-Fi Settings**.

Click the target Wi-Fi network, change the SSID and password of the Wi-Fi network, and click **Save**.

**Caution**

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




## 2.2 Hiding the SSID

### 2.2.1 Overview

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

### 2.2.2 Getting Started

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

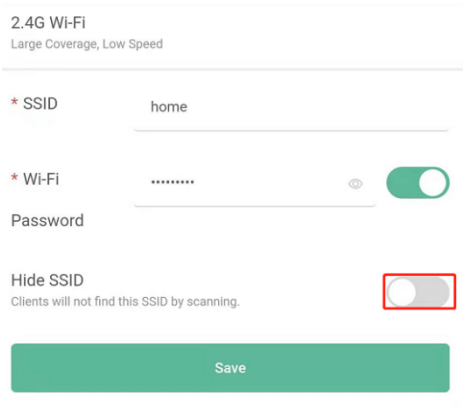
### 2.2.3 Configuration Steps

Choose **Wi-Fi** > **Wi-Fi Settings**.

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

**Caution**

After the configuration is saved, you have to manually enter the SSID and password before connecting any device to the Wi-Fi network. Therefore, exercise caution when performing this operation.




**Note**

Users need to manually enter the SSID and password each time they connect to a hidden Wi-Fi network. Take an Android-based device as an example: To connect it to a hidden Wi-Fi network, choose **WLAN** > **Add network** > **Network name**, enter the Wi-Fi name, select **WPA**/**WPA2**/**WPA3** from the **Security** dropdown list, enter the password, and click **Connect**.

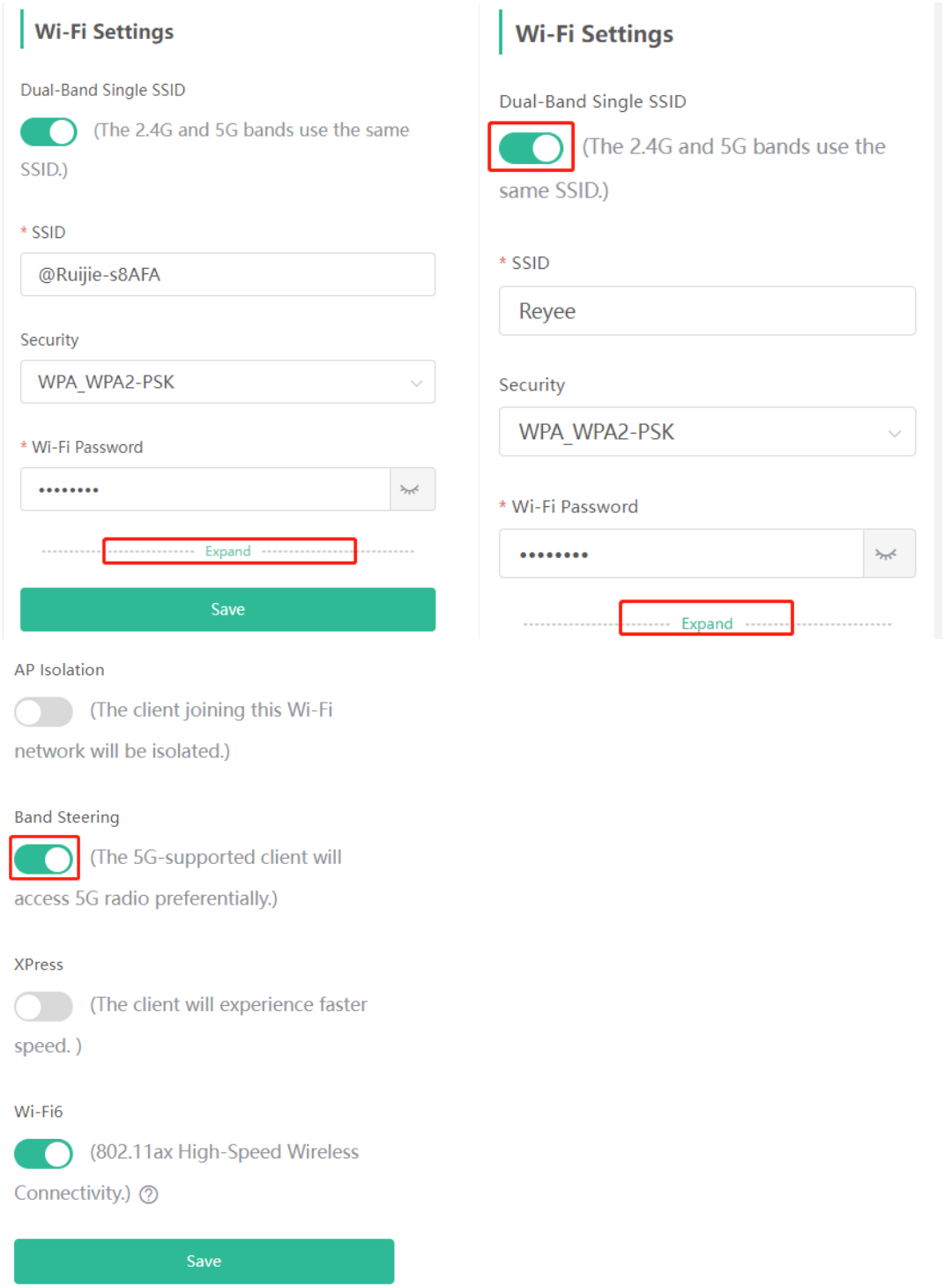
## 2.3 Enabling Band Steering

**Caution**

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

Choose **Wi-Fi** > **Wi-Fi Settings**.

Click **Expand** to expand the advanced configuration. Then click **Band Steering**. The 5G-capable client will access 5G radio preferentially after this function is enabled.




## 2.4 Adding a Wi-Fi Network

### 2.4.1 Overview

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

- **Primary Wi-Fi**: The primary Wi-Fi network is listed in the first line of the page and is enabled by default.

- **Guest Wi-Fi**: This Wi-Fi network is provided for guests and is disabled by default. It supports user isolation, that is, access users are isolated from each other. They can only access the Internet via Wi-Fi, but cannot access each other, improving security.

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

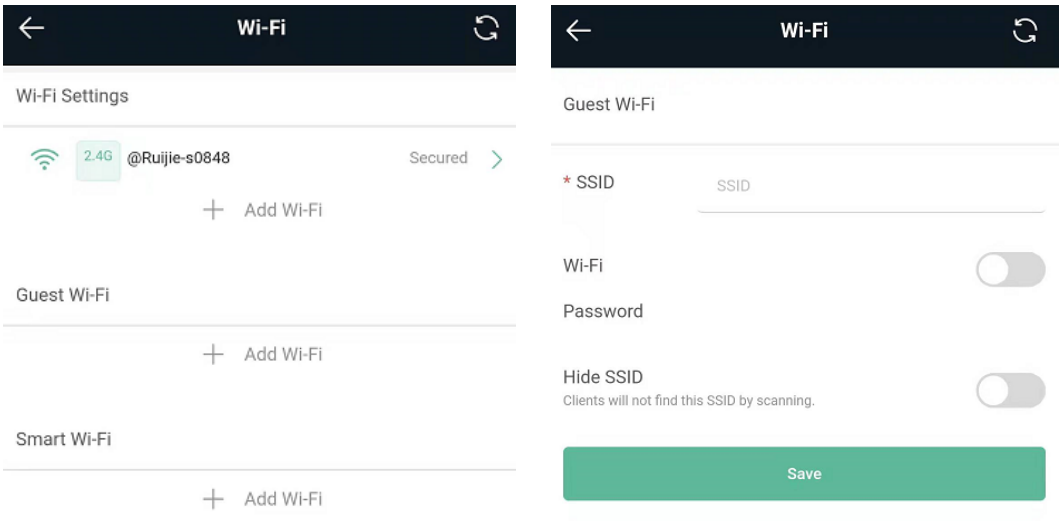
- **Smart Wi-Fi**: The smart Wi-Fi network is disabled by default. Smart clients can connect to the smart Wi-Fi network for long. The smart Wi-Fi network cannot be turned off as scheduled.

### 2.4.2 Configuration Steps

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

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

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




### 2.4.3 Verification and Testing

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




## 2.5 Configuring the Wi-Fi Blacklist or Whitelist

### 2.5.1 Overview

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

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

## 2.5.2 Configuration Steps

Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **WLAN** > **Blacklist/Whitelist**.

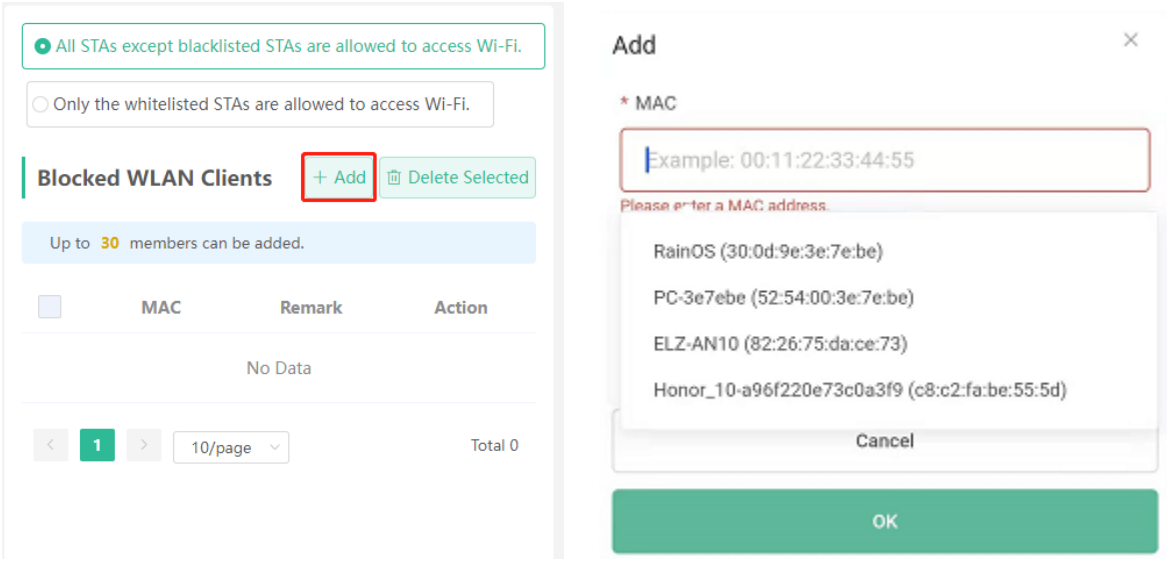
PC View: Choose **More** > **WLAN** > **Blacklist/Whitelist**.

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

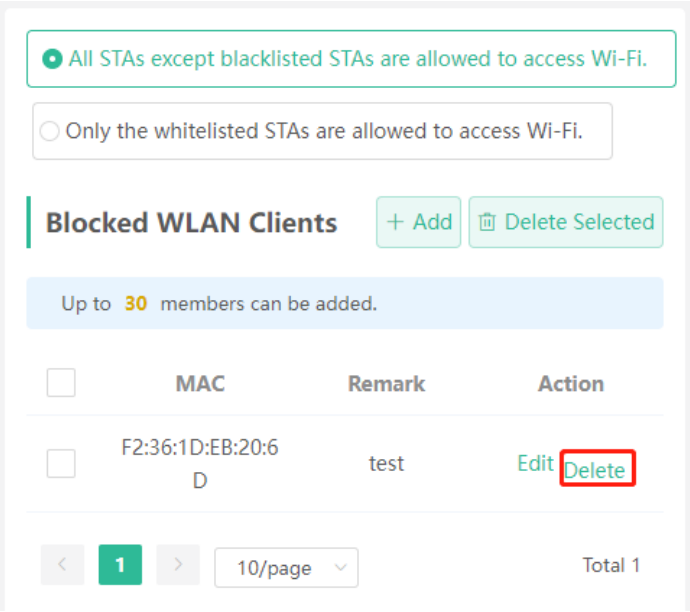
In the pop-up dialog box, enter the MAC address and remarks of the client to be blacklisted. The device displays information about the connected clients. Select a client, and it will be added to the blacklist automatically. Click **OK** to save the configuration. The client will be disconnected and prevented 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.




