Ruijie Reyee RG-EW 300 PRO

Web-based Configuration Guide

ReyeeOS 1.204

Document Version: V1.0
Date: 2022-06-19
Copyright © 2022 Ruijie Networks

Copyright

Copyright © 2022 Ruijie Networks

All rights are reserved in this document and this statement.

Without the prior written consent of Ruijie Networks, any organization or individual shall not reproduce, extract, back up, modify, or propagate the content of this document in any manner or in any form, or translate it into other languages or use some or all parts of the document for commercial purposes.

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, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. Except for the agreement in the contract, Ruijie Networks makes no explicit or implicit statements or warranties with respect to the content of this document.

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

This manual is designed merely as a user guide. Ruijie Networks has tried its best to ensure the accuracy and reliability of the content when compiling this manual, but it does not guarantee that the content of the manual is completely free of errors or omissions, and all the information in this manual does not constitute any explicit or implicit warranties.

Preface

Intended Audience

This document is intended for:

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

Technical Support

- The official website of Ruijie Reyee: https://www.ruijienetworks.com/products/reyee

Conventions

1. GUI Symbols

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

2. Signs

This document also uses signs to indicate some important points during the operation. The meanings of these signs are as follows:

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.

Note

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

Instruction

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.

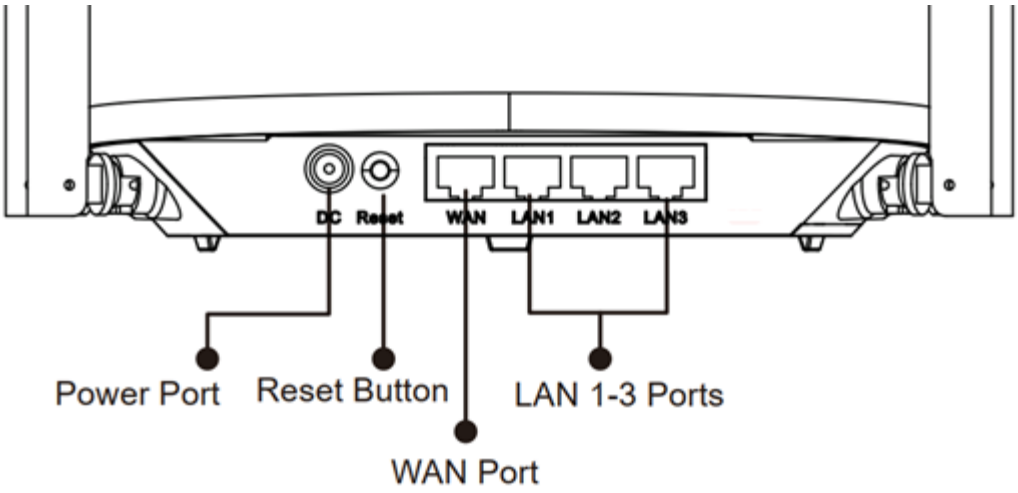
1 Fast Internet Access

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. The port nearest to the **Reset** button is the wide area network (WAN) port. The ports from left to right are WAN, LAN1, LAN2, and LAN3.



- Wireless Connection

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

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.

Note

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

EW300-Pro 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. The wireless repeater mode includes the repeater mode and wireless Internet service provider (WISP) mode.

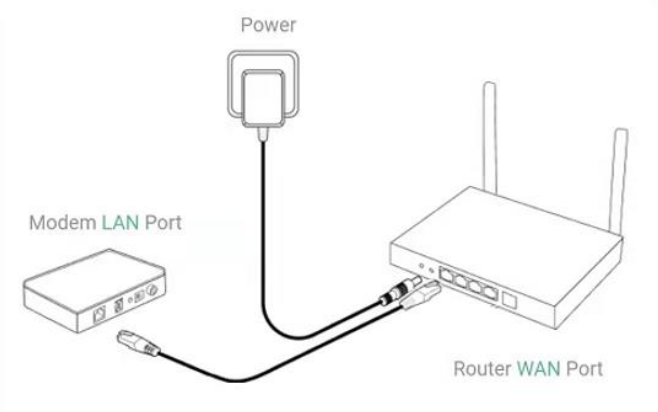
Instruction

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 port nearest to the **Reset** button on the EW300-Pro 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

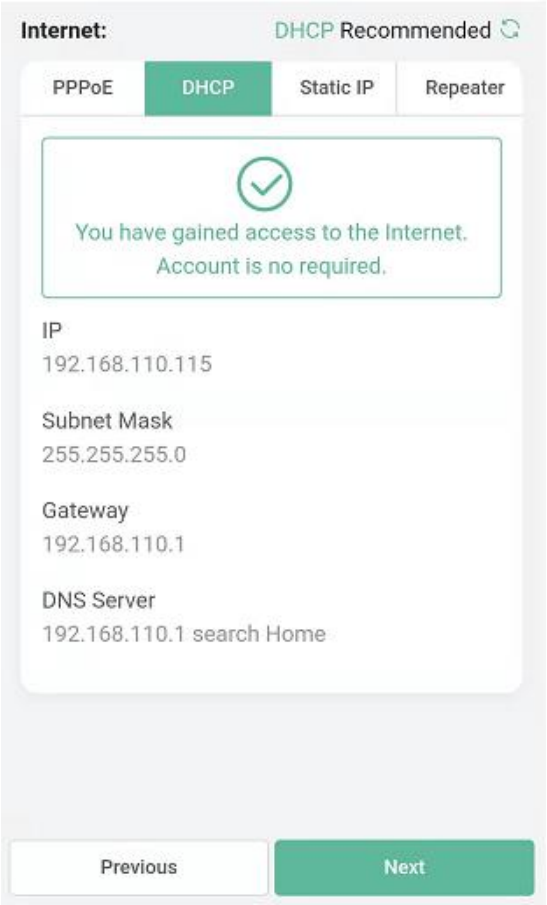
Click **Configure** and select the Internet connection type confirmed by the carrier.

- **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.

Note

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.

- **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

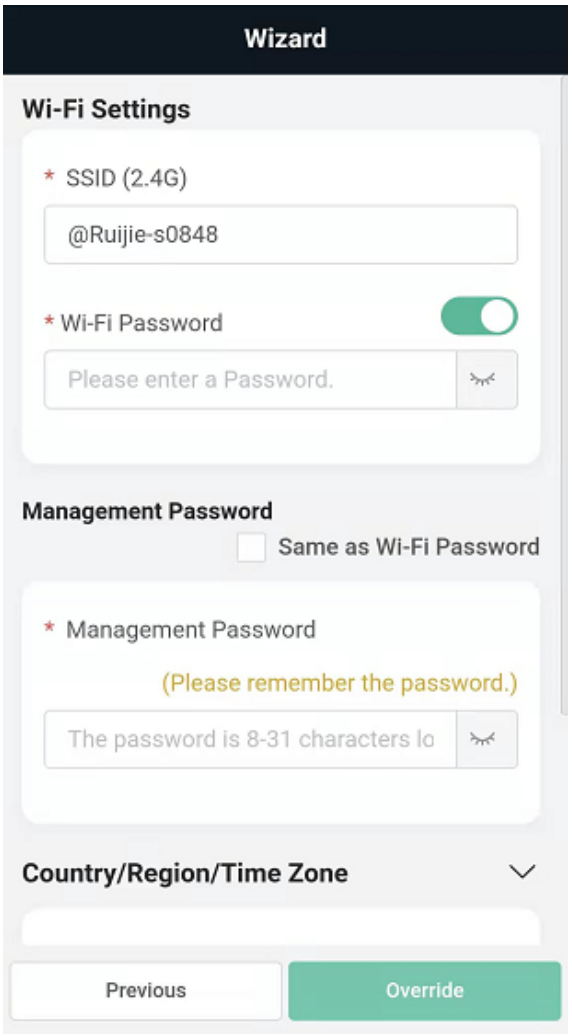
(1) **Setting the SSID and Wi-Fi password**: The device has no Wi-Fi password by default, indicating that the Wi-Fi network is an open network. You are advised to configure a complex password to enhance the network security. The password must be a string of 8 to 31 characters, which can contain uppercase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

(2) **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**.

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

(4) **Setting time**: Set the system time. The network time server is enabled by default to provide the time service. You are advised to select the actual time zone.

(5) **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.



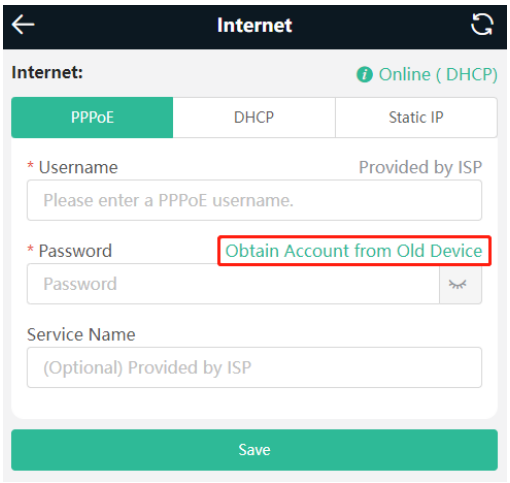
1.4.3 Verification and Testing

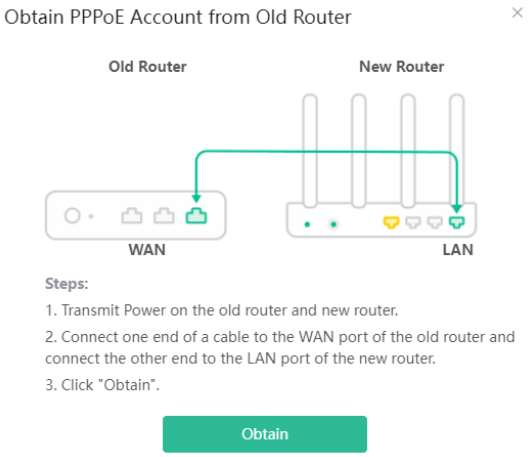
You can access the Internet after connecting to the Wi-Fi network. Log in to the management page (the default address is 192.168.110.1). The main page shows the Internet connection status and real-time upstream and downstream traffic data.

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 a network 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 a network cable is available, you are advised to connect the secondary router to the primary router through the wired connection.
- If no network 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.

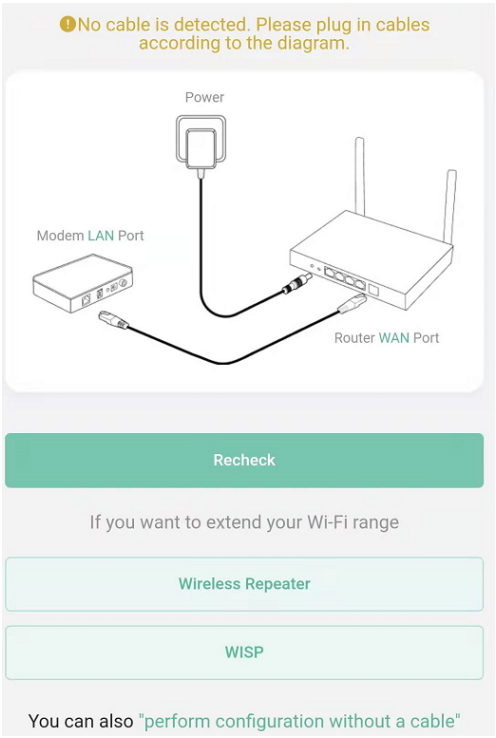
1.5.2 Configuration Steps

Wired Connection: After plugging in a network 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 a network cable.

Note

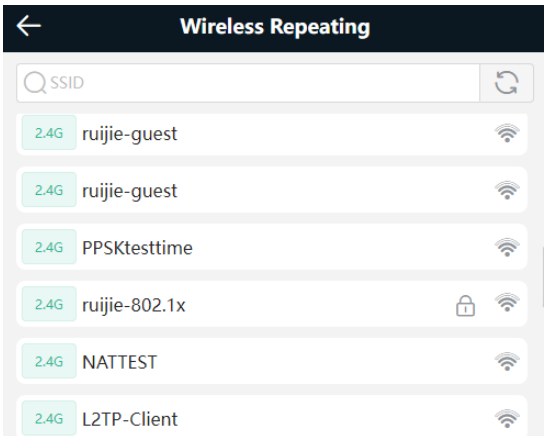
No network cable is required in the wireless repeater mode. The wireless network stability can be affected by many factors. Therefore, the wired connection is recommended.

