Ruijie Reyee RG-EW1300G Wi-Fi Router

ReyeeOS 1.308 Configuration Guide

Document Version: V1.0
Date: 2024-09-30

Copyright

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all of the products, services, or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

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

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

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

Preface

Technical Support

- Official website of Ruijie Reyee: https://reyee.ruijie.com
- Technical Support Website: https://reyee.ruijie.com/en-global/support
- Case Portal: https://www.ruijienetworks.com/support/caseportal
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Online Robot/Live Chat: https://reyee.ruijie.com/en-global/rita

Conventions

1. GUI Symbols

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

2. Signs

The signs used in this document are described as follows:

Danger

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

Warning

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

Caution

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

Note

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

Specification

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

3. Note

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

Contents

1 Change Description

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

1.1 ReyeeOS 1.308

1.1.1 Hardware Change

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

Model	Hardware Version
RG-EW1300G	1.xx

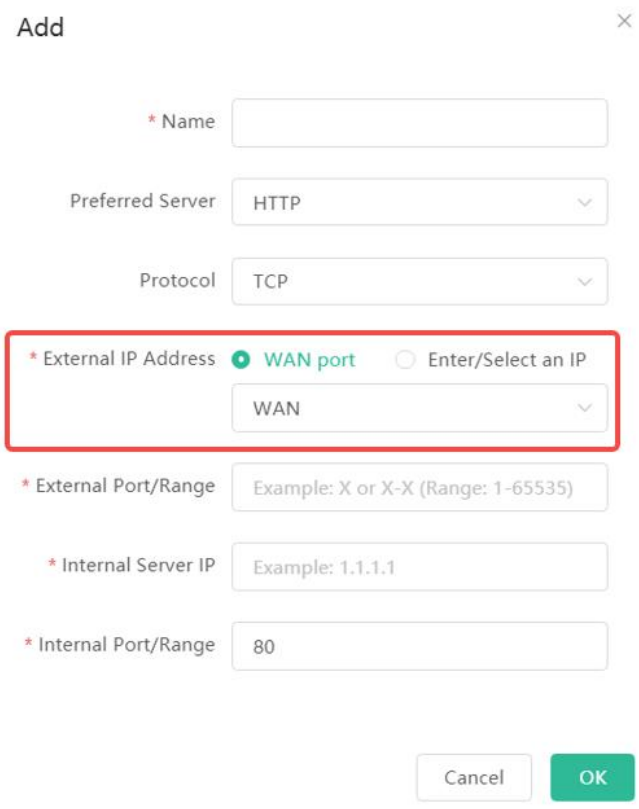
1.1.2 Software Feature Change

1. New Feature — L2TP

L2TP is now supported as an Internet connection type for WAN ports. For details, see Section 2.4.1 Configuring the Internet Connection Type.

2. Changed Feature — Upgraded the Port Mapping

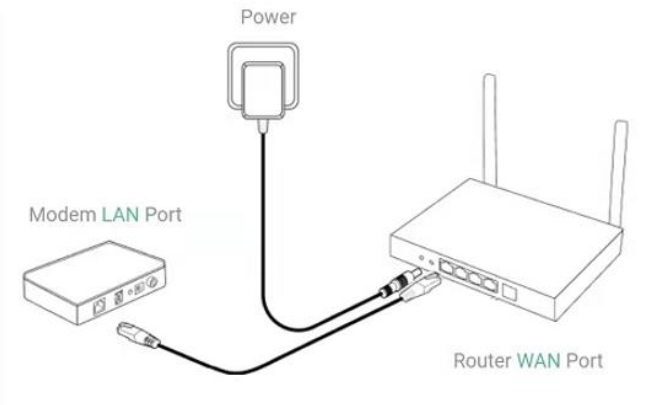
- Before the change: Port mapping can not be configured for a selected WAN interface.
- After the change: Port mapping now can be configured for a selected WAN interface. For details, see Section 6.10 Configuring Port Mapping.



2 Quick Setup (As a Primary Router)

2.1 Getting Started

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



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

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

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

2.2 Connecting to the Router

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

- Wired Connection

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

- Wireless Connection

On a smartphone or laptop, search for the Wi-Fi network **@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.

2.3 Logging In

After a PC is connected to the router in the initial state, the setup page is displayed. If the setup page is not displayed, enter the device IP address in the address bar of the browser to navigate to the login page, and then enter the password to log in.

Table 2-1 Default Configuration

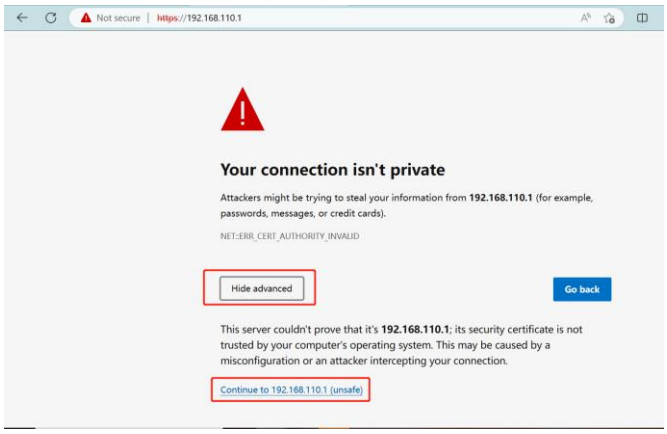
Item	Default Value
Device IP address (http or https)	192.168.110.1
Password	No password is required at your first login. You can configure the router directly.

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

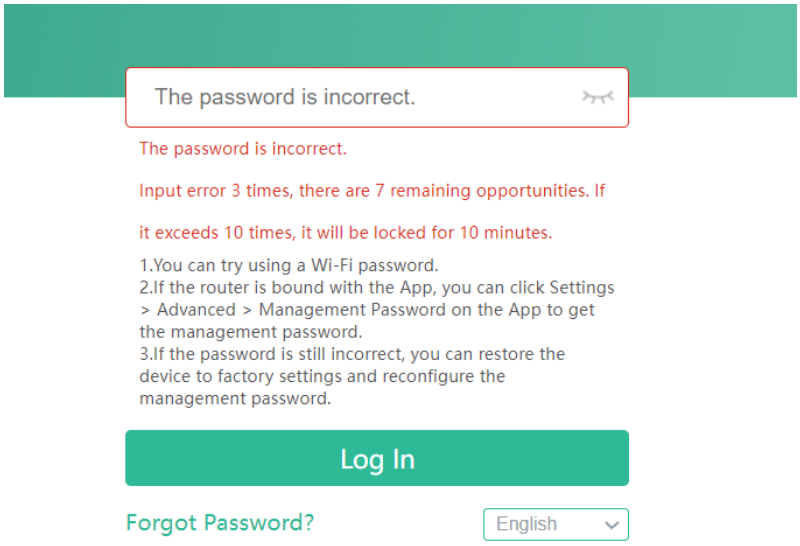
- Supported browsers: Google Chrome, and Internet Explorer 9 to 11. If an unsupported browser is used, you may encounter various errors or problems such as garbled text or formatting errors.
- If you forget the IP address or password, hold down the **Reset** button for more than 10 seconds to restore the router to factory settings. After restoration, you can use the default IP address and password to log in.

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

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



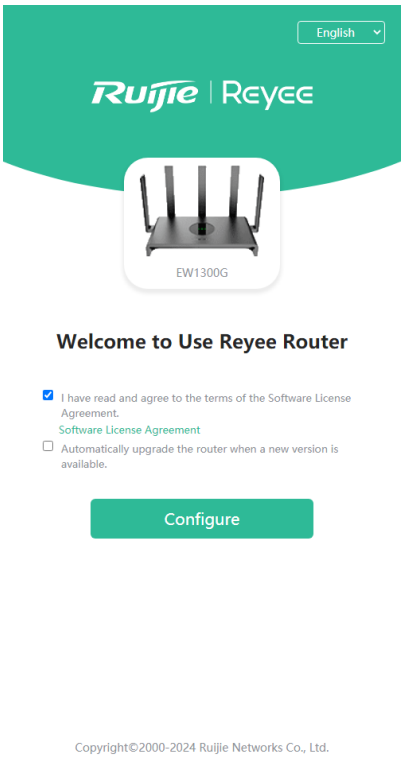
- If you forget your password and enter the incorrect password to log in, you will need to wait for 10 minutes after each 10 unsuccessful attempts.



2.4 Configuration Steps

2.4.1 Configuring the Internet Connection Type

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



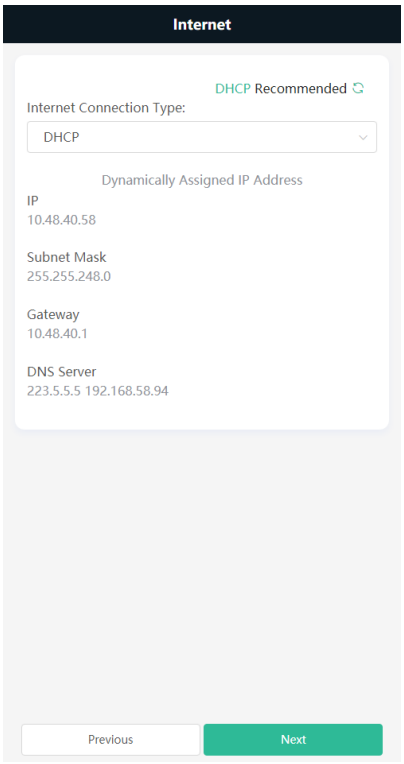
Note

When the system detects that the device's WAN port is connected to an Ethernet cable, and has an active Internet connection, it will skip Internet setup, and will display the Wi-Fi setup page.

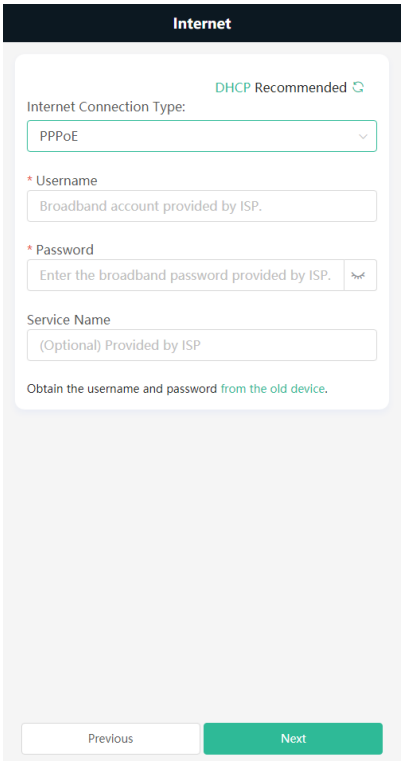
- **DHCP**: The router detects whether it can obtain an IP address from a DHCP server by default. If the router connects to the Internet successfully, you can click **Next** without entering an account.

  Caution

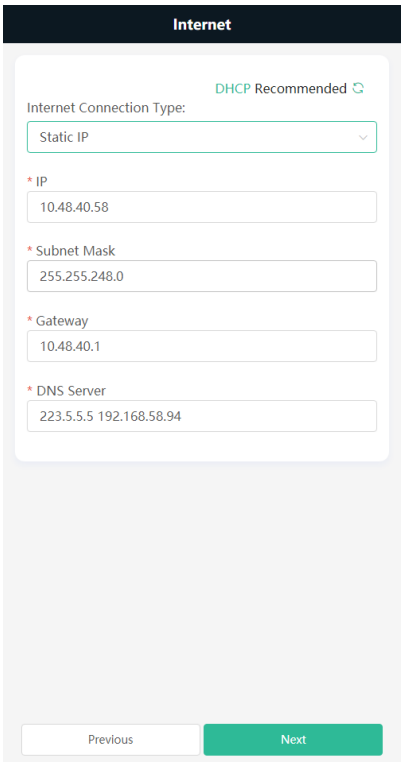
  If the IP address delivered by the primary router is 192.168.110.0, the router will automatically change the IP address of its LAN port to 192.168.111.1 to avoid IP address conflict. Do not change the configuration of the primary router. You can differentiate routers by checking the router model and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



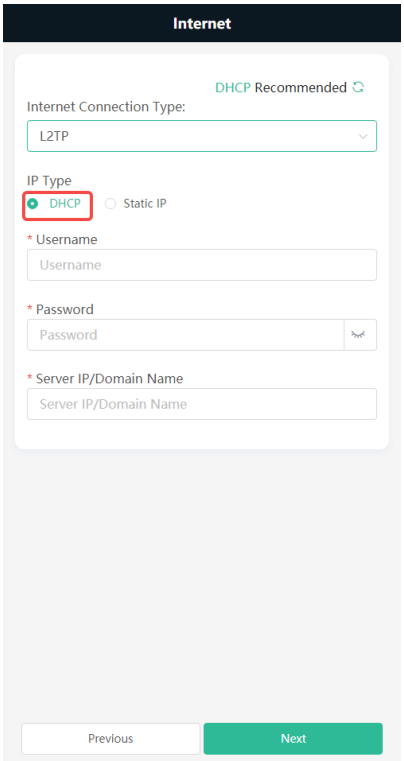
- **PPPoE**: Click **PPPoE**, and enter the username, password. Click **Next**.

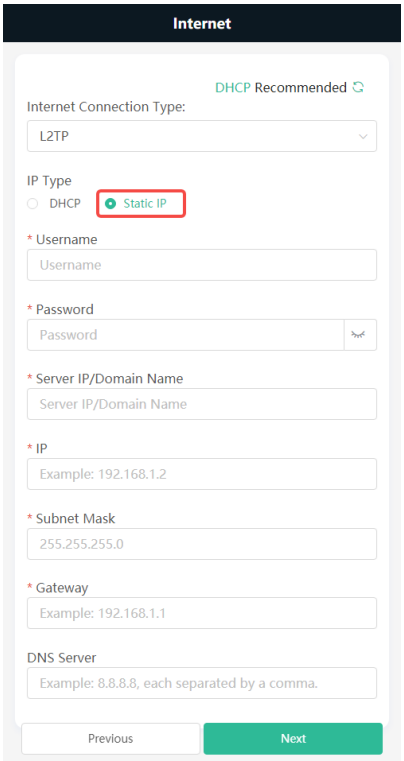


- **Static IP**: Enter the IP address, subnet mask, gateway, and DNS server, and click **Next**.



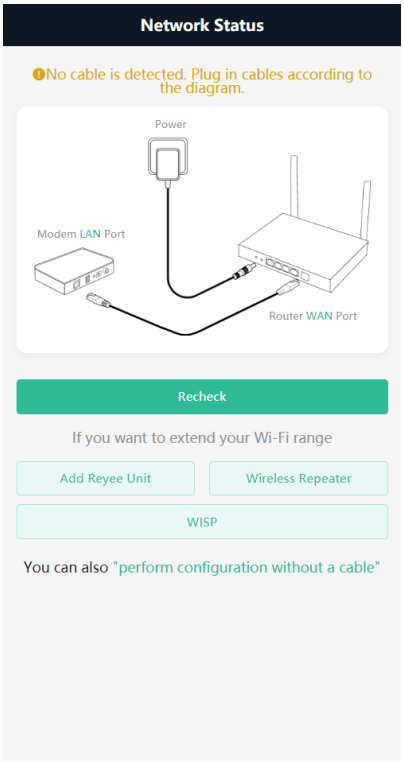
- **L2TP:** Select the IP address allocation type based on the L2TP VPN server information provided by the ISP:
  - DHCP: Enter the username, password, and server IP or domain name provided by the L2TP service provider, and click **Next**.
  - Static IP: In addition to the username, password, and server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





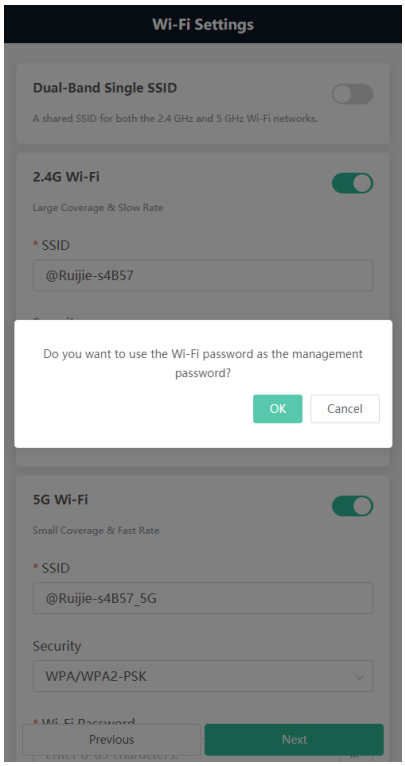
Note

If the Ethernet cable is unplugged, you will be prompted to connect the Ethernet cable first. Click **perform configuration without a cable** below to connect the Ethernet cable. You can connect the Ethernet cable to the router's WAN port as indicated in the diagram, and click **Recheck** to re-check the connection status. Alternatively, you can click **Perform configuration without a cable** to enter the Internet setup page directly.

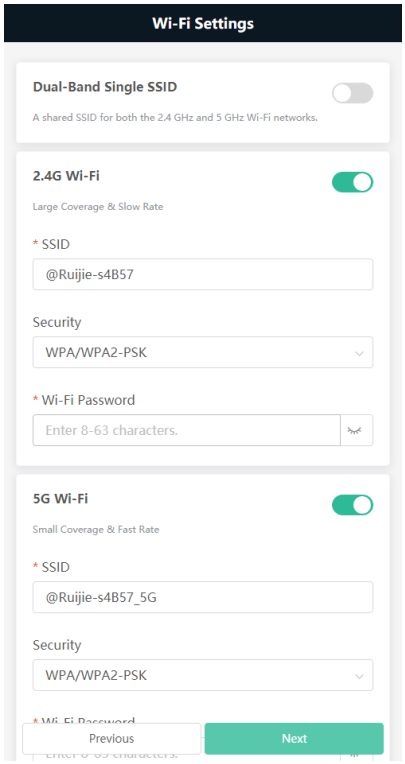


2.4.2 Configuring a Wi-Fi Network

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



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



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

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

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

Note

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

- **Setting the SSID and Wi-Fi password**: The router has no Wi-Fi password by default, indicating that the Wi-Fi network is an open network.

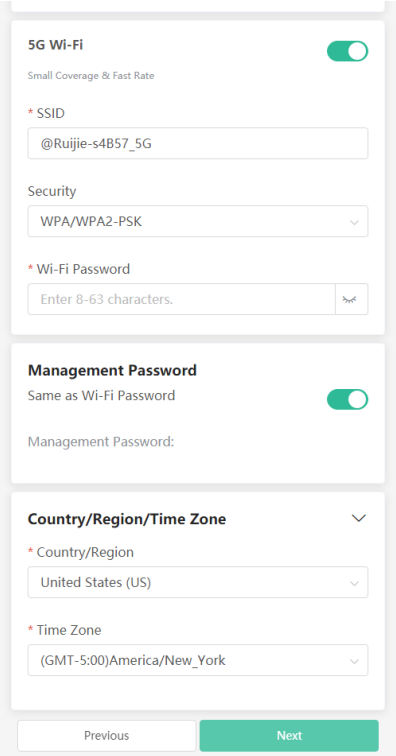
  You are advised to configure a complex password to enhance the network security. The password must be a string of 8 to 63 characters, which can contain uppercase and lowercase letters, digits, and English characters, but cannot contain special characters such as single quotation marks ('), double quotation marks (“), or spaces. The same Wi-Fi password will be used for the 2.4G Wi-Fi, and 5G Wi-Fi.

  Set an SSID for the 2.4G Wi-Fi, and 5G Wi-Fi, respectively. If **Dual-Band Single SSID** is enabled, set only one SSID.

  Note

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

- **Management Password:** Click **Same as Wi-Fi Password** to set the Management Password same as the Wi-Fi Password.
- **Setting the country or region**: The Wi-Fi channel may vary from country to country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.
- **Setting time zone**: Set the system time. The network time server is enabled by default to provide the time service. You are advised to select the actual time zone.



(3) Click **Next**. The Wi-Fi network will be restarted.

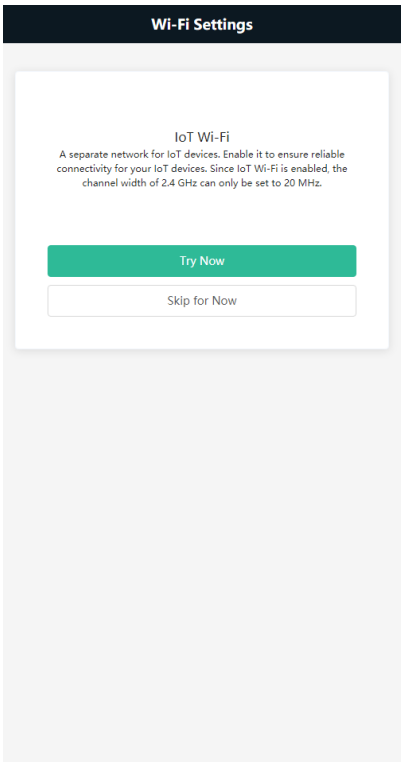
2.4.3 Configuring IoT Wi-Fi

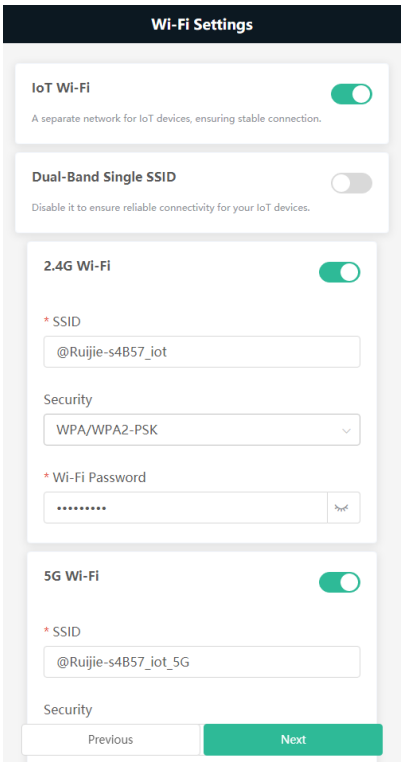
A separate network for IoT devices. Enable it to ensure reliable connectivity for your IoT devices.

Note

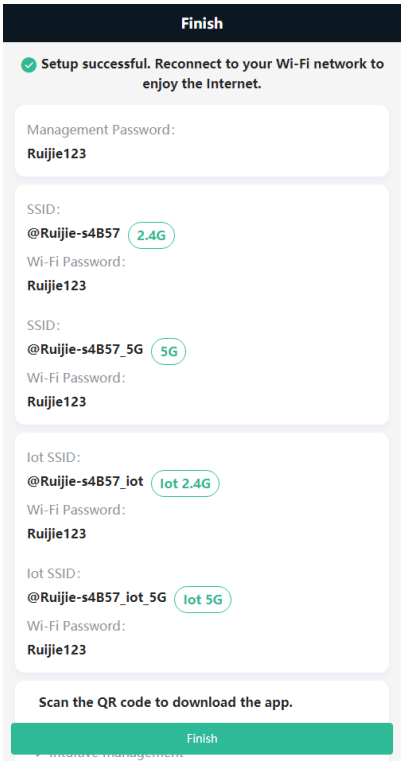
Only smart home devices supporting IEEE 802.11b/g standards can connect to the IoT Wi-Fi.

Dual-Band Single SSID is disabled by default for the IoT Wi-Fi to ensure reliable connectivity for your IoT devices.





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



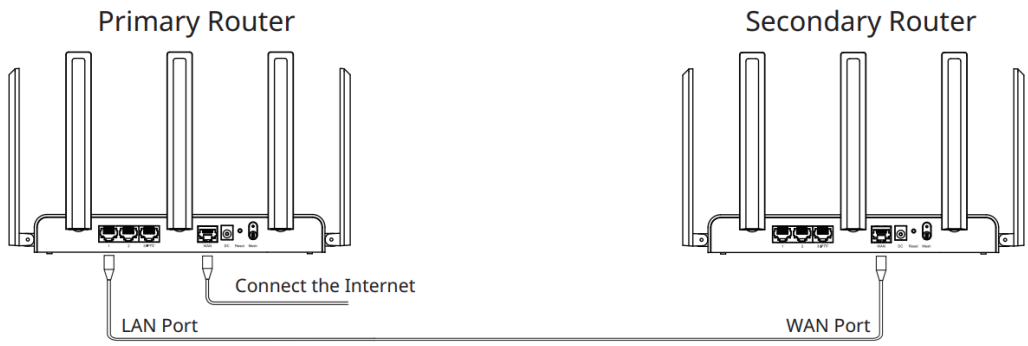
3 Quick Setup (As a Secondary Router)

3.1 Getting Started

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

3.2 Connecting to Primary Router

3.2.1 Wired Connection



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

(2) Power the secondary router on. Wait for the SYS LED on the secondary router to be steady on. Then, press the **Reyee Mesh** button on the primary router to establish wired connection. The default SSID and password of the secondary router are automatically synchronized to be the same as those on the primary router.

Note

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

3.2.2 Wireless Connection

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

1. Wireless Connection by using the Reyee Mesh function

When both the primary router and secondary router are Reyee Home Wi-Fi routers, you can enable the Reyee Mesh feature to extend the Wi-Fi range of the primary router.

(1) Place the second router within 2 meters of the primary router, power it on and wait for it to start up.

(2) Press the **Reyee Mesh** button on the primary router to complete the wireless Reyee Mesh networking in 2 minutes. The SSID and password of the secondary router are automatically synchronized with those of the primary router.

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

Caution

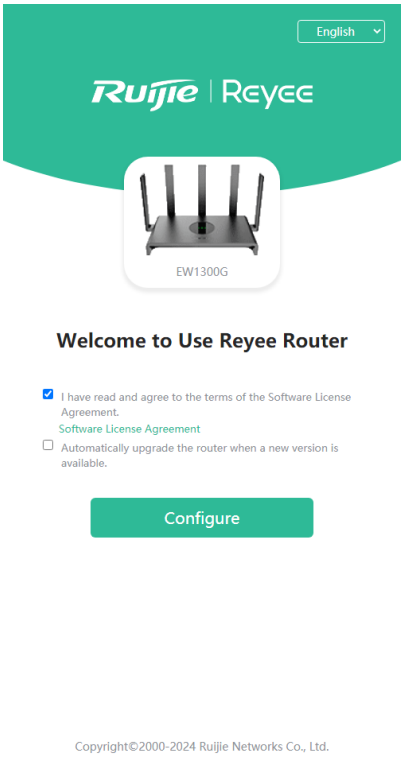
No Ethernet cable is required in the wireless repeater mode. The wireless network stability can be affected by many factors. Therefore, the wired connection is recommended.

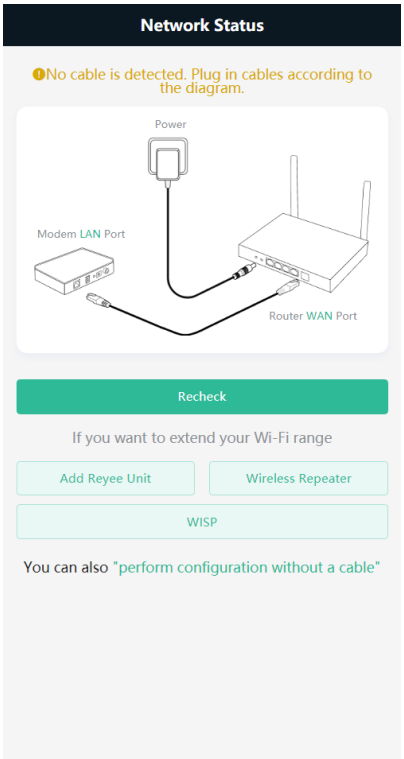
2. Wireless Connection by Web configuration

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

Connect the router to a power source and log in to the web interface. For details, see 2.2 Connecting to the Router and 2.3 Logging In.

Click **Configure**.



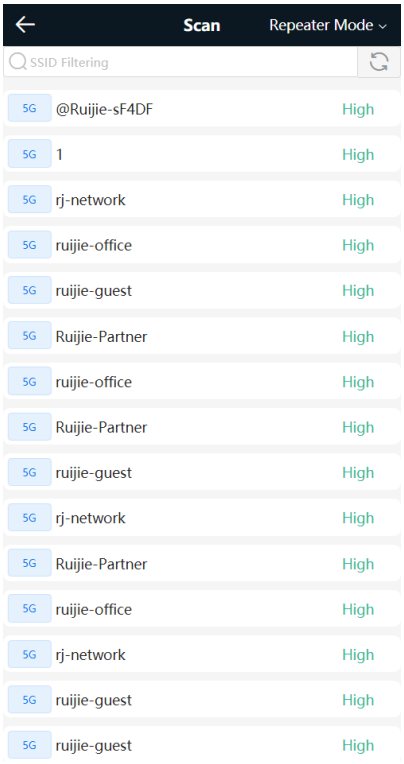


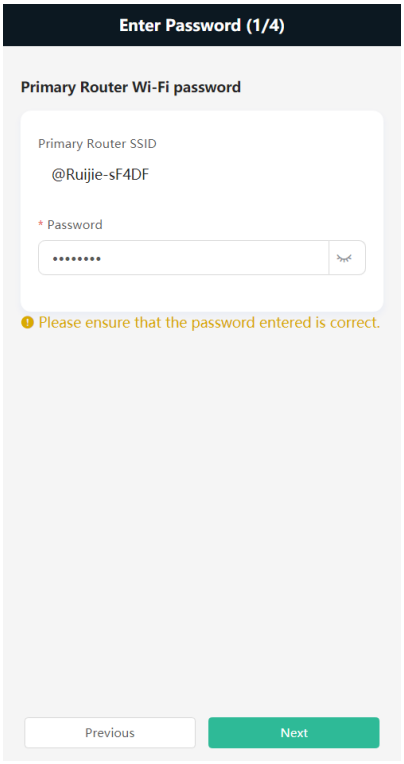
- Wireless Repeater

(1) Select Wireless Repeater.