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




## 2.6 Enabling Smart Optimization

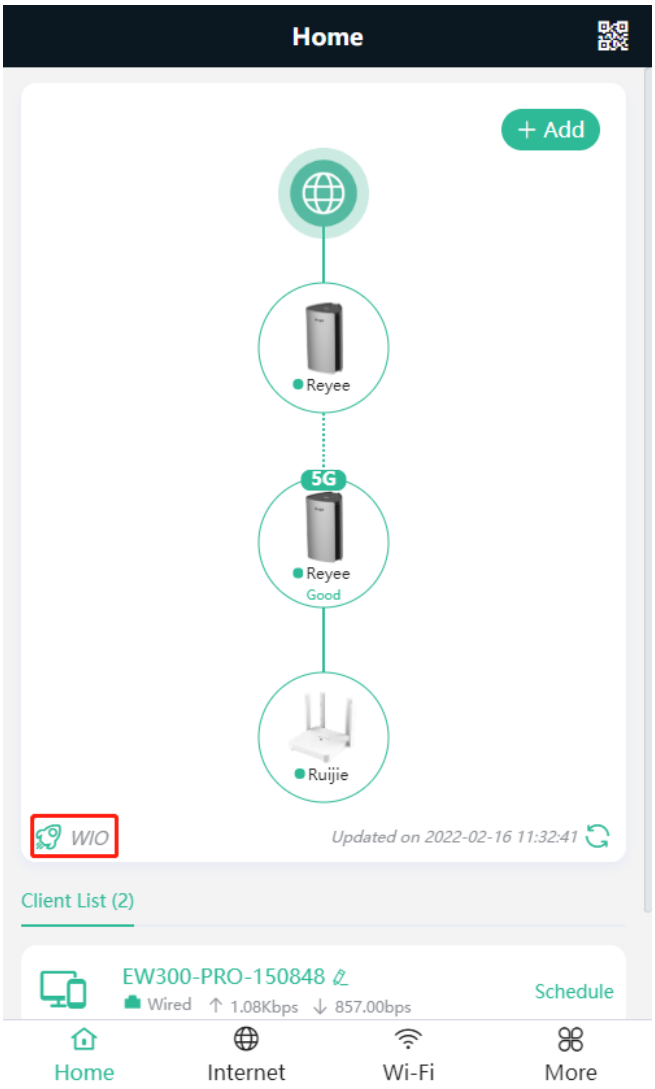
Mobile Phone View: Choose **Home** > **WIO**

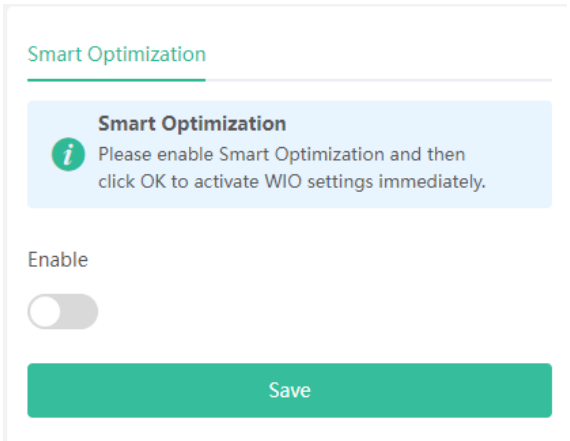
PC View: Choose **More** > **WLAN** > **WIO**

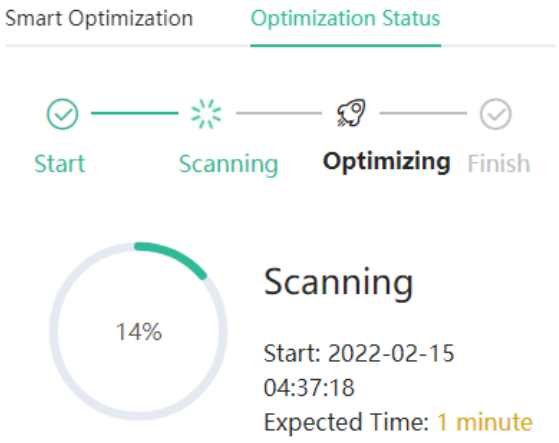
Smart optimization can help improve user experience by making roaming smooth. You are advised to enable optimization after roaming becomes insensitive. The optimization will start immediately after it is enabled. You can click **Optimization Status** to view the optimization progress.

**Note**

- This menu is displayed only when the secondary router is online.
- Smart optimization can improve roaming sensitivity, but the wireless signal may become weaker after optimization.


Home
+ Add
Reyee
5G
Reyee
Good
Ruijie
WIO
Updated on 2022-02-16 11:32:41
Client List (2)
EW300-PRO-150848
Wired 1.08Kbps 857.00bps
Schedule
Home
Internet
Wi-Fi
More


Smart Optimization
Smart Optimization
Please enable Smart Optimization and then click OK to activate WIO settings immediately.
Enable
Save


Smart Optimization
Optimization Status
Start
Scanning
Optimizing
Finish
14%
Scanning
Start: 2022-02-15 04:37:18
Expected Time: 1 minute

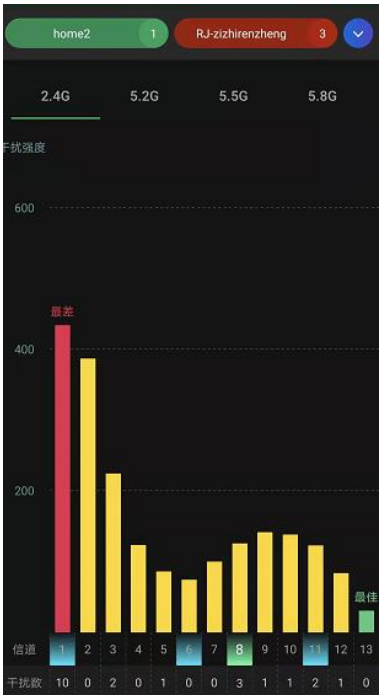
# 2.7 Optimizing the Wi-Fi Network

## 2.7.1 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 4.5. You can also analyze the wireless environment around the router and select appropriate parameters.

## 2.7.2 Getting Started

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




## 2.7.3 Configuration Steps

- Optimizing the radio channel

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

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

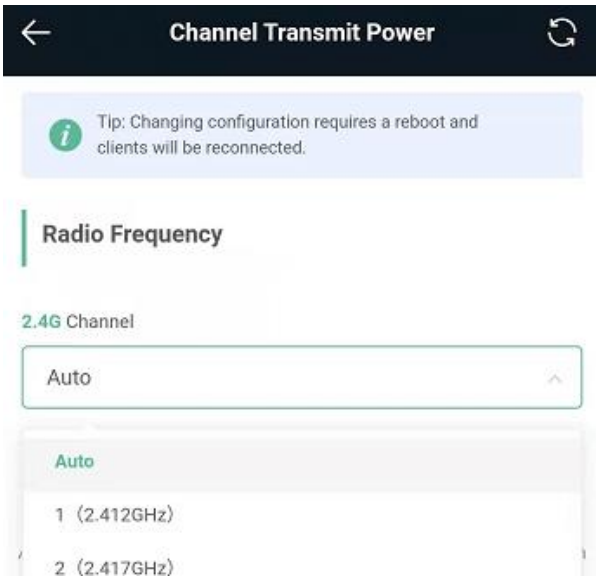
Choose the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. Excess clients connected to a channel can bring stronger wireless interference.

**Note**

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

**Caution**

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




- Optimizing the channel width

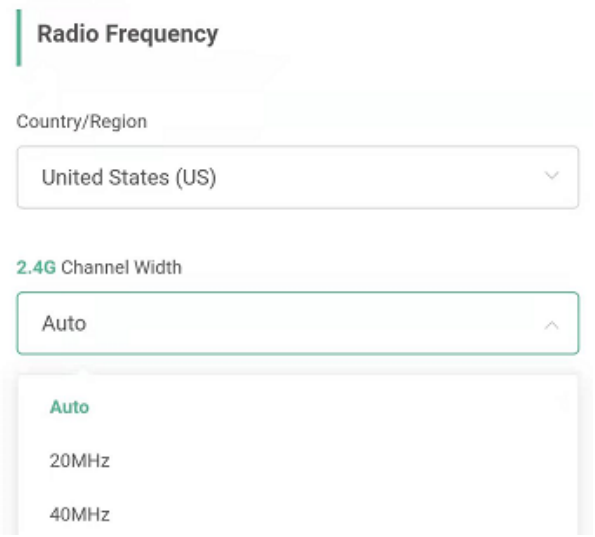
Mobile Phone View: Choose **More**> **Country(Region)/Channel Width**.

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

If the interference is severe, choose a lower channel width to avoid network stalling. The router supports the 20 MHz and 40 MHz channel width. The Wi-Fi network speed is more stable when the channel width is smaller, and a larger channel width makes the device more prone to interference. After changing the channel width, click **Save** to make the configuration take effect immediately.

**Caution**

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




- Optimizing the transmit power

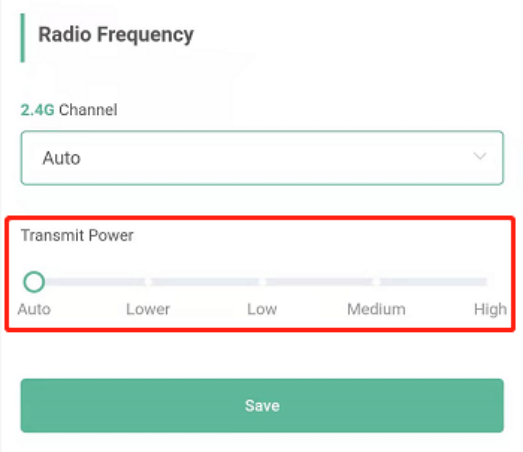
Mobile Phone View: Choose **More** > **Channel Transmit Power**.

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

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

**Caution**

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




- Configuring the roaming sensitivity (optional)

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

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

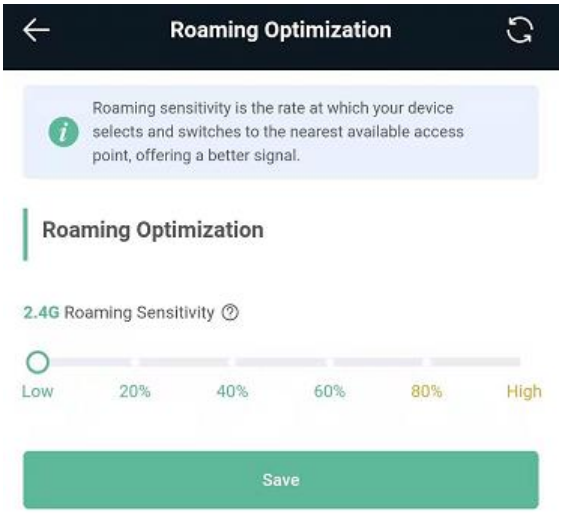
Clients such as mobile phones support the roaming function but the sensitivity level may not be high enough. The roaming sensitivity enables the device to actively disconnect a client from the Wi-Fi network when the client is far away, forcing the client to re-select the nearest signal and thus improving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

The default value (low sensitivity) is recommended.

**Caution**

After the change, the Wi-Fi network will restart, and clients need to reconnect to the W-Fi network.

High sensitivity level may cause unnecessary Wi-Fi network disconnection. Therefore, exercise caution when performing this operation.




## 2.8 Configuring the Healthy Mode

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

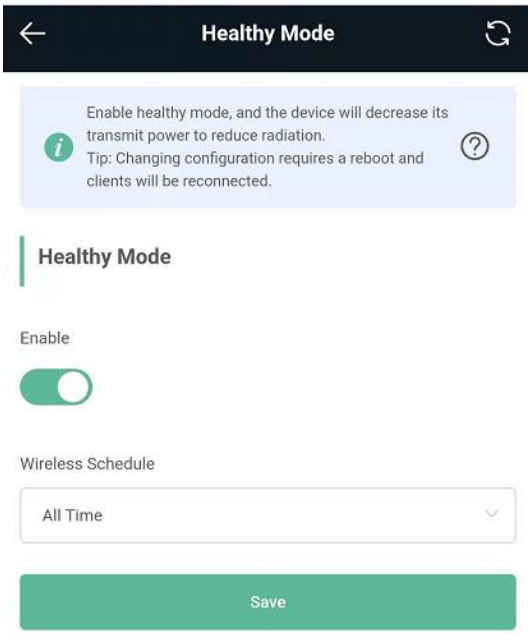
PC View: Choose **More** > **WLAN** > **Wi-Fi** > **Healthy Mode**.

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

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

**Note**

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


Healthy Mode
Enable healthy mode, and the device will decrease its transmit power to reduce radiation.
Tip: Changing configuration requires a reboot and clients will be reconnected.
Healthy Mode
Enable
Wireless Schedule
All Time
Save

# 3 Networks Settings

## 3.1 Configuring Internet Connection Type

Choose **More** > **Switch to PC view** > **More** > **Basics** > **WAN**.

The router supports three Internet connection types: PPPoE, DHCP, and static IP. For details, see 1.4 .

## 3.2 Changing the Address of a LAN Port

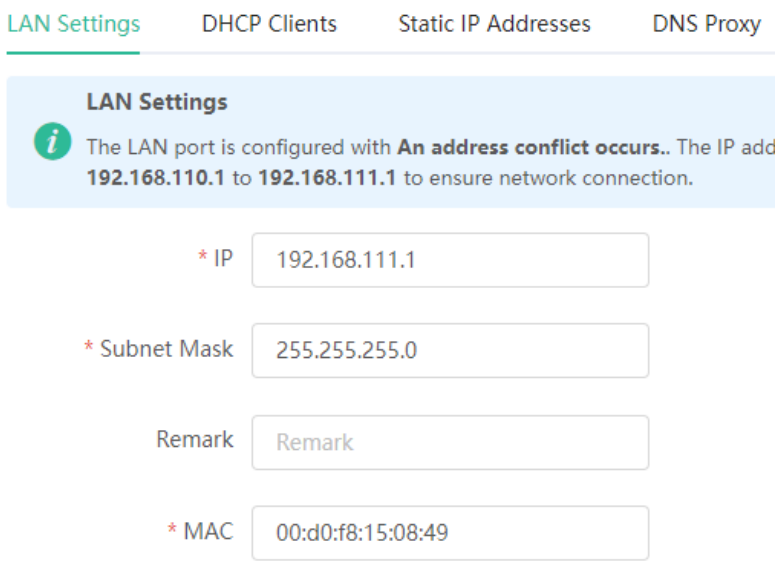
Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Basics** > **LAN**.

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

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

**Caution**

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




## 3.3 Changing the MAC Address

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

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

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

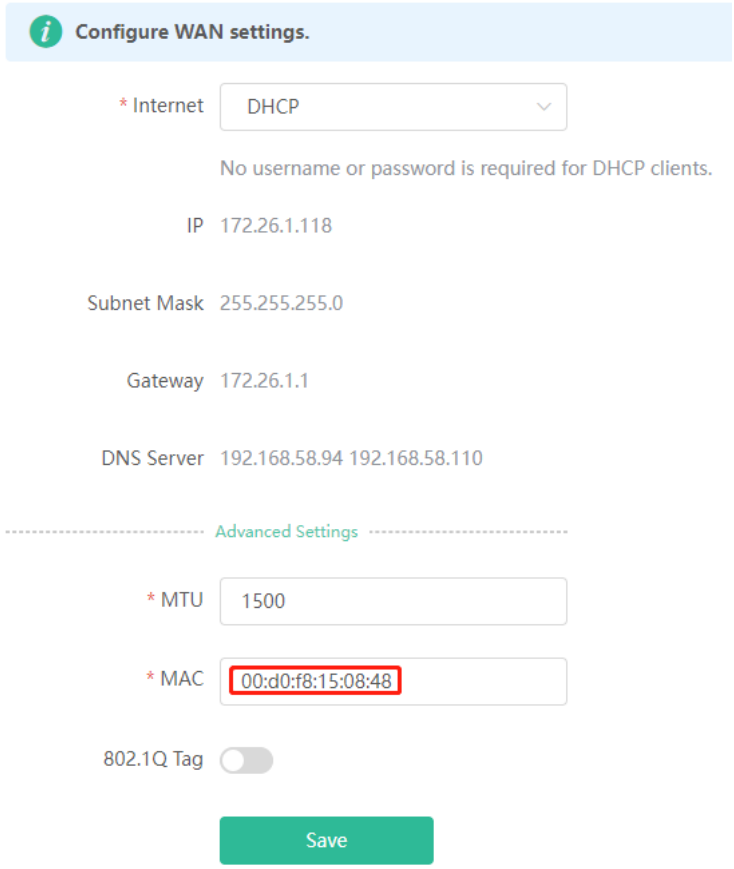
Enter the MAC address in the format of 00:11:22:33:44:55.