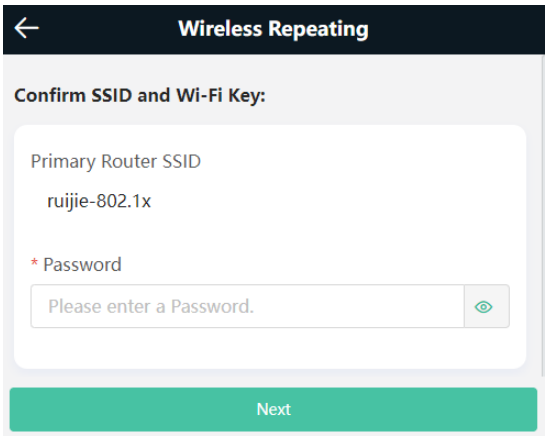


(1) Select **Wireless Repeater** or **WISP**.

- 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.

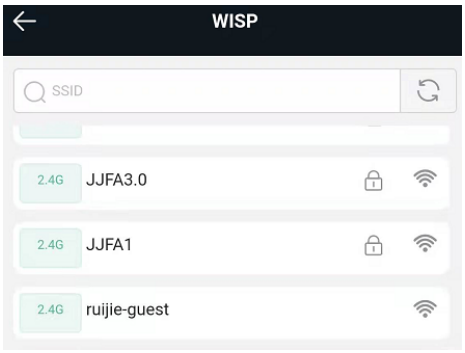


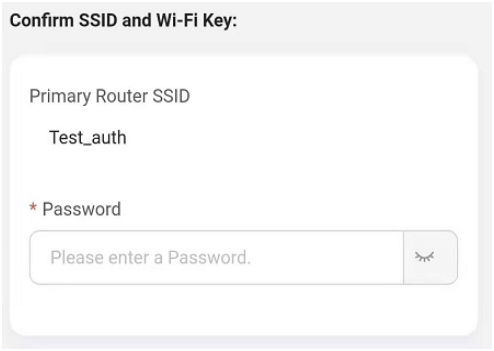


- Wireless ISP mode: Click **WISP**. On the displayed network setup page, click **Next** to automatically obtain an IP address. If the primary router cannot deliver an IP address, select **Static IP**. Select the SSID of the primary router and enter the Wi-Fi password to connect to the primary router.

  In wireless ISP mode, the device still supports the routing and DHCP functions, the IP addresses of clients connected to the primary router are assigned by the primary router and the IP addresses of clients connected to the secondary router are assigned by the secondary router. When the device connects to the Internet

through wireless connection, the wired WAN port becomes a LAN port for use by clients.





(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.

2 Wi-Fi Network Settings

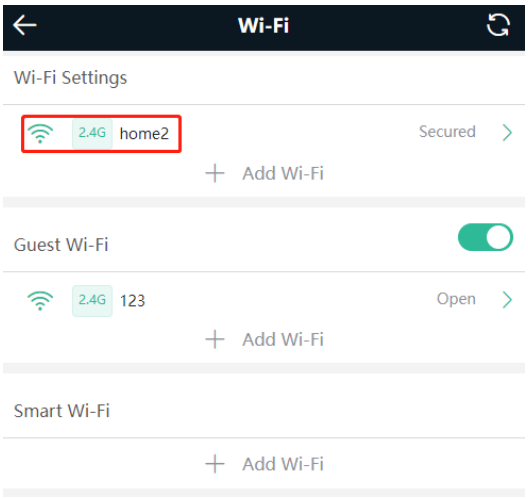
2.1 Changing the SSID and Password

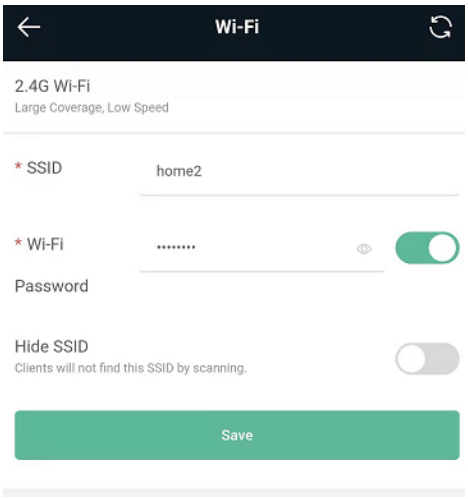
Choose **Wi-Fi** > **Wi-Fi Settings**.

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

Note

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.

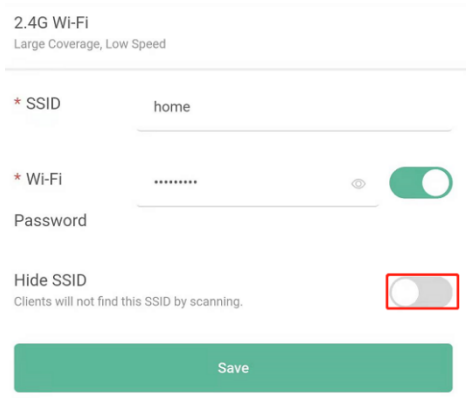
2.2.3 Configuration Steps

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

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

Note

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.



Instruction

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 Adding a Wi-Fi Network

2.3.1 Overview

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

- **Master Wi-Fi**: The master 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.

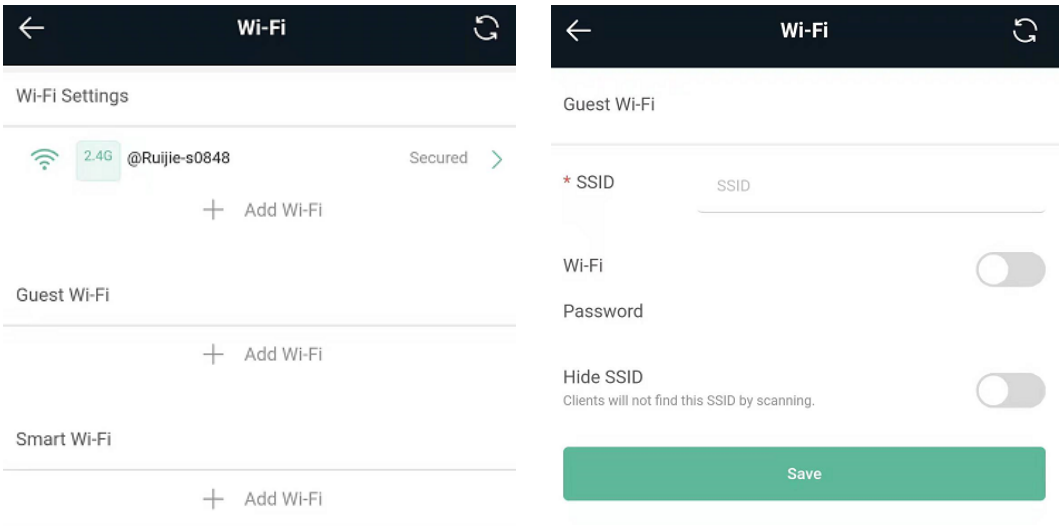
- **Smart Wi-Fi**: The smart Wi-Fi network is disabled by default. Smart clients can connect to the smart Wi-Fi network for long. The smart Wi-Fi network cannot be turned off as scheduled.

2.3.2 Configuration Steps

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

The page displays the master 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**.



2.3.3 Verification and Testing

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

2.4 Configuring the Wi-Fi Blacklist or Whitelist

2.4.1 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.

2.4.2 Configuration Steps

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

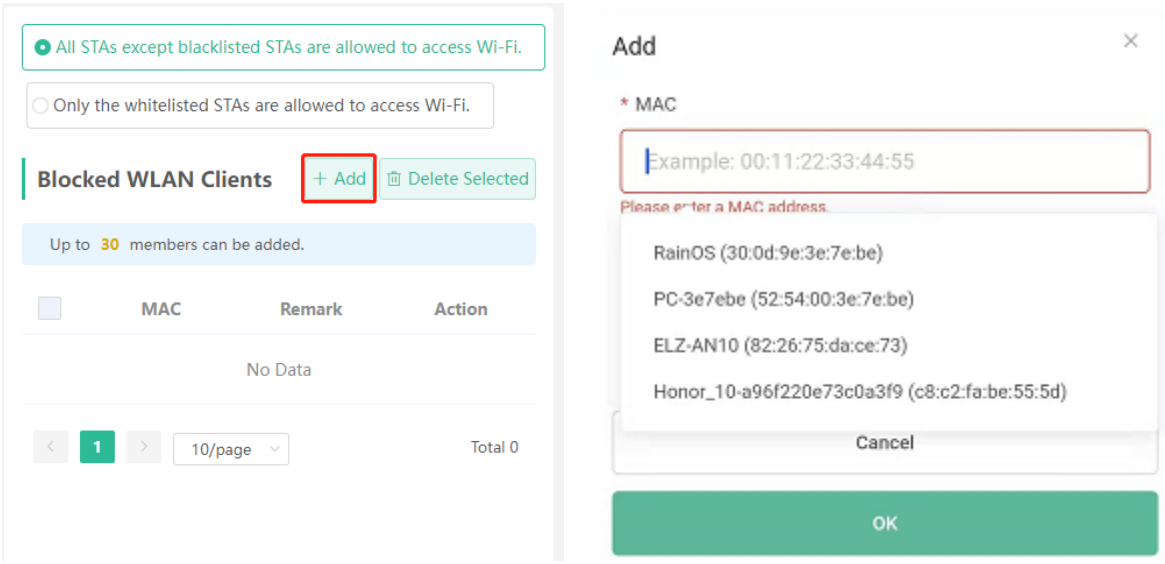
PC View: Choose **More** > **WLAN** > **Blacklist/Whitelist**.

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

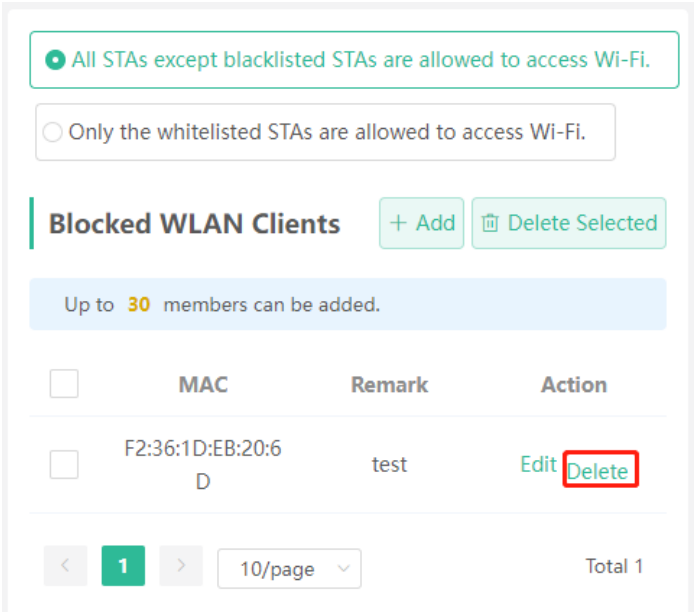
In the pop-up dialog box, enter the MAC address and remarks of the client to be blacklisted. The device displays information about the connected clients. Select a client, and it will be added to the blacklist automatically. Click **OK** to save the configuration. The client will be disconnected and prevented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

Note

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.