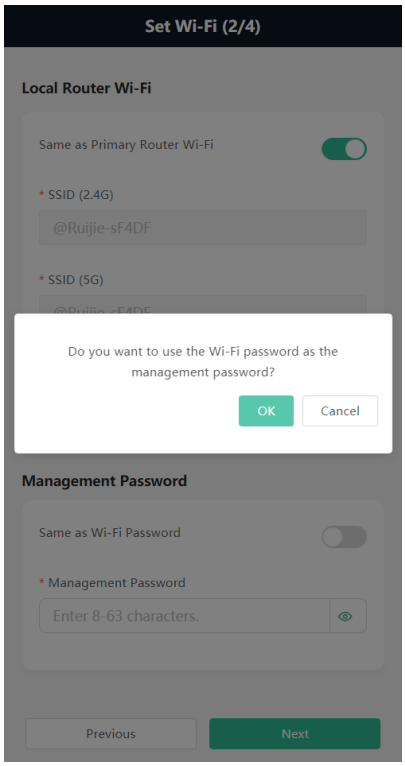
Wireless repeater mode: Click **Wireless Repeater**, and the SSID of the primary router, and enter the Wi-Fi password to connect to the primary router.

- 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.



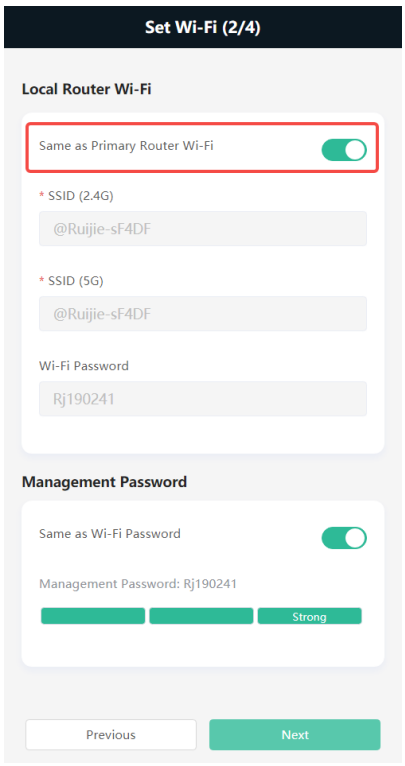


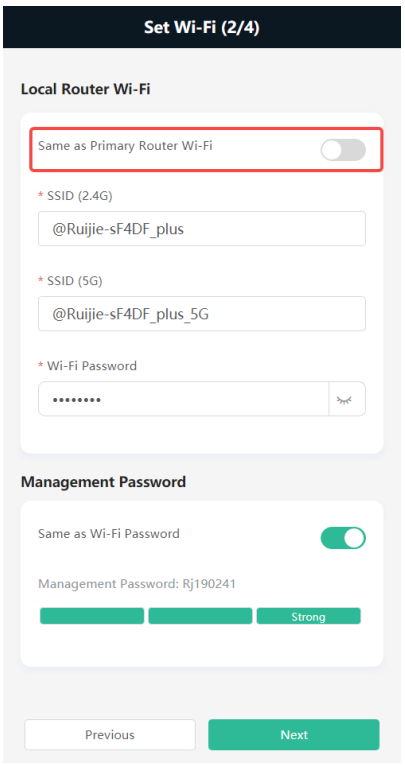
(2) Click **Next**. Click **OK** to set the management password same as the Wi-Fi Password. Click **Cancel** to set a new management password on the **Wi-Fi Settings** page.



(3) On the **Set Wi-Fi** page that opens, set the SSID and management password for the extender.

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





Note

Click **Same as Wi-Fi Password** to set the Management Password same as the Wi-Fi Password.

(4) Configuring IoT Wi-Fi

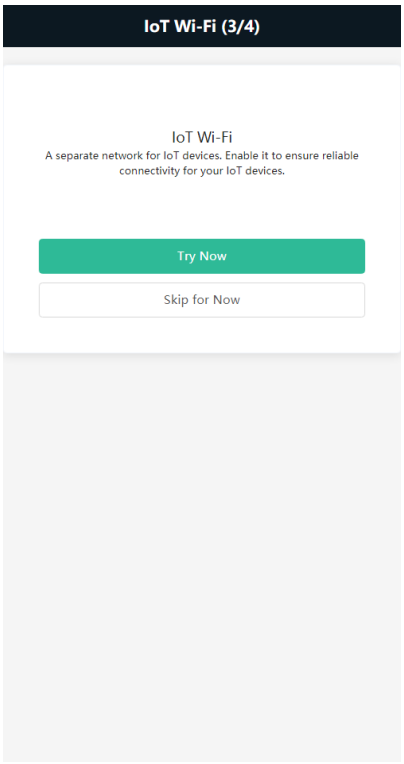
A separate network for IoT devices. Enable it to ensure reliable connectivity for your IoT devices.

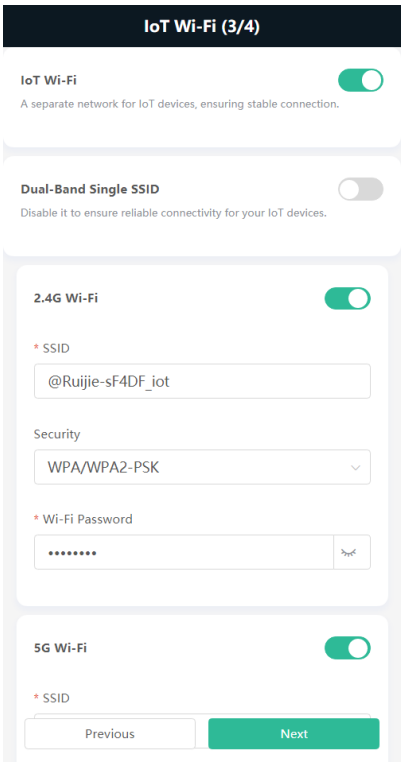
Note

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

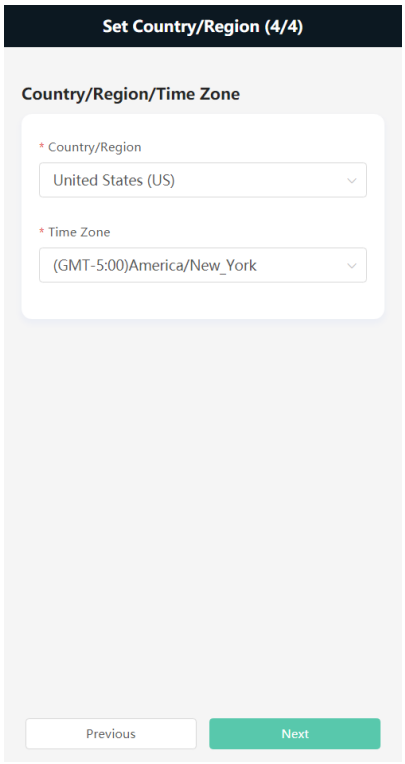
Dual-Band Single SSID is enabled by default for the IoT Wi-Fi, and the 2.4G SSID will be consistent with the 5G SSID. When this function is disabled, you can disable 2.4G or 5G Wi-Fi networks separately, and set different passwords for 2.4G and 5G SSIDs.

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

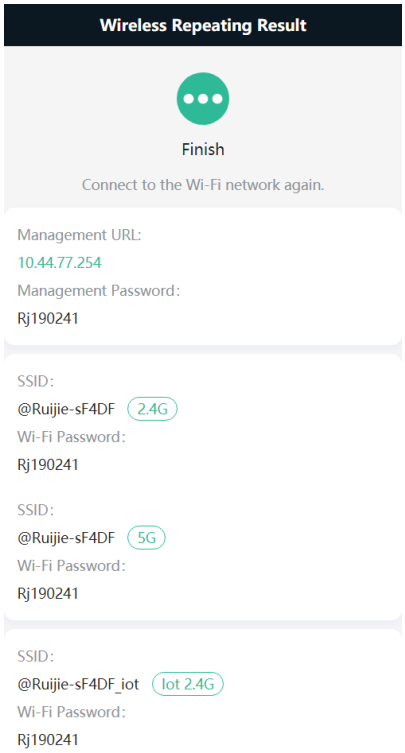




(5) Choose the **Country/Region** and **Time Zone.** You are advised to choose the correct country or region, as well as the appropriate time zone.



(6) Click **Next**.



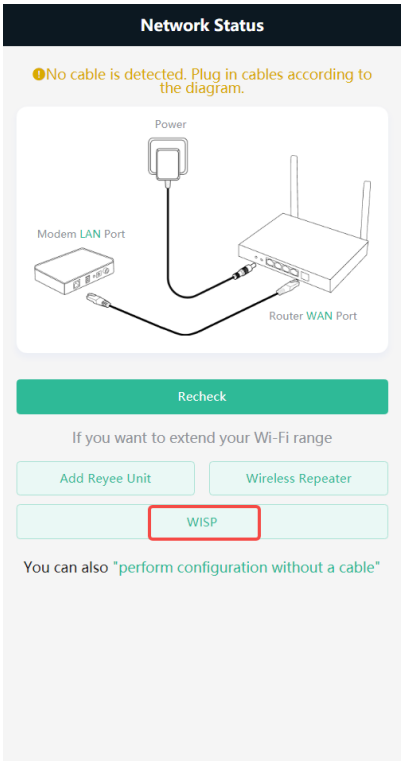
- **WISP**

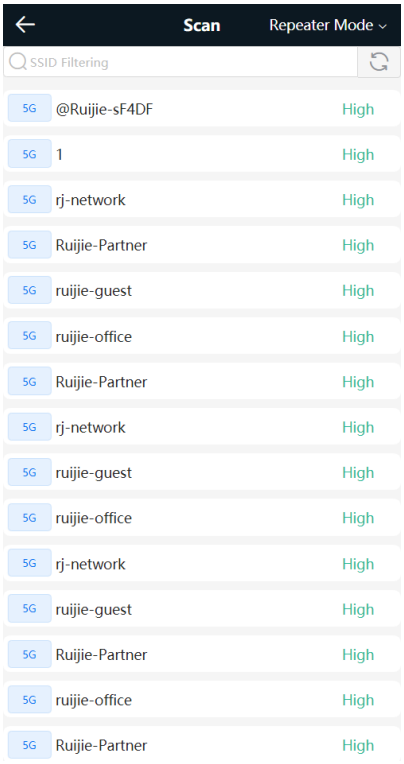
  In this mode, the device enables multiple users to share Internet connection from WISP. The LAN port devices share the same IP from WISP through Wireless port. While connecting to WISP, the Wireless port works as a WAN port. The Ethernet port acts as a LAN port

Note

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

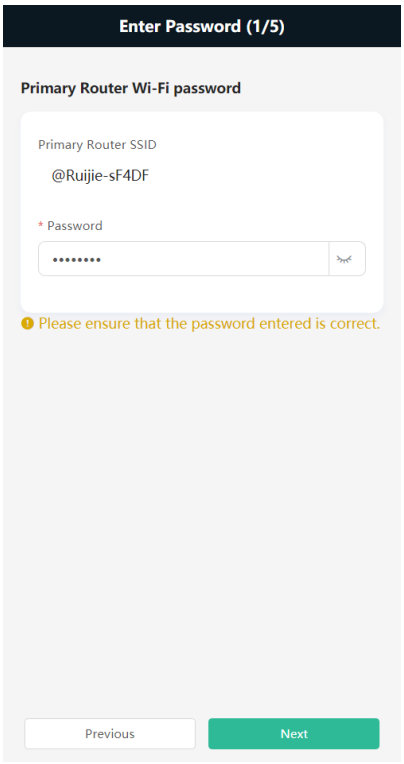
(1) Click **WISP**. Select the Wi-Fi of the primary router.

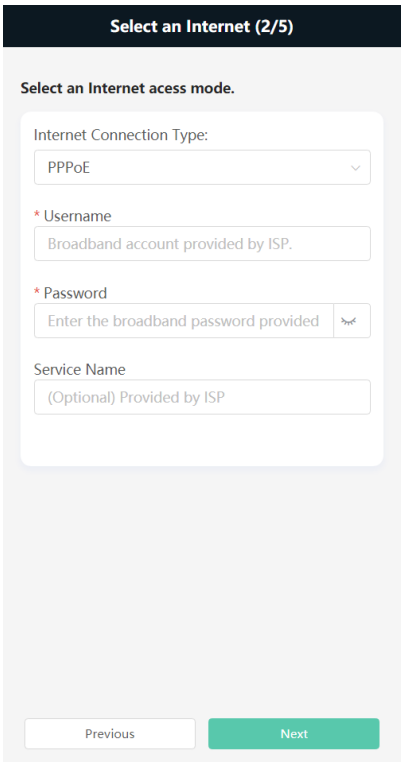


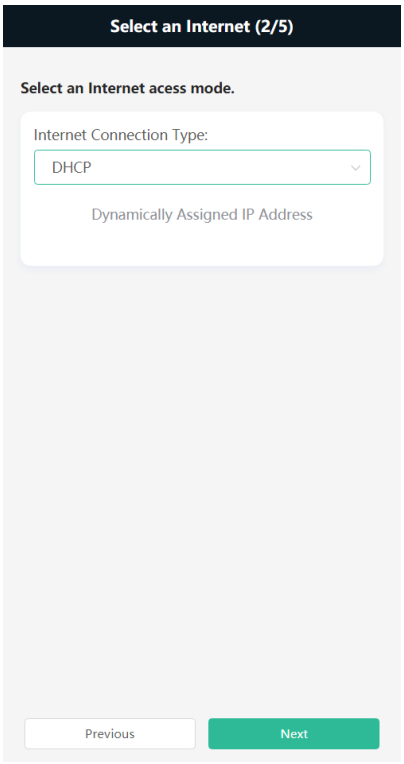


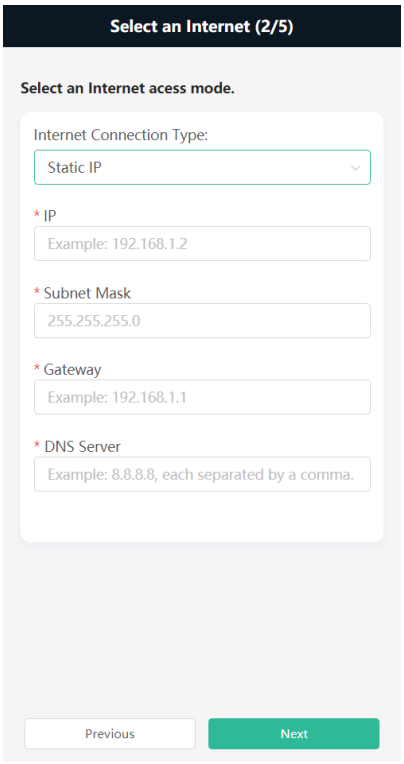
(2) Enter the password of the primary router Wi-Fi, and select an Internet access mode. For details, see 2.4.1 Configuring the Internet Connection Type.

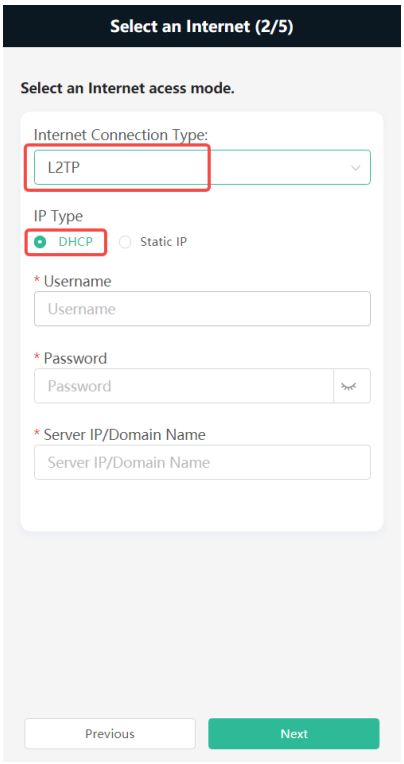
- Select DHCP and the extender will automatically obtain an IP address.
- If the primary router cannot assign IP addresses, select **Static IP**.
- In the PPPoE mode, a username, a password, and possibly a service name are needed.
- If the Internet connection type provided by the ISP is L2TP, then select **L2TP**. Select the IP address allocation type based on the actual situation, and enter the username, password, and other information.

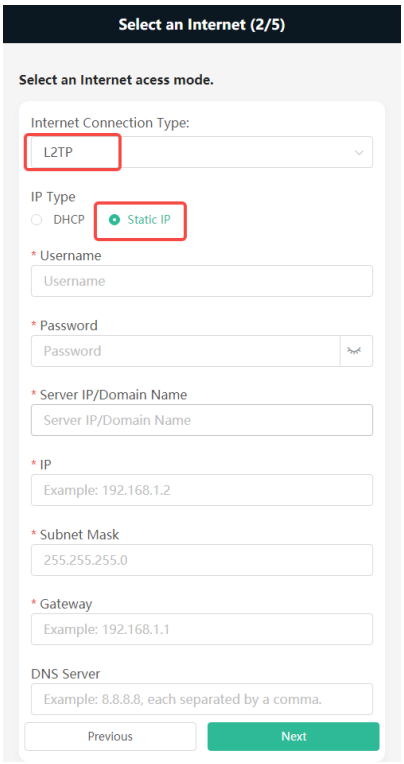

Enter Password (1/5)
Primary Router Wi-Fi password
Primary Router SSID
@Ruijie-sF4DF
* Password
Please ensure that the password entered is correct.
Previous
Next


Select an Internet (2/5)
Select an Internet acess mode.
Internet Connection Type:
PPPoE
* Username
Broadband account provided by ISP.
* Password
Enter the broadband password provided
Service Name
(Optional) Provided by ISP
Previous
Next

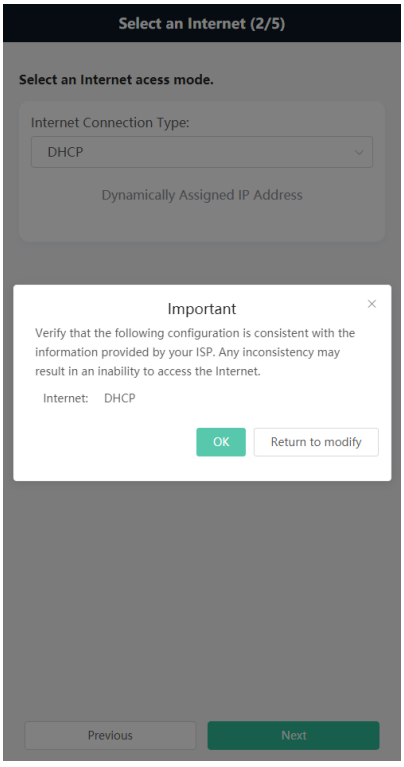

Select an Internet (2/5)
Select an Internet acess mode.
Internet Connection Type:
DHCP
Dynamically Assigned IP Address
Previous
Next


Select an Internet (2/5)
Select an Internet acess mode.
Internet Connection Type:
Static IP
* IP
Example: 192.168.1.2
* Subnet Mask
255.255.255.0
* Gateway
Example: 192.168.1.1
* DNS Server
Example: 8.8.8.8, each separated by a comma.
Previous
Next



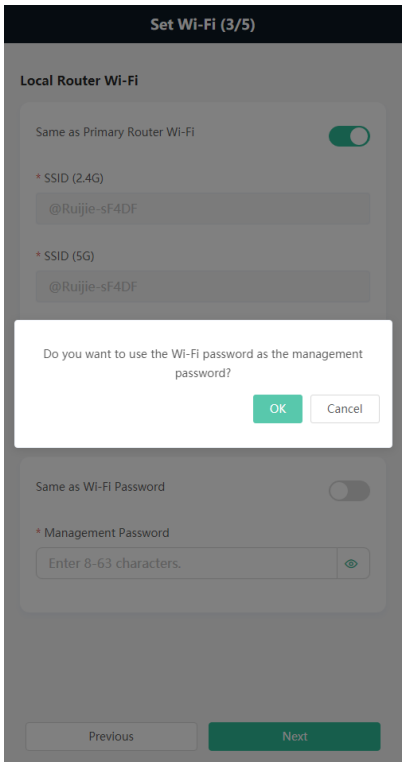


Click **Next**. Verify the Internet settings. Then, click **OK**.



(3) Click **Next**. On the **Set Wi-Fi** page that opens, enter the Wi-Fi SSID and password and management password for the extender.

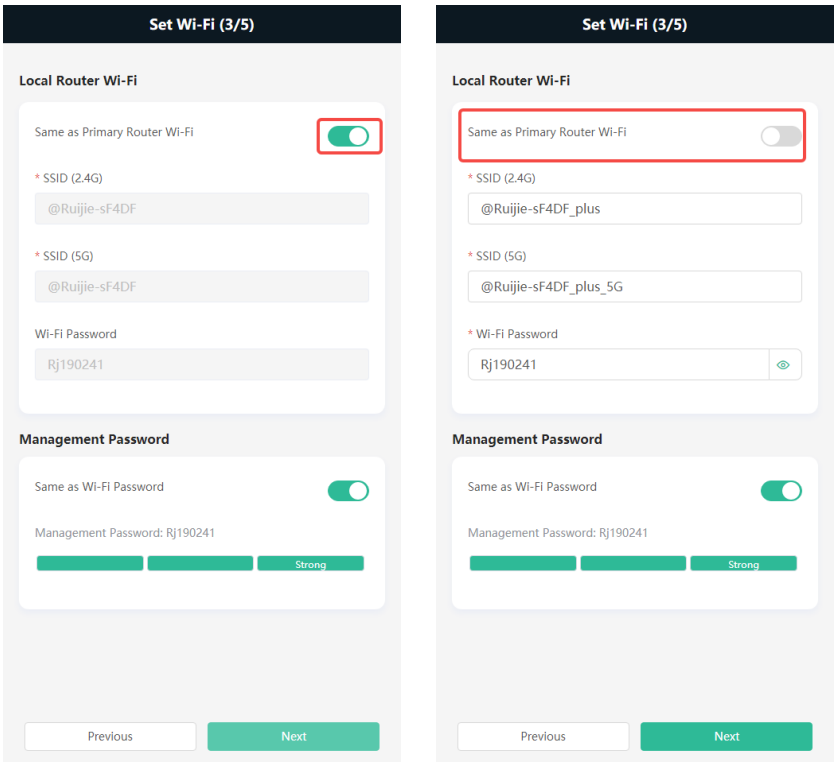
Click **OK** to set the management password same as the Wi-Fi Password. Click **Cancel** to set a new management password on the **Wi-Fi Settings** page.



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

Note

Click **Same as Wi-Fi Password** to set the Management Password same as the Wi-Fi Password.



(4) Configuring IoT Wi-Fi

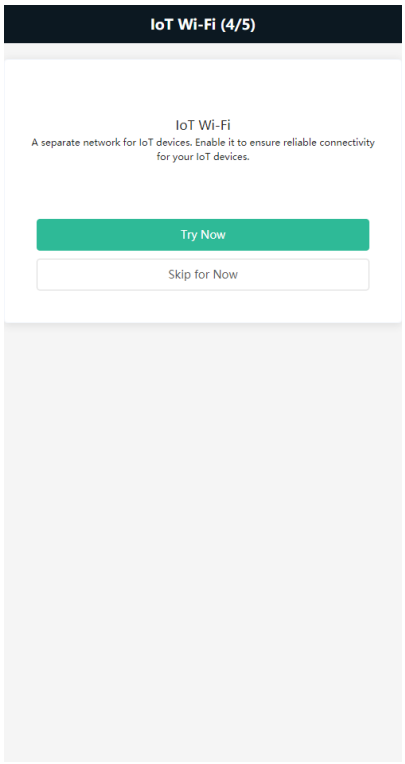
A separate network for IoT devices. Enable it to ensure reliable connectivity for your IoT devices.

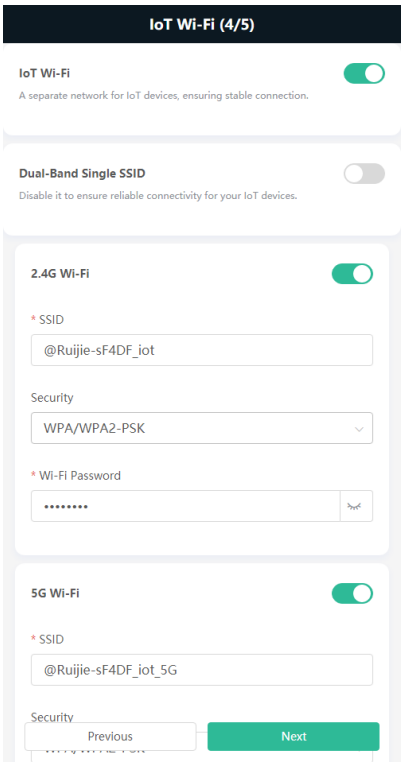
Note

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

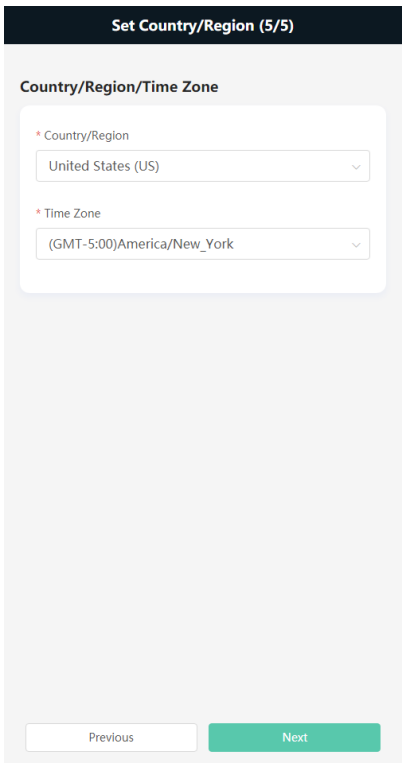
Dual-Band Single SSID is enabled by default for the IoT Wi-Fi, and the 2.4G SSID will be consistent with the 5G SSID. When this function is disabled, you can disable 2.4G or 5G Wi-Fi networks separately, and set different passwords for 2.4G and 5G SSIDs.

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

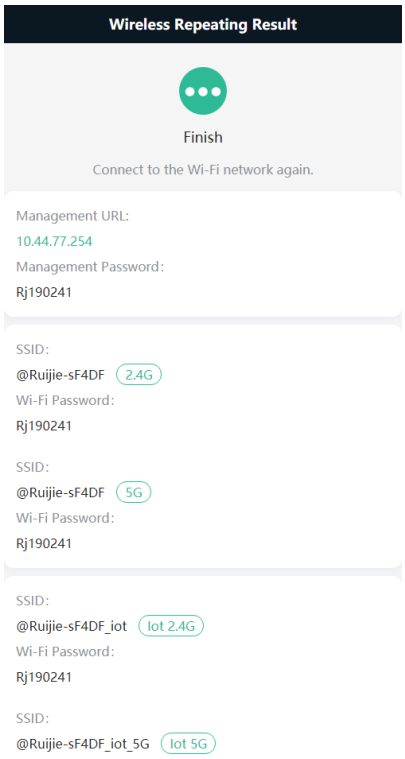




(5) Choose the **Country/Region** and **Time Zone.** You are advised to choose the correct country or region, as well as the appropriate time zone.



(6) Click **Next** to complete the configuration.



3.3 Verification and Testing

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

3.4 Manage the Device after Successful Setup

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

1. Connecting the Device

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

Note

If the router is in WISP mode, you are advised to connect your PC to the router via a wired connection.

- **Wired Connection**

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

- **Wireless Connection**

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

2. Logging In to the Web Interface

- Login using the default IP address

  Enter the default IP address (192.168.110.1) or https://192.168.110.1 in the address bar of your browser, and press **Enter**. The login page is displayed. For details, see 2.3 Logging In.

- Login using an obtained IP address

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

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

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

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

4 Wi-Fi Network Settings

4.1 Changing the SSID and Password

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

Click the target Wi-Fi network.