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

**Caution**

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

**Figure 3-1 WAN Port Settings**




## 3.4 Changing the MTU

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

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

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

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

For details about the page, see Figure 3-1.

## 3.5 Configuring the Repeater Mode

### 3.5.1 Wired Repeater

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

Choose **More** > **Switch to PC view** > **More** > **Basics** > **Repeater Mode**

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

**Caution**

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

**Figure 3-2 Wired Repeater Settings**

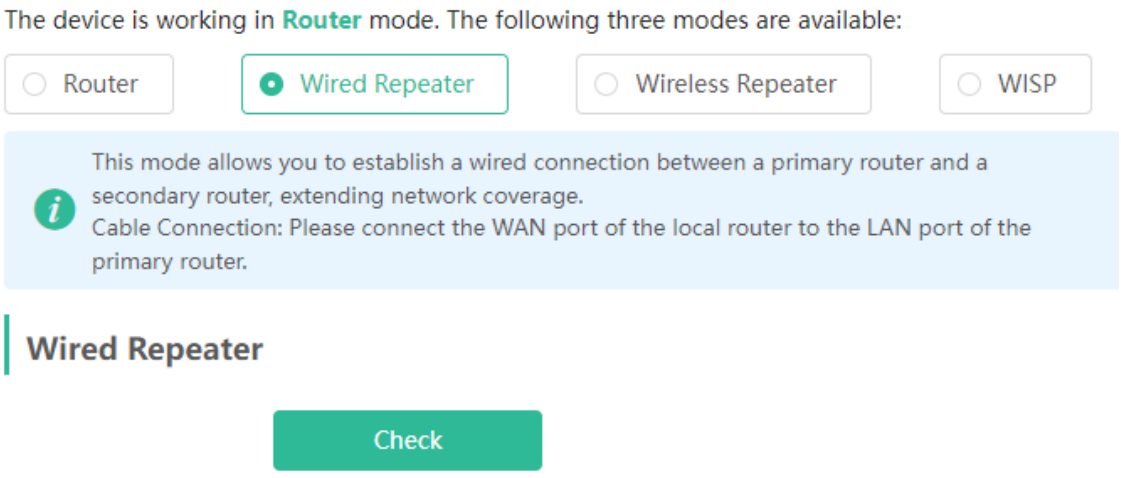
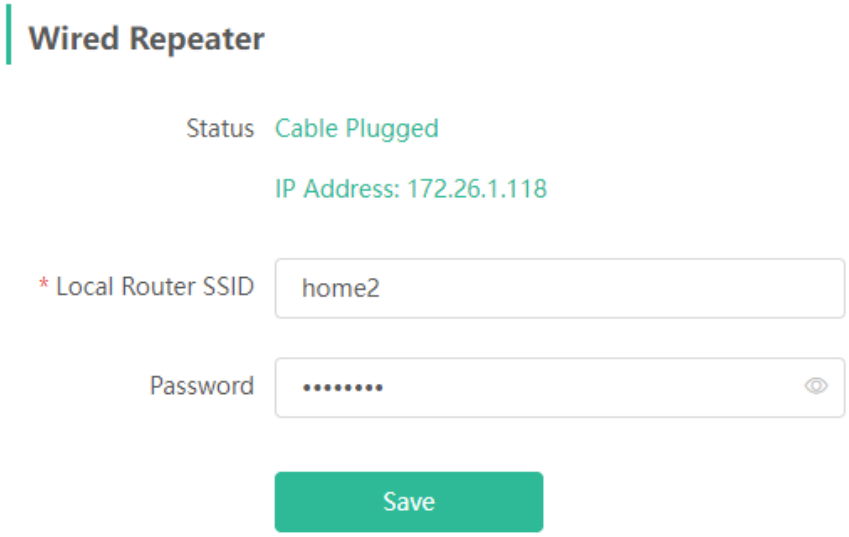


**Figure 3-3 After Clicking Check**




## 3.5.2 Wireless Repeater

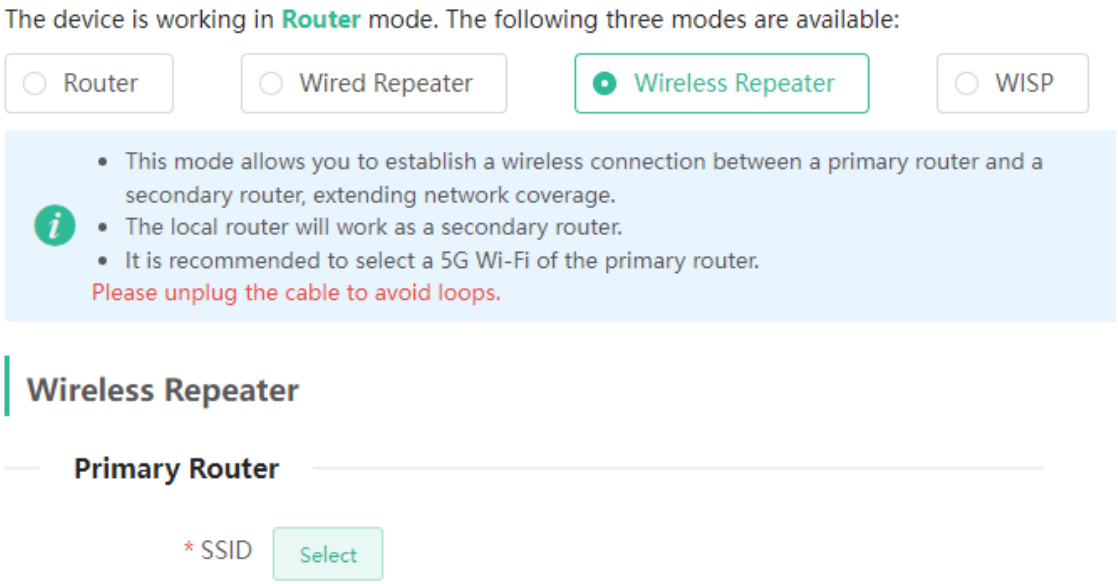
The wireless repeater mode extends the Wi-Fi coverage of the primary router.

**Note**

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

Choose **More** > **Switch to PC view** > **More** > **Basics** > **Repeater Mode**

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



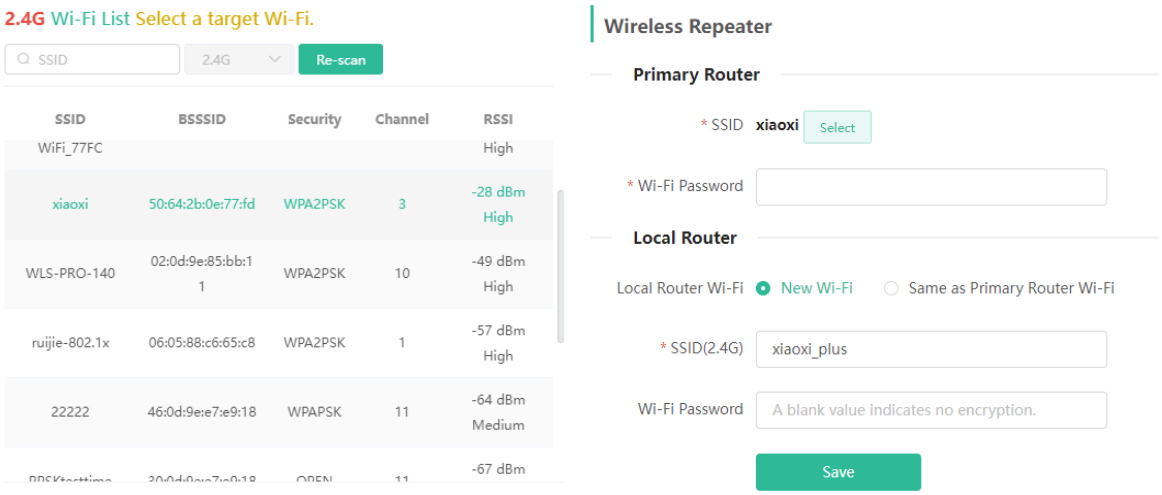
(2) Select the Wi-Fi signal of the primary router and enter its Wi-Fi password. You can configure a new Wi-Fi network or have a Wi-Fi network the same as that of the primary router:

- If you select **Same as Primary Router Wi-Fi**, the Wi-Fi settings of the primary router are automatically synchronized to the current router. Generally, clients merge Wi-Fi signals with the same SSID into one Wi-Fi signal, and they can search out only the Wi-Fi signal of the primary router.
- If you select **New Wi-Fi**, you can set a local SSID and password. Clients will search out a Wi-Fi signal different from the primary router Wi-Fi signal.

**Caution**

After the configuration is saved, the Wi-Fi network will be disconnected and you need to connect to the new Wi-Fi network. Exercise caution when performing this operation. Remember the new SSID and password.

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




# 3.6 Configuring IPv6 Address

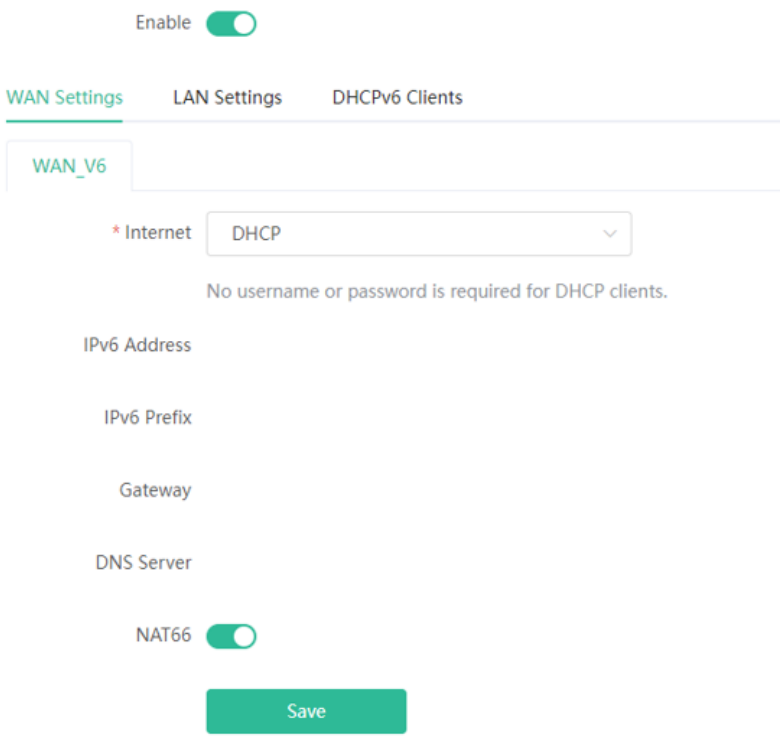
With the popularity of the network, the IPv4 address fails to meet demands. The 128-bit IPv6 address solves the problem of IPv4 address exhaustion.