2.5 Optimizing the Wi-Fi Network

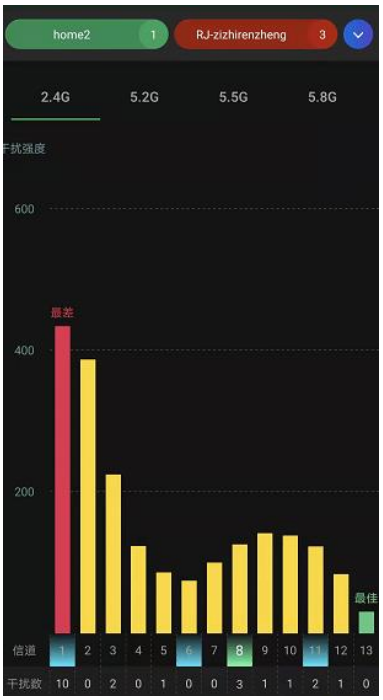
2.5.1 Overview

The device detects the surrounding wireless environment and selects the appropriate configuration upon power-on. However, network stalling caused by wireless environment changes cannot be avoided. Restarting the router

is a convenient and effective method to cope with network stalling. The router supports scheduled restart. For details, see 4.5 "Configuring Scheduled Reboot". You can also analyze the wireless environment around the router and select appropriate parameters.

2.5.2 Getting Started

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



2.5.3 Configuration Steps

- Optimizing the radio channel

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

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

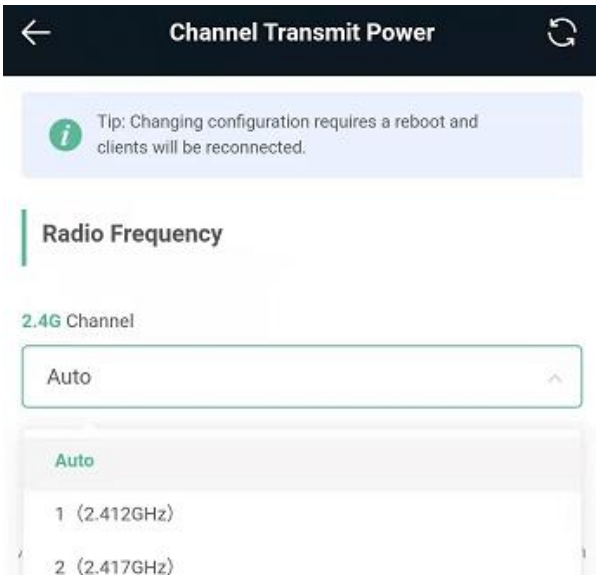
Choose the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. Excess clients connected to a channel can bring stronger wireless interference.

Instruction

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

Note

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



- Optimizing the channel width

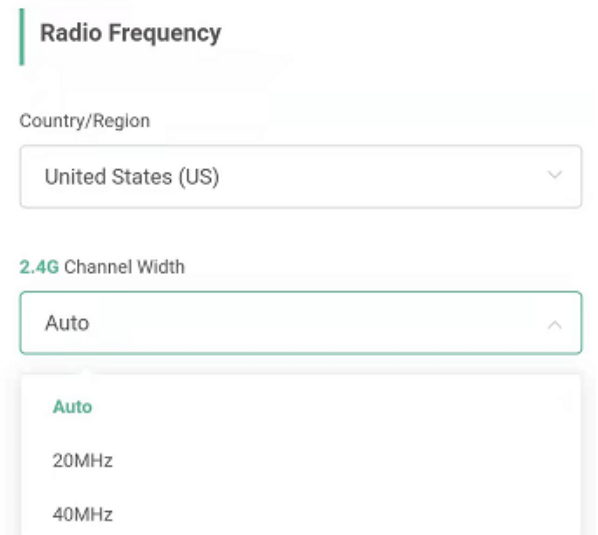
Mobile Phone View: Choose **More**> **Country(Region)/Channel Width**.

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. You are advised to select 20MHz channel width. After changing the channel width, click **Save** to make the configuration take effect immediately.

Note

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

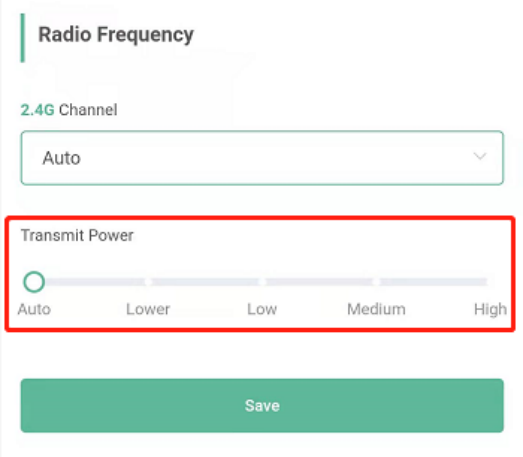
Mobile Phone View: Choose **More** > **Channel Transmit Power**.

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.

Note

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**.

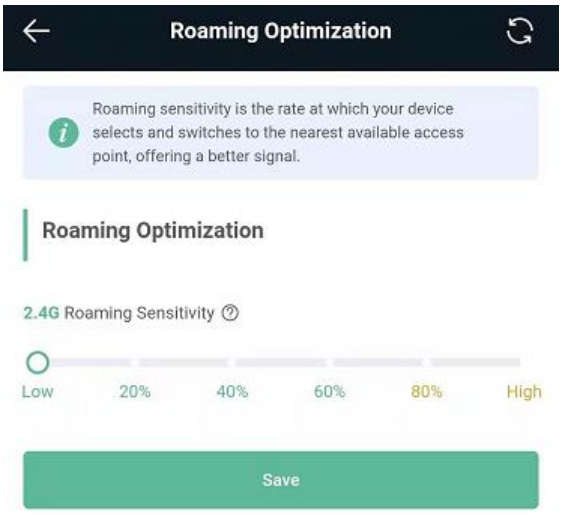
Clients such as mobile phones support the roaming function but the sensitivity level may not be high enough. The roaming sensitivity enables the device to actively disconnect a client from the Wi-Fi network when the client is far away, forcing the client to re-select the nearest signal and thus improving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

The default value (low sensitivity) is recommended.

Note

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.



2.6 Configuring the Healthy Mode

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

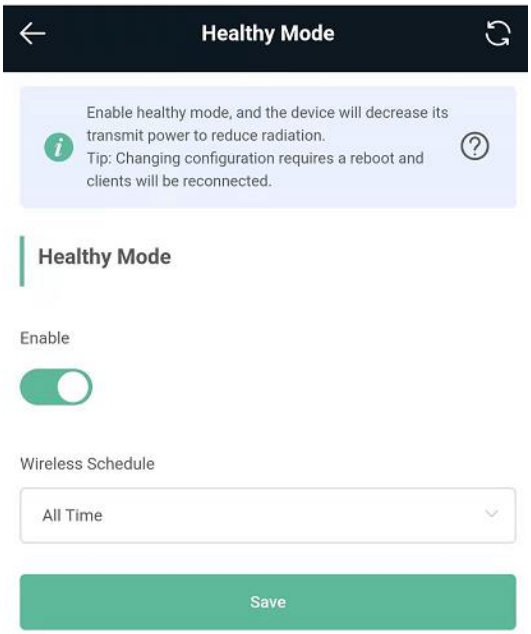
PC View: Choose **More** > **WLAN** > **Wi-Fi** > **Healthy Mode**.

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.

Instruction

All Ruijie wireless 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

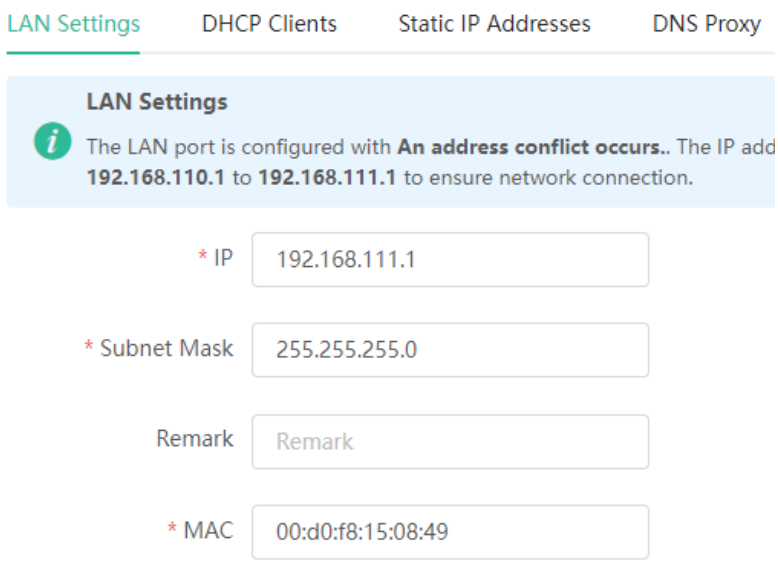
Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Basics** > **LAN**.

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.

Note

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**.

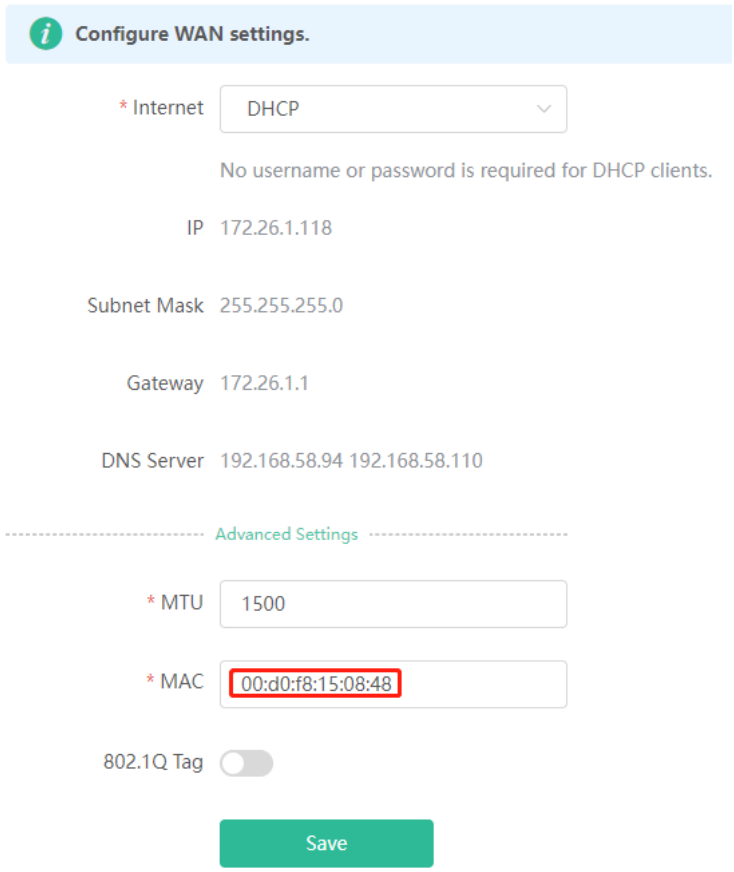
Enter the MAC address in the format of 00:11:22:33:44:55.

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

Note

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 a network 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/WISP**.

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.