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

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

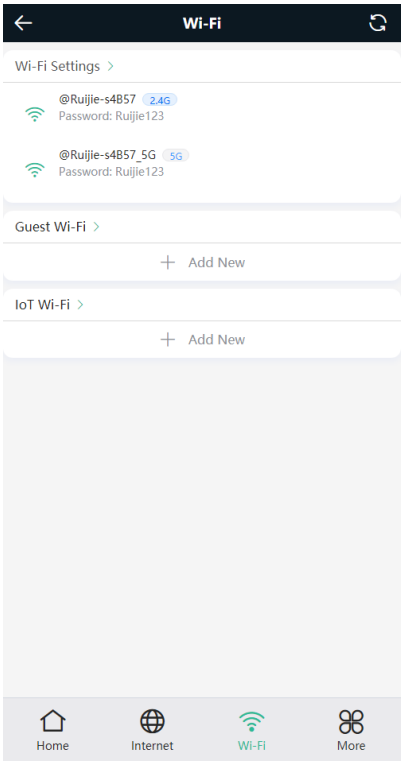
Caution

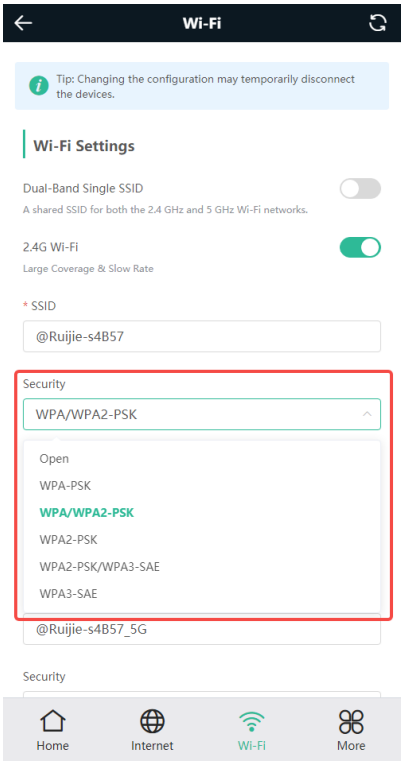
After the configuration is saved, all online clients will be disconnected from the Wi-Fi network. Users need to enter the new password to connect to the Wi-Fi network.

You can set the encryption type and Wi-Fi password for different types of Wi-Fi networks such as 2.4G Wi-Fi, 5G Wi-Fi, Guest Wi-Fi, and IoT Wi Fi.

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

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





4.2 Enabling Band Steering

Caution

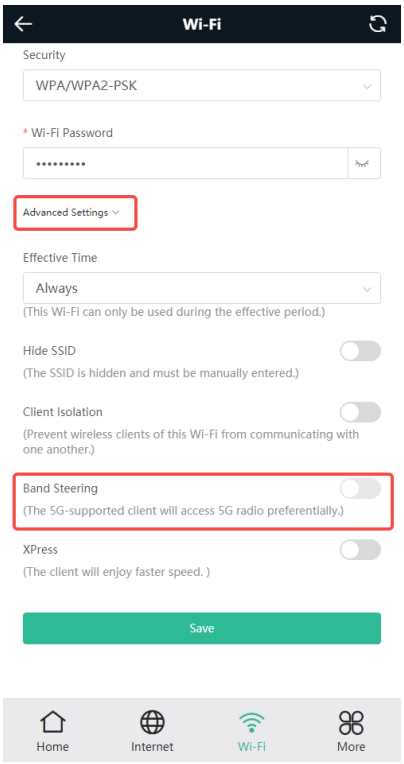
Before enabling the band steering, you must enable the dual-band integration. Because the client can automatically choose to steer to either band only when the 2.4G and 5G bands use the same SSID.

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

Click the target Wi-Fi network.

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

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



4.3 Hiding the SSID

4.3.1 Overview

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

4.3.2 Getting Started

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

4.3.3 Configuration Steps

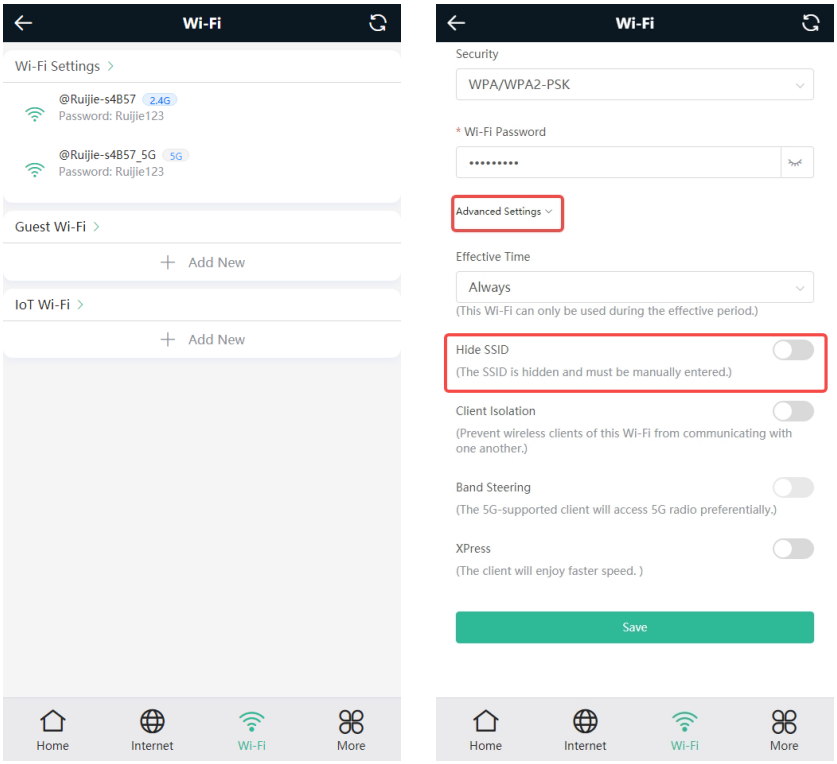
Smartphone View: **Wi-Fi** > **Wi-Fi Settings**

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

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

Caution

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



Note

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

4.4 Adding Wi-Fi Networks

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

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

Click the target Wi-Fi network.

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

4.4.1 Adding Other Types of Wi-Fi Networks

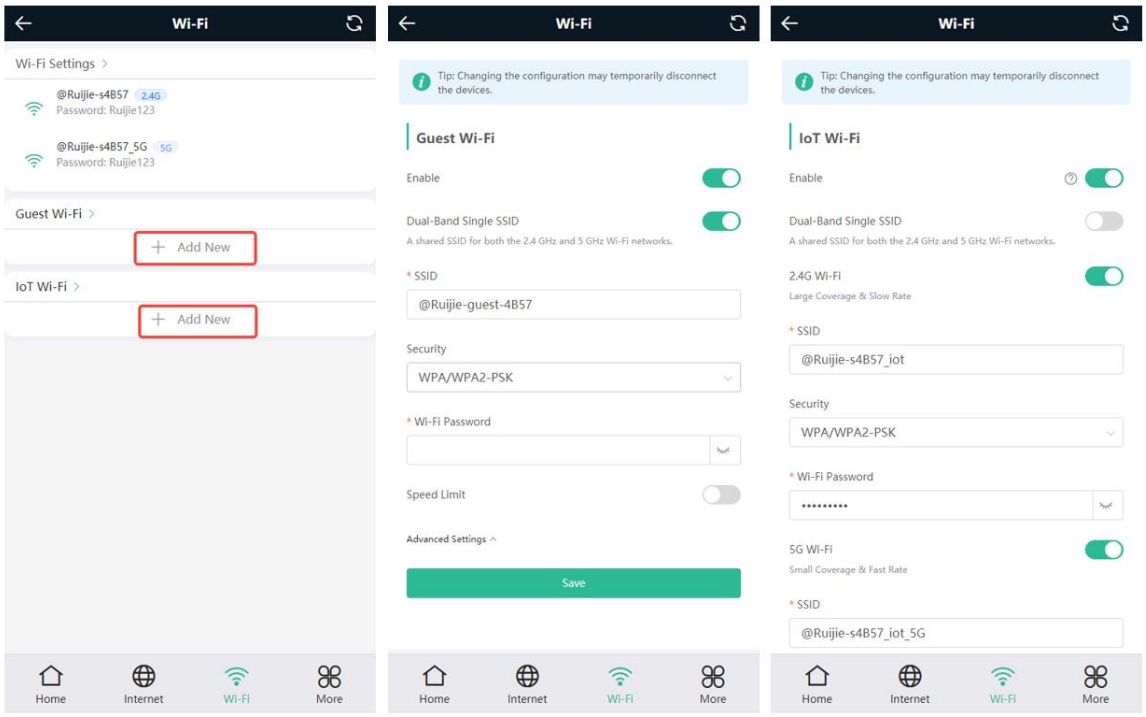
1. Overview

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

- **Primary Wi-Fi**: The primary Wi-Fi network is listed in the first line of the page and is enabled by default.
- **Guest Wi-Fi**: This Wi-Fi network is provided for guests and is disabled by default. It supports user isolation, that is, access users are isolated from each other. They can only access the Internet via Wi-Fi, but cannot access each other, improving security.
- **IoT Wi-Fi**: The IoT Wi-Fi network is disabled by default. Smart clients can connect to the IoT Wi-Fi network for long. You can set an effective time for the IoT Wi-Fi network which will only be enabled during the set effective time.

2. Configuration Steps

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



- **Dual-Band Single SSID:** After this function is enabled, the 2.4G SSID will be consistent with the 5G SSID. For the host Wi-Fi network, when this function is disabled, you can disable 2.4G or 5G Wi-Fi networks separately, and set different passwords for 2.4G and 5G SSIDs.
- **Effective Time:** For the **Primary Wi-Fi** network and **IoT Wi-Fi**, options include Always, Weekdays, Weekends and Custom. When Custom is selected, you can select a custom effective time. This Wi-Fi can only be used during the effective period.

  The **Guest Wi-Fi** network can be turned off as scheduled. Options include Never Disable, Disable 1 Hour Later, Disable 6 Hours Later, Disable 12 Hours later and Other Time. When the time expires, the guest network is off.
- **Client Isolation/Guest Isolation**: This feature is supported by **Wi-Fi Settings**, **Guest Wi-Fi** and **IoT Wi-Fi**.

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

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

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

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

- **XPress**: After this function is enabled, the device sends game packets preferentially, providing more stable wireless network for games.

4.5 Configuring the Wi-Fi Blocklist or Allowlist

4.5.1 Overview

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

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

Note

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

4.5.2 Configuration Steps

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

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

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

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

In the pop-up dialog box, enter the MAC address and remarks of the client to be blocklisted.

Select a client, and it will be added to the blocklist automatically. Click **OK** to save the configuration. The client will be disconnected and prevented from connecting to the Wi-Fi network.

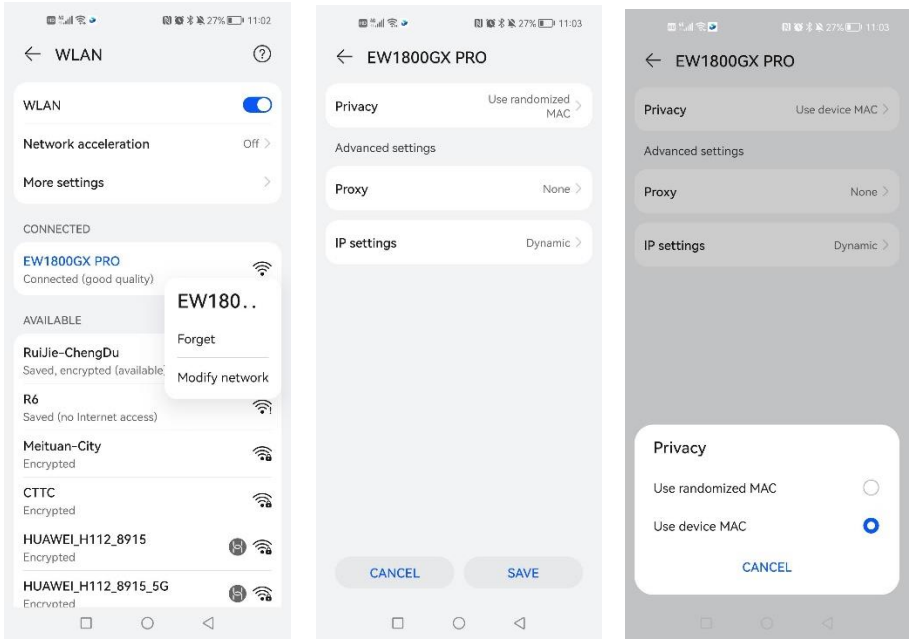
Caution

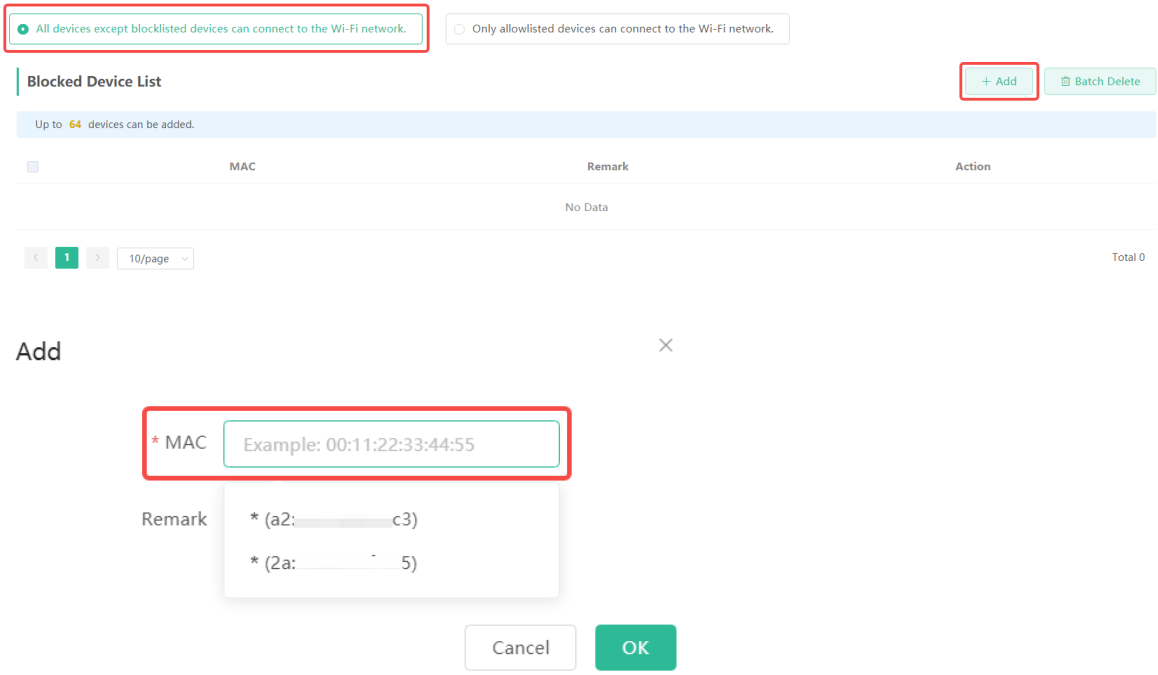
This configuration prevents some devices from connecting to the Wi-Fi network. Exercise caution when performing this operation.

Note

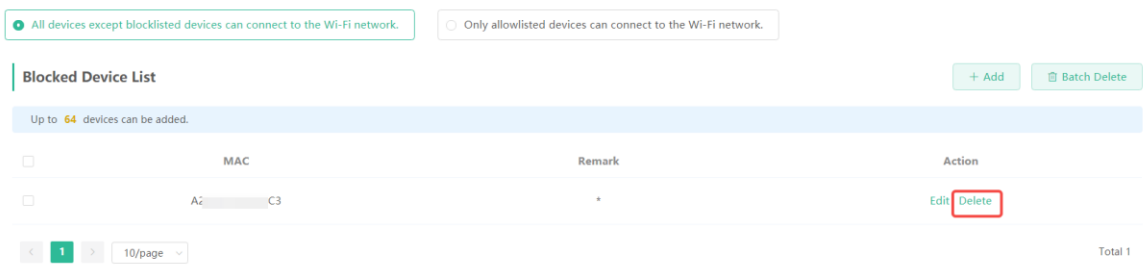
To use this function, you must disable the randomized MAC address on the mobile device. The following example shows how to disable the randomized MAC address on an Android device.

Open the WLAN page of your device, press and hold the SSID broadcast by the router, and then choose **Modify network** > **Privacy** > **Use device MAC** to complete the configuration.





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



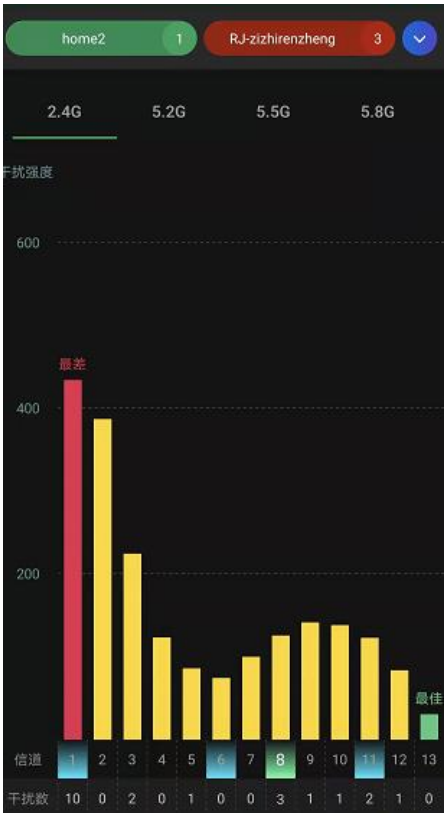
4.6 Optimizing the Wi-Fi Network

4.6.1 Overview

The device detects the surrounding wireless environment and selects the appropriate configuration upon power-on. However, network stalling caused by wireless environment changes cannot be avoided. Restarting the router is a convenient and effective method to cope with network stalling. The router supports scheduled restart. For details, see 7.6 Configuring Scheduled Reboot. You can also analyze the wireless environment around the router and select appropriate parameters.

4.6.2 Getting Started

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



4.6.3 Configuration Steps

- Optimizing the radio channel

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

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

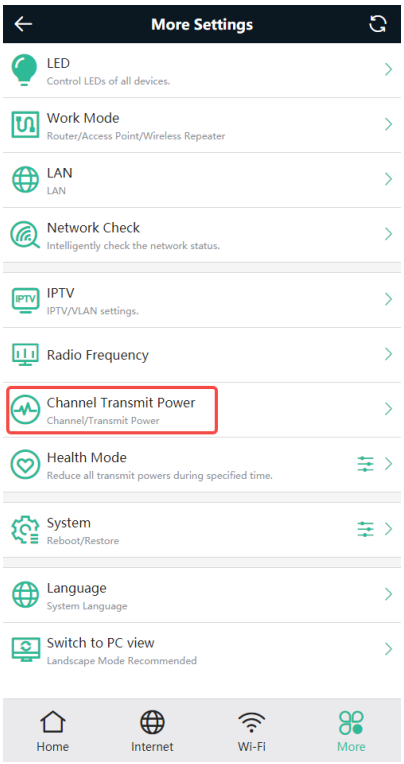
Choose the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. Excess clients connected to a channel can bring stronger wireless interference.

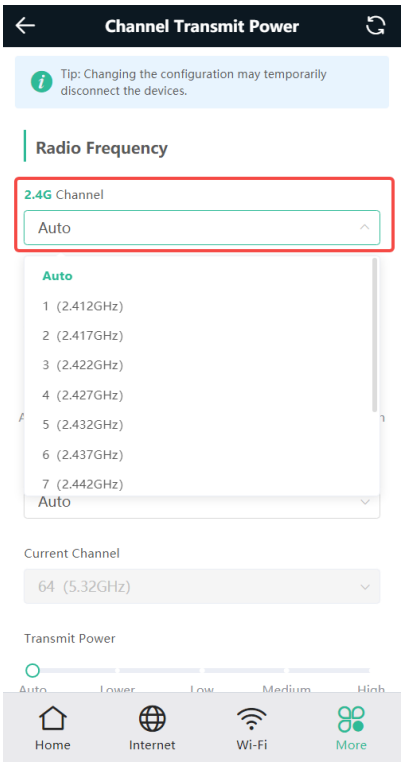
Note

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

Caution

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





- Optimizing the channel bandwidth

Smartphone View: Choose **More**> **Radio Frequency**.

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

If the interference is severe, choose a lower channel bandwidth to avoid network stalling.

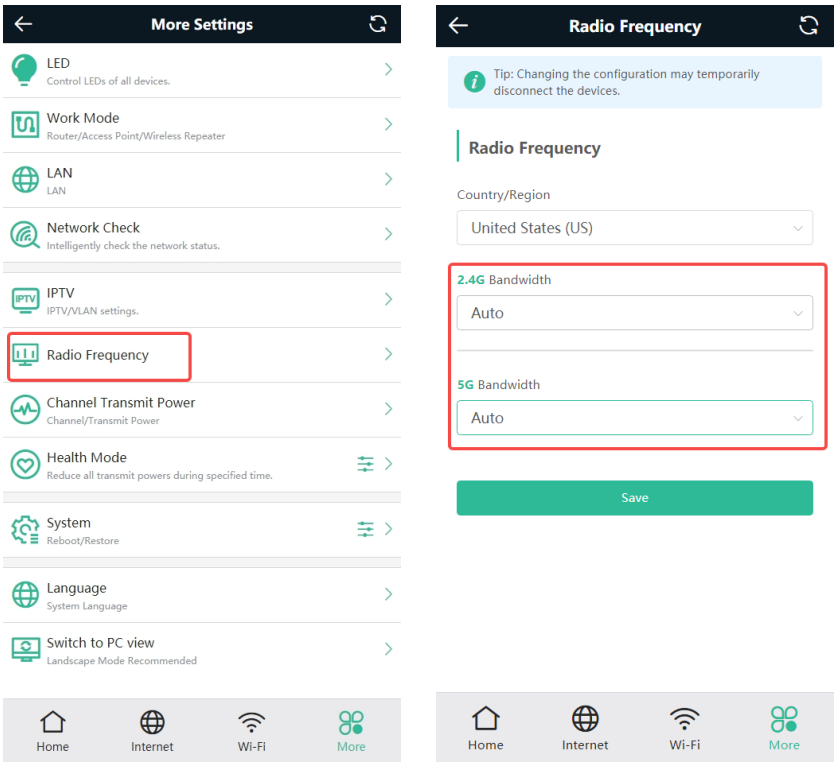
You can select 20MHz and 40MHz bandwidths for the 2.4GHz band, or 20MHz, 40MHz, 80MHz and 160MHz for the 5GHz band. The default value is "Auto", indicating that the bandwidth will be automatically selected based on the wireless environment.

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

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

Caution

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



- Optimizing the transmit power

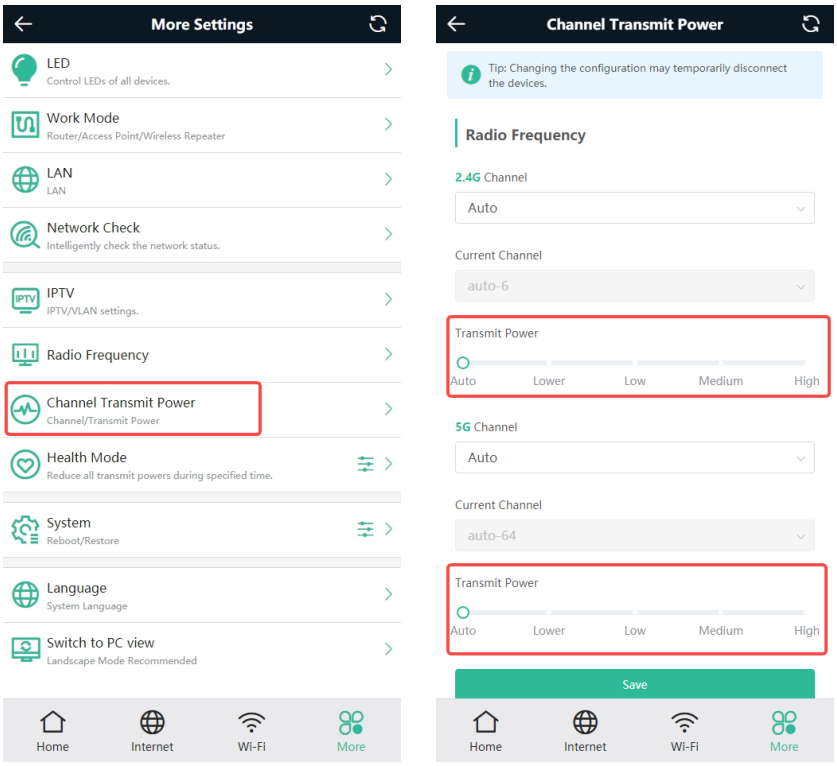
Smartphone View: Choose **More** > **Channel Transmit Power**.

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

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

Caution

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



4.7 Configuring the Health Mode

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

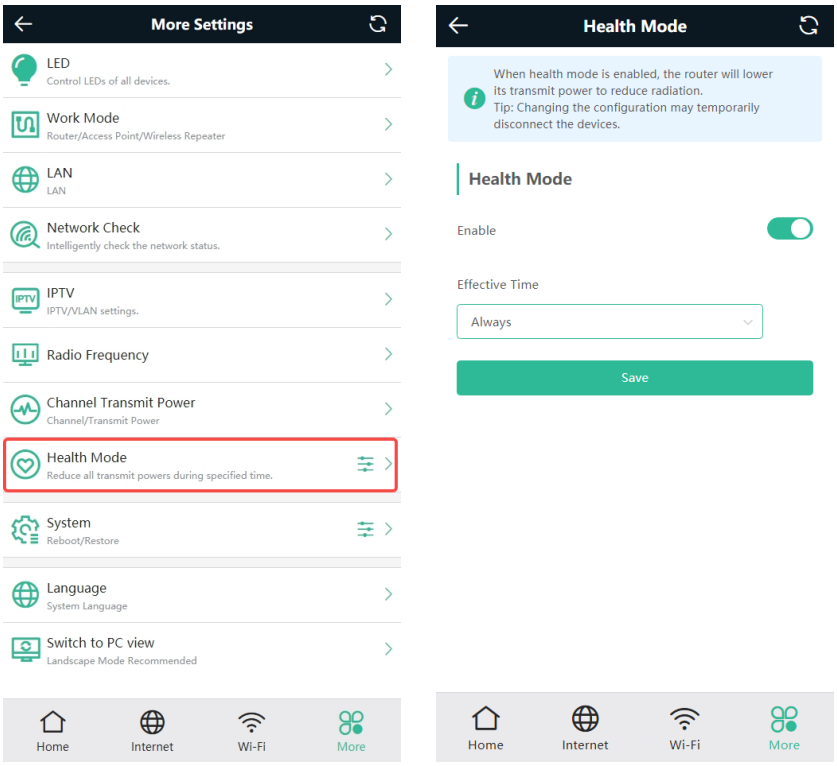
PC View: Choose **More** > **WLAN** > **Wi-Fi** > **Health Mode**.

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

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

Note

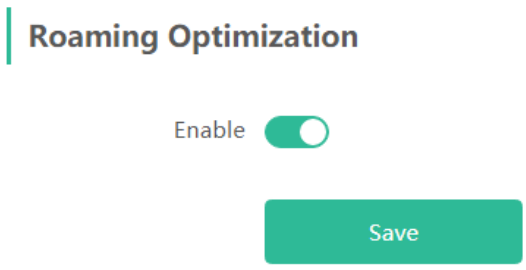
All Mesh Routers have undergone stringent radiation detection and evaluation, and comply with IEC/EN62311, EN 50385 and other standards. Wi-Fi networks will not affect human health and you can be rest assured to use them.



4.8 Enabling Roaming Optimization

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

PC View: Choose **More** >**WLAN > Wi-Fi > Roaming Optimization.**Click **Enable** to enable Roaming Optimization. Terminal devices can connect to the new router to maintain their original Internet services.



5 Configuring Work Mode

5.1 Access Point

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

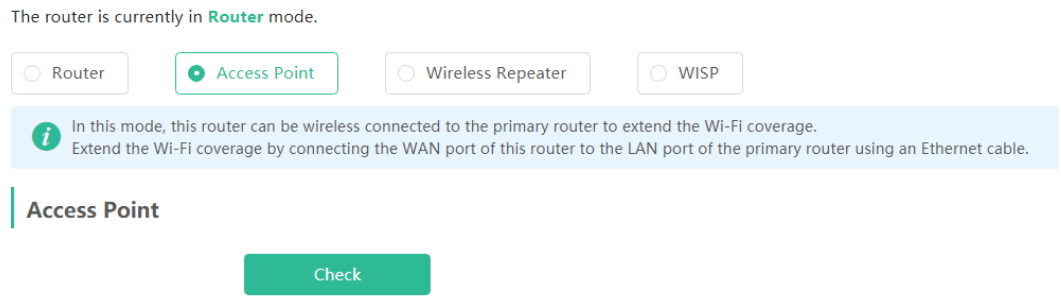
PC View: Choose **More** > **Work Mode**.