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

## 3.6.1 Configuring the IPv6 Address of the WAN Port

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

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



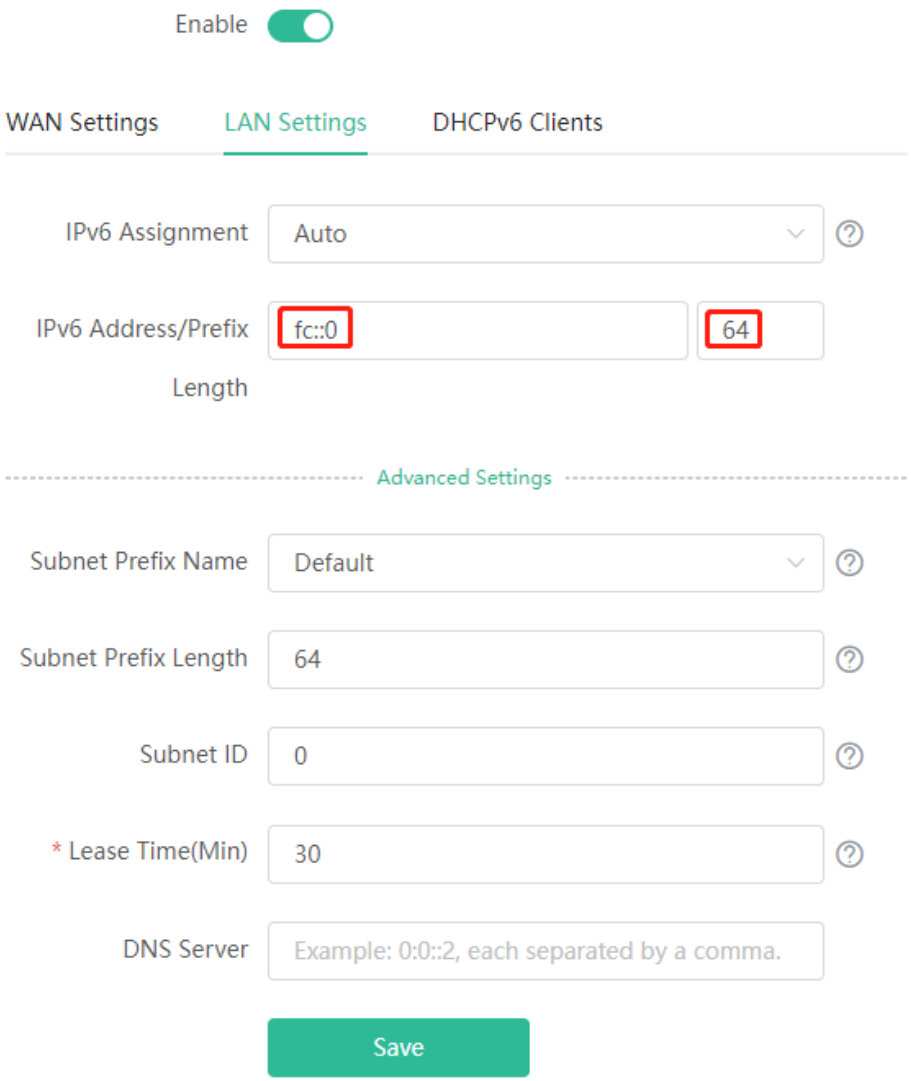

### 3.6.2 Configuring the IPv6 Address of the LAN Port

Click **LAN Settings.**

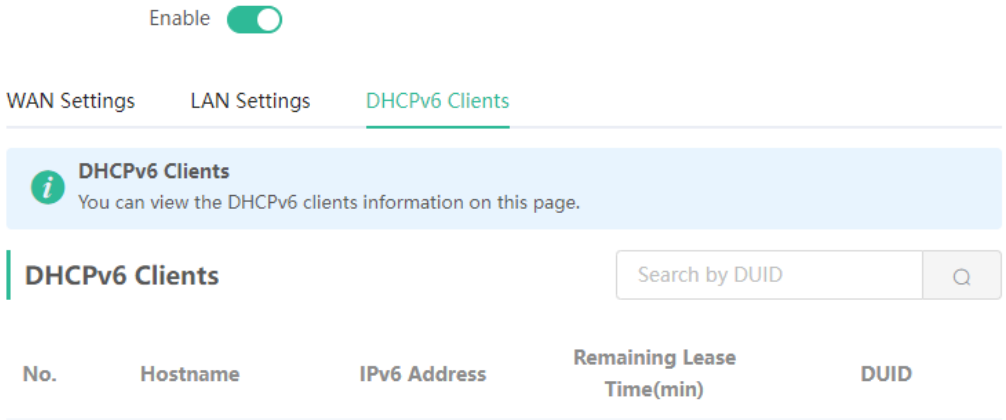
**IPv6 Assignment**: Choose **Auto** to use both DHCPv6 mode and SLAAC mode to allocate address. Choose **Null** to assign no address. You are advised to choose **Auto**.

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

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




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



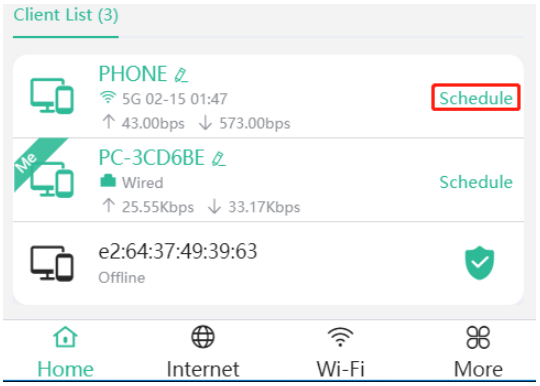
## 3.7 Enabling Parental Control

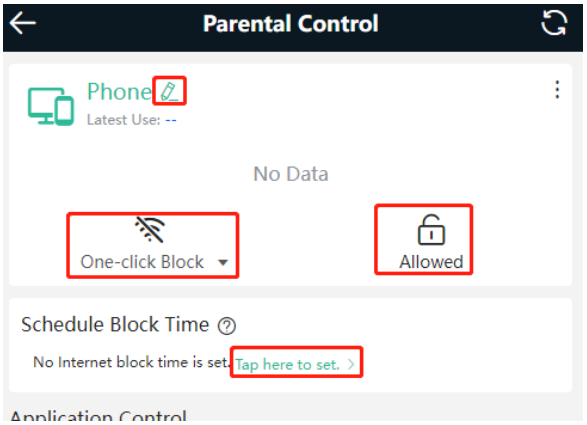
Mobile Phone View: Choose **Home** > **Schedule** or .

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

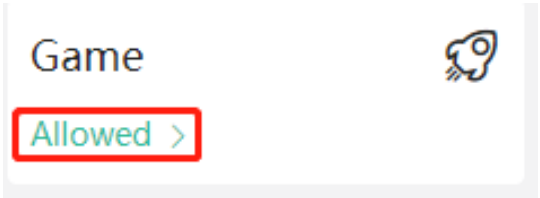
Select a client and click **Schedule**. Click **Schedule** to navigate to the **Parental Control** page. Click to modify the remarks of the client.

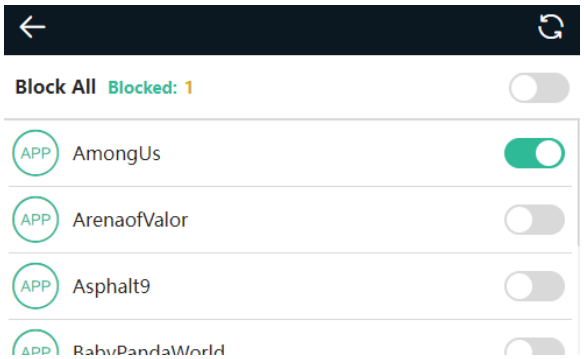
Click **One-click Block** to choose to disconnect the client from the network immediately, 10 minutes, 30 minutes or 60 minutes later. Click **Allowed** to allow the client to access the Internet immediately. Click **Tap here to set** to set a specific period for Internet access block.




Click **Application Control** to select and block the specific application.



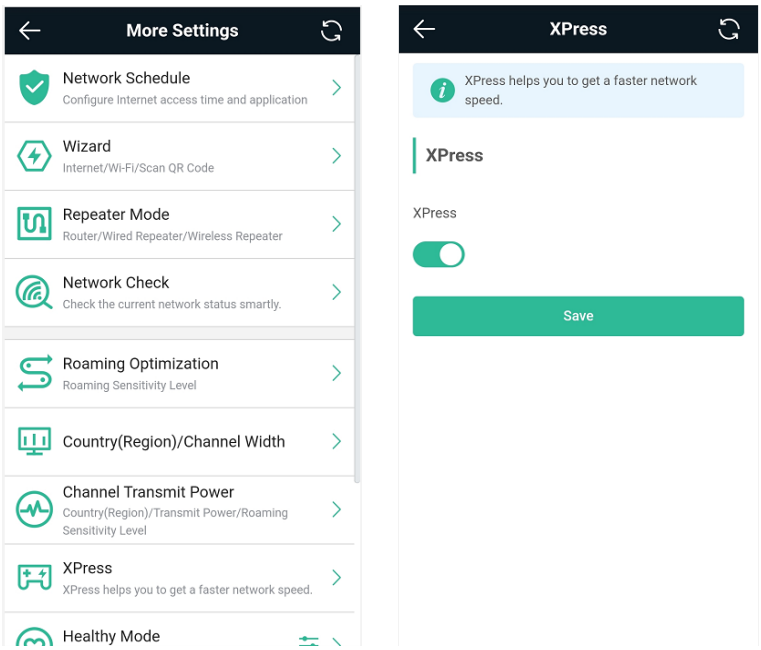




## 3.8 Configuring XPress

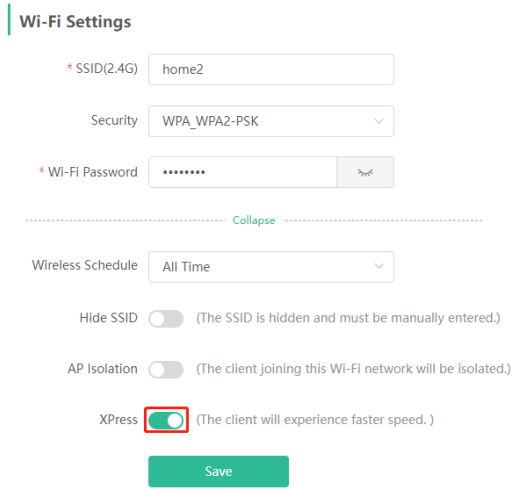
Mobile Phone View: Choose **More** > **XPress**.

PC View: Choose **WLAN** > **Wi-Fi** > **Wi-Fi Setting** > **Expand** > **XPress**.

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




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




# 3.9 Configuring Port Mapping

## 3.9.1 Overview

- Port mapping maps the IP address of a device on the LAN to an external network in the form of a combination of a WAN IP address and a port number, so as to provide the external network access service.
- Scenario 1: When you need to access IP cameras or PCs at home while you are away from home, port mapping needs to be configured.
- Scenario 2: When a server needs to be set up in the home network for Internet access, port mapping or demilitarized zone (DMZ) needs to be configured.
- Port mapping maps the WAN port IP address of a router to an internal network host and port so that Internet users can proactively access hosts on the LAN.

- DMZ forwards all packets from the Internet to DMZ hosts to provide the Internet access service.

### 3.9.2 Getting Started

- Confirm the IP address of the target device in the internal network and service port ID.
- Ensure that port mapping is available in the internal network.

### 3.9.3 Configuration Steps

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

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

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

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

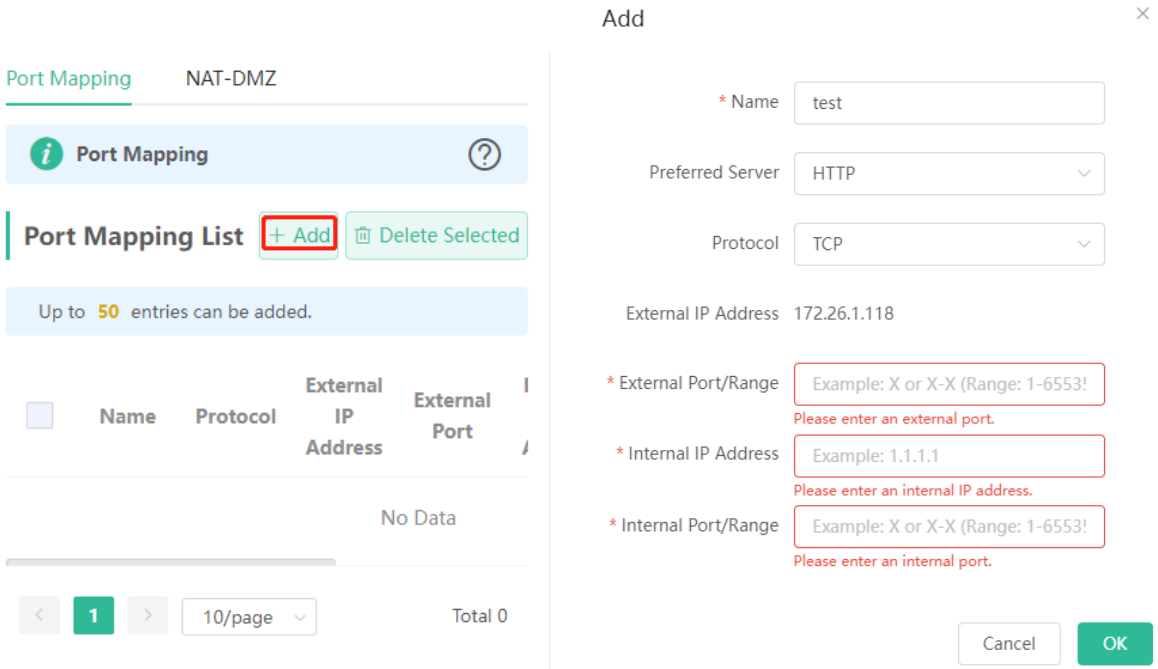
**Preferred Server**: Select a service to be mapped, such as HTTP or FTP. The device will automatically fill in the internal port number of the service. If you are not sure of the service, you can select **Custom**.

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

**External Port/Range**: Enter the port number used for external network access. You need to check the port number in software, such as camera monitoring software.

**Internal IP Address**: 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.



### 3.9.4 Verification and Testing

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

### 3.9.5 Solution to a Test Failure

(1) Use a new external port number and perform a test again. The test often fails on the ports blocked by firewalls of some ISPs.

(2) Enable the remote access permission on the server. The common cause is that remote access is disabled on the server by default. As a result, the internal network access is successful but the access across different network segments fails.

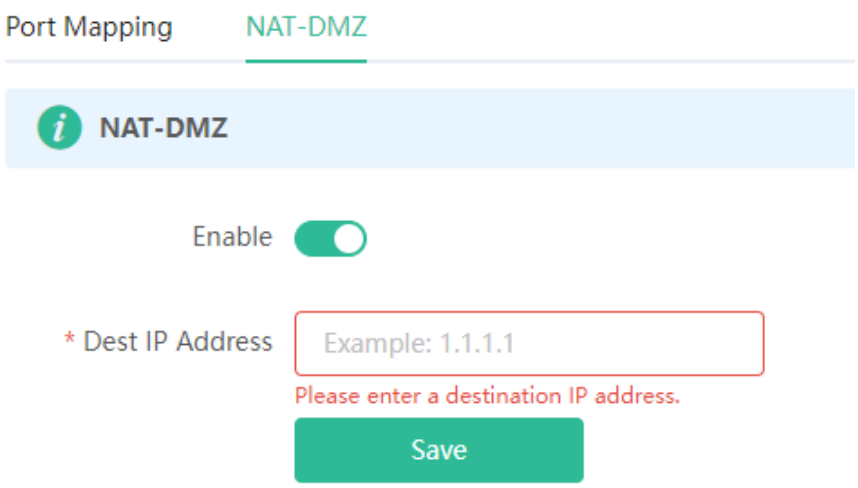
(3) Enable the DMZ service. For details, see DMZ Configuration Steps. The common cause is that port configuration is incorrect or incomplete.

### 3.9.6 DMZ Configuration Steps

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

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

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




## 3.10 Configuring DHCP Server

### 3.10.1 Overview

The DHCP server function enables a router to automatically assign IP addresses to clients so that clients connected to the LAN ports or Wi-Fi network of the router obtain IP addresses for Internet access. When multiple routers are connected through LAN ports, a DHCP server conflict will occur. In this case, you need to disable

the DHCP server function and keep the DHCP service only on one router available. Otherwise, some devices may be disconnected from the network from time to time.