Note

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

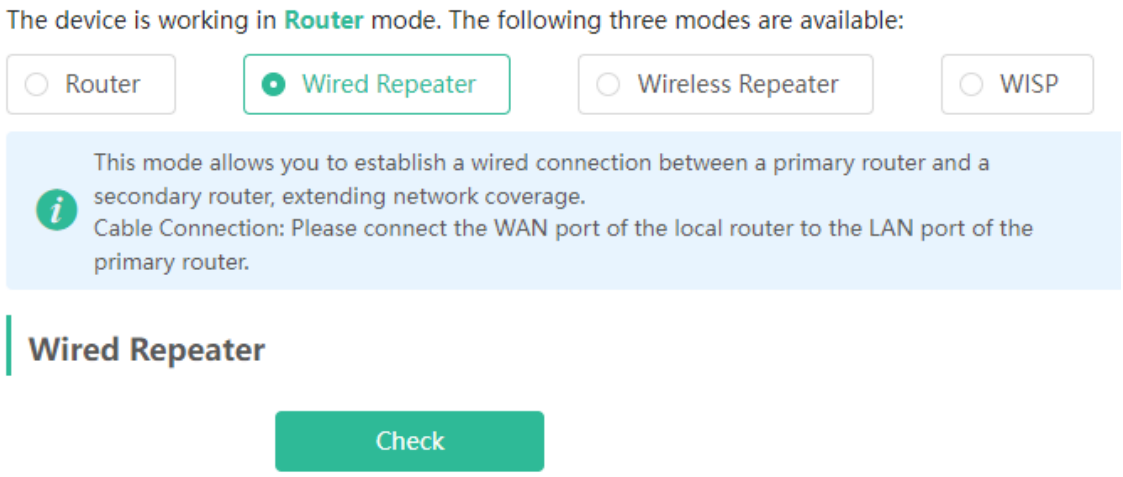
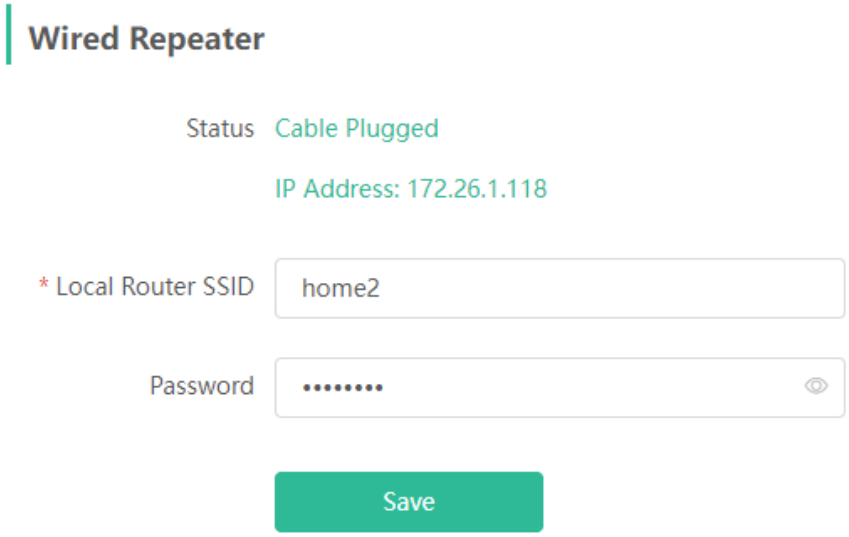


Figure 3-3 After Clicking Check



3.5.2 Wireless Repeater

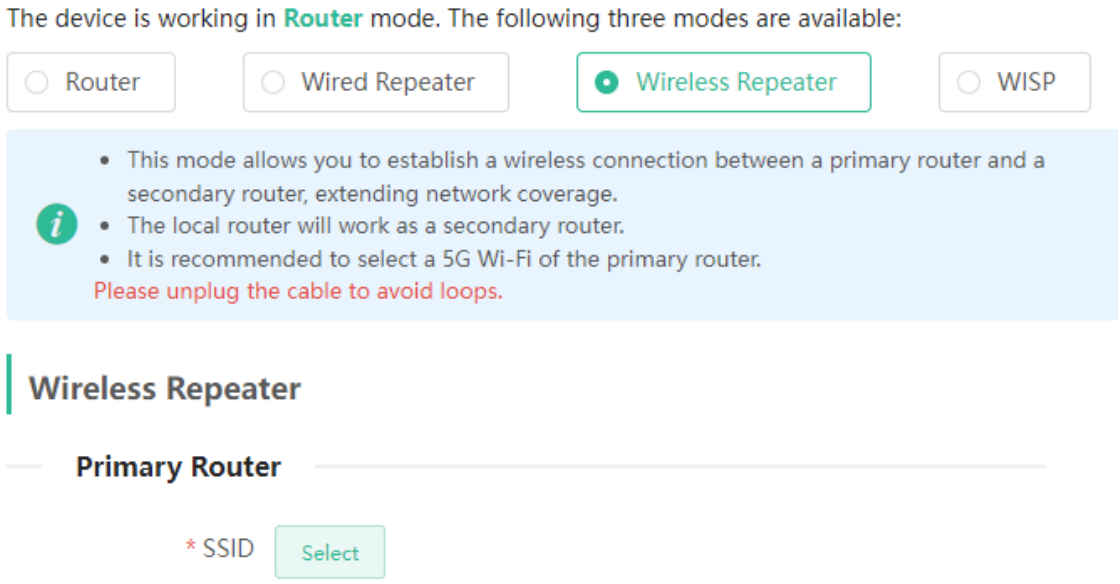
The wireless repeater mode extends the Wi-Fi coverage of the primary router.

Instruction

- The wireless repeater mode will affect the network speed and stability. You are advised to plug in a network cable and select the wired repeater mode if a network 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/WISP**.

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



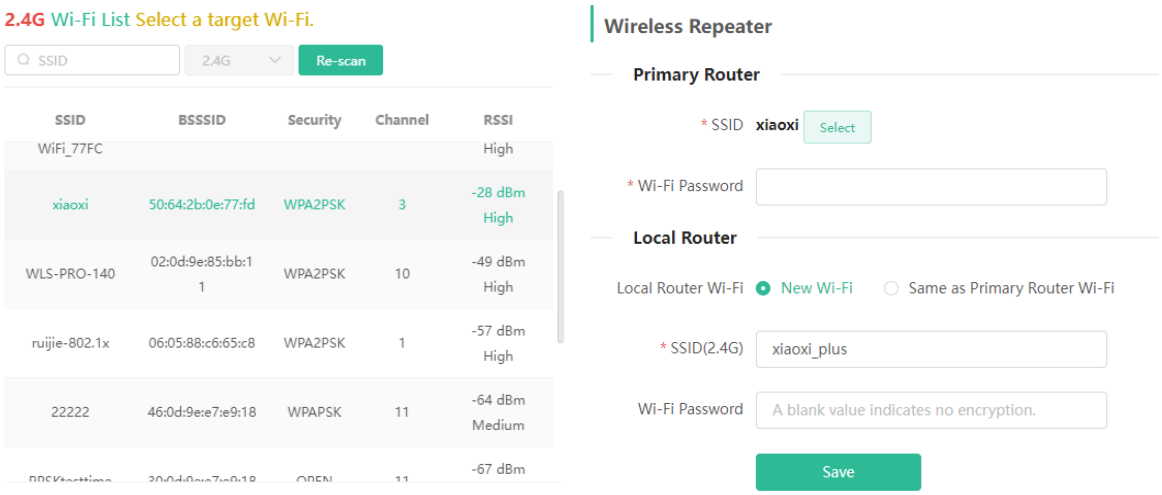
(2) Select the Wi-Fi signal of the primary router and enter its Wi-Fi password. You can configure a new Wi-Fi network or have a Wi-Fi network the same as that of the primary router:

- 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.

Note

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

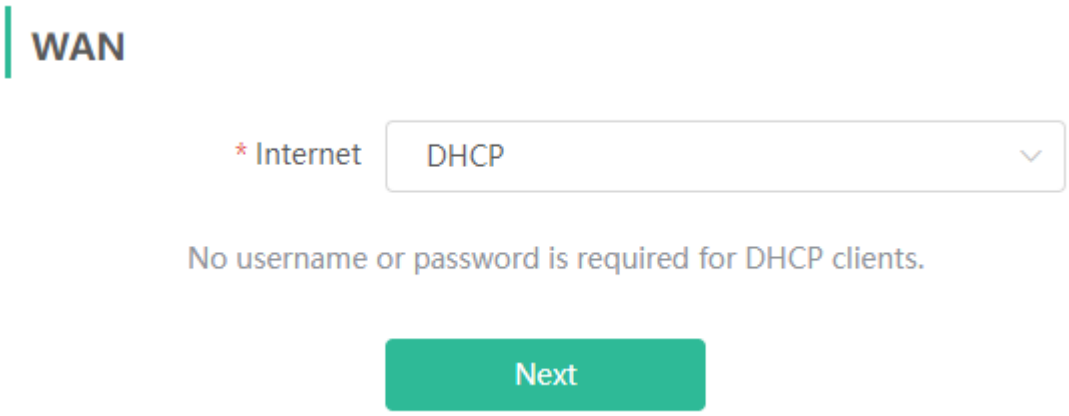


3.5.3 WISP

WISP allows users to establish their own WLANs for Internet access in public spaces, including coffee shops, hotels, airports, or restaurants.

(1) Choose **More** > **Switch to PC view** > **More** > **Basics** > **Repeater/WISP**.

Click **WISP**, select the Internet connection type, and click **Next**.



(2) Click **Select**, select a Wi-Fi signal, and click **Save**. See Figure 3-4 "Selecting the Wi-Fi Signal of the Primary Router and Connecting to the Wi-Fi Network".

Note

After you click **Save**, the Wi-Fi network will restart. You need to connect to the new Wi-Fi network. Exercise caution when performing this operation. Remember the SSID and password.

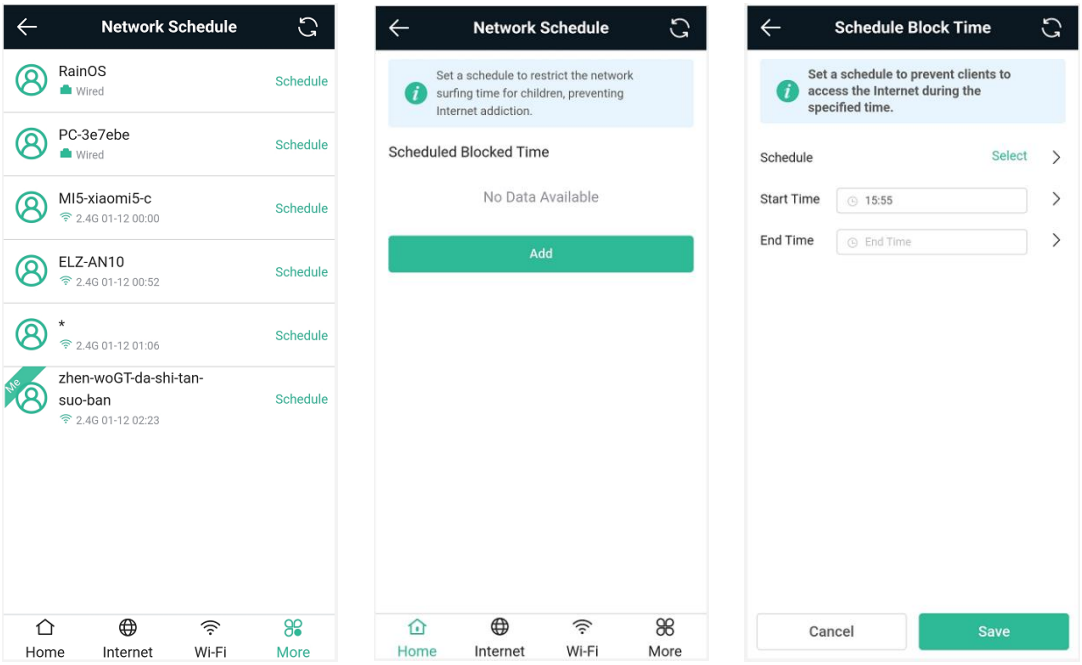
3.6 Controlling the Internet Access Time Range

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

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

Select a client and click **Schedule**. Click **Add** and set the time range in which Internet access is blocked. In the specified time range, the client is prevented from accessing the Internet.

In a PC view, you can select **Weekdays** or **Weekends** to block the Internet access of a client, or set **Blocked Time** to **Custom** and set a specific time range for blocking Internet access.