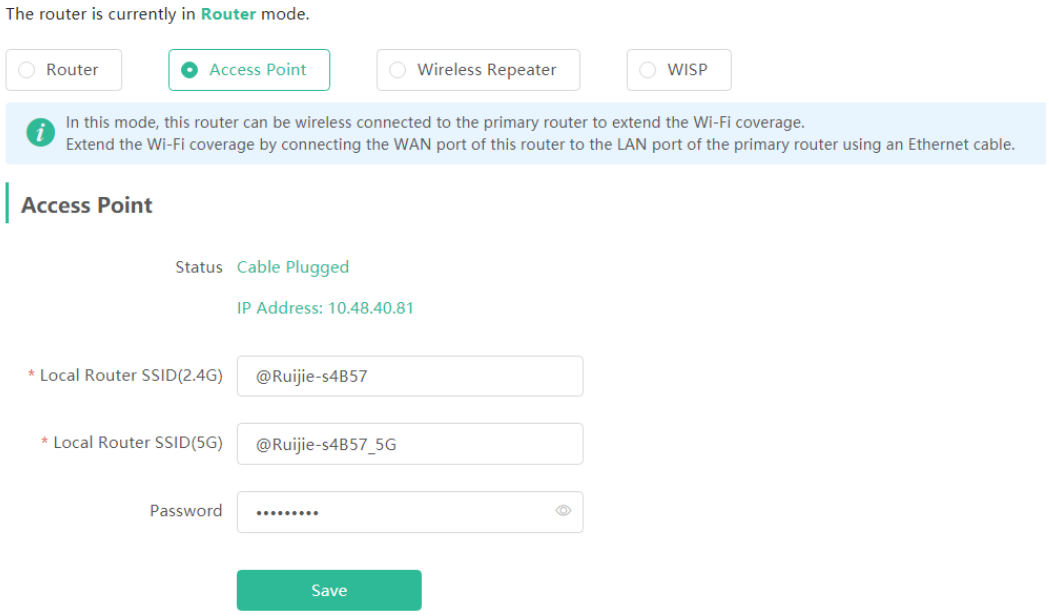
Connect the WAN port of this router to a LAN port of the primary router using an Ethernet cable.

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

Caution

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





5.2 Wireless Repeater

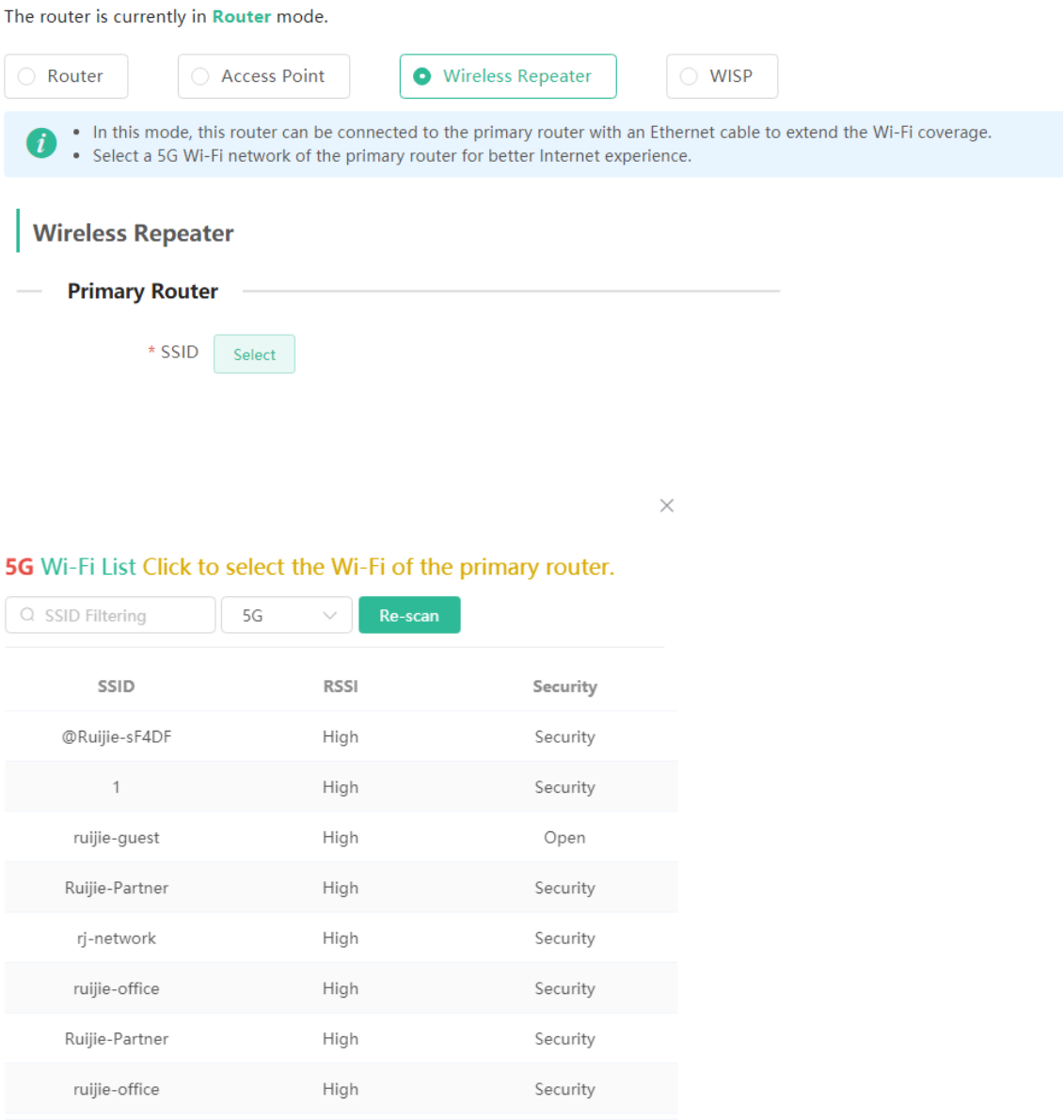
Smartphone View: Choose **More** > **Work Mode**.

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

Note

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

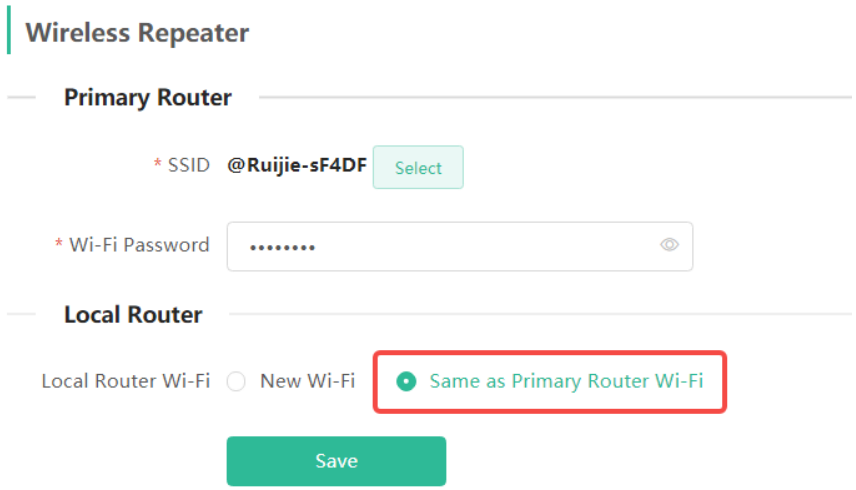
(1) Click **Wireless Repeater**. Verify that the Ethernet cable is unplugged, then click **Cable Unplugged**. Click **Select**, the Wi-Fi list is displayed. By default, a 5 GHz Wi-Fi list is displayed. To view a 2.4 GHz Wi-Fi list, click the **5G** drop-down box and select **2.4G**. You are advised to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



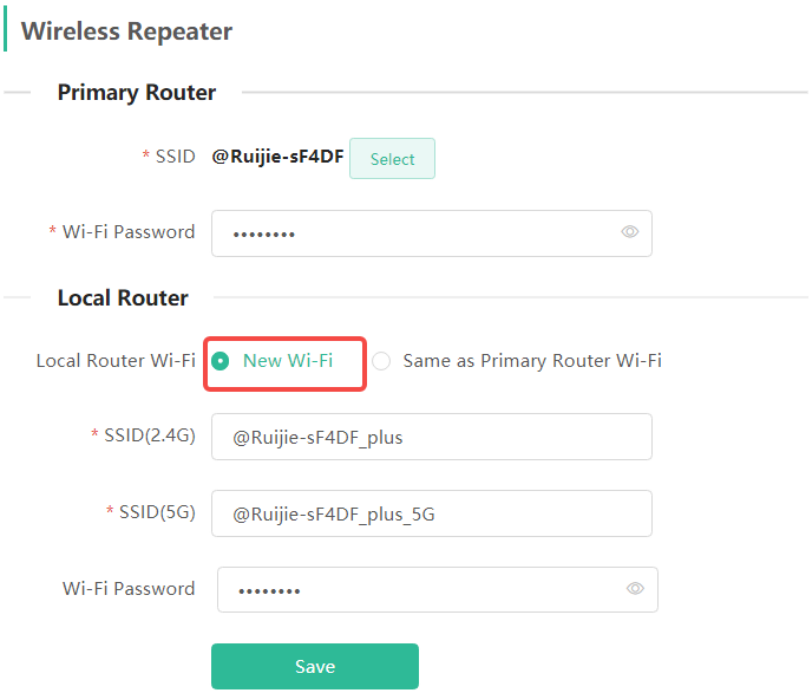
(2) Select the Wi-Fi network of the primary router to be relayed. The **Local Router** configuration item is displayed. If the primary router's Wi-Fi network is encrypted, enter the Wi-Fi password.

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

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



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



Caution

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

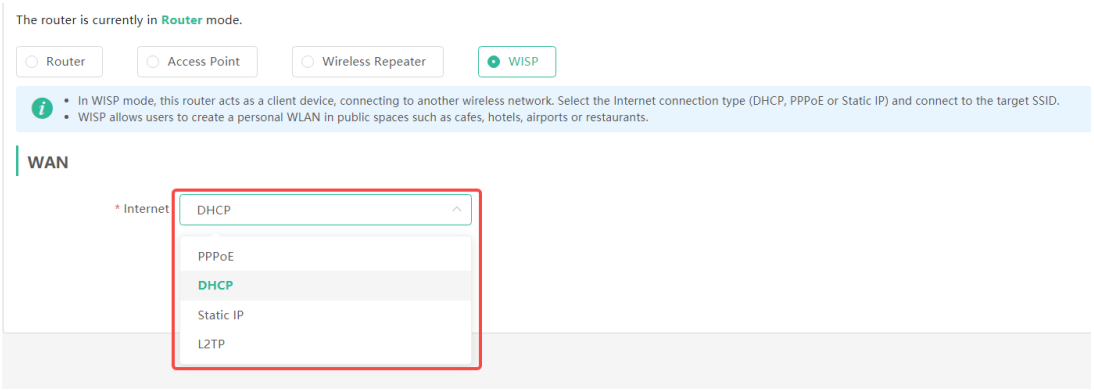
5.3 WISP

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

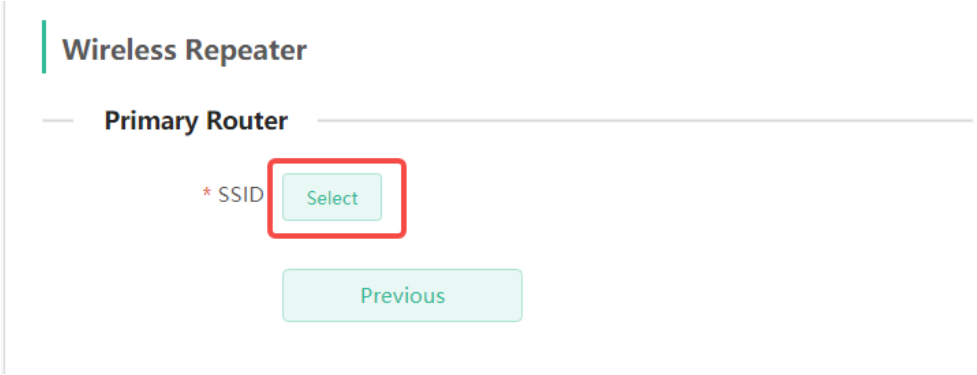
PC View: **More** >**Work Mode**

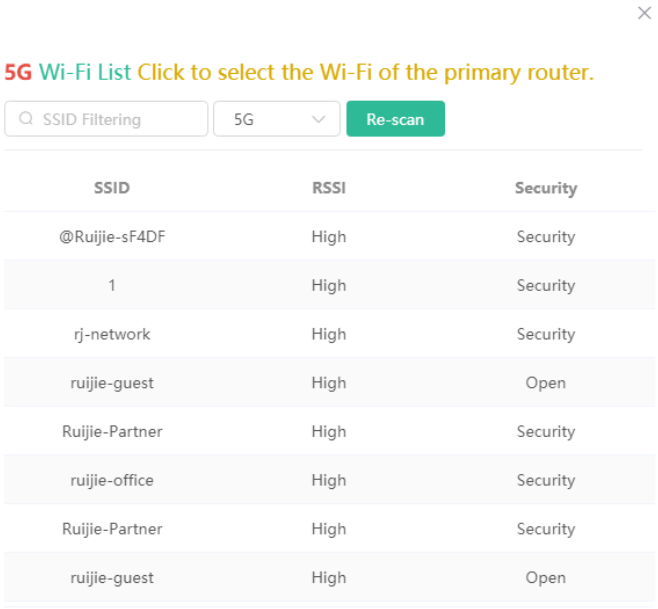
WISP allows users to establish their own WLAN for Internet access in public spaces, including coffee, hotel, airport or restaurant.

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



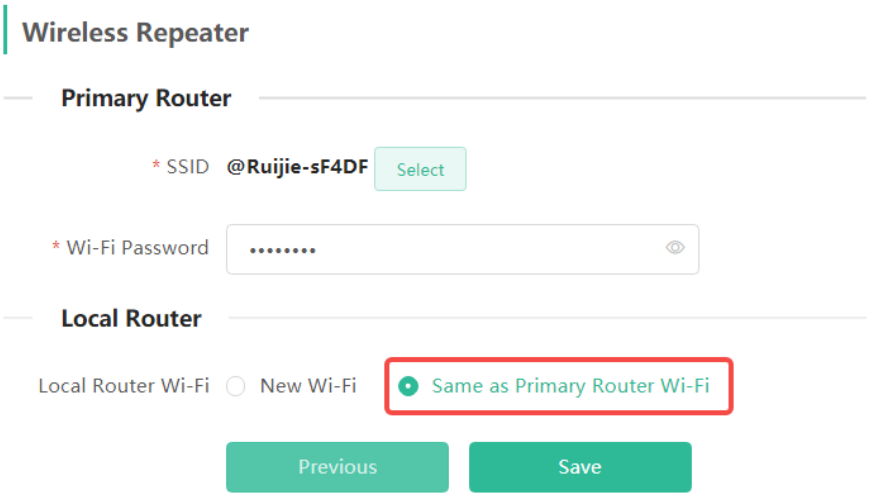
(2) Select the Wi-Fi signal of the primary router and enter its Wi-Fi password.



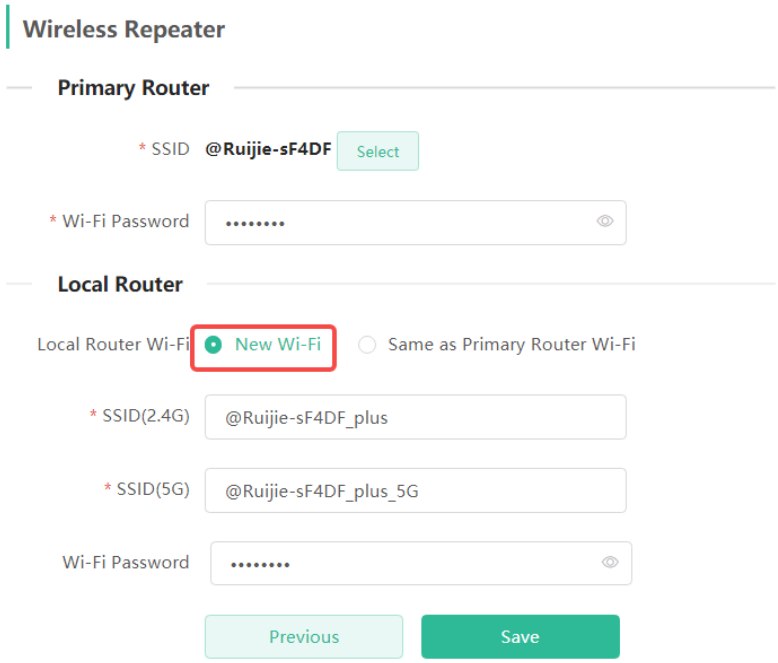


(3) You can configure a new Wi-Fi network or have a Wi-Fi network the same as that of the primary router:

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



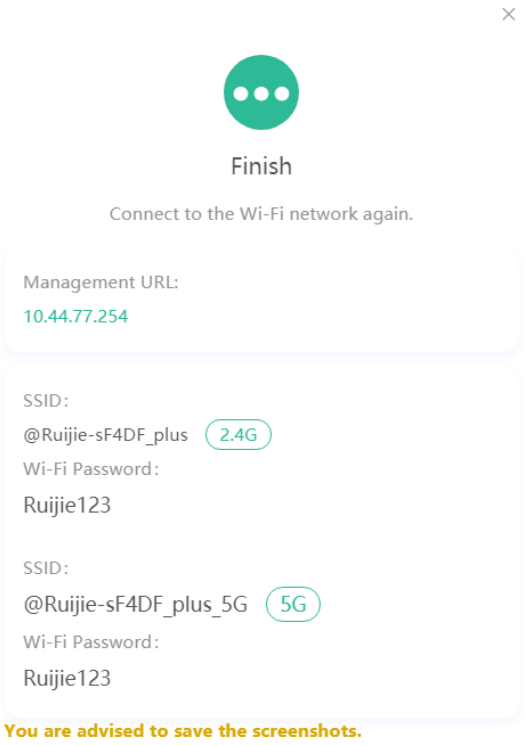
- If you select **New Wi-Fi**, you can set a local SSID and password. Clients will search out a Wi-Fi signal different from the primary router Wi-Fi signal.



(4) Click **Save**.

Caution

After the configuration is saved, the Wi-Fi restarts. The clients need to connect to the new Wi-Fi. Remember the configured Wi-Fi name and password, and exercise caution when performing the configuration.



6 Configuring Network Settings

6.1 Configuring Internet Connection Types

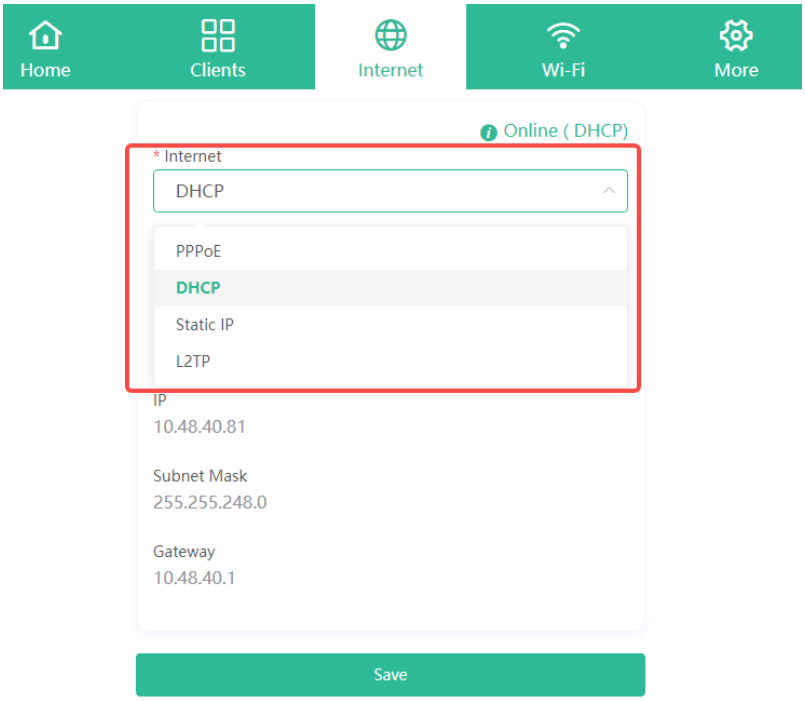
Caution

This feature is supported in router mode.

Smartphone View: Choose **Internet**.

PC View: Choose **Internet.**

The router supports four Internet connection types: PPPoE, DHCP, static IP, and L2TP. For details, see 2.4.1 Configuring the Internet Connection Type.



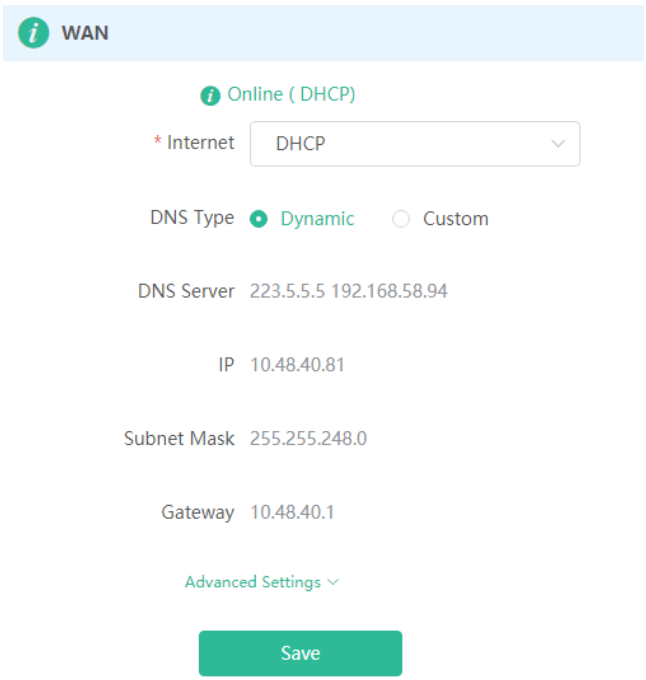
6.2 Configuring WAN Settings

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

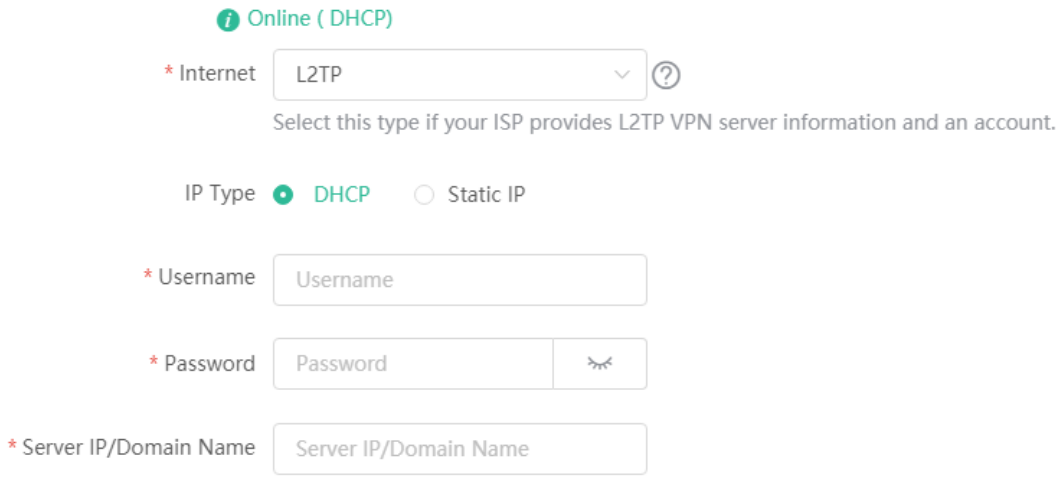
PC View: **More** > **Basics** > **WAN Settings.**

1. Configuring Internet connection types

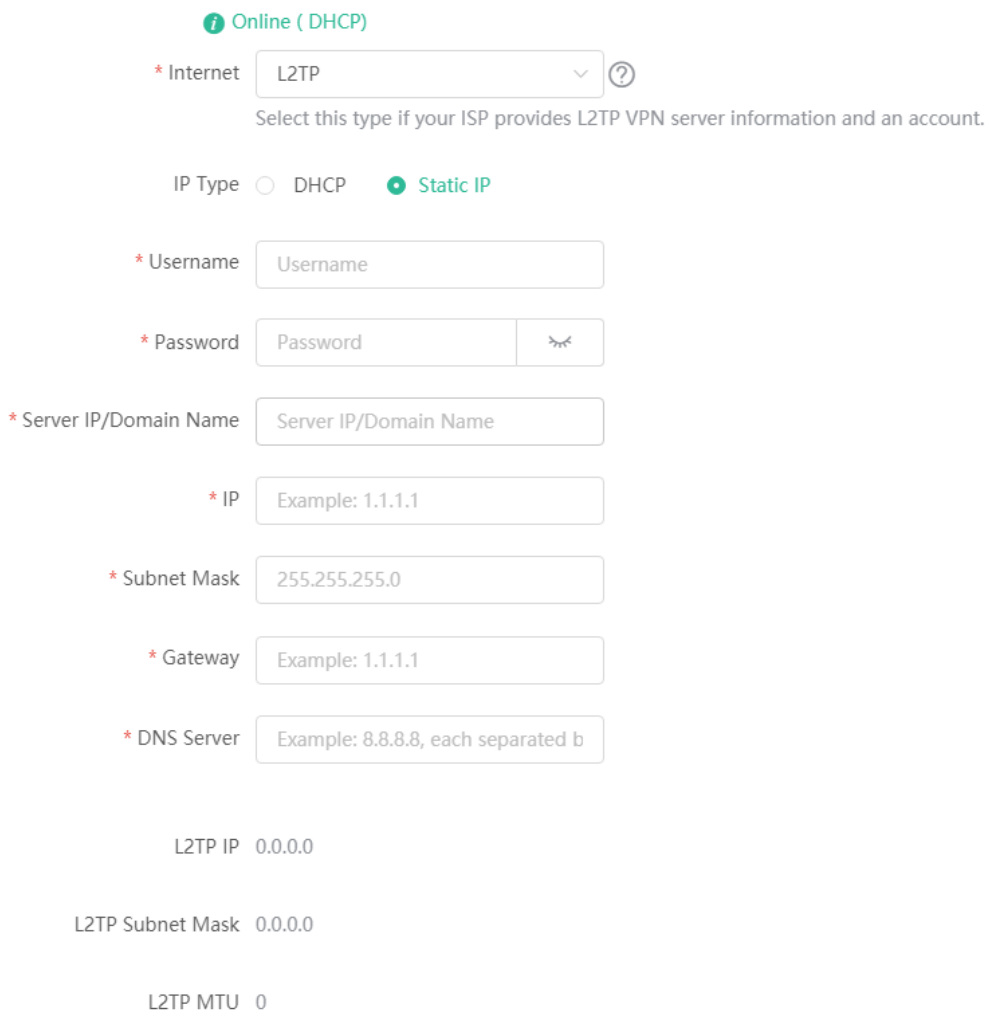
This router supports single WAN links.



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



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



2. Changing the MAC Address

Caution

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

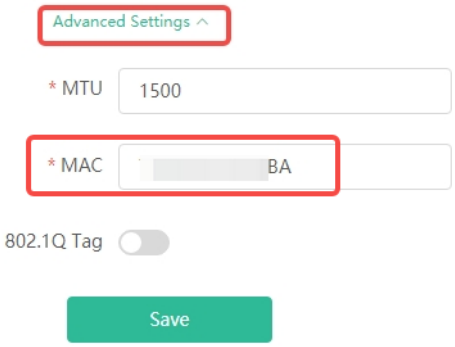
The ISP may restrict the access of devices with unknown MAC addresses to the Internet for the sake of security. In this case, you can change the MAC address of the WAN port to another address. You are advised to use the MAC address of an old router that is allowed to access the Internet (the MAC address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

Click **Advanced Settings**. Enter the MAC address in the format of 00:11:22:33:44:55.