## 3.10.2 Configuration Steps

### 1. Configuring the DHCP Server Function

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

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

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

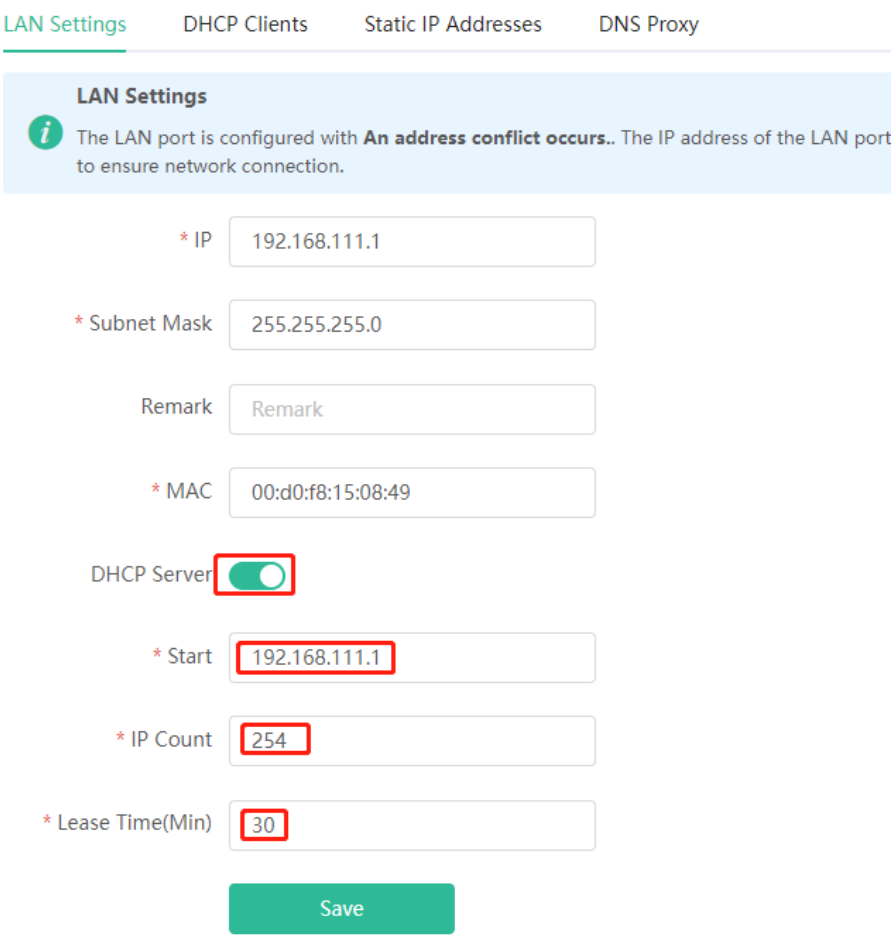
**Caution**

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

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

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

**Lease Time (Min)**: Enter the address lease time period. When a client keeps connected, the lease is automatically renewed. If a lease is not renewed due to the client disconnection or network instability, the IP address will be reclaimed after the lease period expires. After the client connection is restored, the client requests an IP address again. The default lease period is 30 minutes.

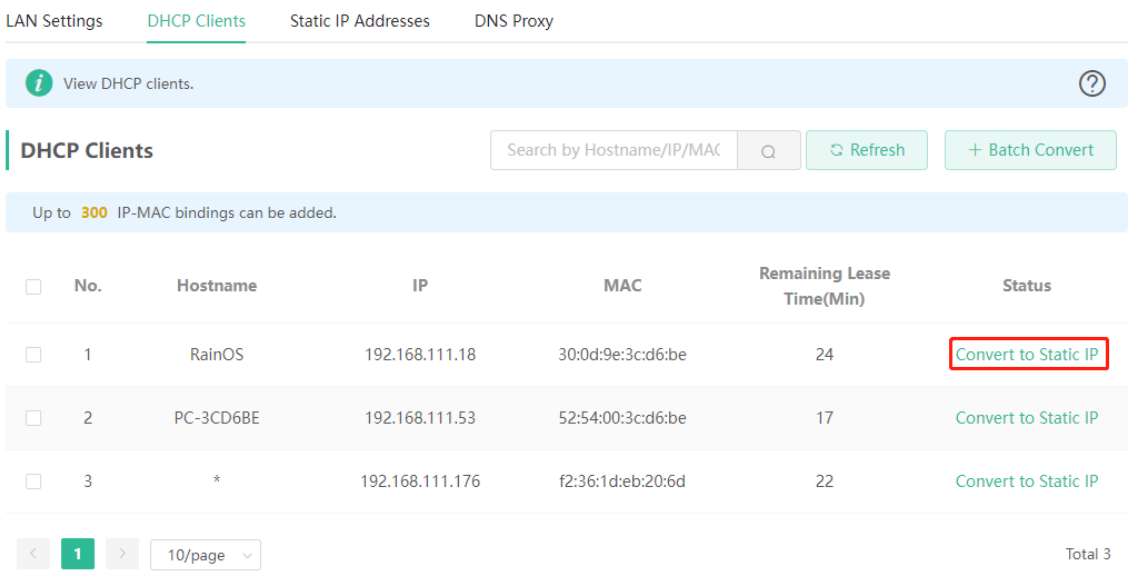



## 2. Displaying Online DHCP Clients

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

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

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

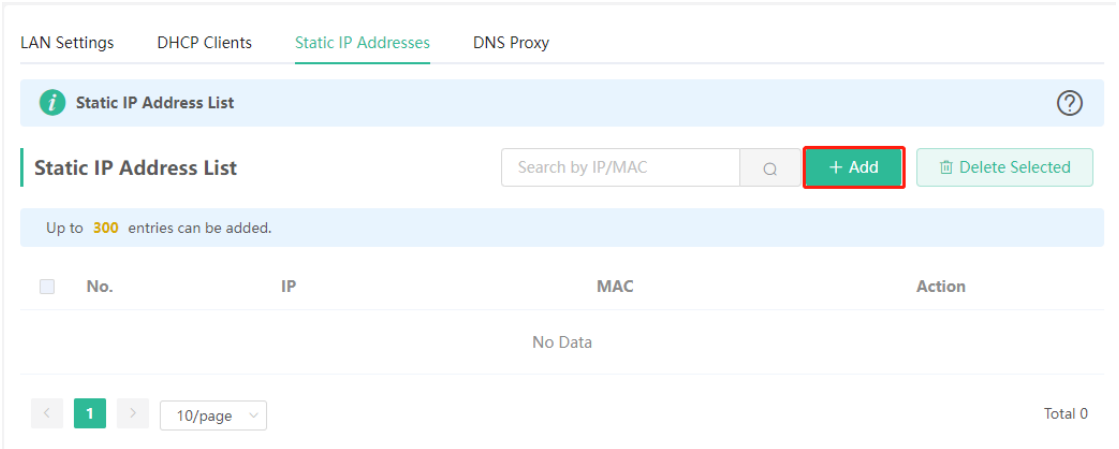



### 3. Displaying the DHCP Static IP Address Table

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

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

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




## 3.11 Configuring DNS

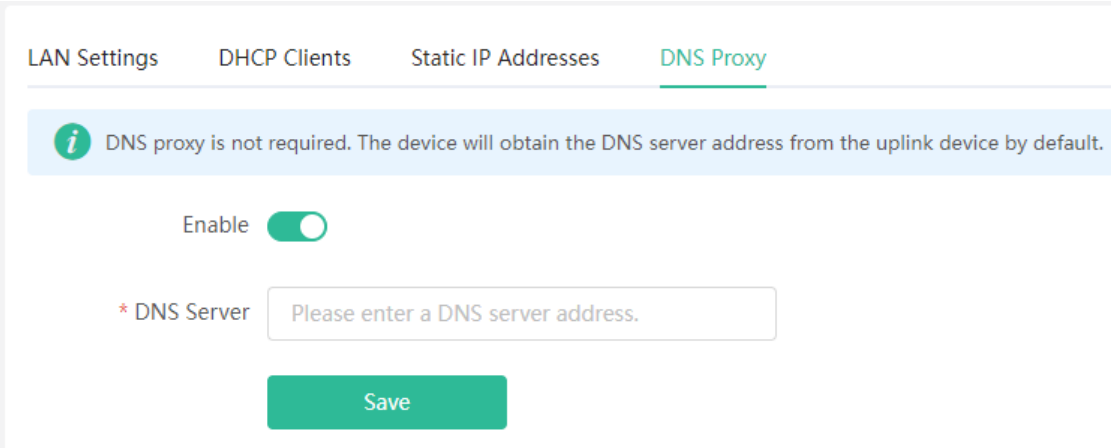
The domain name system (DNS) proxy configuration is not mandatory. The device obtains the DNS server address from the uplink device by default.

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

PC View: Choose **More** > **Baiscs** > **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.




## 3.12 Configuring DDNS

### 3.12.1 Overview

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

### 3.12.2 Getting Started

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

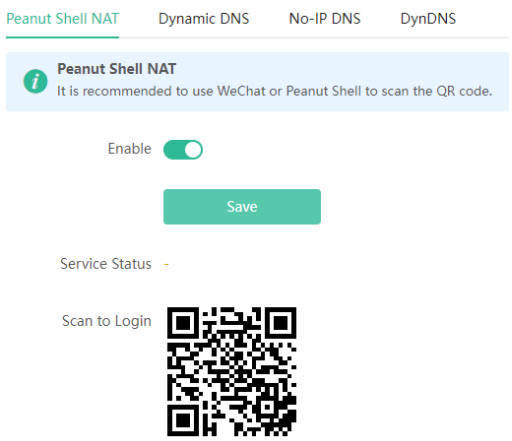
### 3.12.3 Configuration Steps

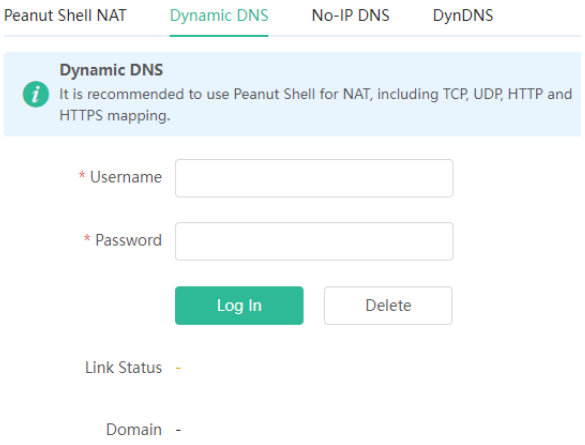
Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Advanced** > **Dynamic DNS** > **Dynamic DNS**.

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

Peanut Shell NAT is a more advanced version of DDNS and can be used when an internal network IP address is configured for the WAN port. Peanut Shell NAT is recommended. Click **Enable** and then click **Save**. The service status and QR code for login appear in the lower part of the page. Scan the QR code to log in by using WeChat or PeanutHull app (the QR code shown in the figure below is not available. Scan the QR code displayed on your device).

If you select **Peanut Shell NAT**, **Dynamic DNS**, **No-IP DNS**, or **DynDNS**, enter the registered account and password, and click **Log In**. The connection status and domain name will be displayed in the lower part of the page.




## 3.13 Configuring APR Binding and Guard

### 3.13.1 Overview

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

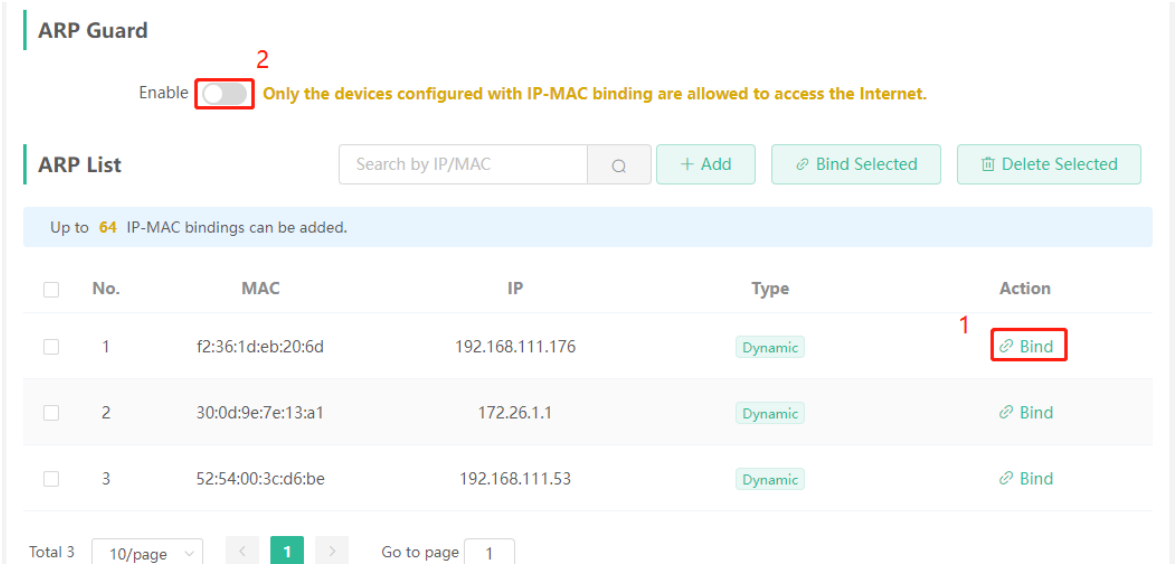
### 3.13.2 Configuration Steps

(1) Binding ARP information

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

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

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




(2) Enabling ARP guard

Turn on the switch below **ARP Guard** to enable the ARP guard function. After ARP guard is enabled, only clients whose IP address and MAC address are bound are allowed to access the Internet.

**Caution**

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

## 3.14 Connecting to IPTV

IPTV is an Internet television service provided by ISP.

### 3.14.1 Getting Started

- Check whether the IPTV service has been provisioned.
- Check whether the local IPTV service is of the VLAN or Internet Group Management Protocol (IGMP) type. If the local IPTV is of the VLAN type, confirm the VLAN ID. If you are not sure of the IPTV type, contact your local ISP.