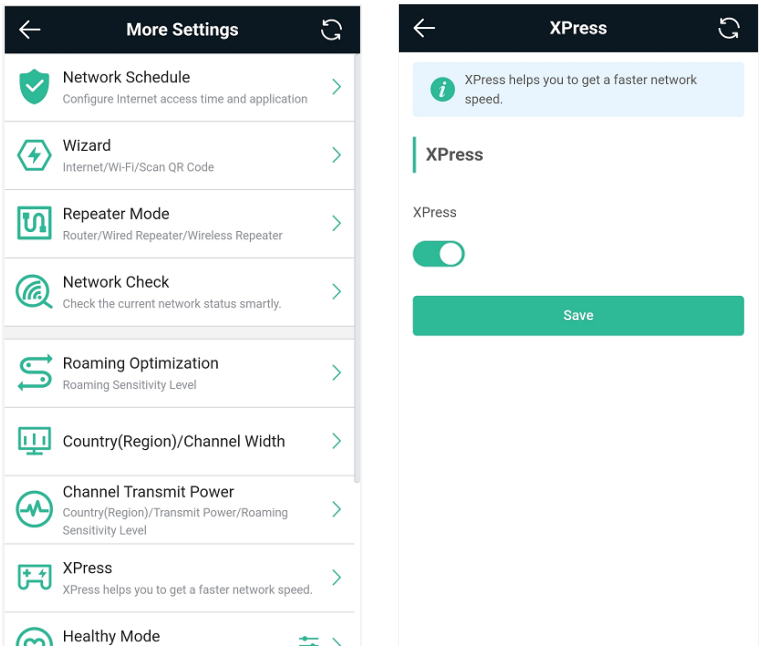


3.7 Configuring XPress

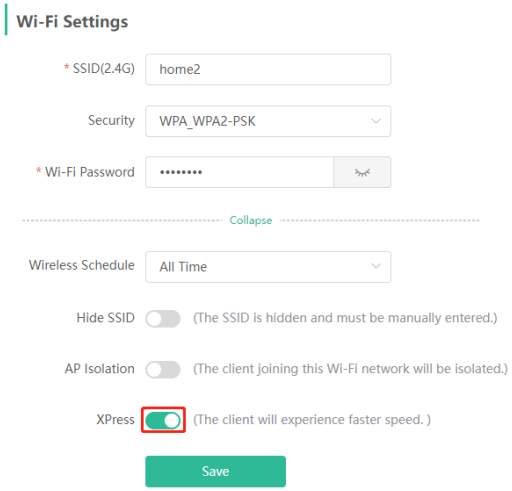
Mobile Phone View: Choose **More** > **XPress**.

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.



3.8 Configuring Port Mapping

3.8.1 Overview

Port mapping maps the IP address of a device on the LAN to an external network in the form of a combination of a WAN IP address and a port number, so as to provide the external network access service.

- Scenario 1: When you need to access IP cameras or PCs at home while you are away from home, port mapping needs to be configured.
- Scenario 2: When a server needs to be set up on the home network for Internet access, port mapping or demilitarized zone (DMZ) needs to be configured.

Port mapping maps the WAN port IP address of a router to an internal network host and port so that Internet users can proactively access hosts on the LAN.

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

3.8.2 Getting Started

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

3.8.3 Configuration Steps

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

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

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

Name: Enter a name for ease of maintenance.

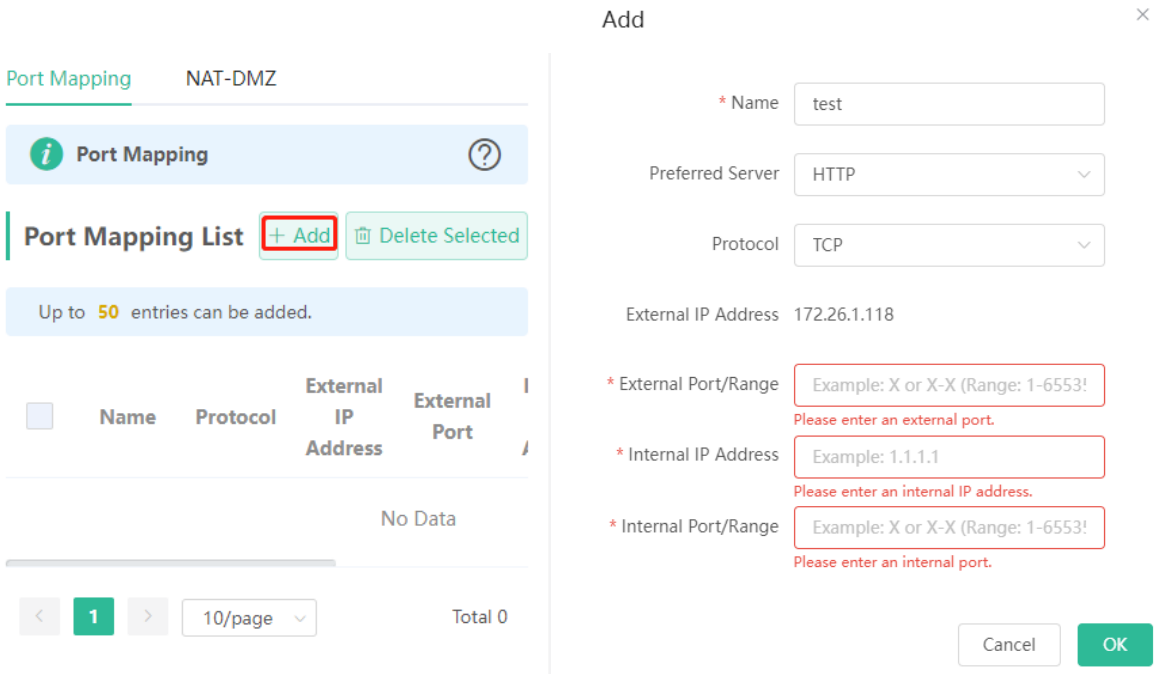
Preferred Server: Select a service to be mapped, such as HTTP or FTP. The device will automatically fill in the internal port number of the service. If you are not sure of the service, you can select **Custom**.

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

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

Internal 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.



3.8.4 Verification and Testing

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

3.8.5 Solution to a Test Failure

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

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

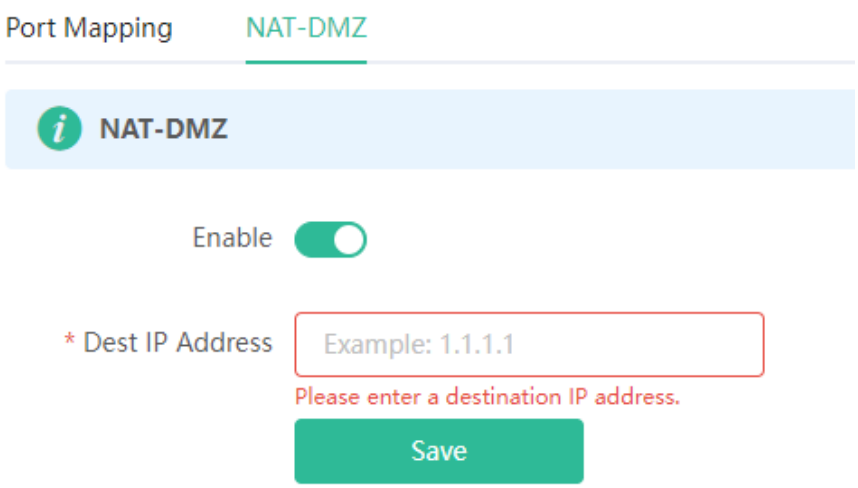
(3) Enable the DMZ service. For details, see DMZ Configuration Steps. The common cause is that port configuration is incorrect or incomplete.

3.8.6 DMZ Configuration Steps

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

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

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



3.9 Configuring DHCP Server

3.9.1 Overview

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

3.9.2 Configuration Steps

1. Configuring the DHCP Server Function

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

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

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

Note

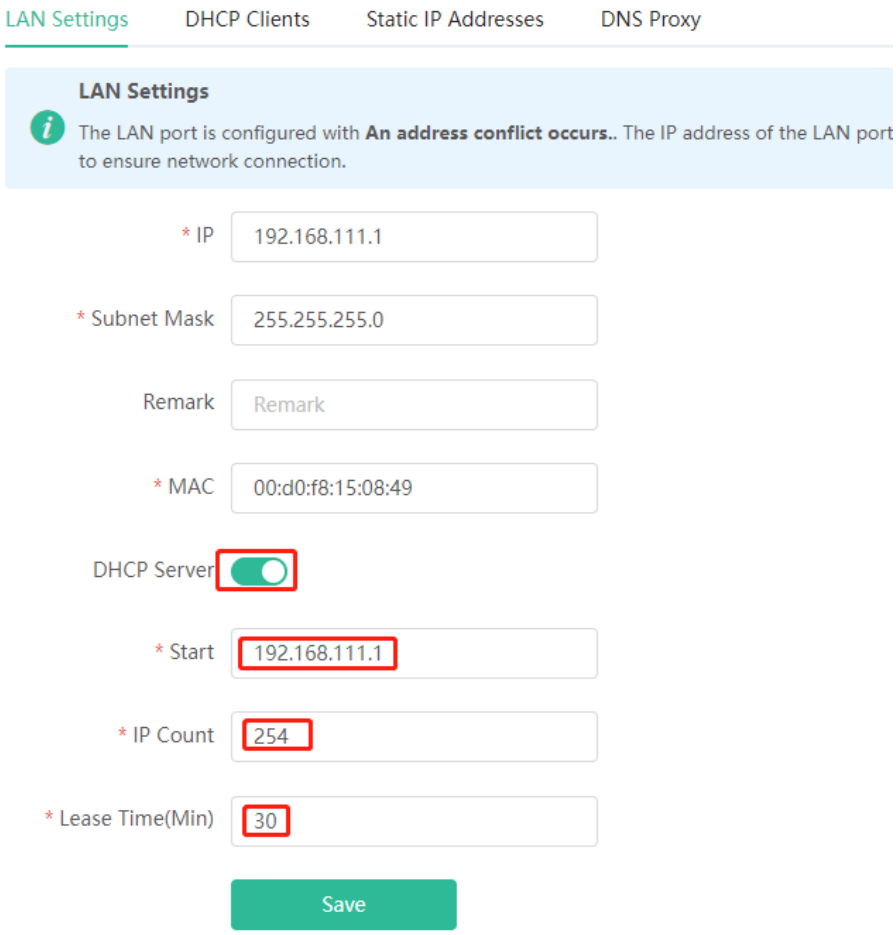
If the DHCP server function is disabled on all routers on the network, clients cannot automatically obtain IP addresses. You need to enable the DHCP server on a router or manually configure a static IP address for each client for Internet access.

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.

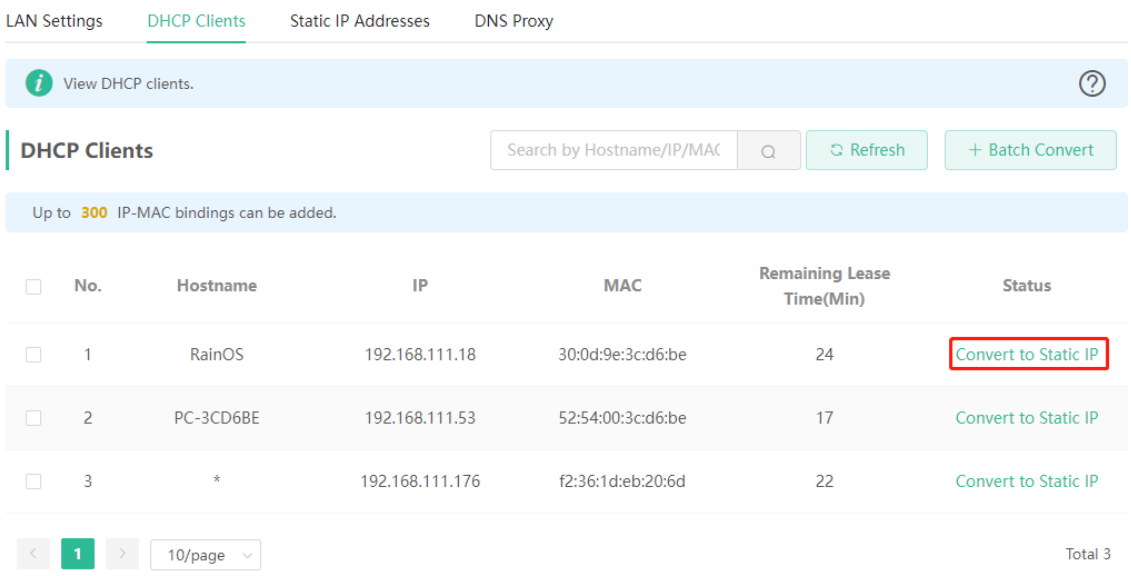


2. Displaying Online DHCP Clients

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.