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

Caution

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



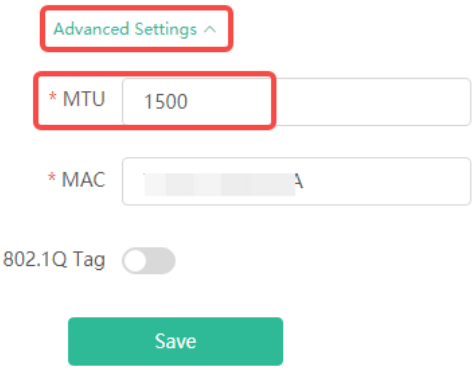
3. Modifying MTU

Caution

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

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

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

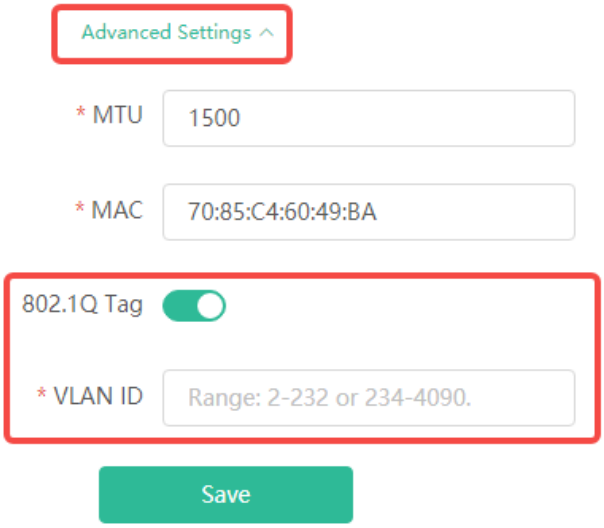


4. Configuring the VLAN Tag

Caution

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

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

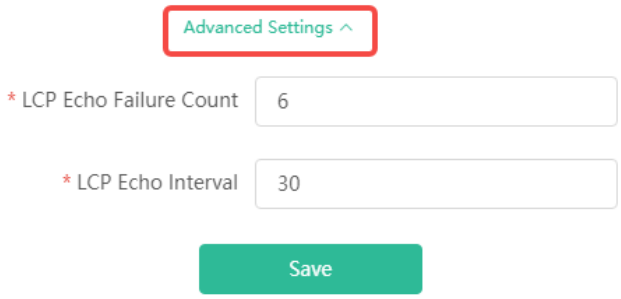


5. Configuring LCP Parameters

Caution

This function is only supported when the Internet Connection Type is set to PPPoE or L2TP.

The Link Control Protocol (LCP) is used to monitor and maintain the connection status of point-to-point links. The LCP Echo mechanism periodically sends Echo requests based on the **LCP Echo Interval** setting. If the number of sent Echo packets reaches the **LCP Echo Failure** threshold without any responses, the link will be considered disconnected, and the device will attempt to re-establish the network connection.



6.3 Changing the Address of a LAN Port

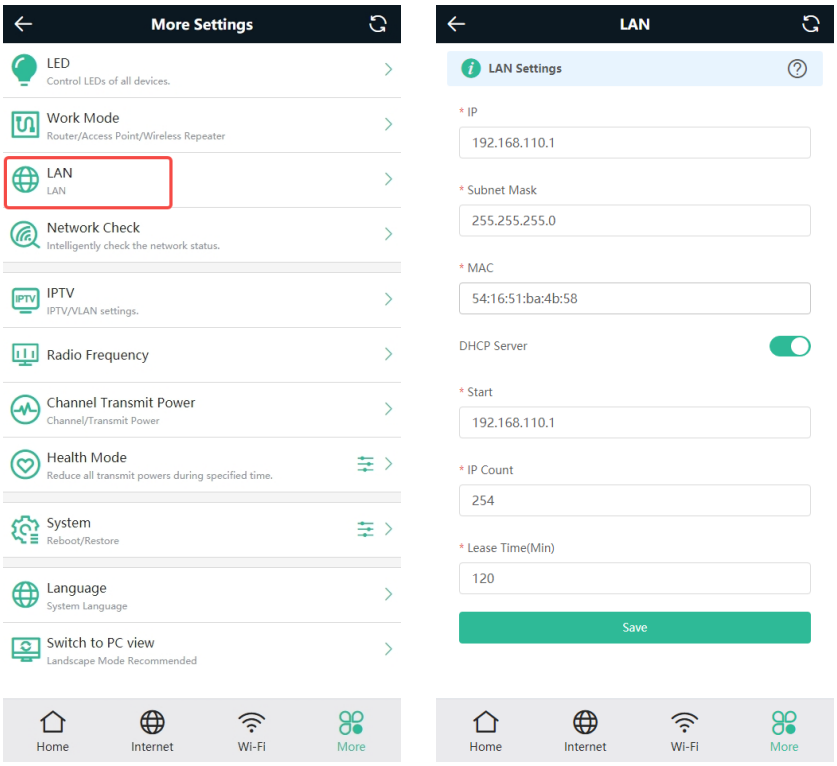
Smartphone View: Choose **More** > **LAN**.

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

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

Caution

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



6.4 Connecting to IPTV

Caution

This feature is supported in router mode.

IPTV is an Internet television service provided by ISP.

6.4.1 Getting Started

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

6.4.2 IPTV Configuration Steps (VLAN Type)

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

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

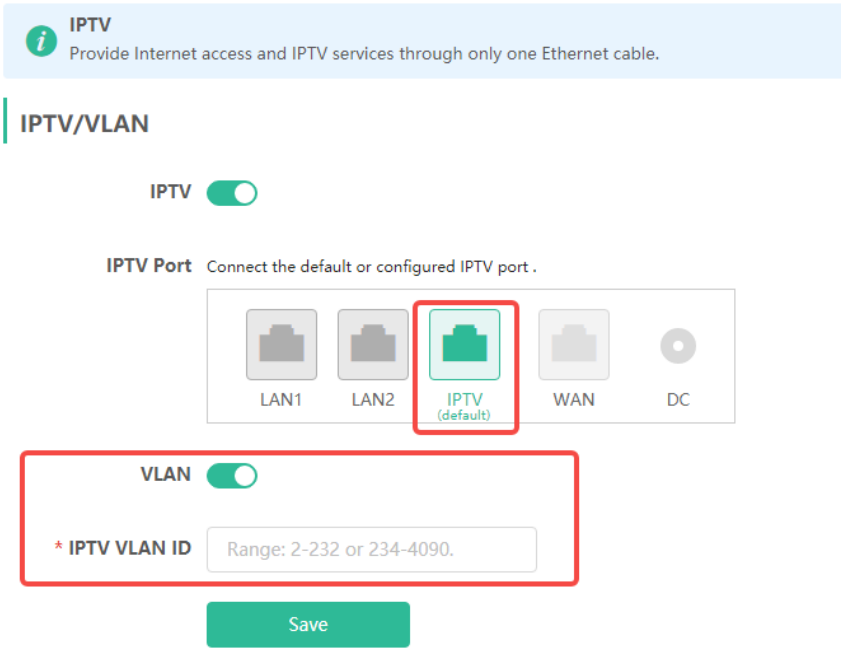
Click to enable IPTV, and select the LAN port to be connected to the IPTV STB.

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

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

Caution

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

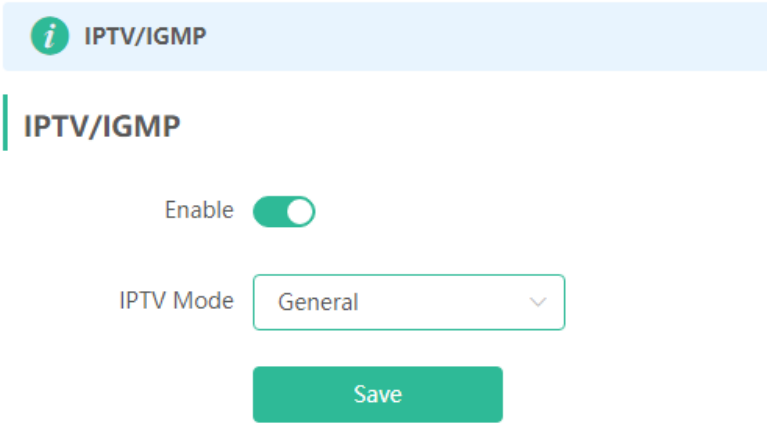


6.4.3 IPTV Configuration Steps (IGMP Type)

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

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

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



6.5 Configuring Wi-Fi/IGMP

6.5.1 Overview

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

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

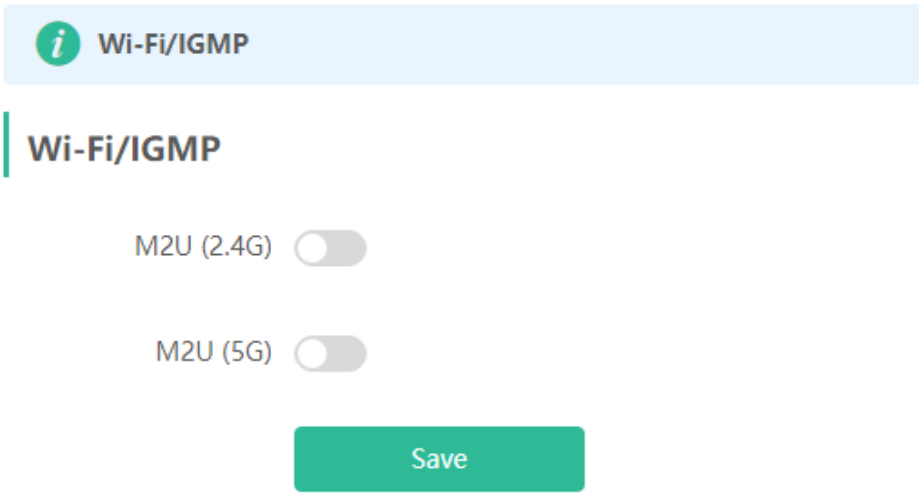
6.5.2 Configuration Steps

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

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

Click **M2U (2.4G)** to enable Wi-Fi/IGMP for 2.4G wireless clients.

Click **M2U (5G)** to enable Wi-Fi /IGMP for 5G wireless clients.



6.6 Configuring IPv6

Caution

This feature is supported in router mode.

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

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

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

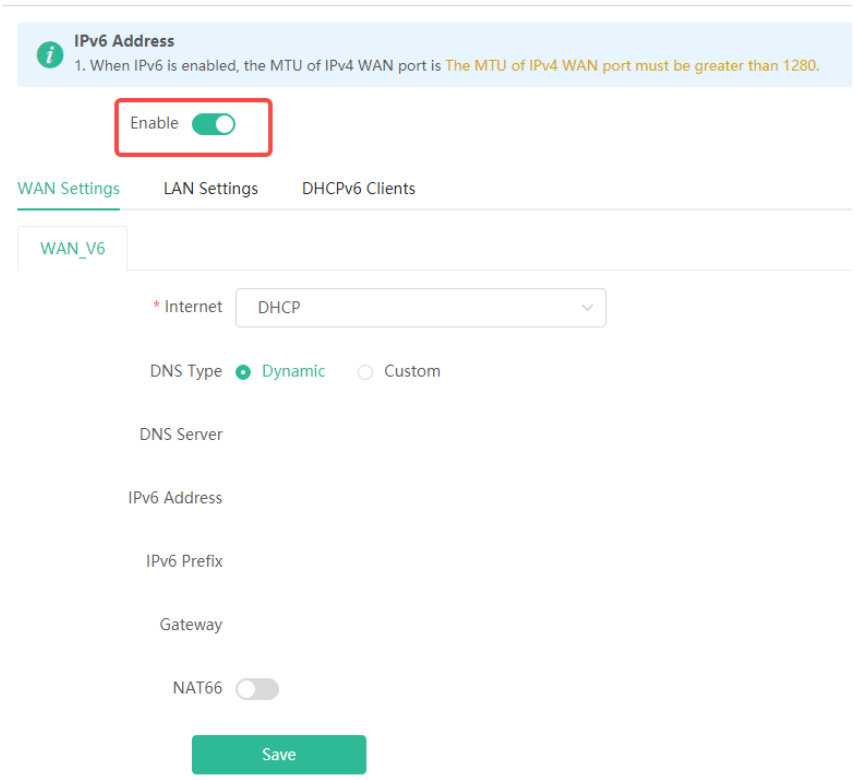
6.6.1 Configuring the IPv6 of the WAN Port

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

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

Caution

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



6.6.2 Configuring the IPv6 of the LAN Port

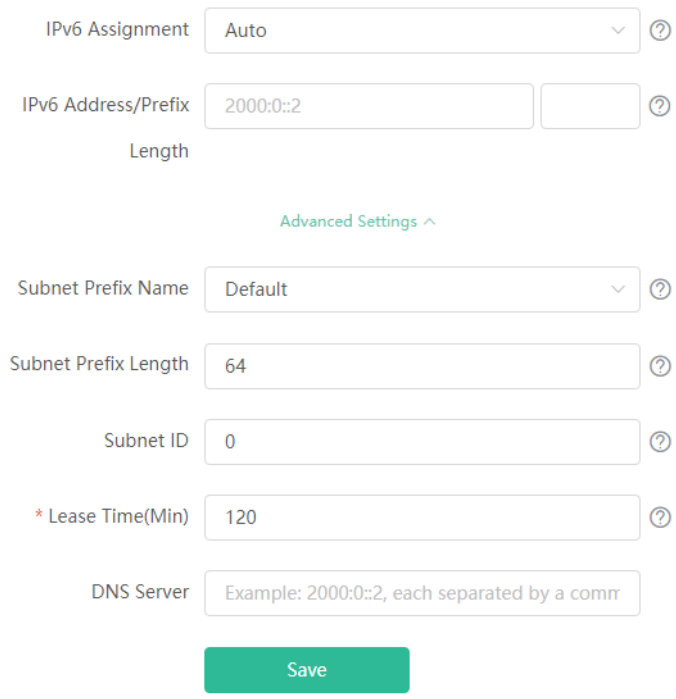
Smartphone View: Choose **More** > **Switch to PC** > **More** > **Basics** > **IPv6** > **LAN Settings**

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

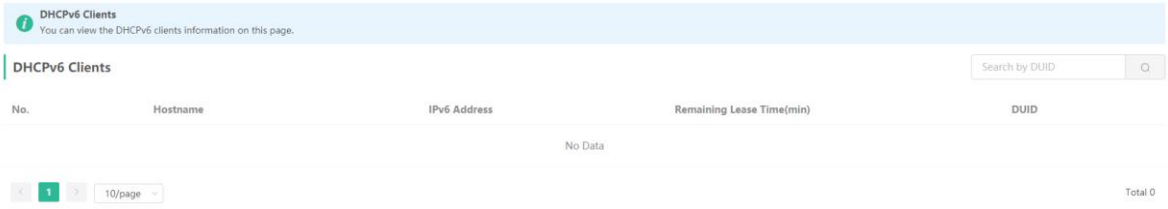
IPv6 Assignment: Choose **Auto** to use both DHCPv6 mode and SLAAC mode to allocate address. Choose **Null** to assign no address. You are advised to choose **Auto**.

IPv6/Prefix Length: If the router fails to obtain an IPv6 prefix, you can configure one manually. Set the subnet prefix length to a value smaller than or equal to 63.

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 from the router.



6.7 Managing Blocking Schedules

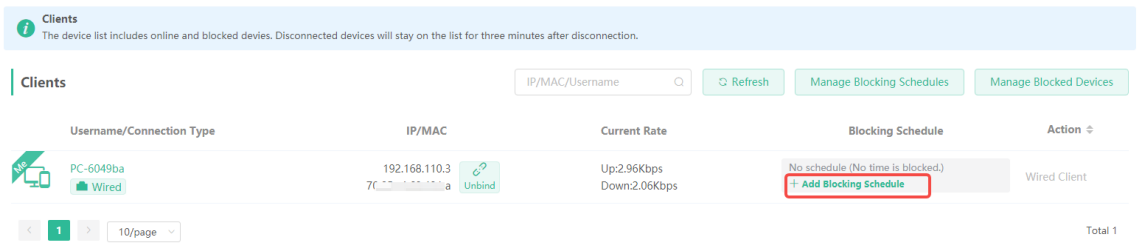
Smartphone View: Choose **More** > **Switch to PC view** > **Clients** > **Manage Blocking Schedules.**

PC View: Choose **Clients** > **Manage Blocking Schedules.**

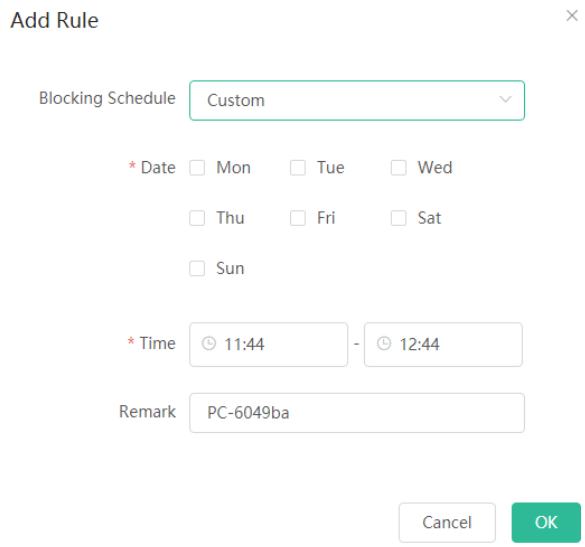
Caution

This function is supported only in router mode.

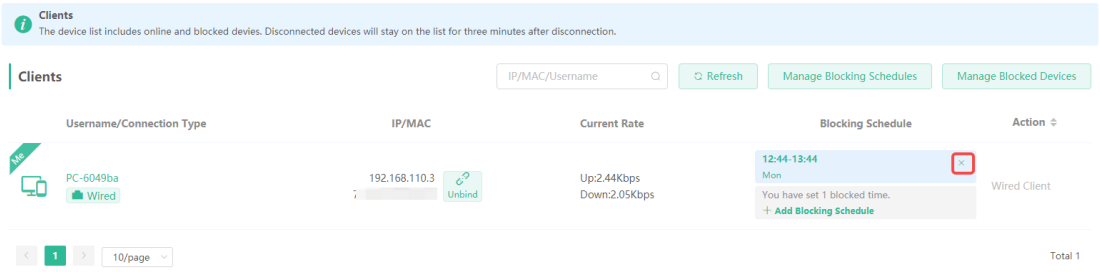
Click **Add Blocking Schedule** to set the Internet block periods. In the block periods, the client cannot access the Internet.



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



Click **Delete** in the upper right corner to lift the restrictions on the client.



6.8 Configuring DHCP Server

Caution

This feature is supported in router mode.

6.8.1 Overview

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

6.8.2 Configuration Steps

1. Configuring the DHCP Server Function

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

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

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

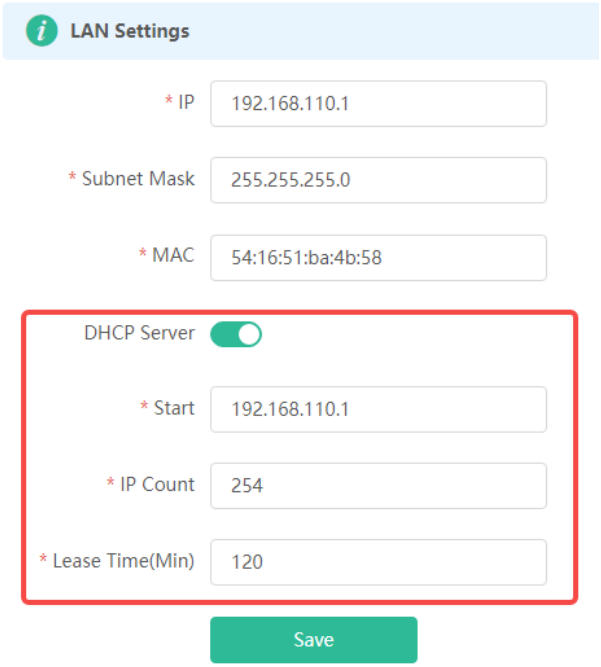
Caution

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

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

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

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

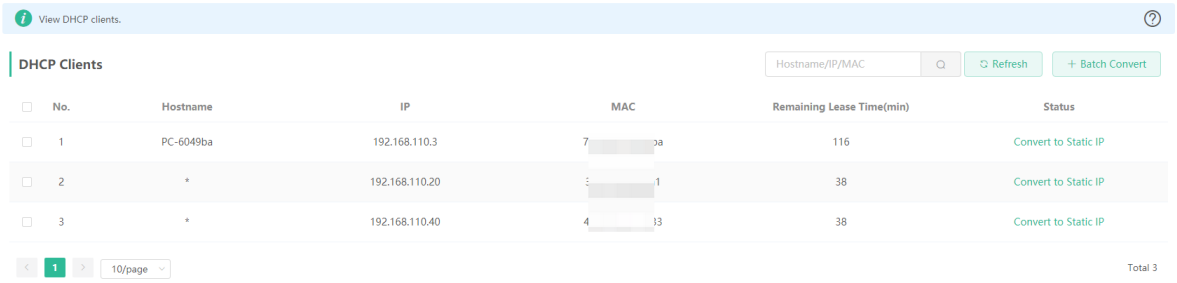


2. Displaying Online DHCP Clients

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

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

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

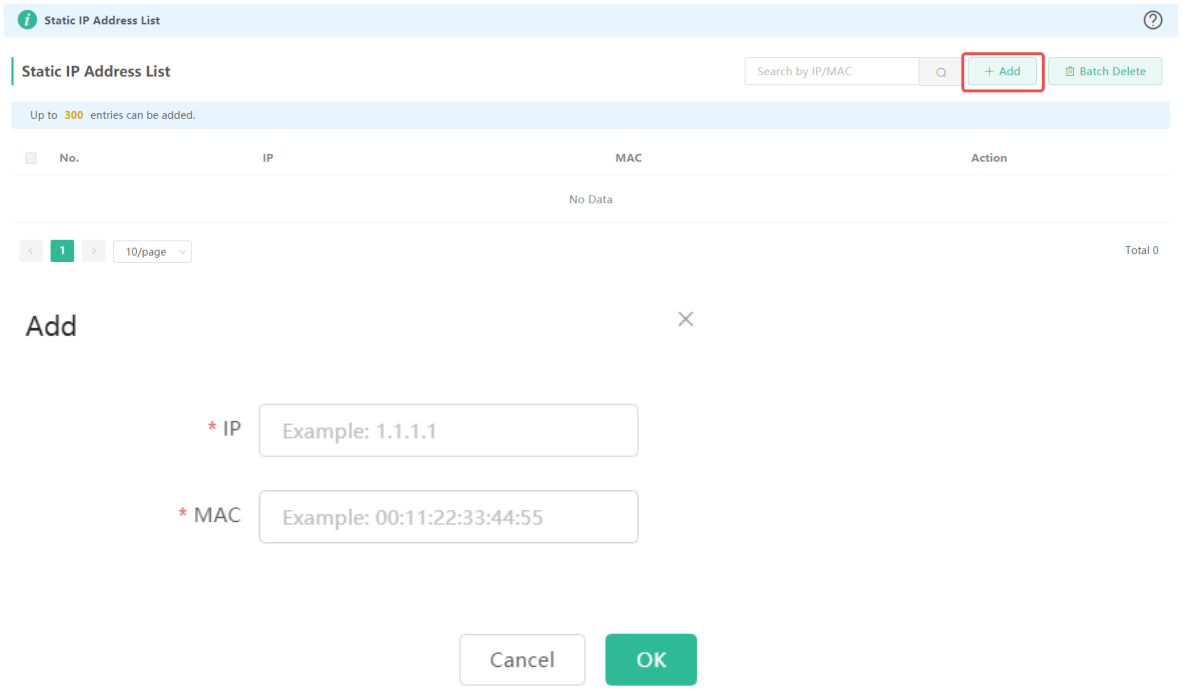


3. Displaying the DHCP Static IP Address Table

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

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

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



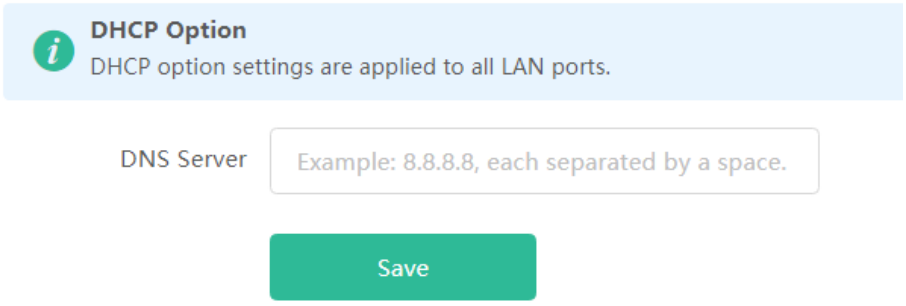
4. Configuring DHCP Option

Smartphone View: Choose **More** > **Switch to PC view** > **More** > **Basics** > **LAN** > **DHCP Option**.

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

Enter the DNS address provided by the ISP, and click **Save**.

The DHCP Option settings are applied to all LAN ports. The **DHCP Option** configuration is optional.



6.9 Configuring DNS Server

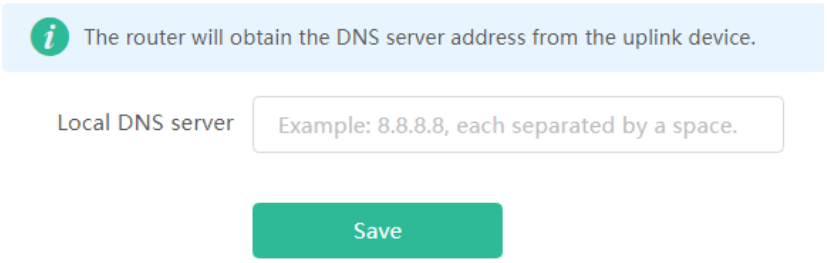
6.9.1 Local DNS Server

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

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

PC View: Choose **More** > **Advanced** > **Local DNS**

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



6.9.2 Configuring DNS Proxy

Caution

This feature is supported in router mode.

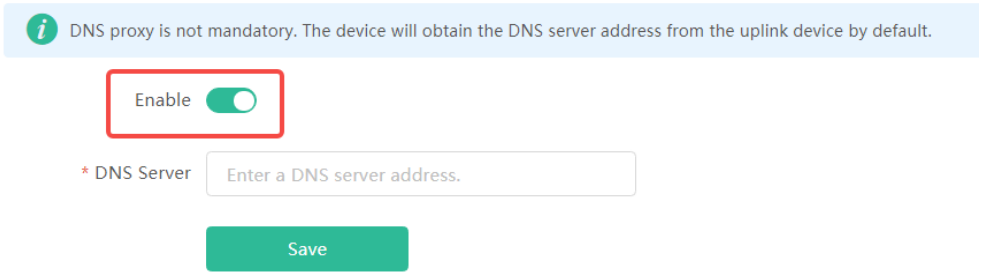
The domain name system (DNS) proxy configuration is not mandatory. The device obtains the DNS server address from the uplink device by default.

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

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

DNS Proxy: The function is disabled by default and the DNS delivered by a carrier is used. If the DNS is incorrectly configured, the network is accessible and the mobile app can access the Internet properly, but the Web page cannot be opened. You are advised to disable the function.

DNS Server: Clients automatically use the DNS service provided by the primary router by default. The default configuration is recommended. After the DNS proxy function is enabled, you can enter the IP address of the DNS server. The available DNS service varies from region to region. You can consult the local ISP.



6.10 Configuring Port Mapping

Caution

This feature is supported in router mode.

6.10.1 Overview

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

6.10.2 Getting Started

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

6.10.3 Configuration Steps

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

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

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

Name: Enter a name for ease of maintenance.

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

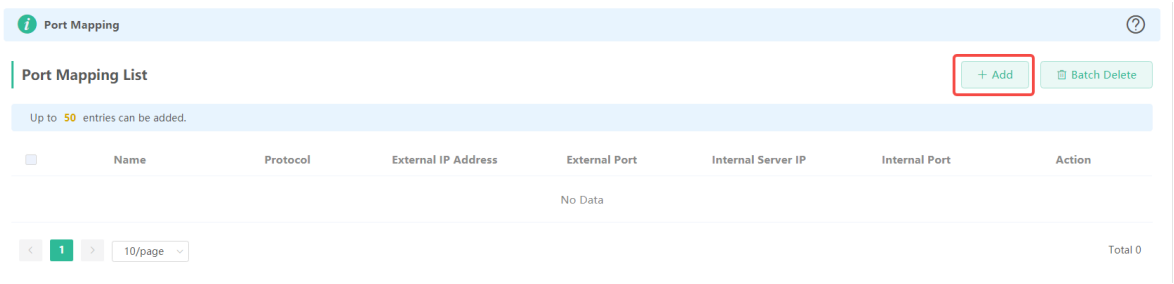
Protocol: Select the transport-layer protocol used by the selected service, such as **ALL**, **TCP**, or **UDP**. The configuration on the server end must be consistent with that on the client end.