### 3.14.2 IPTV Configuration Steps (VLAN Type)

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

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

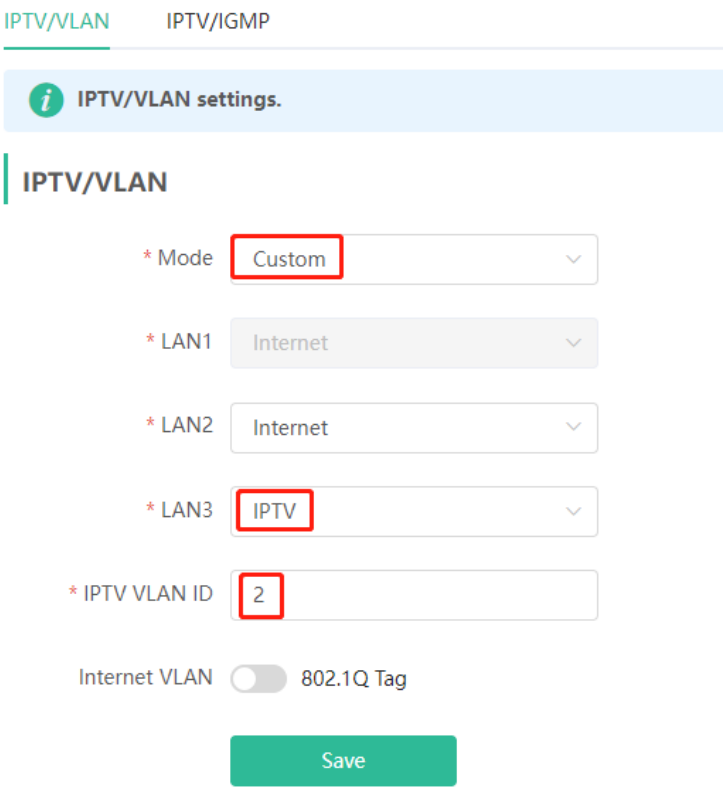
Select a local ISP mode, click the drop-down list of the target port, select **IPTV** from the drop-down list, and enter the VLAN ID provided by the ISP. For example, connect an IPTV set top box (STB) to LAN3 and set the VLAN ID to 2. The configuration is shown in the figure below.

**Internet VLAN**: If a VLAN ID needs to be set for the Internet access service, enable the Internet VLAN function and enter a VLAN ID. The VLAN tag function is disabled by default. You are advised to disable the function unless in special cases.

After the configuration, confirm that the IPTV STB is connected to the specified port properly. Take the following figure as an example, connect the IPTV STB to LAN3.

**Caution**

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

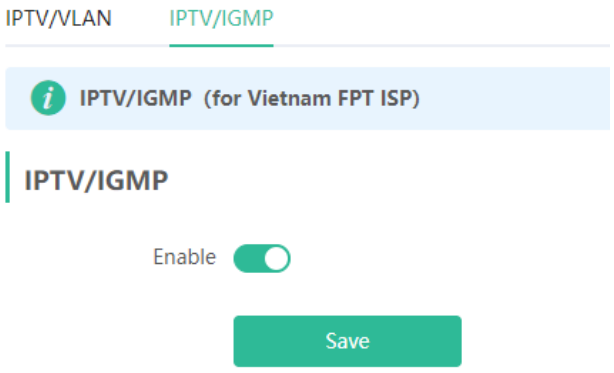



### 3.14.3 IPTV Configuration Steps (IGMP Type)

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

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

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

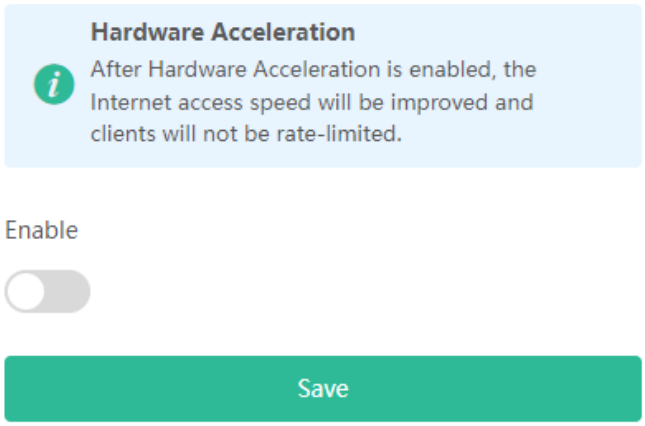



## 3.15 Enabling Hardware Acceleration

Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Advanced** > **Hardware Acceleration**.

PC View: Choose **More** > **Advanced** > **Hardware Acceleration**.

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




**Caution**

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

## 3.16 Enabling Smart Flow Control

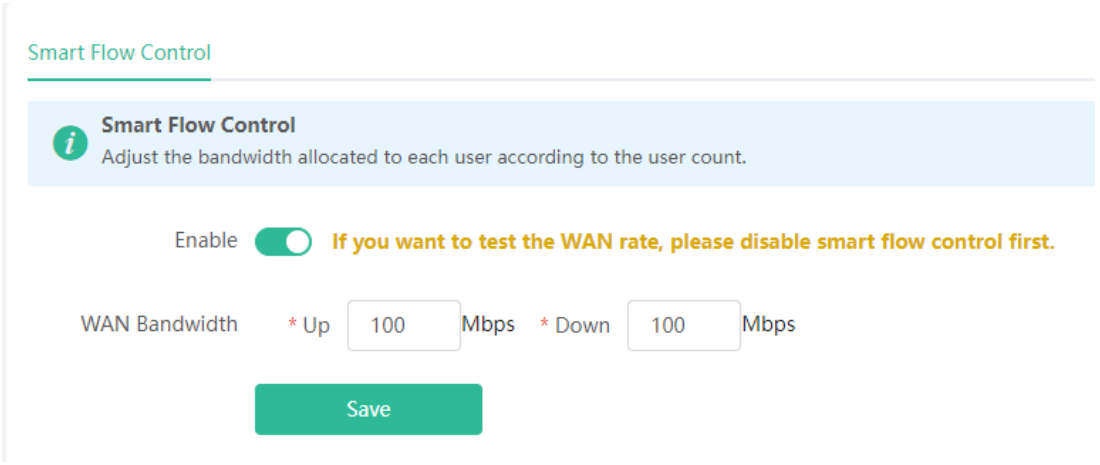
Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Advanced** > **Flow Control** > **Smart Flow Control**.

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

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.

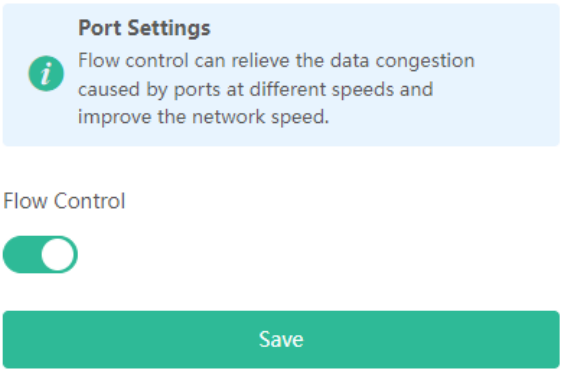



## 3.17 Enabling Port-Based Flow Control

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

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

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




## 3.18 Performing Advanced Network Settings

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

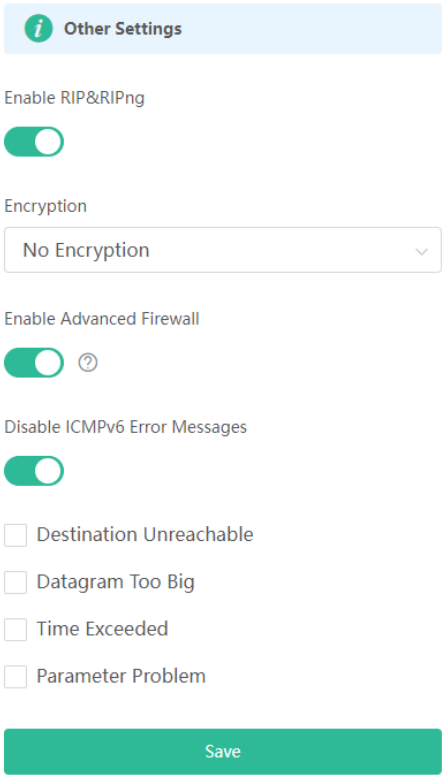
PC View: Choose **More** > **Advanced** > **Other Settings**.

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

**Enable RIP&RIPng**: The dynamic routing protocol can automatically synchronize routing information with other RIP-enabled routers in the network after this function is enabled.

**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.




## 3.19 Configuring UPnP

### 3.19.1 Overview

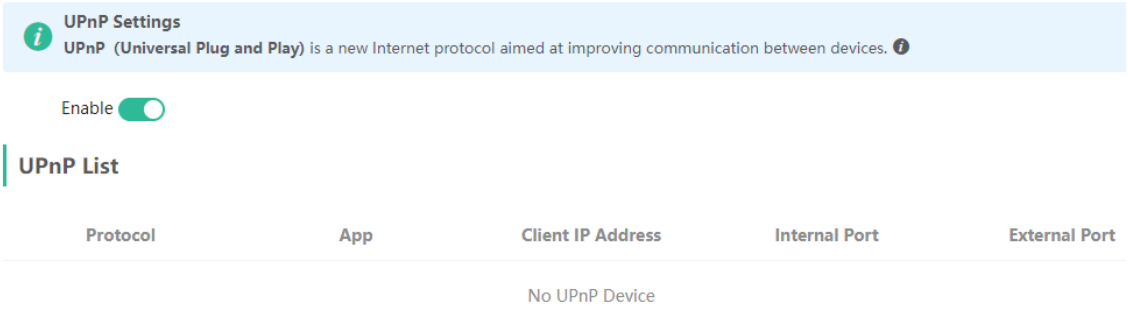
The universal plug and play (UPnP) function can map the port used by a client for Internet access according to the client's request so that related applications run faster or more stably. Common applications that support UPnP include MSN Messenger, Xunlei, BT and PPLive.

### 3.19.2 Configuration Steps

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

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

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



# 3.20 Configuring PPTP VPN

## 3.20.1 Overview

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

## 3.20.2 Configuring PPTP Server

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

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

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

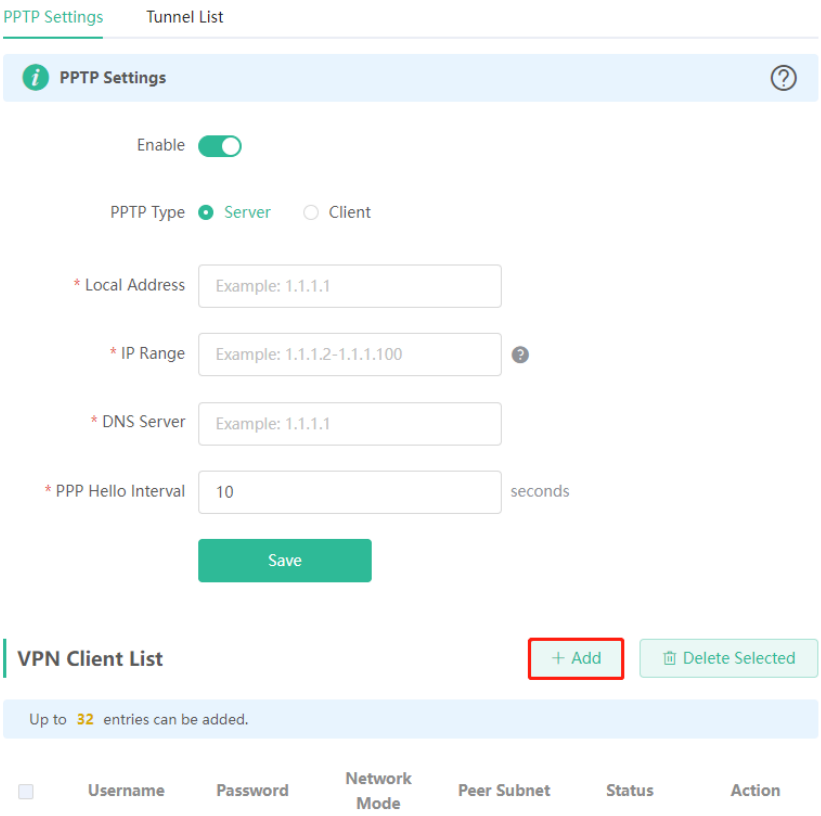
**Local Address**: Enter the local address. It is used as the local virtual IP address of the VPN tunnel for the client to access the server after dialing in.

**IP Range**: Enter the range of IP addresses. The IP addresses in this range will be assigned to clients.

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

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

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

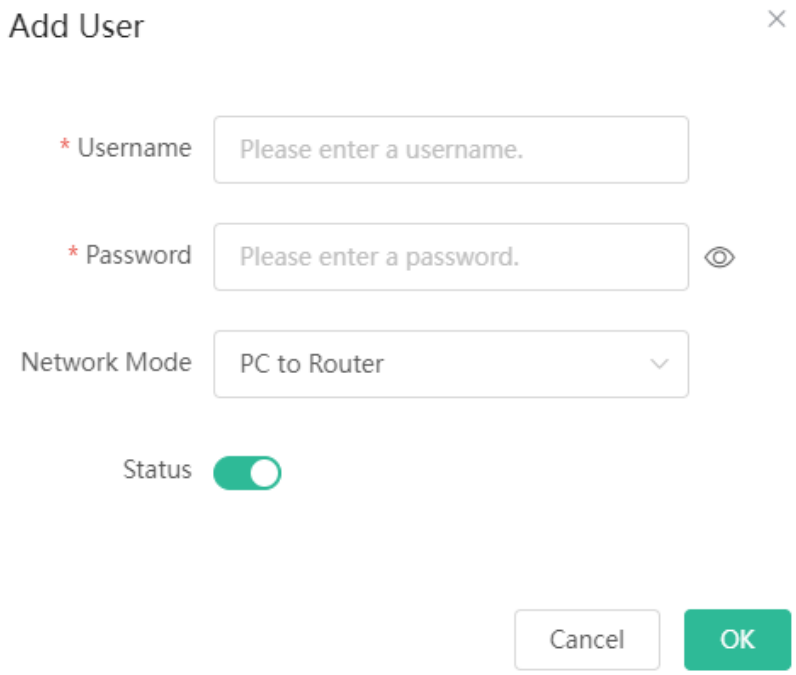



2. Add the PPTP user.

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

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

Enable **Status** and click OK.