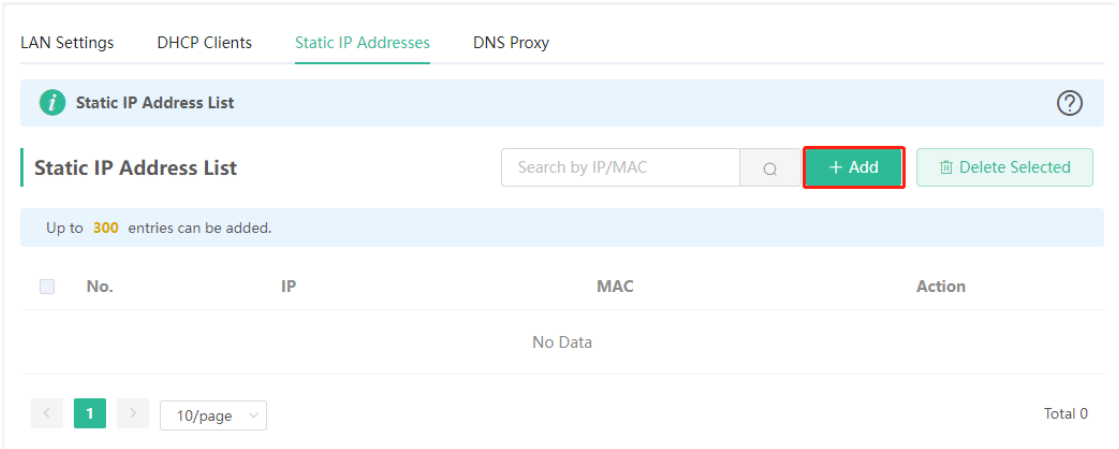


3. Displaying the DHCP Static IP Address Table

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.



3.10 Configuring DNS

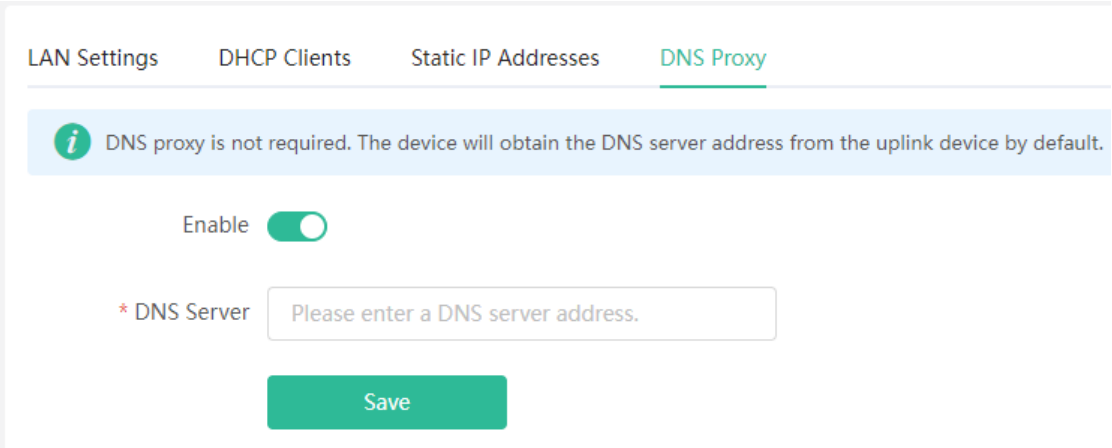
The domain name system (DNS) proxy configuration is not mandatory. The device obtains the DNS server address from the uplink device by default.

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

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



3.11 Configuring DDNS

3.11.1 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 PeanutHull, Dyn DNS, and No-IP DNS.

3.11.2 Getting Started

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

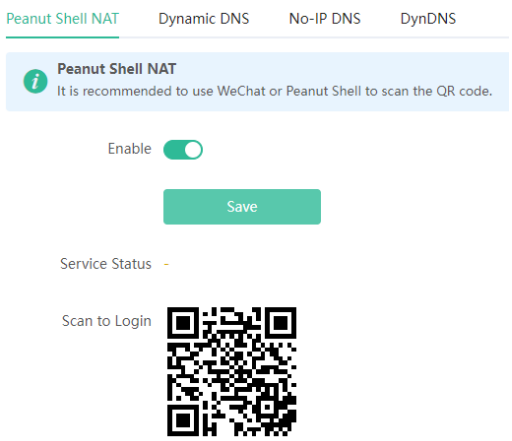
3.11.3 Configuration Steps

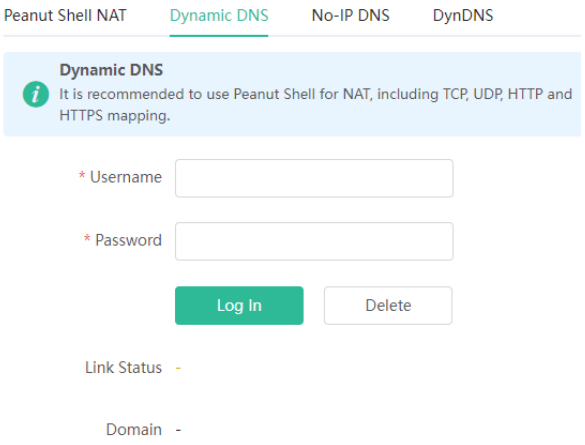
Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Advanced** > **Dynamic DNS** > **Dynamic DNS**.

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.





3.12 Configuring APR Binding and Guard

3.12.1 Overview

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

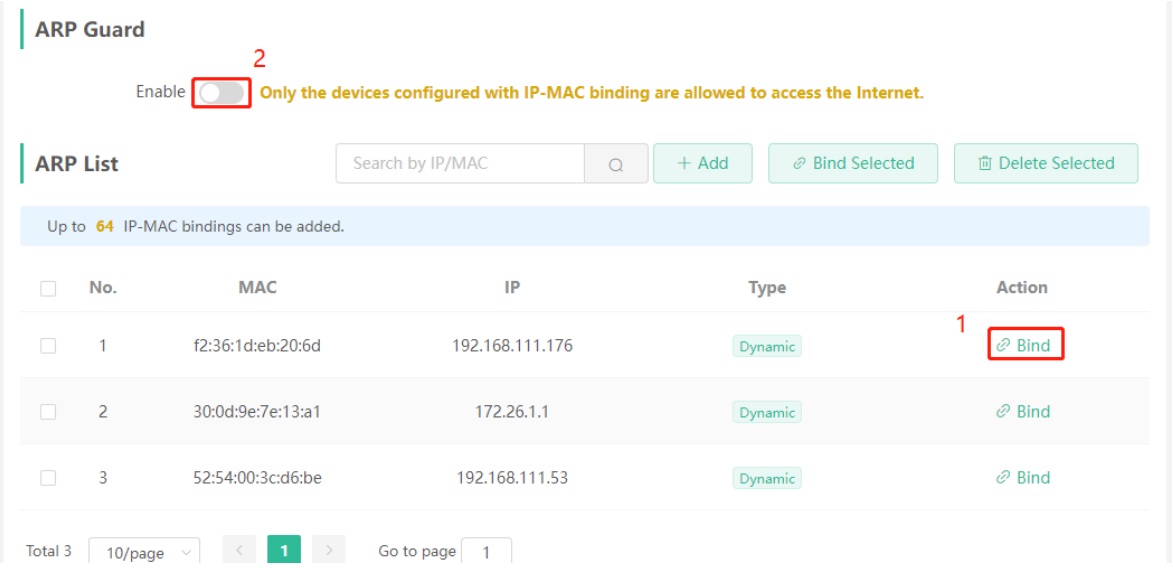
3.12.2 Configuration Steps

(1) Binding ARP information

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

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

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.

Note

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

3.13 Connecting to IPTV

IPTV is an Internet television service provided by ISP.

3.13.1 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.

3.13.2 IPTV Configuration Steps (VLAN Type)

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

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

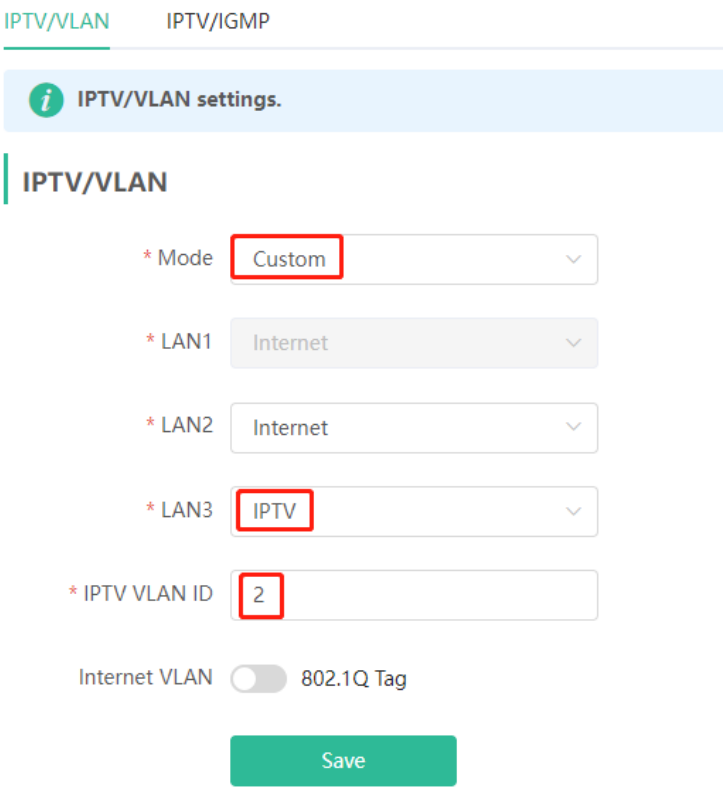
Select a local ISP mode, click the drop-down list of the target port, select **IPTV** from the drop-down list, and enter the VLAN ID provided by the ISP. For example, connect an IPTV set top box (STB) to LAN3 and set the VLAN ID to 2. The configuration is shown in the figure below.

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.

Note

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

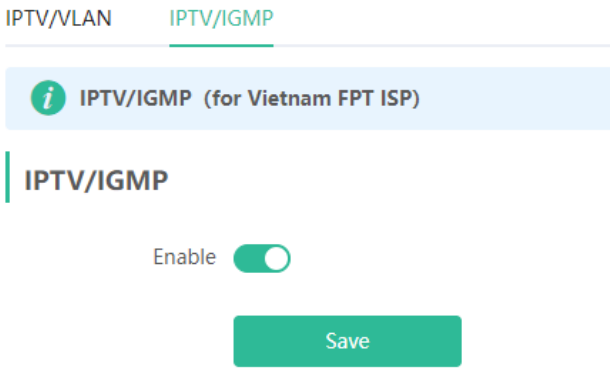


3.13.3 IPTV Configuration Steps (IGMP Type)

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

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



3.14 Enabling Flow Control

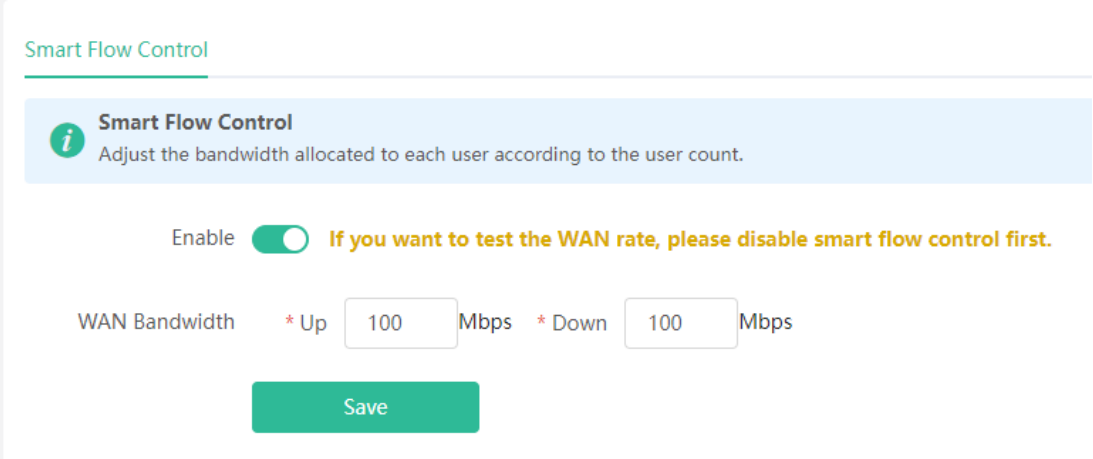
Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Advanced** > **Flow Control** > **Smart Flow Control**.