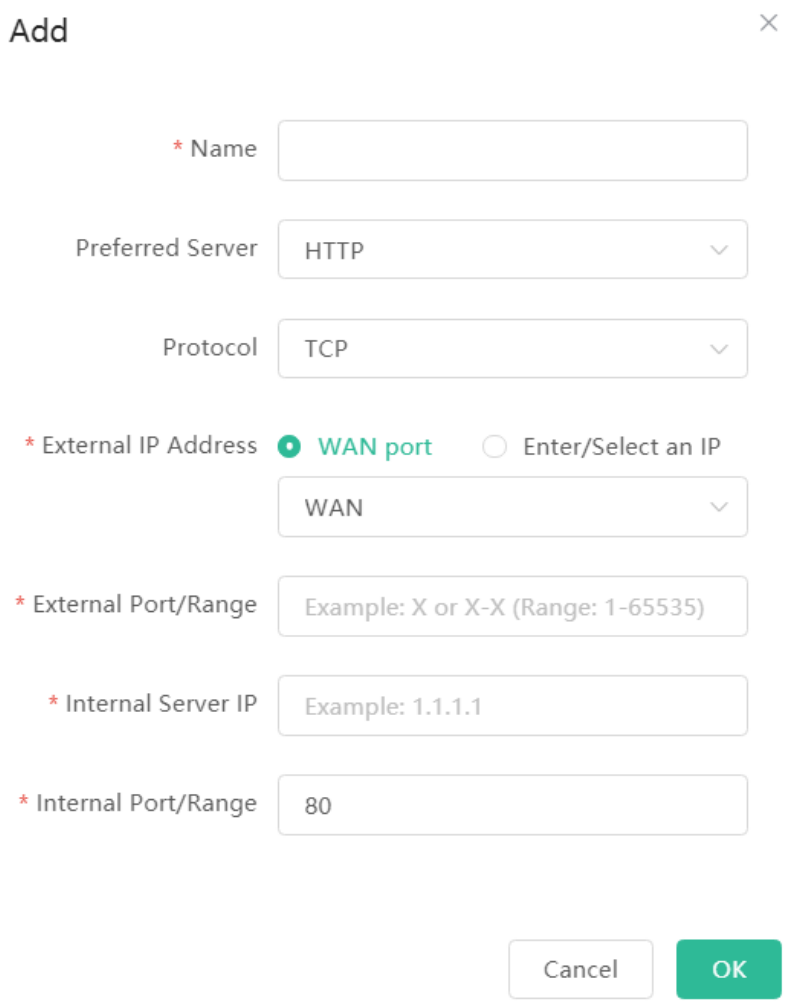
External IP Address: IP address for externet access. If multiple egresses exist on the network, select a specific WAN port IP address as the IP address for externet access.

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

Internal Server IP: Enter the LAN IP address used by external networks to access the device, such as the IP address of an IP camera.

Internal Port/Range: Enter the port number used by an application accessed by external networks, such as port 8080 used by the Web service.





6.10.4 Verification and Testing

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

6.10.5 Solution to a Test Failure

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

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

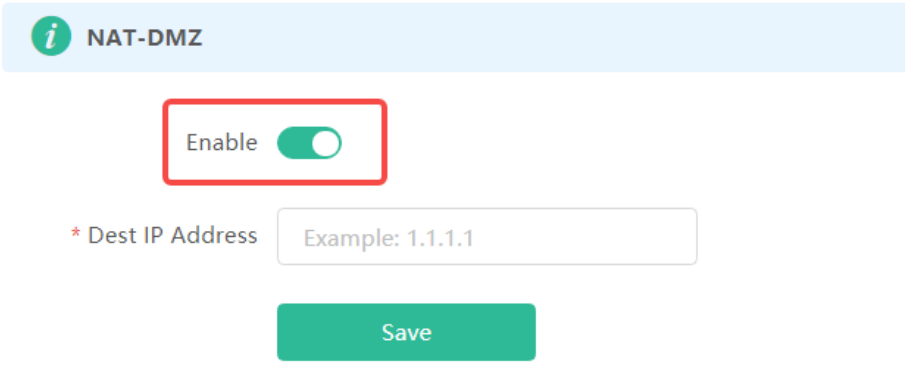
(3) Enable the DMZ service. For details, see 6.10.6 DMZ Configuration Steps. The common cause is that port configuration is incorrect or incomplete.

6.10.6 DMZ Configuration Steps

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

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

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



6.11 Configuring DDNS

6.11.1 Overview

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

6.11.2 Getting Started

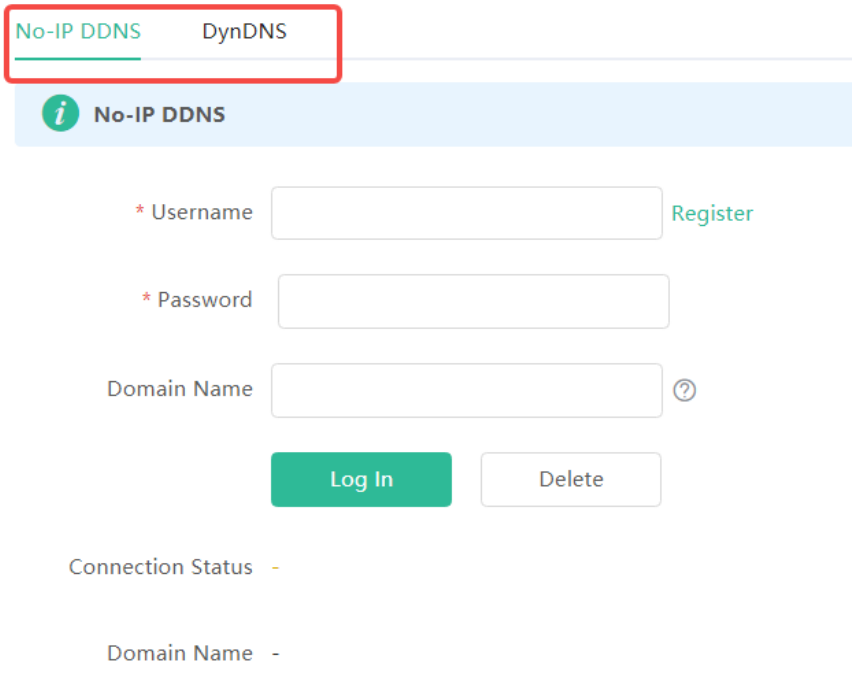
Register an account and domain name at Dyn or No-IP official website.

6.11.3 Configuration Steps

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

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

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



6.12 Configuring Connectivity Detection

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

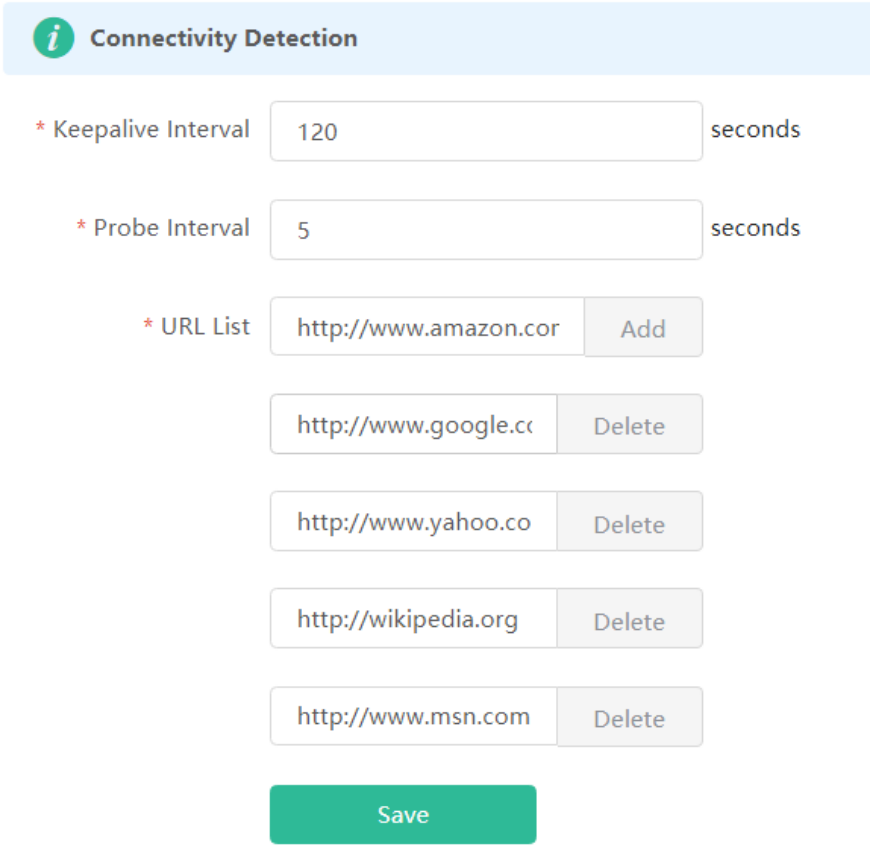
PC View: Choose **More** > **Advanced** > **Connectivity detection**.

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

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

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

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



6.13 Enabling CWMP

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

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

1. Overview

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

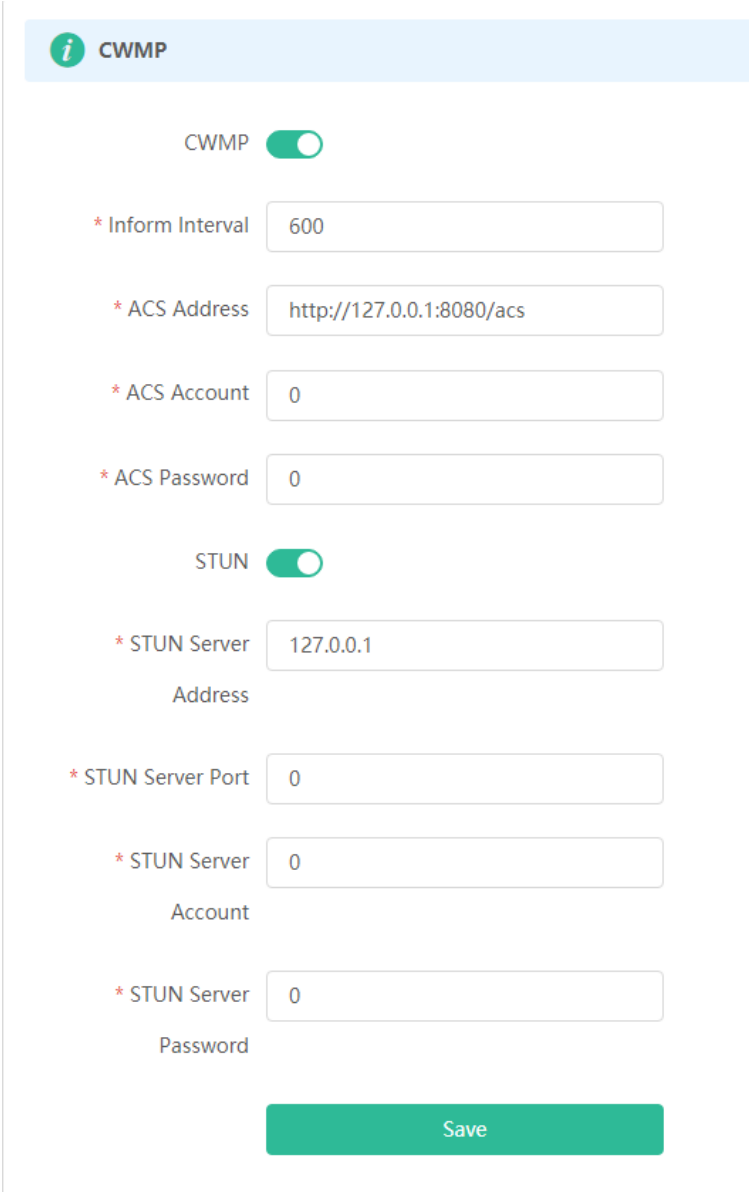
CWMP uses ACS and CPE models to manage devices. With CWMP, CPE can perform mandatory initialization and O&M actions such as service activation, function settings, file upload and download, and system detection.

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

2. Configuration Steps

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

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



6.14 Configuring APR Binding

Caution

This feature is supported in router mode.

6.14.1 Overview

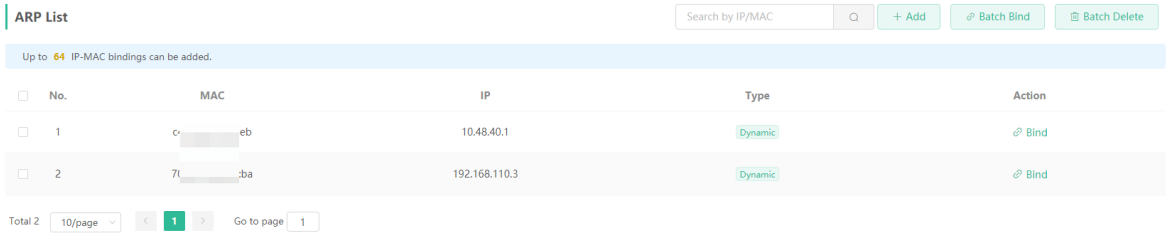
The router learns the ARP table from all devices connected to its ports. You can search for a device by its MAC address, perform ARP binding.

6.14.2 Configuration Steps

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

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

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



6.15 Enabling Smart Flow Control

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

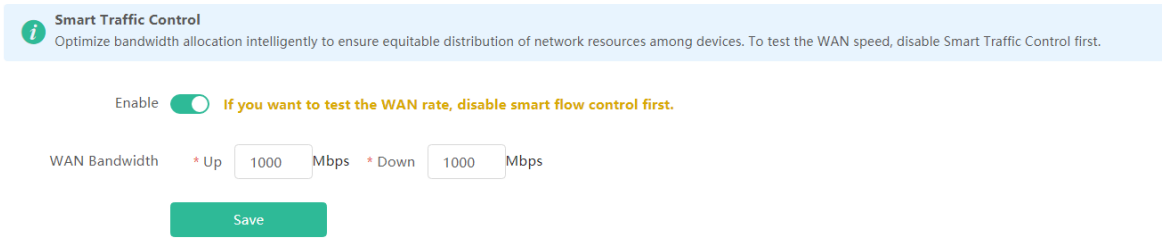
PC View: Choose **More** > **Advanced** > **Flow Control** > **Smart Flow Control**.

1. Enabling Smart Flow Control

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

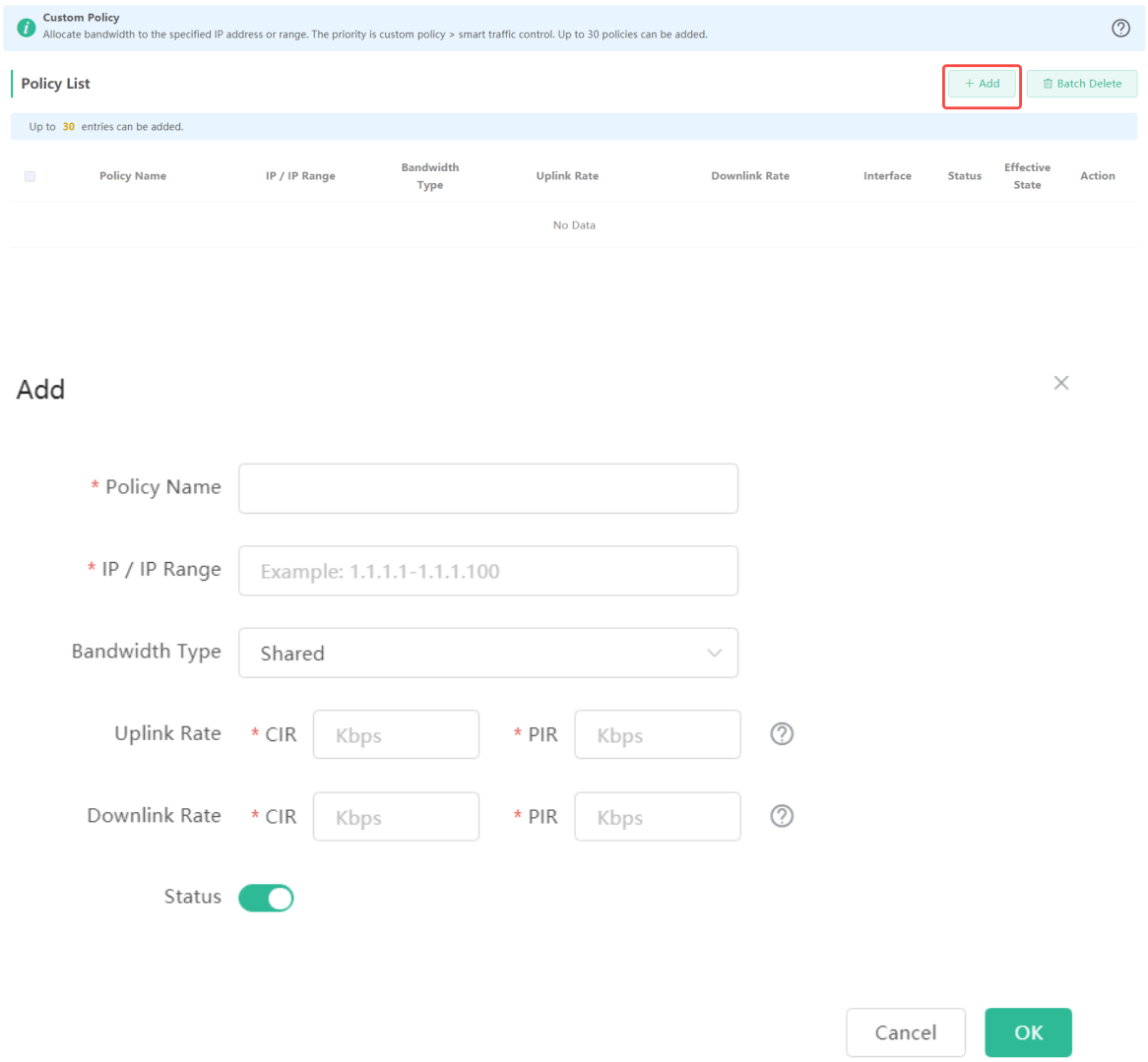
Caution

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



2. Custom Policy

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

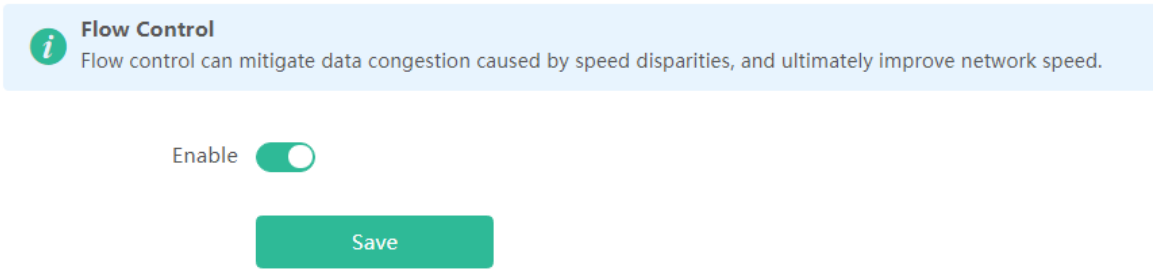


6.16 Enabling Port-Based Flow Control

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

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

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



6.17 Enabling Hardware Acceleration

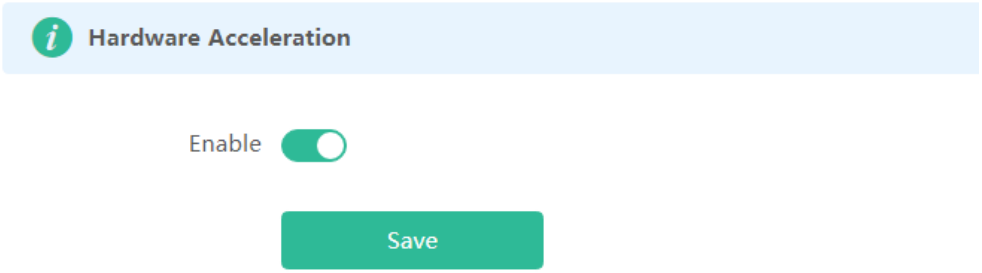
Caution

This feature is supported in router mode.

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

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

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



Caution

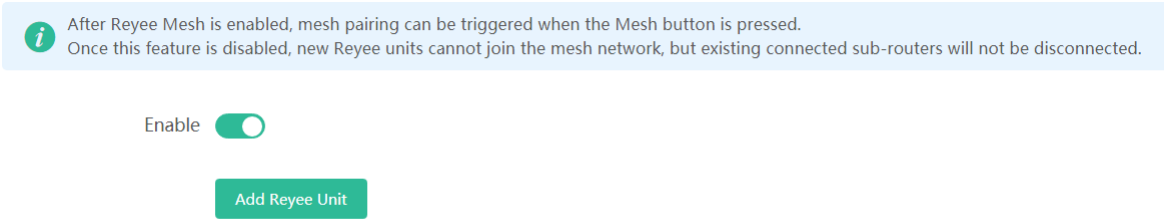
After hardware acceleration is enabled, IPv6 and smart flow control will be disabled.

6.18 Enabling Reyee Mesh

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

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

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



Note

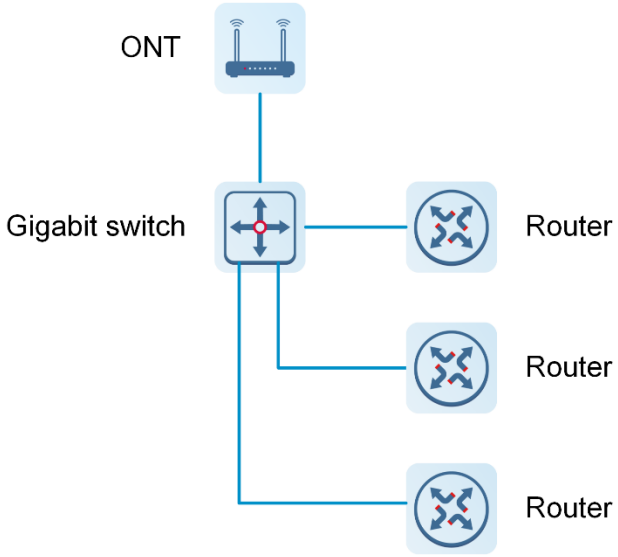
When Reyee Mesh is disabled, bridged mesh repeaters will not be disconnected.

6.19 Configuring Reyee Mesh 3.0

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

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

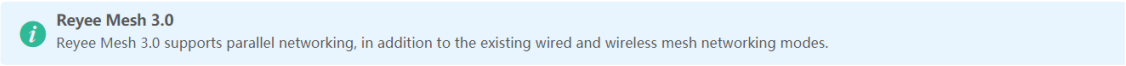
Connect the routers as indicated in the following figure:

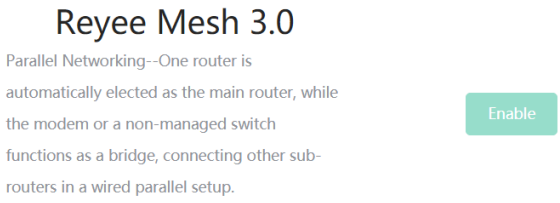


6.19.1 Parallel Networking

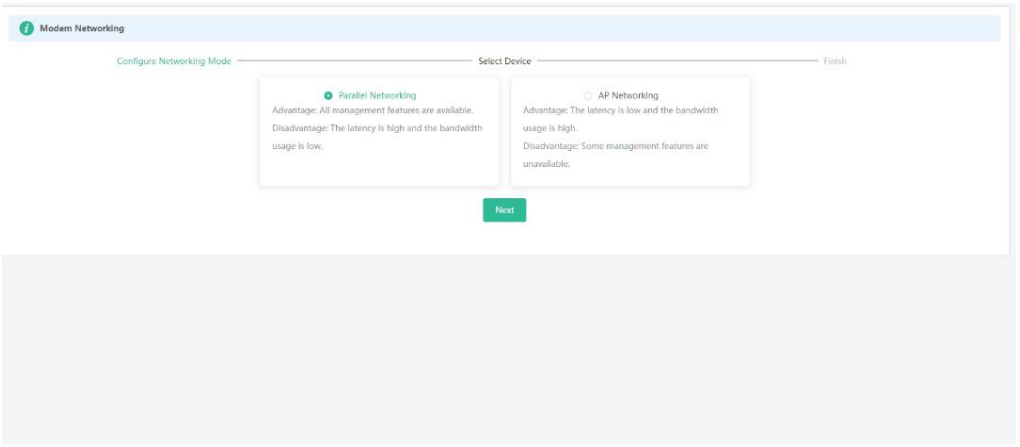
Parallel networking refers to connecting multiple routers in a wired manner to a modem or switch (Gigabit switch), with the modem as the network bridge, and one router elected as the master router. Other routers forward packets to the master router through the modem to access the internet, achieving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

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

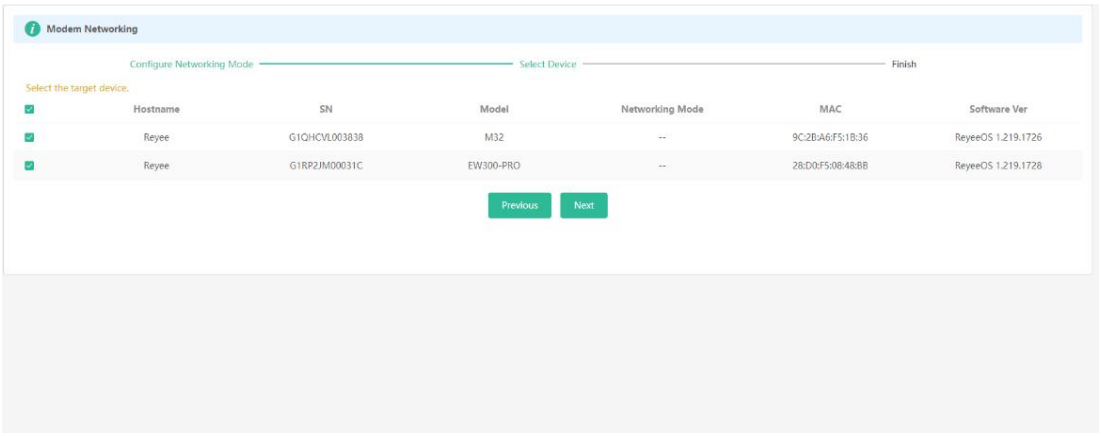




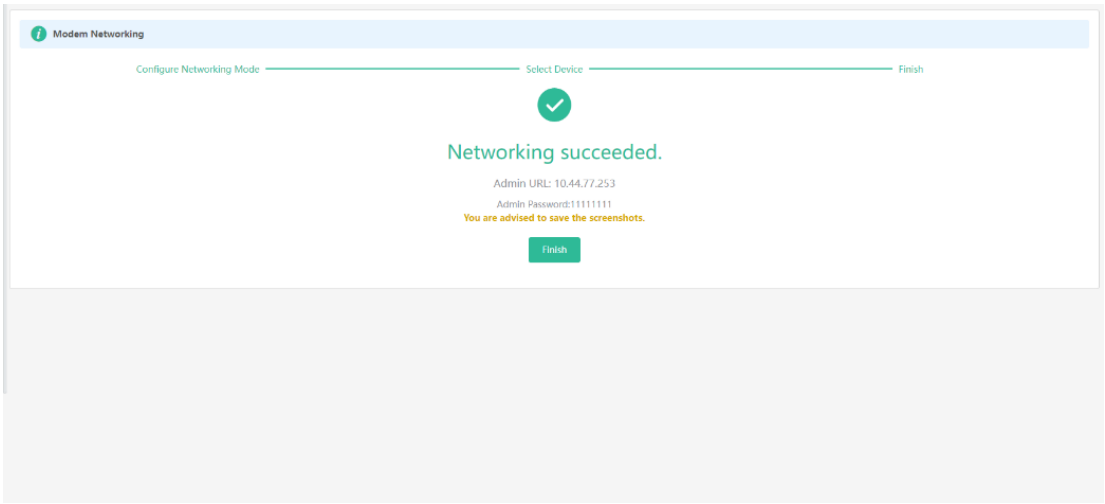
(2) Choose Parallel Networking, and click **Next**.



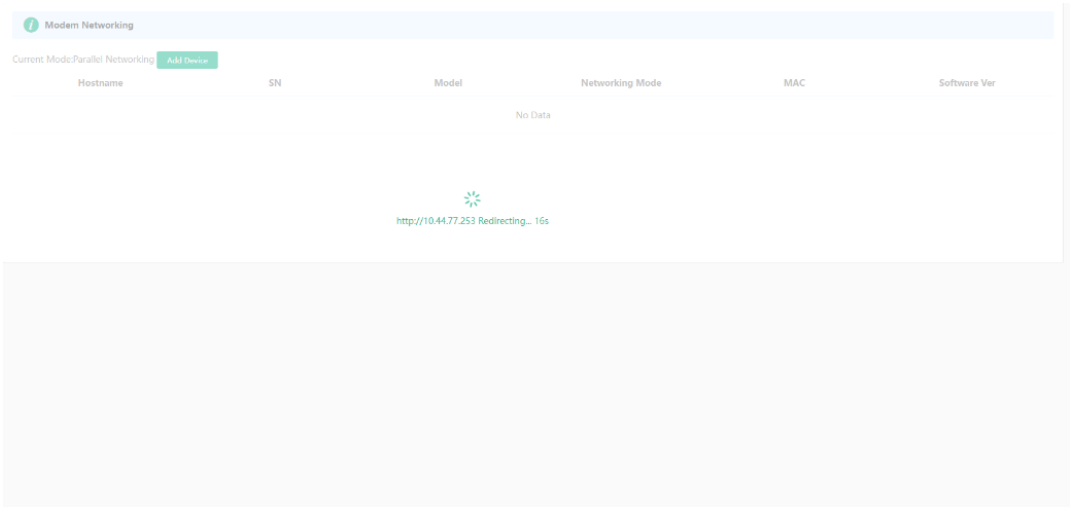
(3) Check routers for the networking.