### 3.20.3 Configuring PPTP Client

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

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

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

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

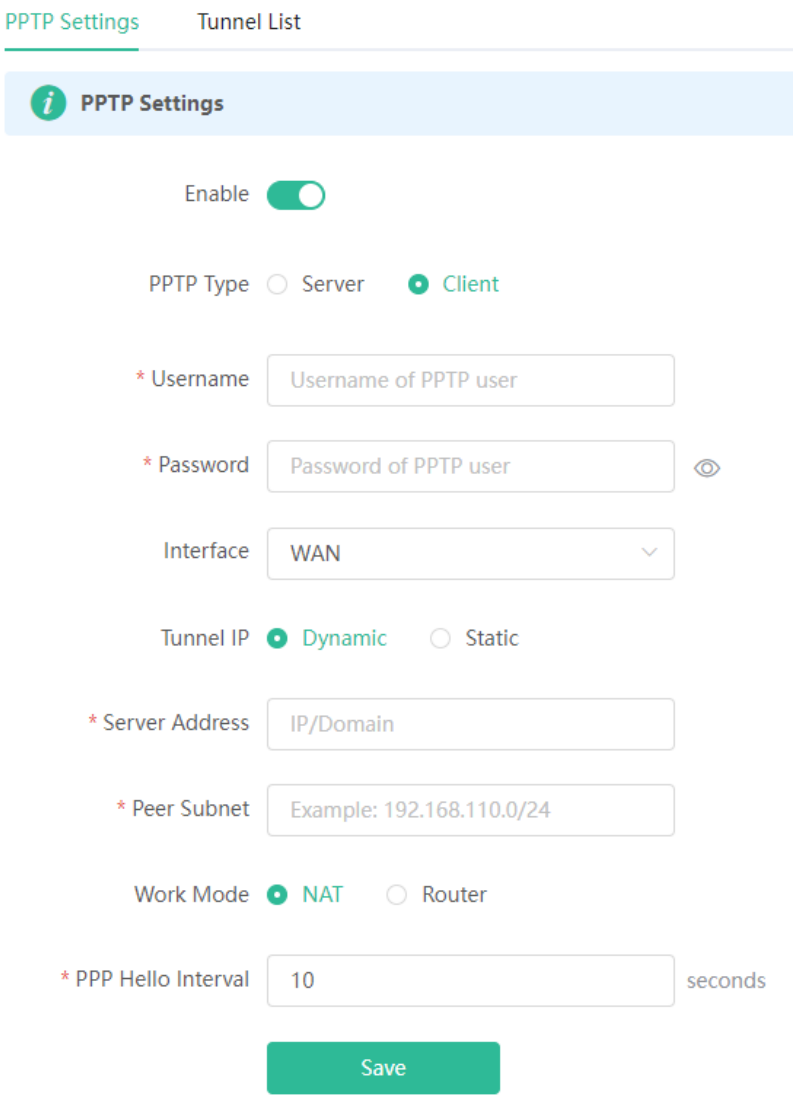
**Server Address**: Enter the WAN port IP address (the public IP is required) or the domain name of the server.

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

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

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

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



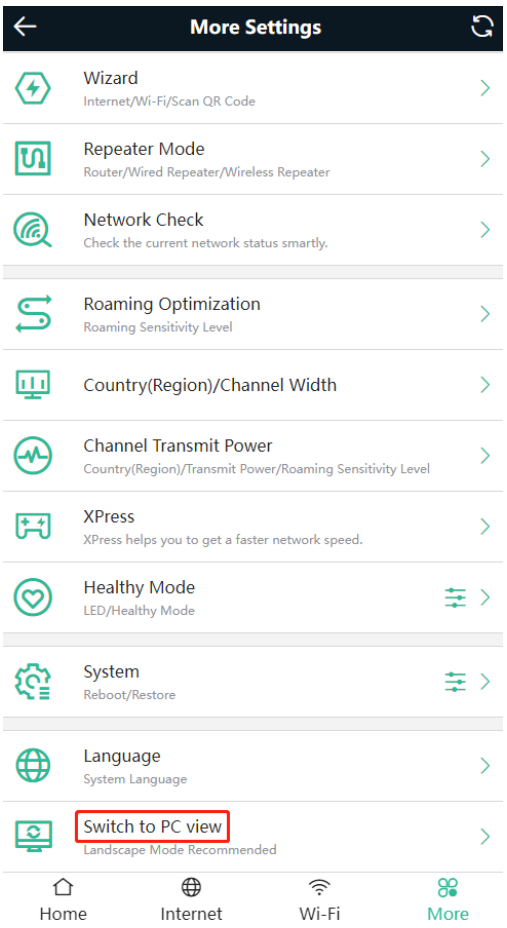

# 4 System Settings

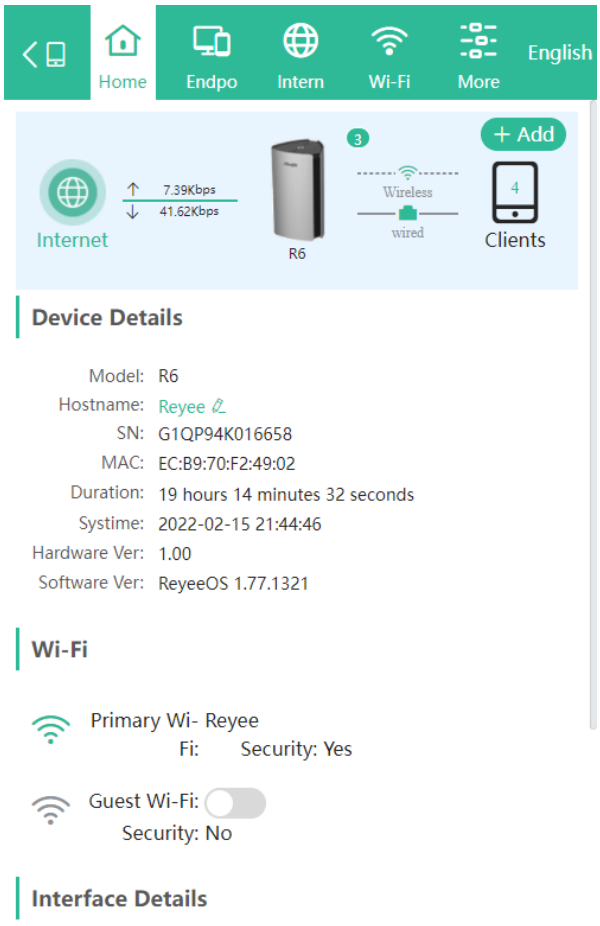
## 4.1 Switching to PC View

Choose **More** > **Switch to PC view**.

The PC view is the screen displayed after you log in from a PC. The page layout is different from that on the mobile phone.

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



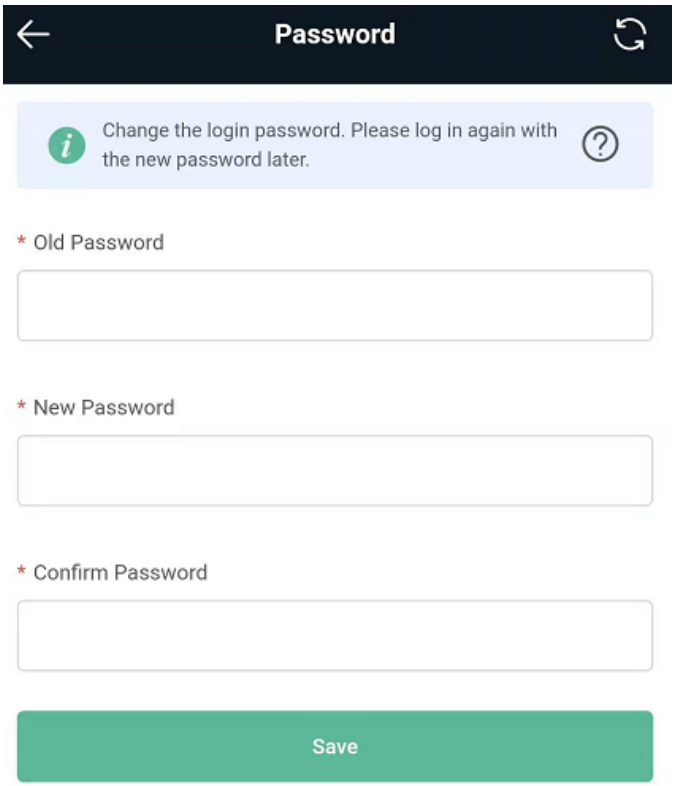




## 4.2 Configuring the Login Password

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

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

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




## 4.3 Restoring Factory Settings

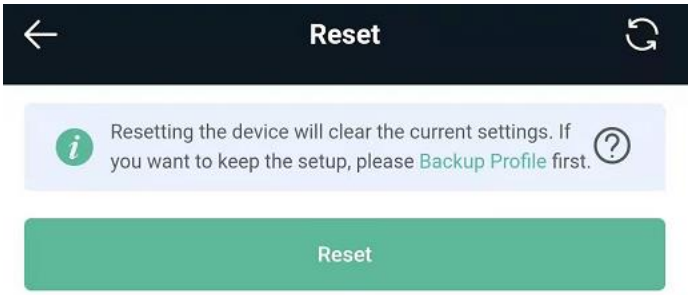
Mobile Phone View: Choose **More** > **System** > **Reset**.

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

Click **Reset** to restore factory settings.

**Caution**

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

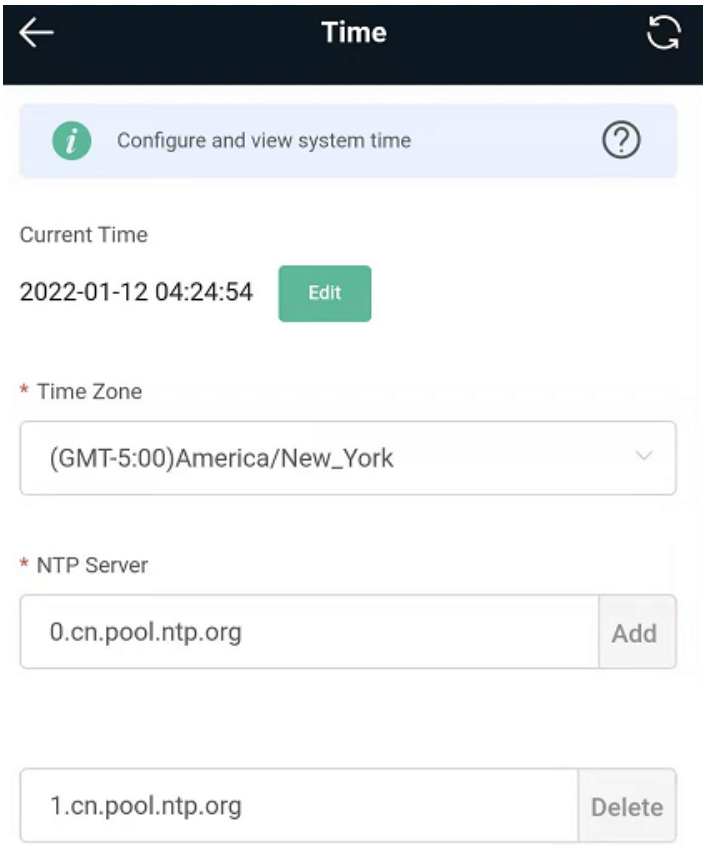


## 4.4 Configuring System Time

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




## 4.5 Configuring Scheduled Reboot

### 4.5.1 Getting Started

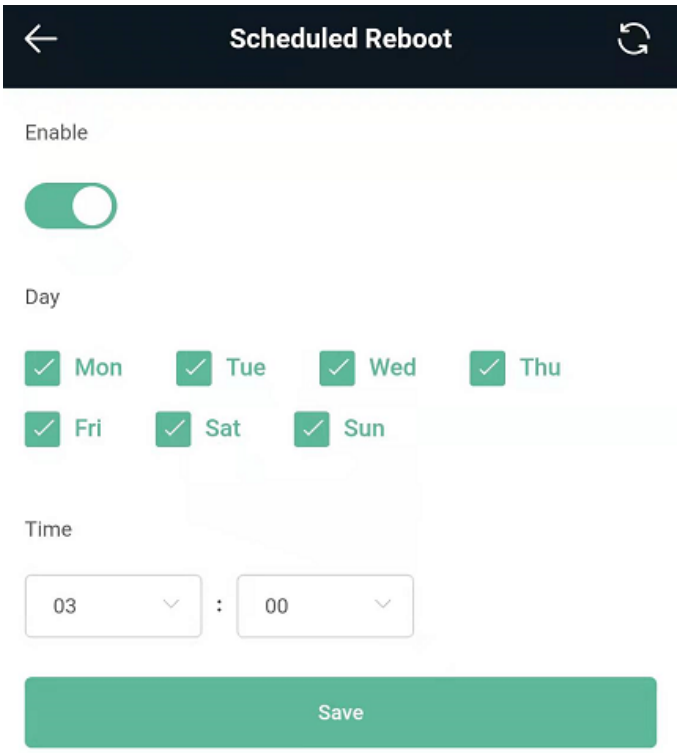
Confirm that the system time is accurate to avoid network interruption caused by device reboot at the wrong time. For details, see 4.4.

### 4.5.2 Configuration Steps

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

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

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




## 4.6 Performing Online Upgrade and Displaying the System Version

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

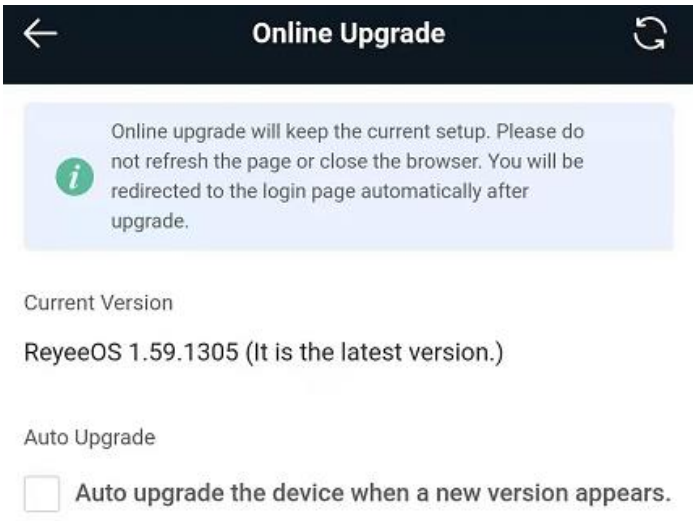
PC View: Choose **More** > **System** > **Upgrade** > **Online Upgrade**.