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.

Note

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



3.15 Configuring UPnP

3.15.1 Overview

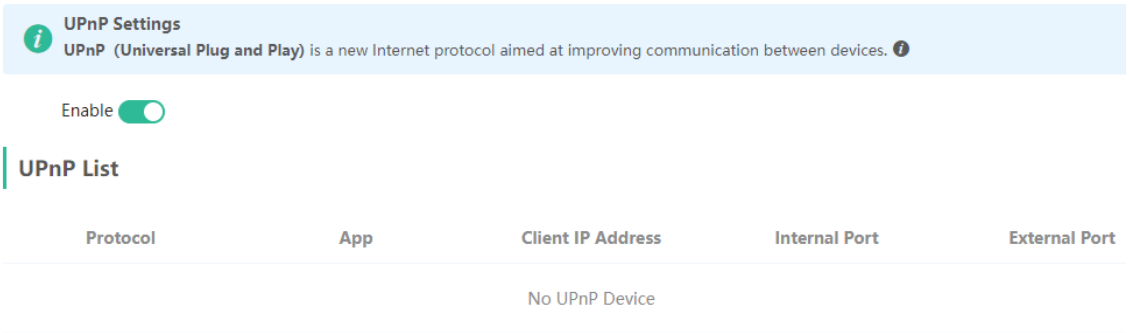
The universal plug and play (UPnP) function can map the port used by a client for Internet access according to the client's request so that related applications run faster or more stably. Common applications that support UPnP include MSN Messenger, Xunlei, BT and PPLive.

3.15.2 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.

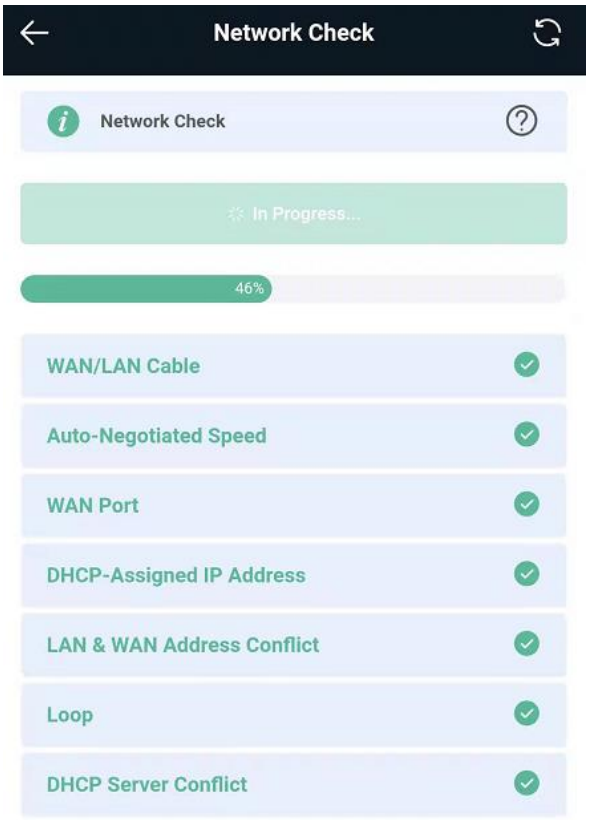


3.16 Diagnosing Network Problems

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 Ruijie Cloud Platform, and provide solutions and suggestions for risk items.



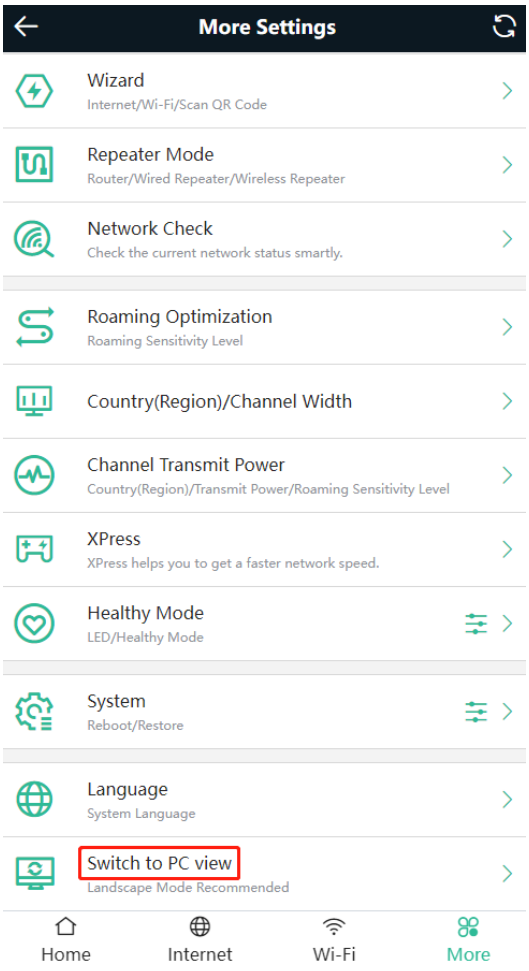
4 System Settings

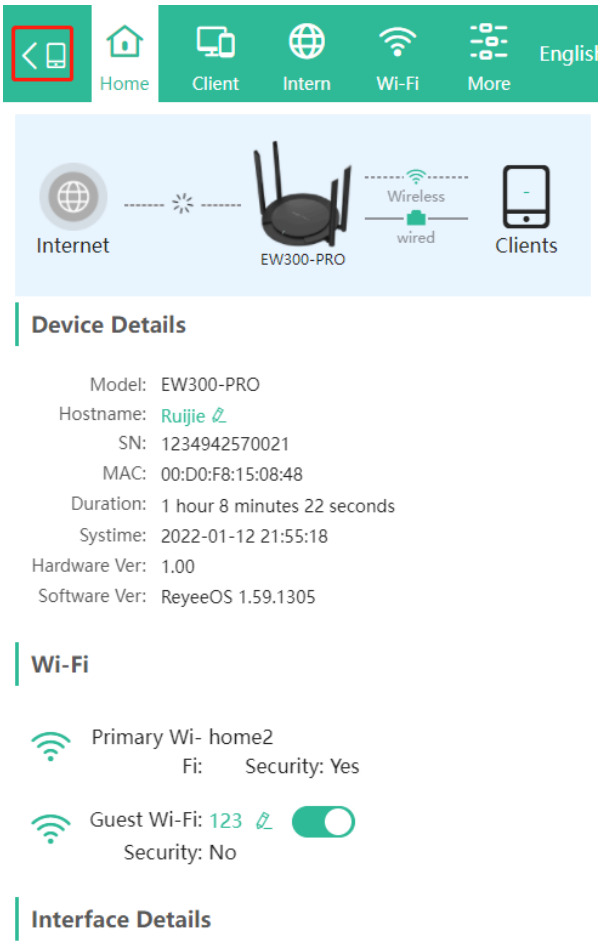
4.1 Switching to PC View

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).



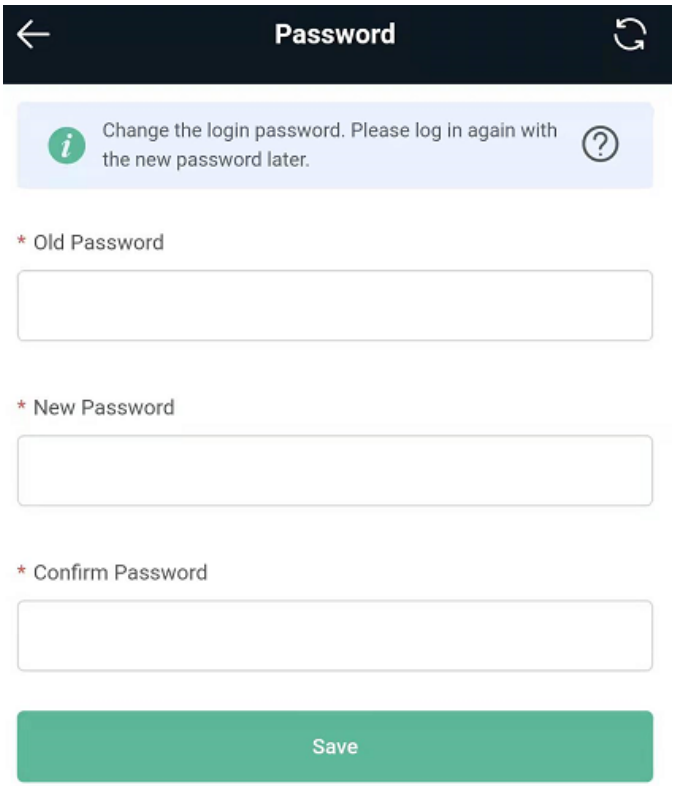


4.2 Configuring the Login Password

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

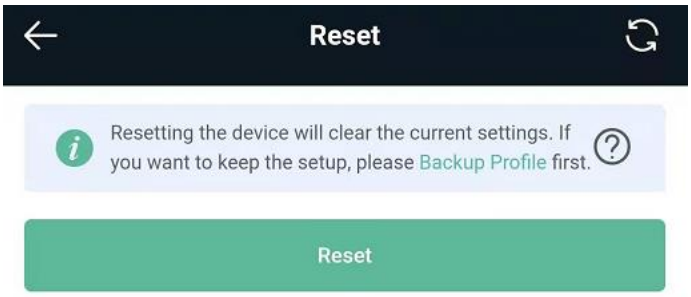
Mobile Phone View: Choose **More** > **System** > **Reset**.

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

Click **Reset** to restore factory settings.

Note

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

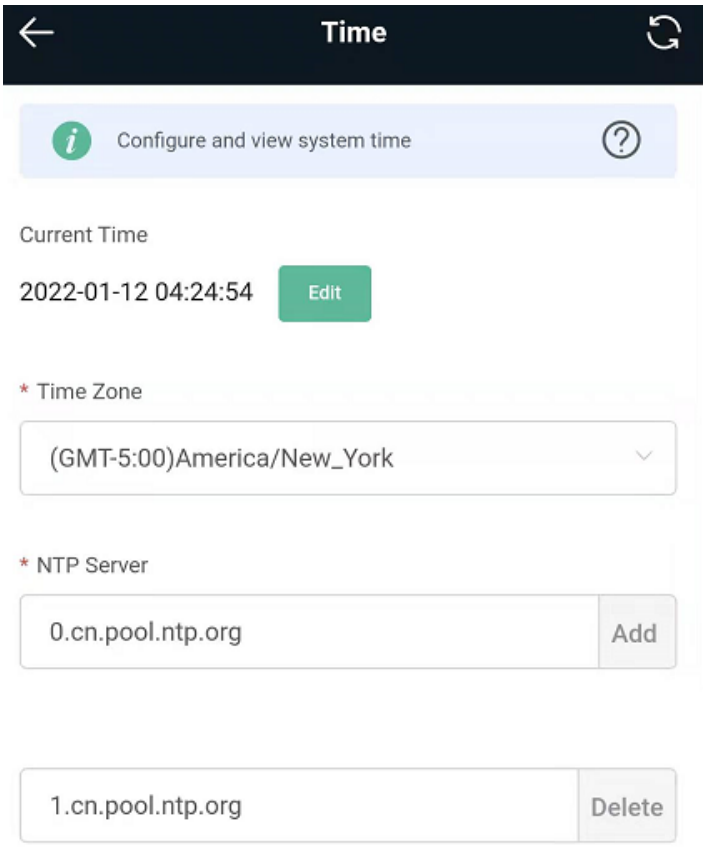


4.4 Configuring System Time

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

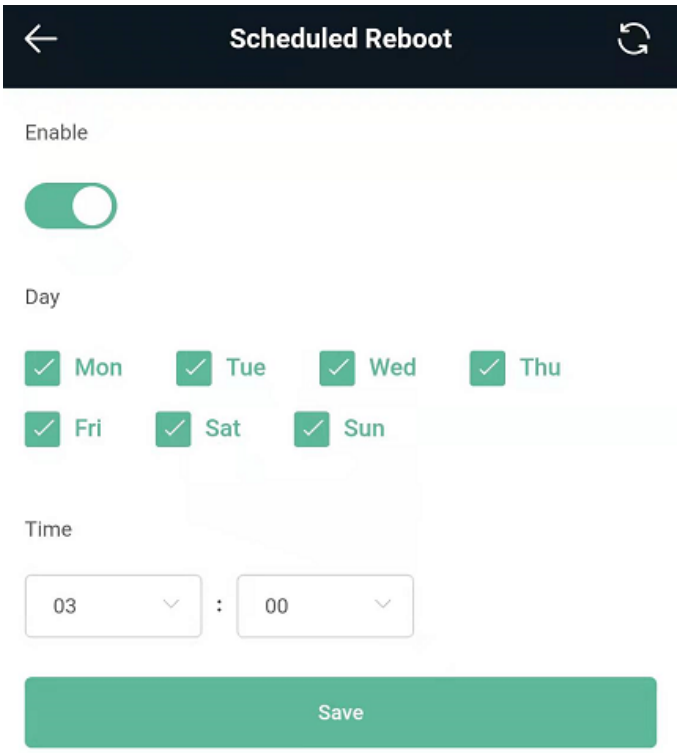
Confirm that the system time is accurate to avoid network interruption caused by device reboot at the wrong time. For details, see 4.4.