(4) Click **Next**.



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

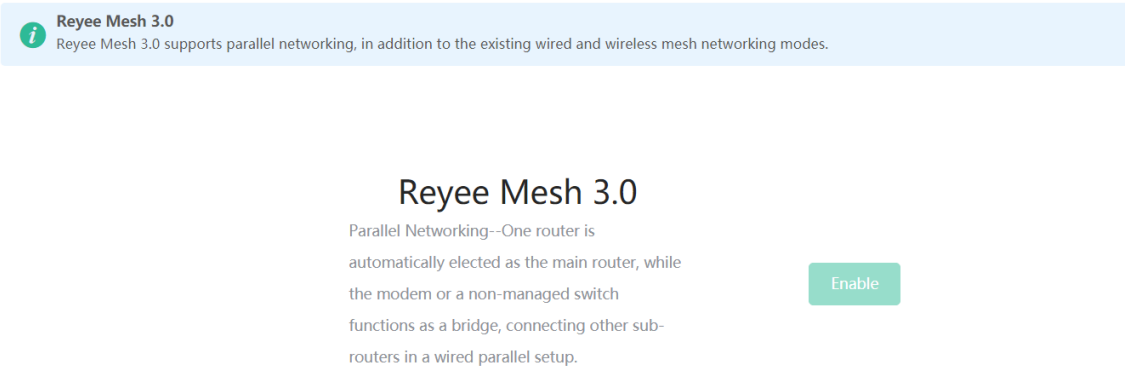


(6) On the master router page that is displayed, enter the password to log in.

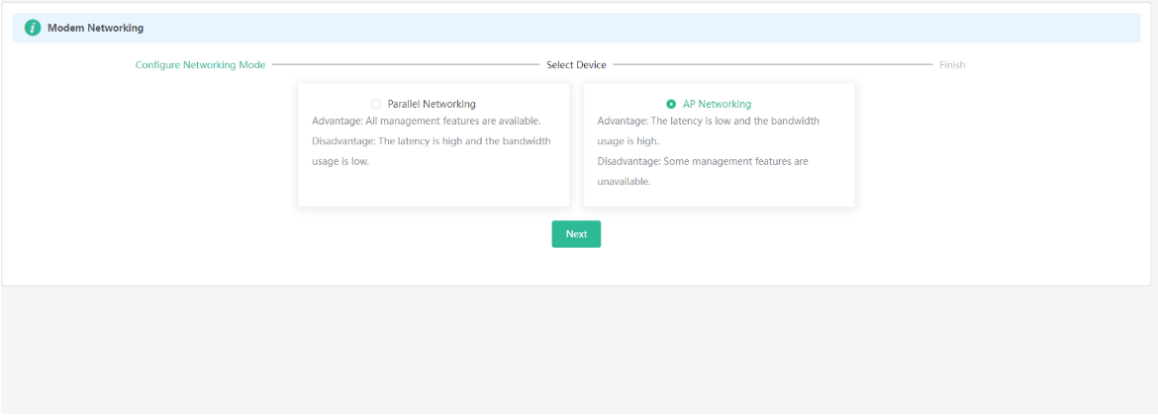
6.19.2 AP Networking

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

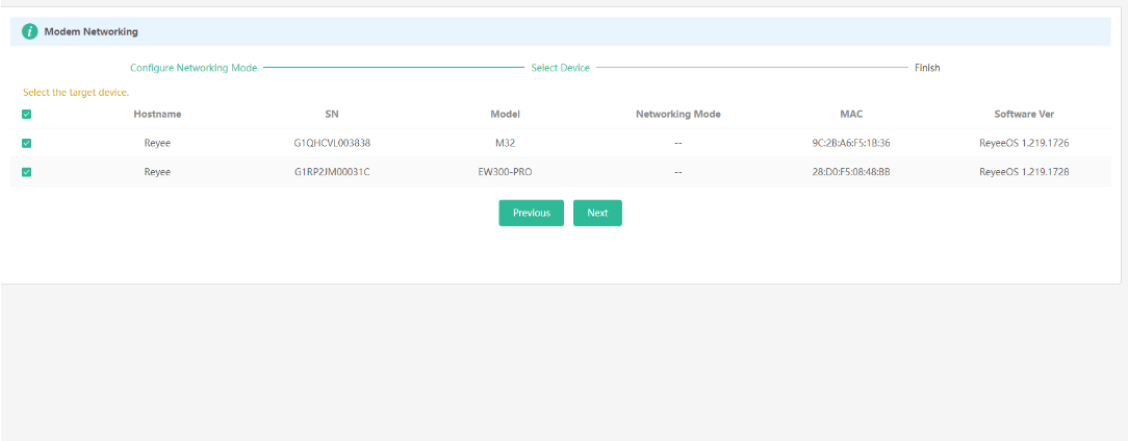
(1) Click **Enable** to enable Reyee Mesh 3.0.



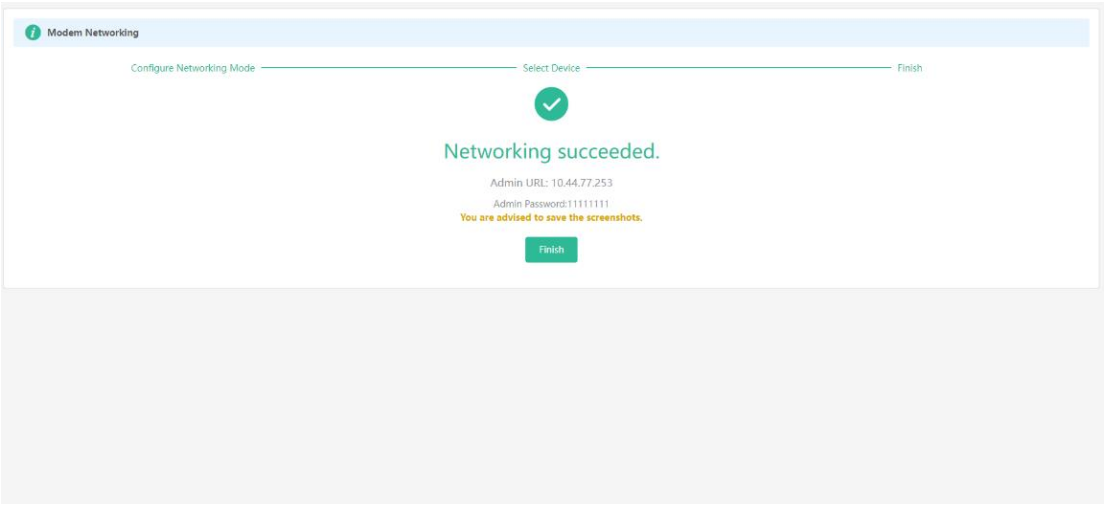
(2) Choose **AP networking**, and click **Next**.



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



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



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

6.20 Configuring UpnP

Caution

This feature is supported in router mode.

6.20.1 Overview

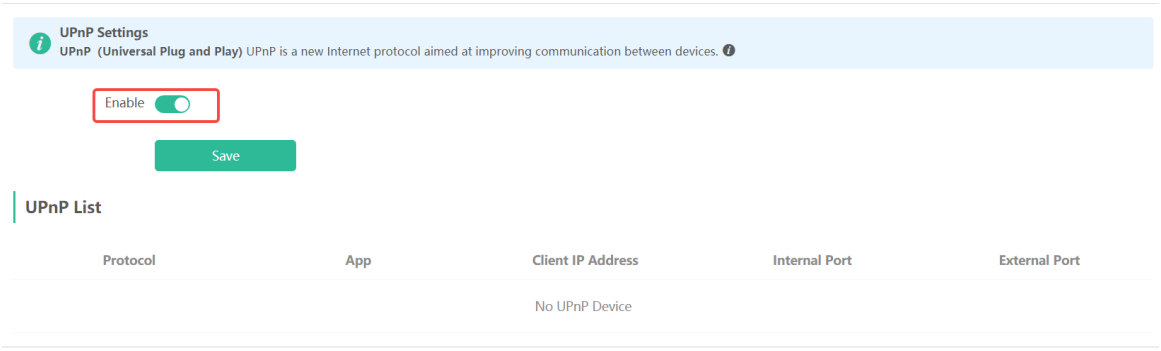
The universal plug and play (UPnP) function can map the port used by a client for Internet access according to the client's request so that related applications run faster or more stably. Common applications that support UPnP include MSN Messenger.

6.20.2 Configuration Steps

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

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

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



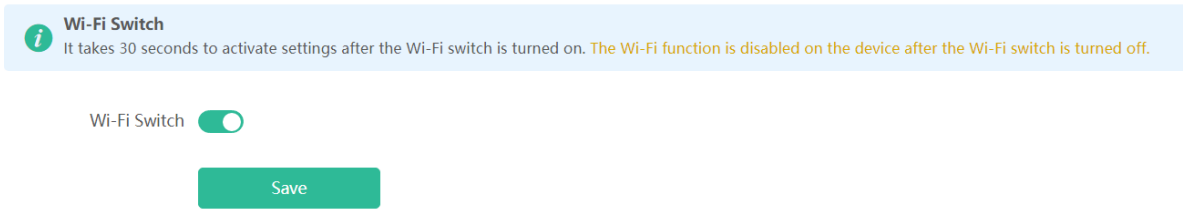
6.21 Enabling Wi-Fi Switch

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

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

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

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

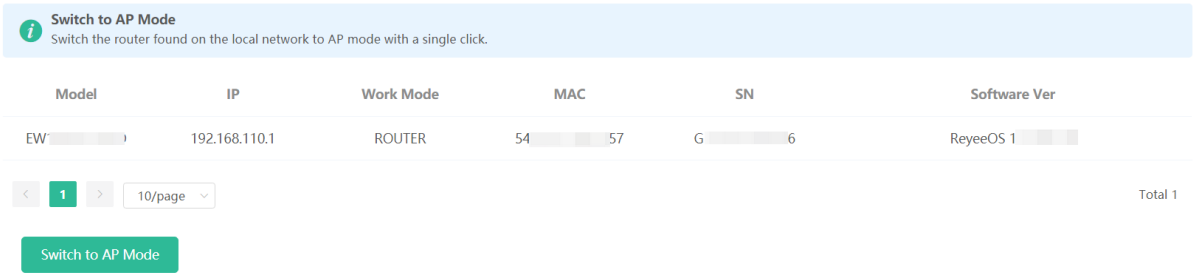


6.22 Switching to AP Mode

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

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

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



6.23 Configuring PPTP VPN

6.23.1 Overview

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

6.23.2 Configuring PPTP Server

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

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

1. Configuring PPTP Server

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

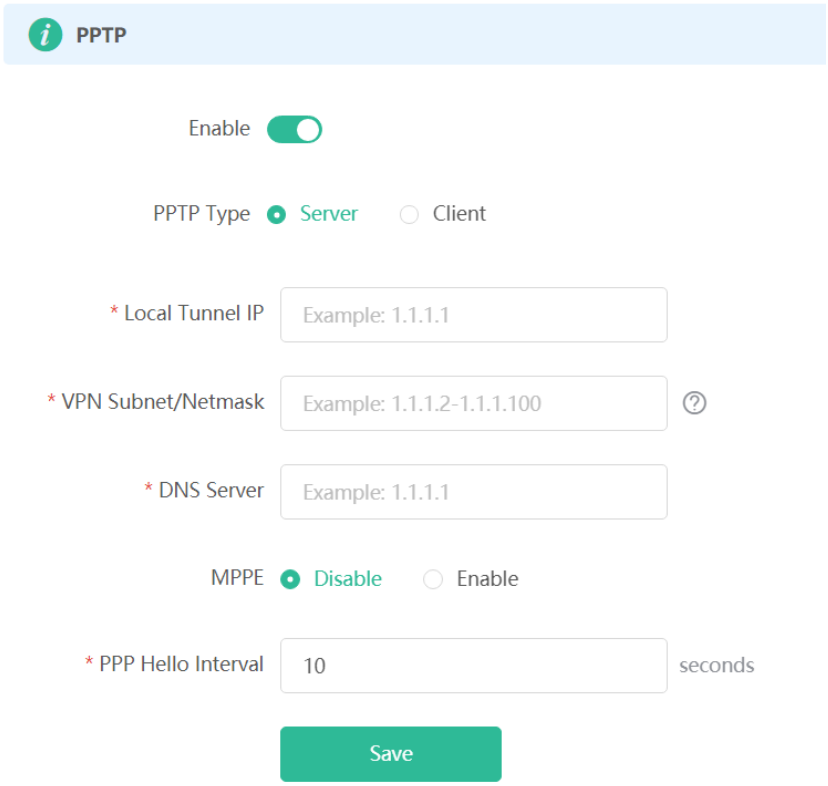
Local Tunnel IP: Enter the local address. It is used as the local virtual IP address of the VPN tunnel for the client to access the server after dialing in.

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

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

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

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



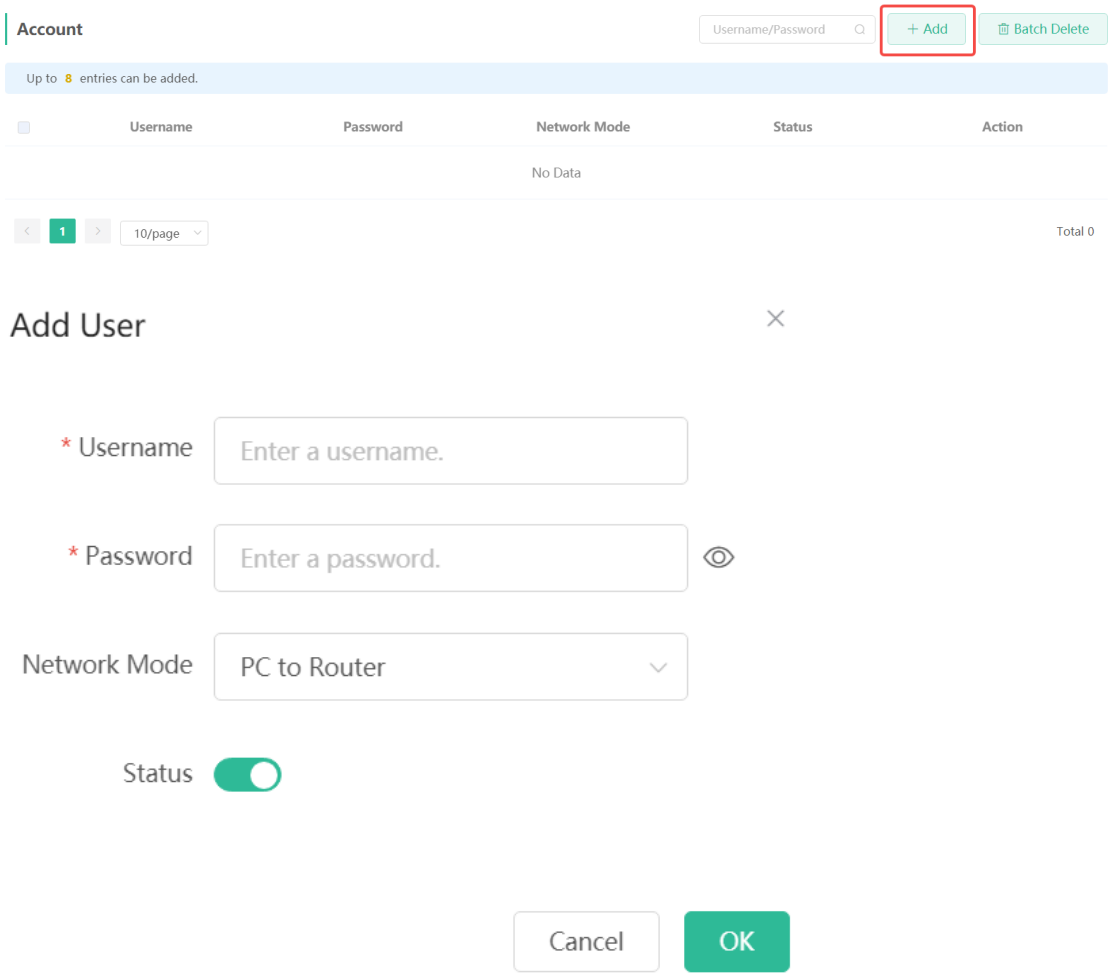
(2) Click **Save** and the device will receive and process the VPN request.

2. Add the PPTP user

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

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

Enable **Status** and click OK.



6.23.3 Configuring PPTP Client

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

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

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

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

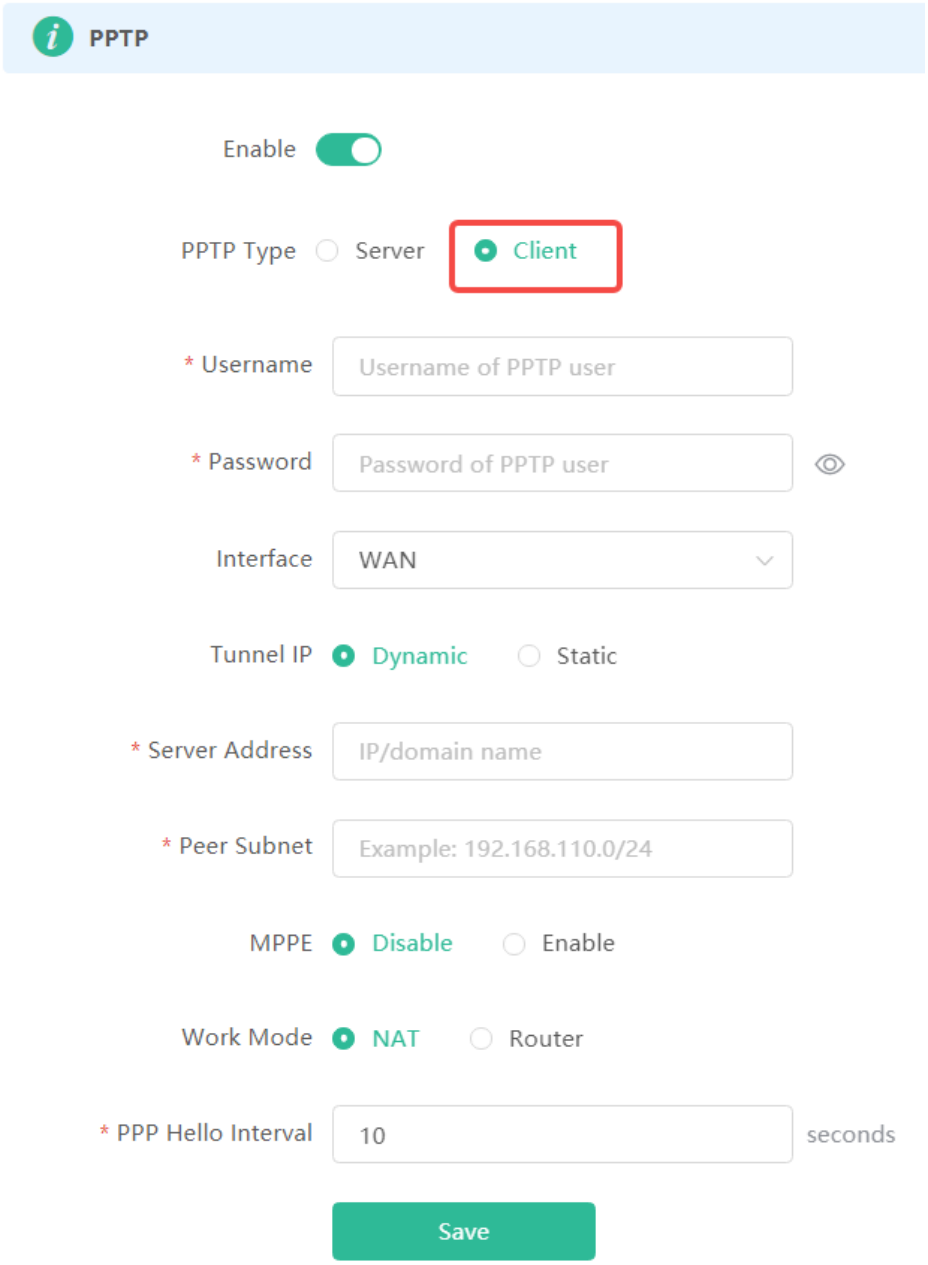
Server Address: Enter the WAN port IP address (the public IP is required) or the domain name of the server.

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

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

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

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



6.24 Configuring OpenVPN

6.24.1 Overview

OpenVPN can be used to establish a secure virtual private tunnel between different sites, or between a client and a site, allowing users to access the intranet over ISP networks. It is a VPN that enables layer 2 and layer 3

tunneling through virtual network cards, supporting various devices such as PCs, smartphones, and routers to establish VPN connections.

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

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

6.24.2 Configuring OpenVPN (Server Mode)

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

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

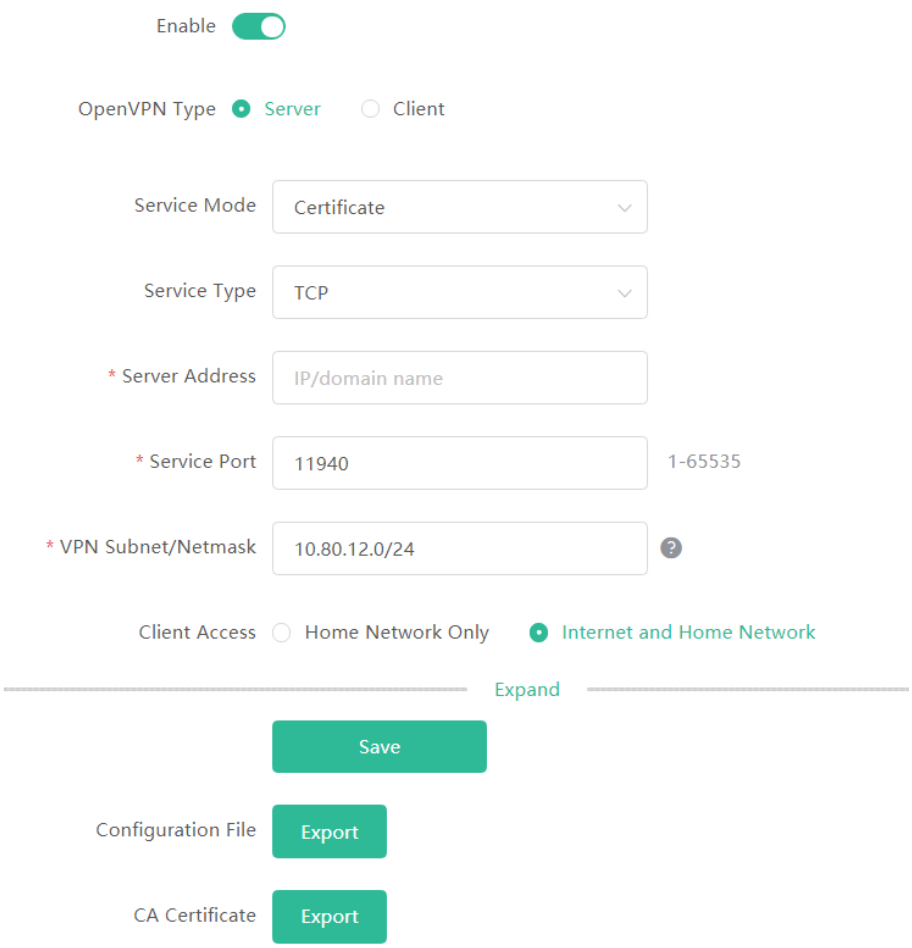
1. Configuring OpenVPN

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

(2) Select Server for the OpenVPN Type.

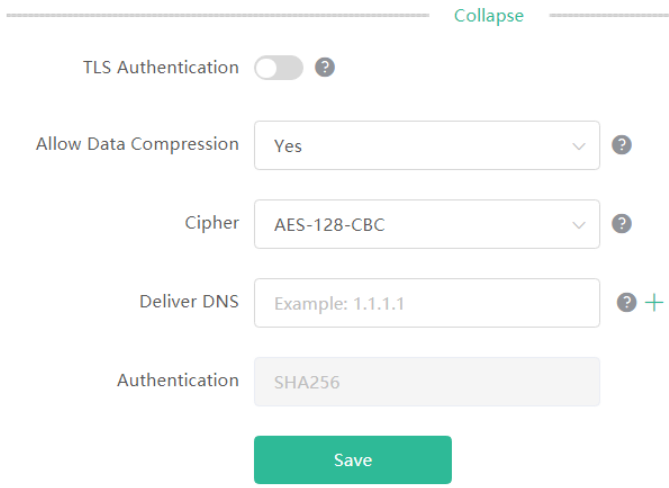
(3) Select the protocol, and enter the server address, port number and other information.

Figure 6-1 Configuring OpenVPN Server



(4) (Optional) Advanced settings.

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



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

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

Table 6-1 Configuration Items of OpenVPN Server Mode

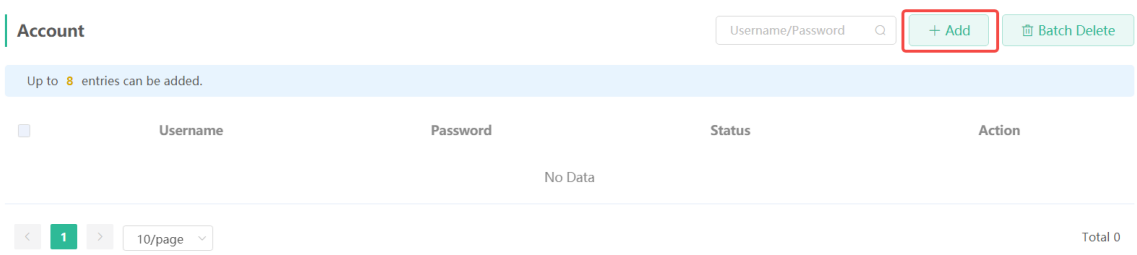
Item	Description
Service Mode	The device supports Account, Certificate and Account & Certificate authentication modes: ● Account mode: The correct account name, password, and CA certificate are required to connect to the server. The configuration is simple. ● Certificate mode: The client needs the correct CA certificate, client certificate, and pre-shared key to connect to the server. ● Account & Certificate mode: The client needs the correct account name, password, CA certificate, client certificate, and pre-shared key to connect to the server. This mode is suitable for scenarios with high security requirements.
Service Type	All communication on OpenVPN is based on a single IP port, using **UDP** or **TCP** protocols. The default value is UDP. You can select TCP for higher performance. TCP protocol can be used to improve the stability of VPN channels in high latency or unstable network conditions.
Server Address	The server address used for client docking, which can be a domain name.
Service Port	The port used by the OpenVPN service process. The official port assigned to OpenVPN is 1194. If the port is occupied or disabled on the local network, the server log will prompt a log indicating port binding failure. In this case, the port number needs to be changed.

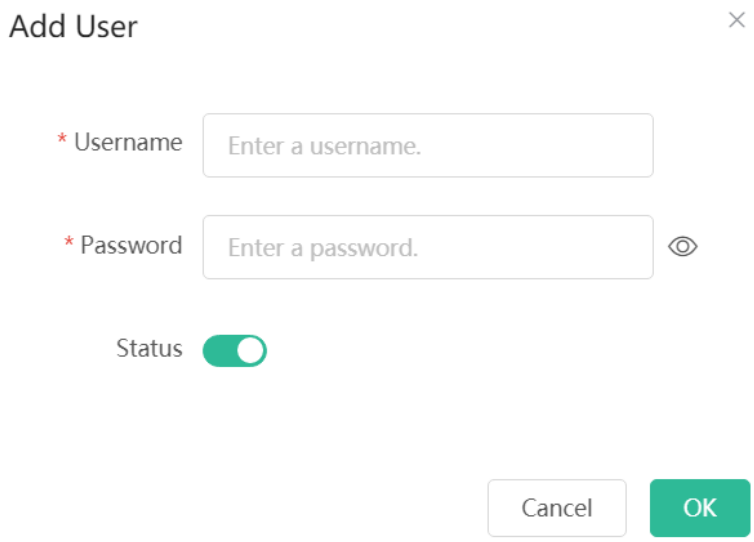
Item	Description
VPN Subnet/Netmask	The IP address pool delivered to VPN clients, in the form of a network segment. The first address in that segment is reserved by the server. For example, if 10.80.12.0/24 is set, then the VPN server address is 10.80.12.1.
Client Access	You can choose **Home Network Only** or **Internet and Home Network** ● **Home Network Only**: The client can only access the LAN segment on the server. ● **Internet and Home Network**: The client can access the LAN and WAN segments on the server. In this mode, all traffic from the client will be forwarded to the server.
TLS Authentication	TLS Authentication can enhance the security of OpenVPN. Once enabled, the client must import the TLS key. (The version of the peer OpenVPN client must be later than 2.40.)
Allow Data Compression	Once enabled, the device will compress the transmitted data to save bandwidth, but it will occupy a certain amount of CPU resources. This configuration must be consistent on the client and the server to avoid any potential connection failures.
Cipher	Encrypts the data to prevent it from being intercepted midway. The default encryption standard is AES-128-CBC. If the server is configured in auto mode, the client can be configured with any data encryption algorithm, which will be automatically matched by the server. If a specific encryption method is configured on the server, the client must be configured with the same encryption method. Otherwise, the connection between the server and the client cannot be established.
Deliver DNS	The information pushed by the server to the client's DNS. Currently only Windows clients are supported.
Authentication	The digest algorithm informed by the server to the client. The default value is SHA256.