You can check the current system version. If there is a new version available, you can click it for an upgrade. The upgrade time can be set. You are advised to set the upgrade time to idle network time, for example, 4:15 a.m.

**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.

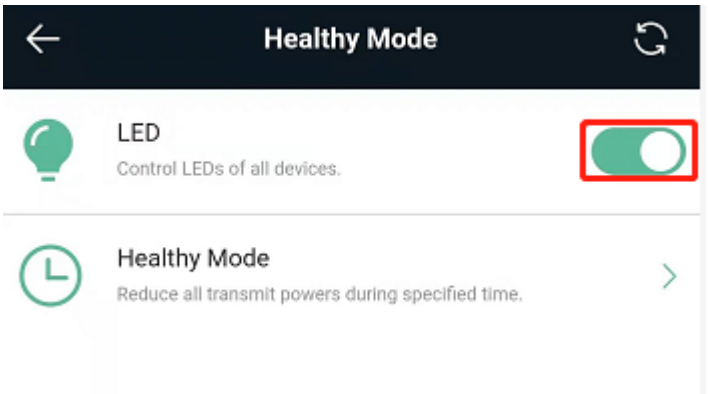
If no new version is detected and online upgrade cannot be performed, check whether the DNS is correctly obtained or go to **More** > **Advanced** > **Local DNS** to set the DNS server for the router.




## 4.7 Turning On/Off the Indicator

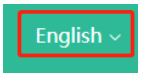
Mobile Phone View: Choose **More** > **Healthy Mode**.

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



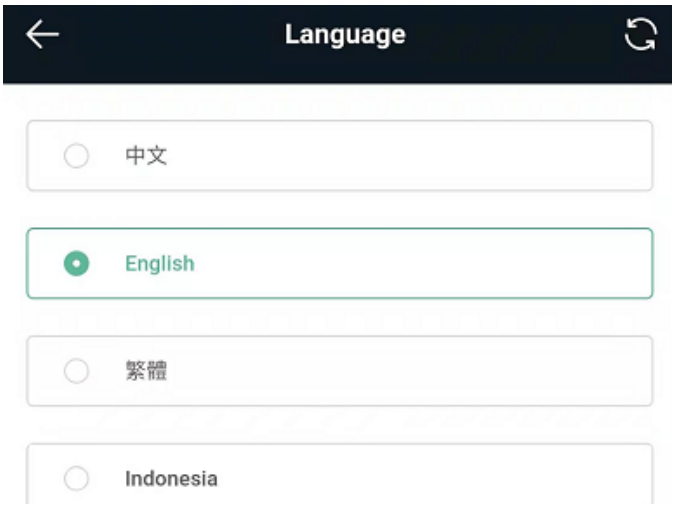

## 4.8 Switching System Language

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

PC View: Click 

in the upper right corner of the page.

Click a required language to switch the system language.

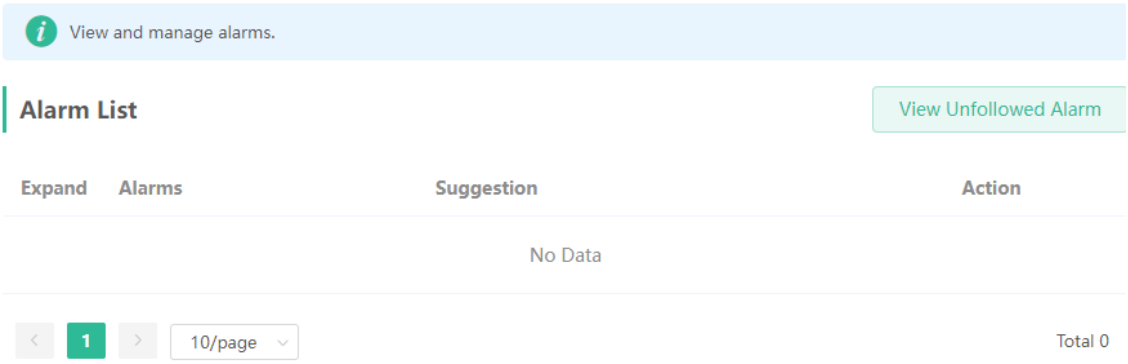



## 4.9 Enabling Alarms

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

PC View: Choose **More** > **Diagnostics** > **Alarms**.

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




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

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

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

**Table 4-1 Alarms and Suggested Action**

| Alarm | Suggested Action |
|---|---|
| The WAN port has no link. | Please check whether a cable is plugged into the WAN port. |
| The port is operating at 10Mbps. | Please check the peer port settings, unplug and re-plug the cable, or replace the cable. |
| There is more than one DHCP server in the LAN network. | Please disable the extra DHCP server in the LAN network. |
| There is more than one DHCP server in the WAN network. | Please disable the extra DHCP server in the WAN network. |
| Address pool of DHCP server is full. | Enlarge the DHCP address pool. |
| WAN & LAN Address Conflict. | Please check the IP addresses of WAN and LAN ports. If the network addresses conflict (including IP address conflict), change the IP of LAN port. |
| The WAN IP address is already in use. | Please check the WAN IP address. If it is a static IP address, please change the IP address. |
| The LAN IP address is already in use. | Please check the LAN IP address. If it is a static IP address, please change the IP address. |
| The IP address of the downlink address is already in 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. |
| There is more than one wireless controller in the network. | Please power off the extra wireless controller. |
| Cloud service is not running. | Please reboot the device. |
| Cloud service is not enabled. | Please contact Ruijie technical support. |
| The device is not connected to the Ruijie Cloud server. | Please reboot the device. |
| MAC address table is full. | Please check whether MAC address spoofing occurs. It is recommended to optimize the topology and |

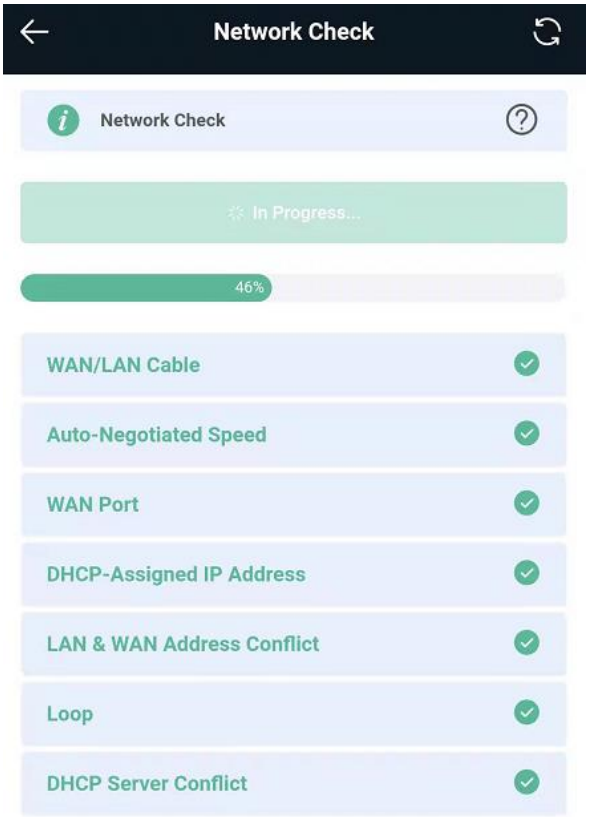
| | |
|---|---|
| | shorten the aging time of the MAC address table. . |
| ARP address table is full. | Please check whether ARP spoofing occurs. It is recommended to optimize the topology and reduce the number of PCs connected to the device. |
| PoE process is not running. | PoE is disabled. If the power is not 0 and the port can supply power normally, no operation is required. |
| PoE total power overload | Please check if the total power of PoE power supply is enough. |
| Loops occur. | Please check the network environment. |
| Power supply is insufficient. | Under voltage may affect device performance or cause device reboot. Please check the power supply of the device. |

## 4.10 Diagnosing Network Problems

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



# 4.11 Network Diagnosis Tools

### 1. Network Test Tool

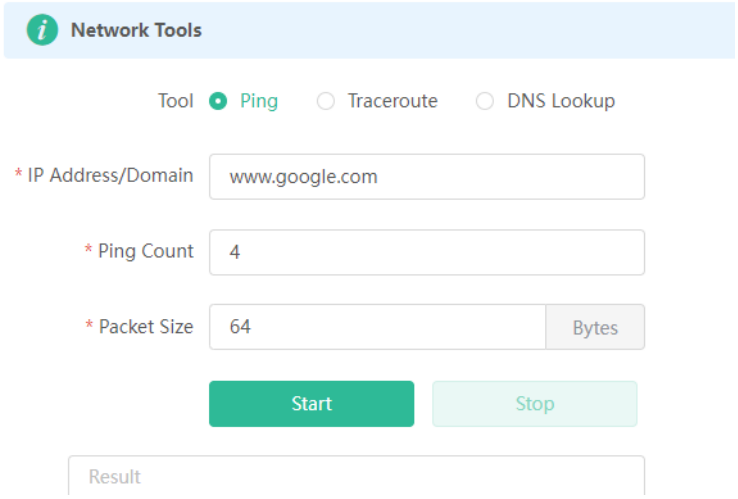
Mobile Phone View: Choose **More** > **System** > **Network Tools**.

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

When you select the ping tool, you can enter the IP address or URL and click **Start** to test the connectivity between the router and the IP address or URL. The message "Ping failed" indicates that the 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

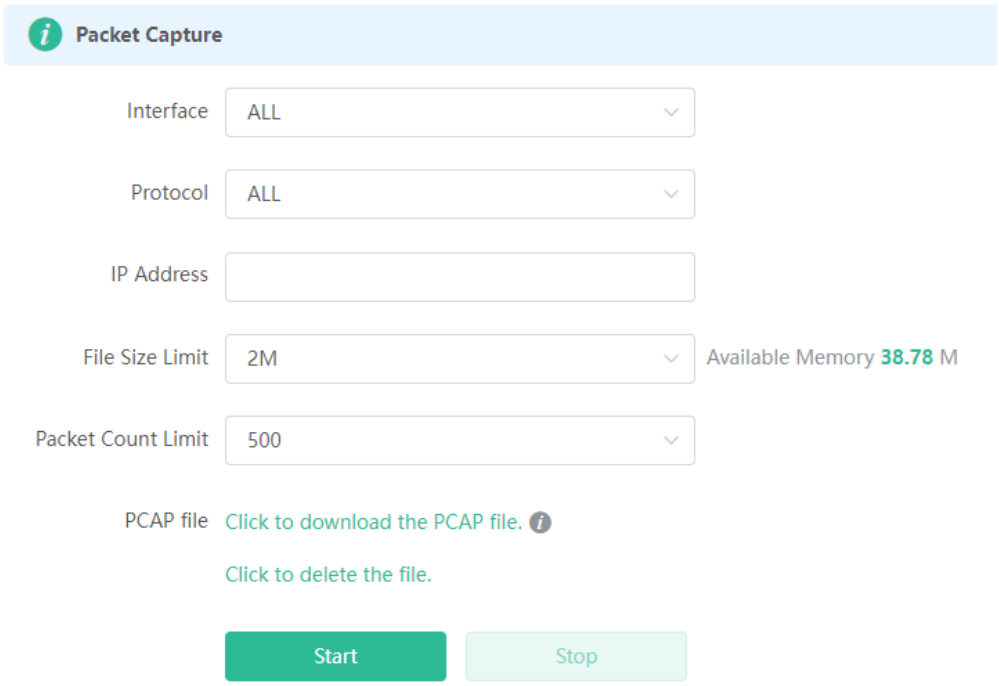
Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Diagnostics** > **Packet Capture**.

PC View: Choose **More** > **Diagnostics** > **Packet Capture**.

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 capture 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.



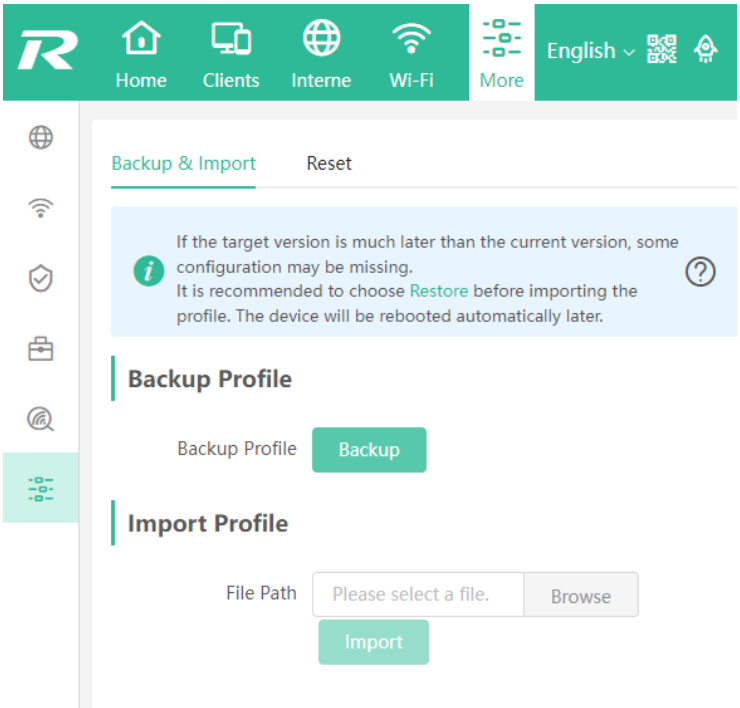

## 4.12 Configuring Config Backup and Import

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

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

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.



## 4.13 Configuring Session Timeout Duration

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

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

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