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**.

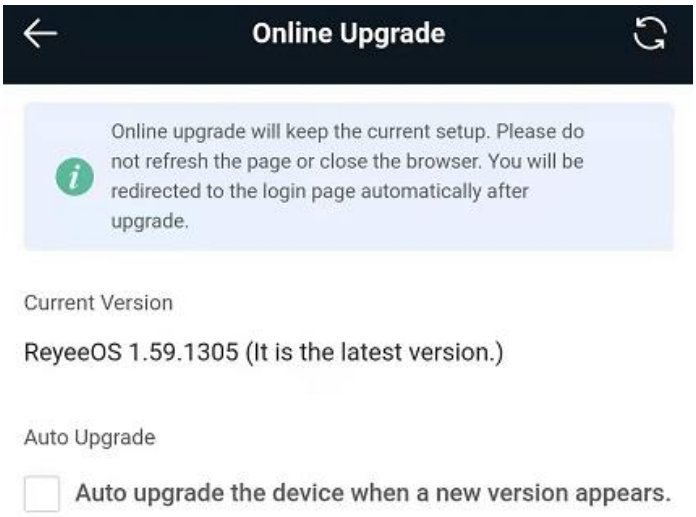
PC View: Choose **More** > **System** > **Upgrade** > **Online Upgrade**.

You can check the current system version. If there are updates, you can click them for an update. The update time can be set. You are advised to set the update time to idle network time, for example, 4:15 a.m.

Note

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

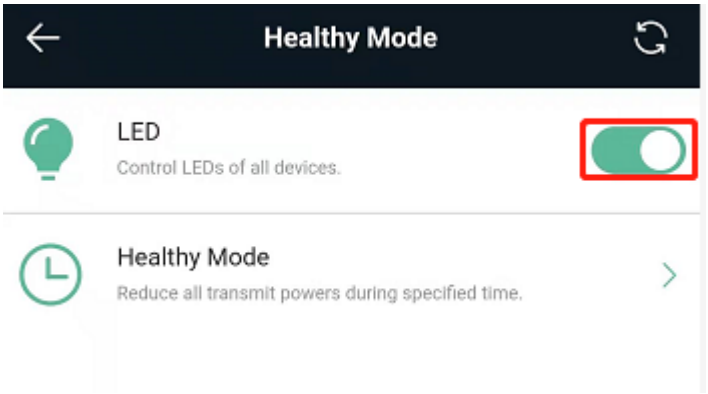
If no version update is detected and online upgrade cannot be performed, check whether the DNS is correctly obtained or go to **More** > **Advanced** > **Local DNS** to set the DNS server for the router.



4.7 Turning On/Off the Indicator

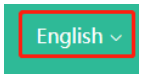
Mobile Phone View: Choose **More** > **Online Upgrade**.

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



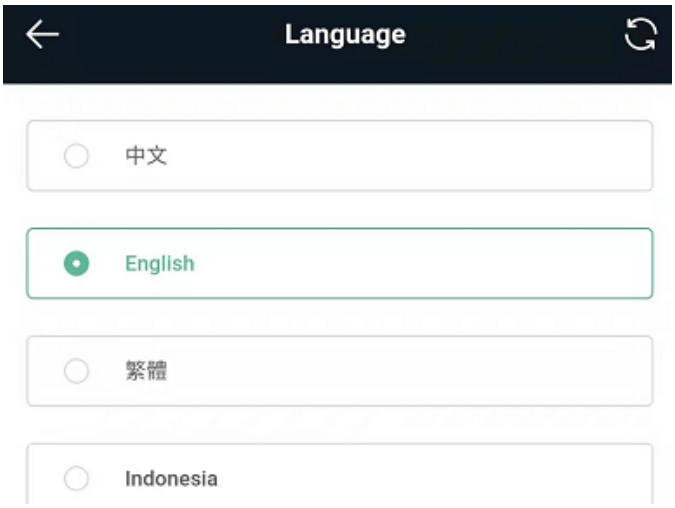
4.8 Switching System Language

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 Network Diagnosis Tools

1. Network Test Tool

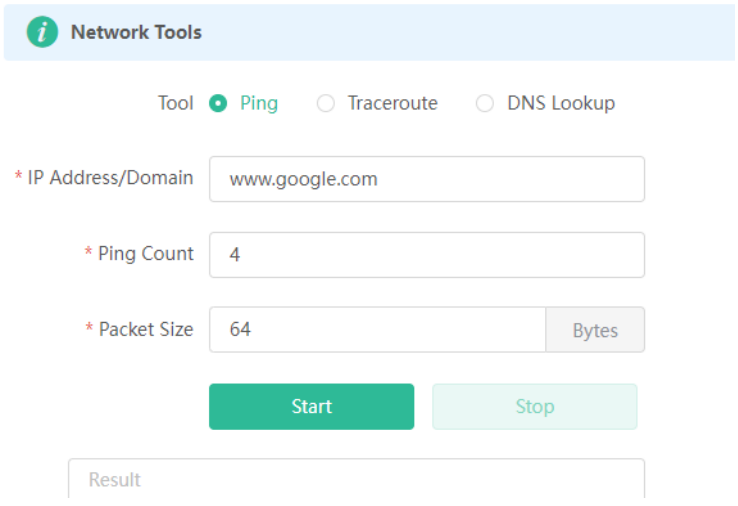
Mobile Phone View: Choose **More** > **System** > **Network Tools**.

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

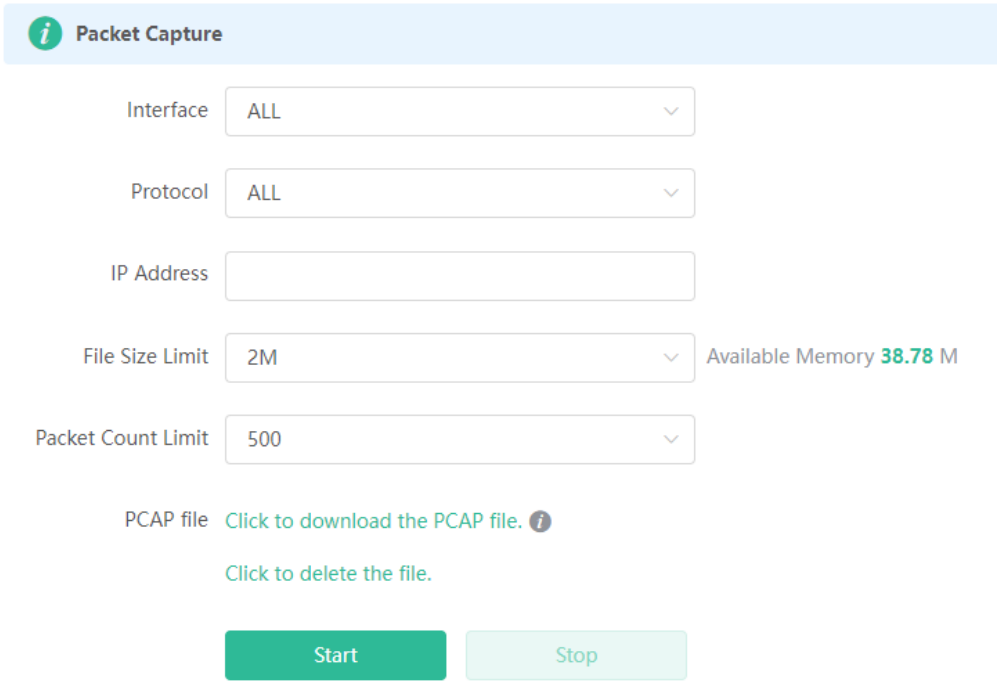
Mobile Phone View: Choose **More** > **Switch to PC view** > **More** > **Diagnostics** > **Packet Capture**.

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.

Note

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



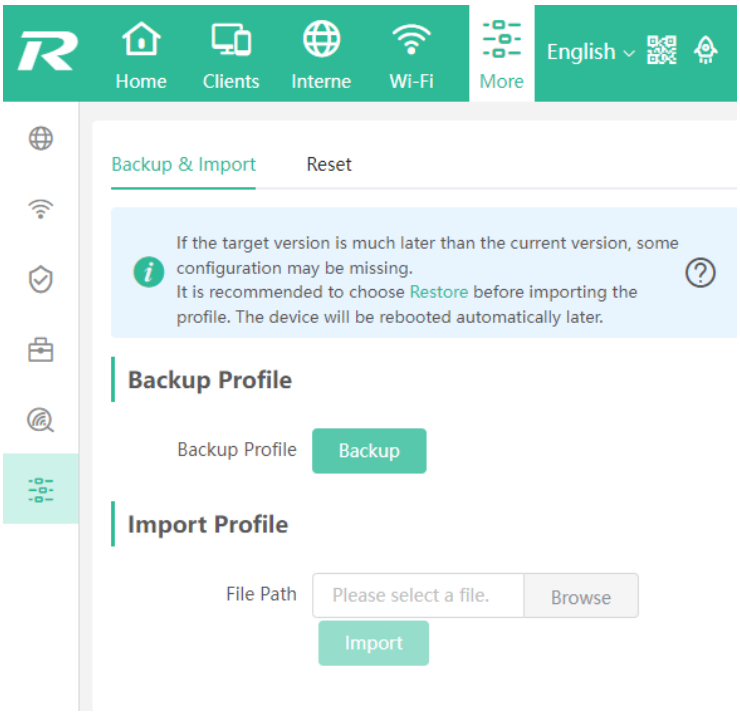
4.10 Configuring Config Backup and Import

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

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

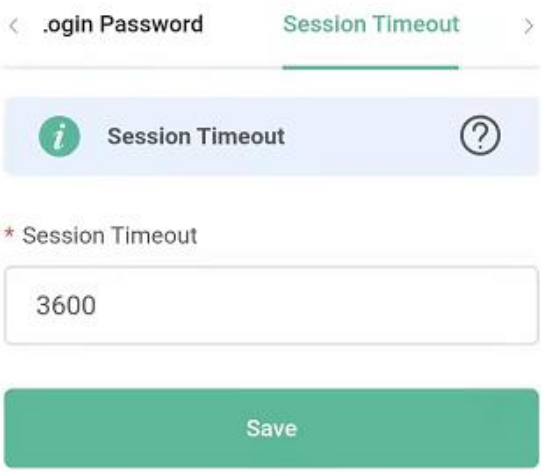
Configure backup: Click **Backup** to download a configuration file locally.

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.



4.11 Configuring Session Timeout Duration

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

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

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.