2. Adding OpenVPN clients

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

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





6.24.3 Configuring OpenVPN (Client Mode)

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

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

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

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

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

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

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

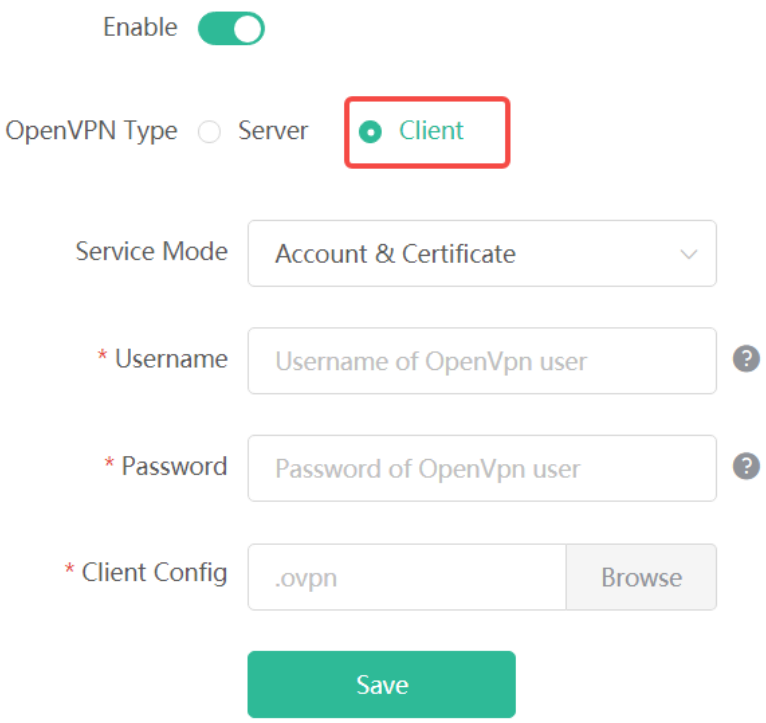


Table 6-2 Configuration Items of OpenVPN Client Web Setting Configuration Mode

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

6.24.4 Typical Configuration Example

1. Requirements

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

2. Topology

3. Notes

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

4. Configuring OpenVPN Server (Device A)

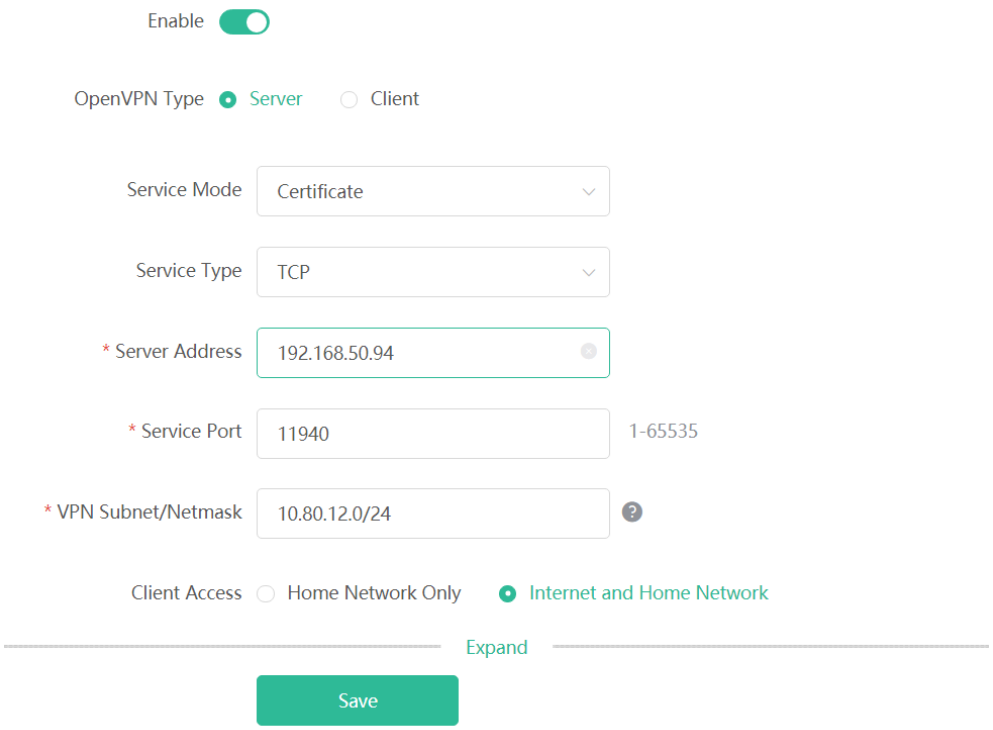
(1) Log in to the web interface of the router, and choose **VPN** > **OpenVPN**. Then, flip on the toggle switch next to **Enable** to enable the OpenVPN function. On the page that is displayed, enter the IP address of the WAN port as the service address, as well as other required parameters.

Use the default settings unless there are specific requirements.

Note

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

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

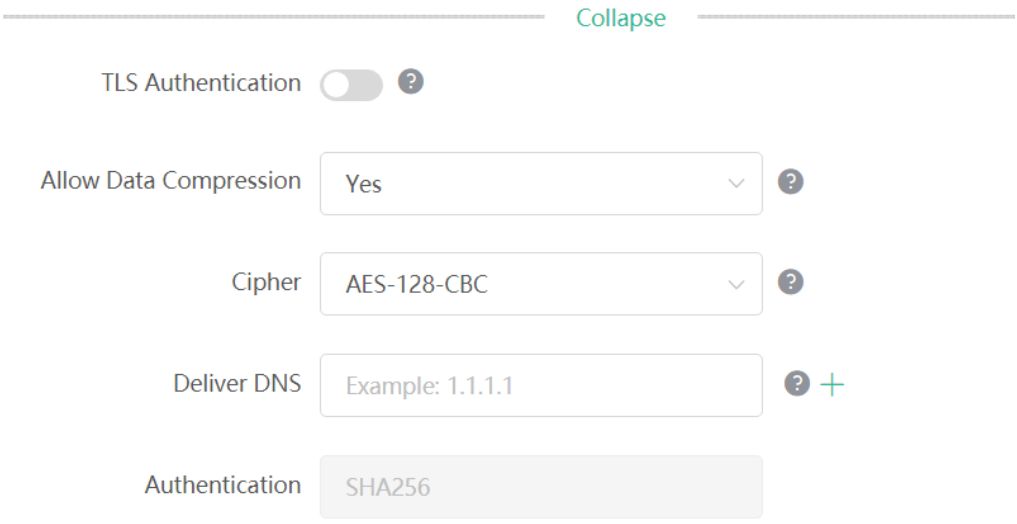


(2) Click **Save**. The OpenVPN settings are saved.

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

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

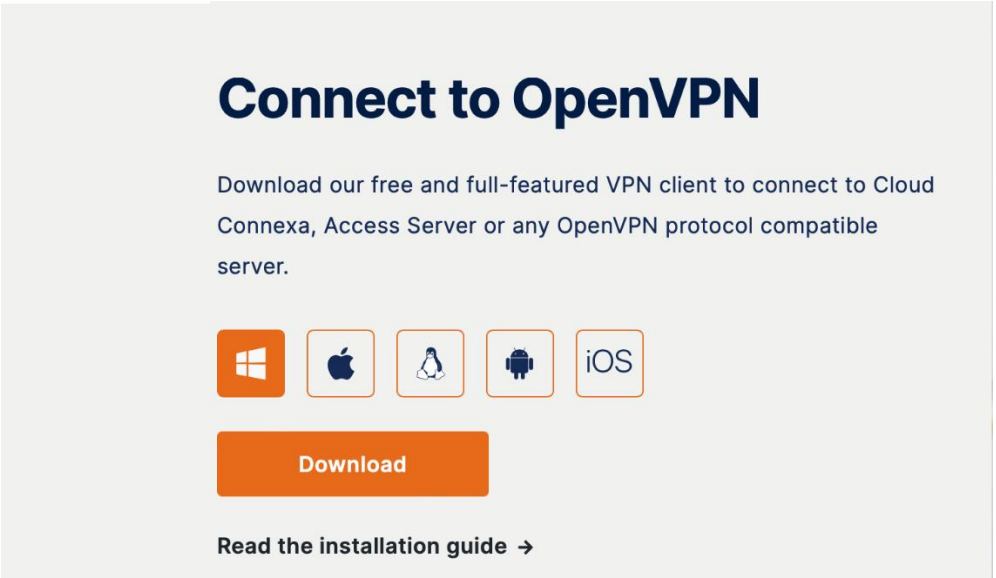
(4) Click **Expand** to show advanced settings. Use the default values unless there are specific requirements.



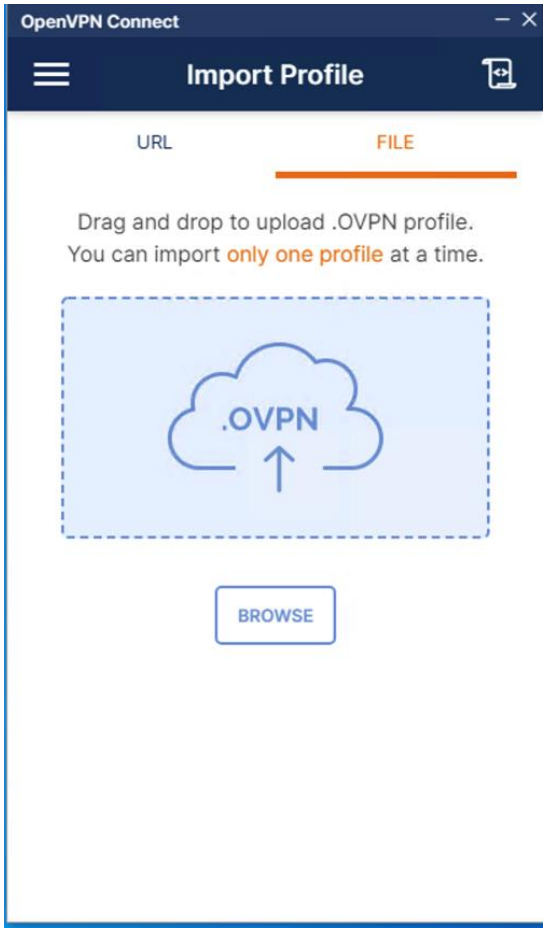
(5) Click **Export** next to **Configuration File** to export the .ovpn file which can be imported on the client side. Unless there are specific requirements, you do not need to export the CA certificate.

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

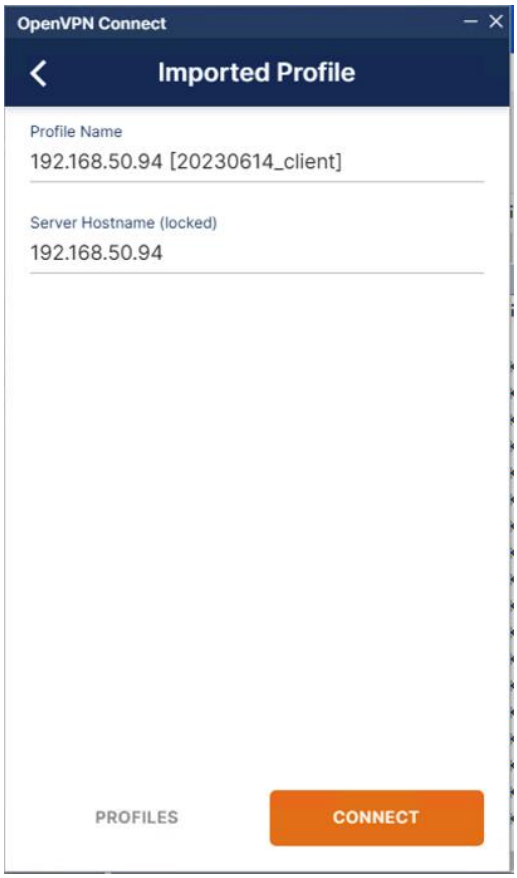
(1) Download the OpenVPN client (https://openvpn.net).



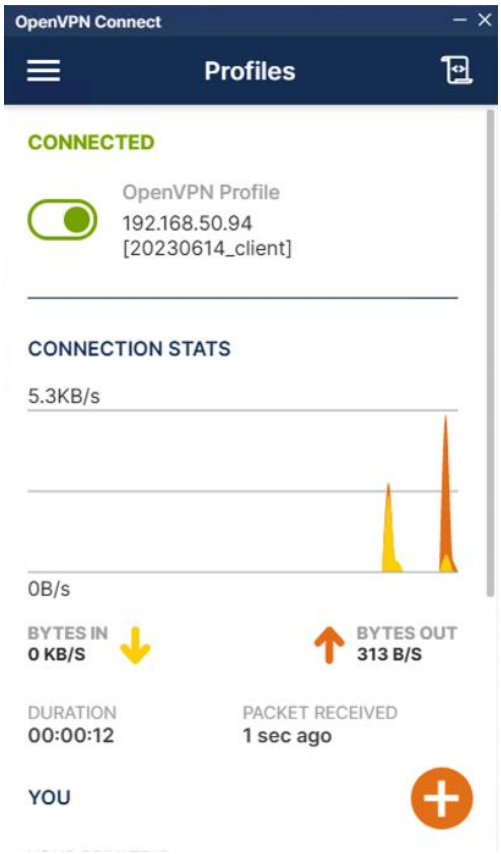
(2) Open the Windows OpenVPN client and choose the **File** tab.



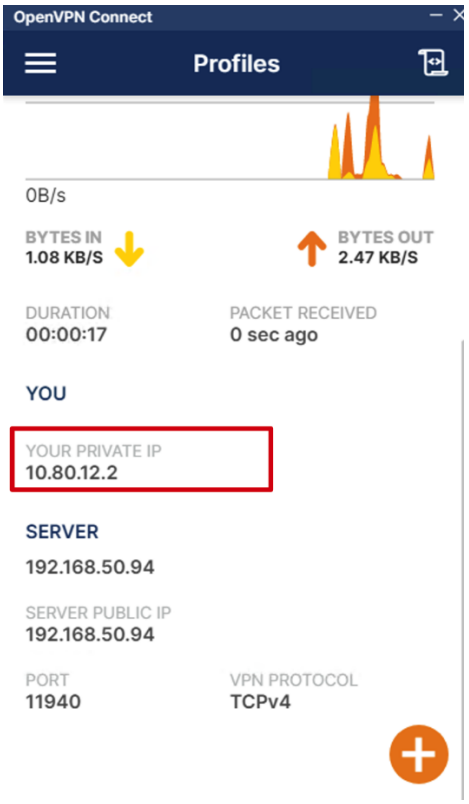
(3) Click **BROWSE** and select the .ovpn file exported from the server side.



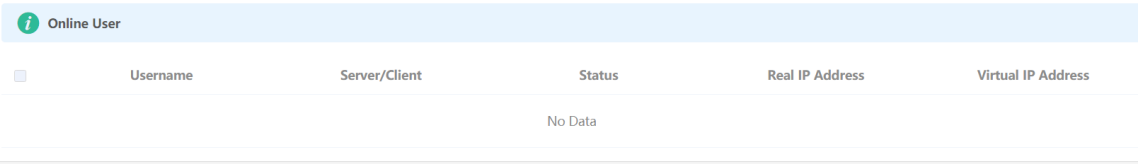
(4) Click **CONNECT** to connect to the OpenVPN server.



(5) Check the obtained virtual IP addresses.



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



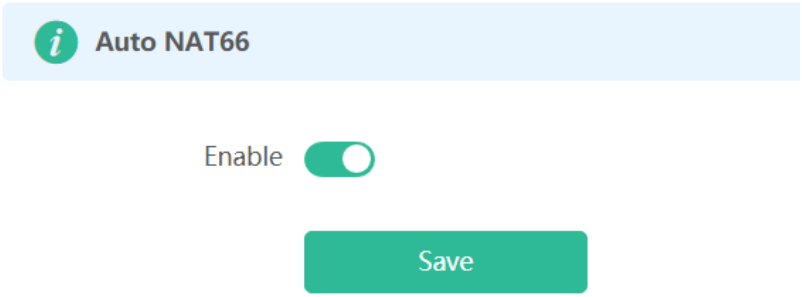
6.24.5 Configuring Auto NAT66

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

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

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

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



6.25 Other Settings

Caution

This feature is supported in router mode.

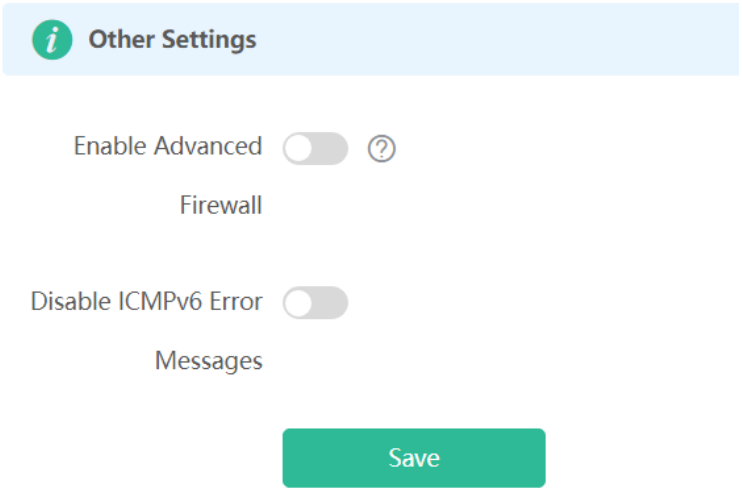
Smartphone View: Choose **More** > **Switch to PC view** > **More** > **Advanced** > **Other Settings**.

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

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

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

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



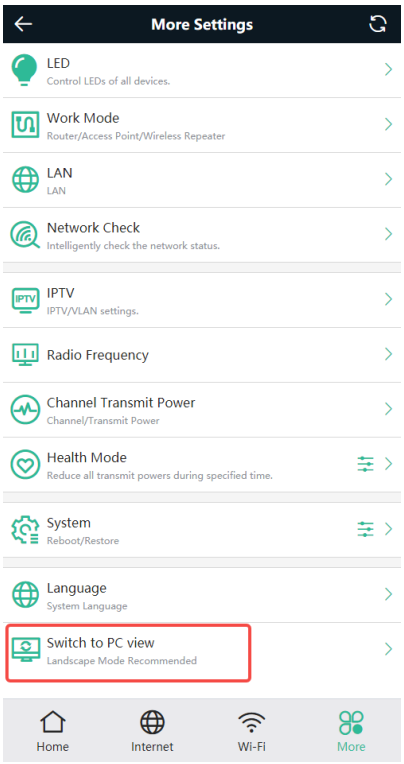
7 System Settings

7.1 Switching to PC View

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

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

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

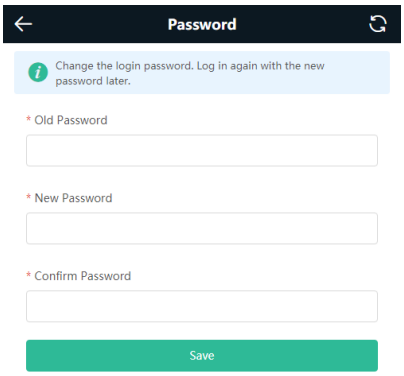


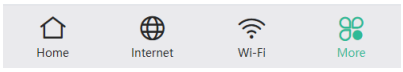
7.2 Configuring the Login Password

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

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

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





7.3 Remote Access

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

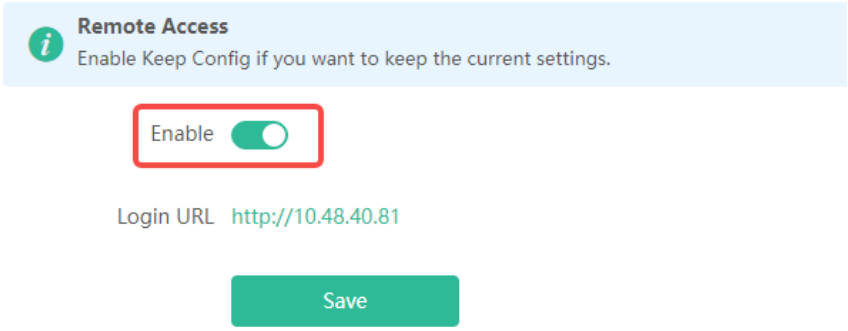
PC View: Choose **More** > **System** > **Login > Remote Access**.

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

Caution

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

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



7.4 Restoring Factory Settings

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

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

Click to enable **Keep Config** to retain the network configuration, Wi-Fi settings, time zone and other configurations after the router is restored to factory settings.

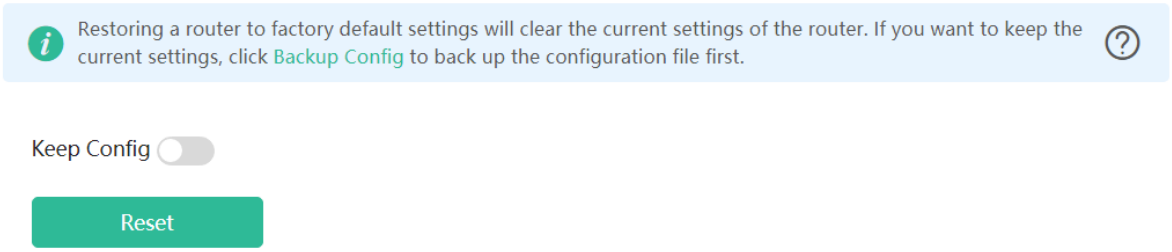
Click **Reset** to restore factory settings.

Caution

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

Note

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

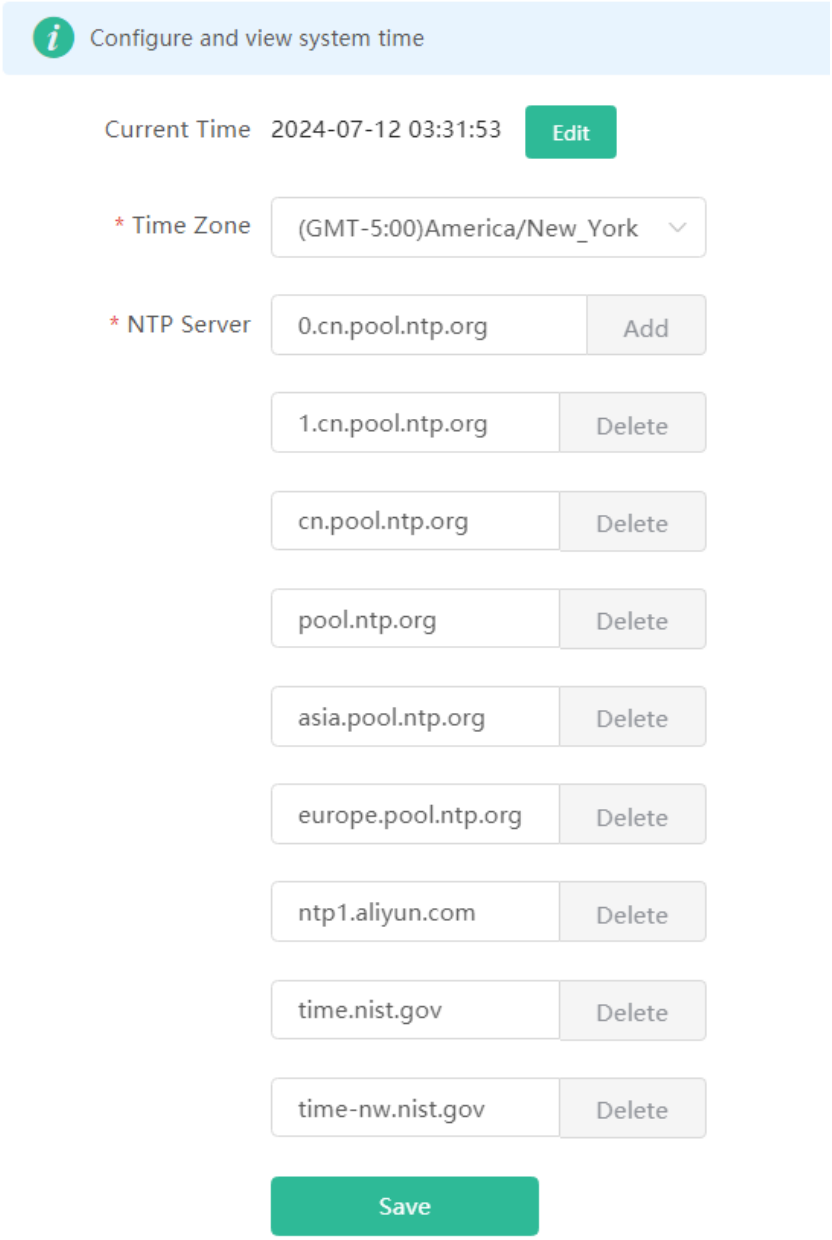


7.5 Configuring System Time

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

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

You can view the current system time. If the time is incorrect, check and select the local time zone. If the time zone is correct but time is still incorrect, click **Edit** to manually set the time. In addition, the router supports Network Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete local servers as required.



7.6 Configuring Scheduled Reboot

7.6.1 Getting Started

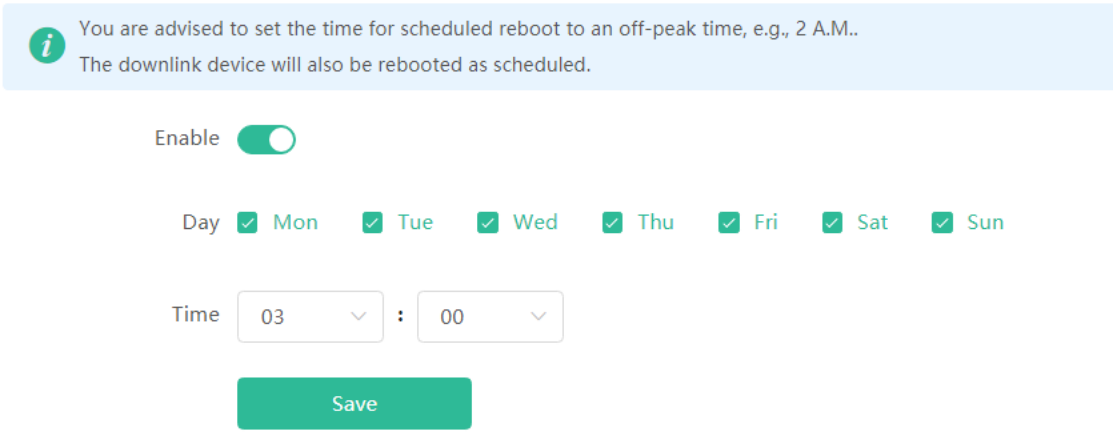
Confirm that the system time is accurate to avoid network interruption caused by device reboot at the wrong time. For details, see 7.5 Configuring System Time.

7.6.2 Configuration Steps

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

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

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



7.7 Performing Online Upgrade and Displaying the System Version

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

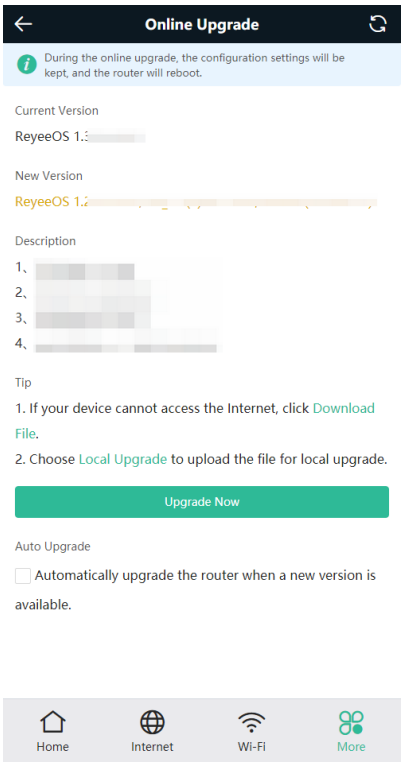
PC View: Choose **More** > **System** > **Upgrade** > **Online Upgrade**.

You can check the current system version. If there is a new version available, you can click it for an upgrade.

Caution

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

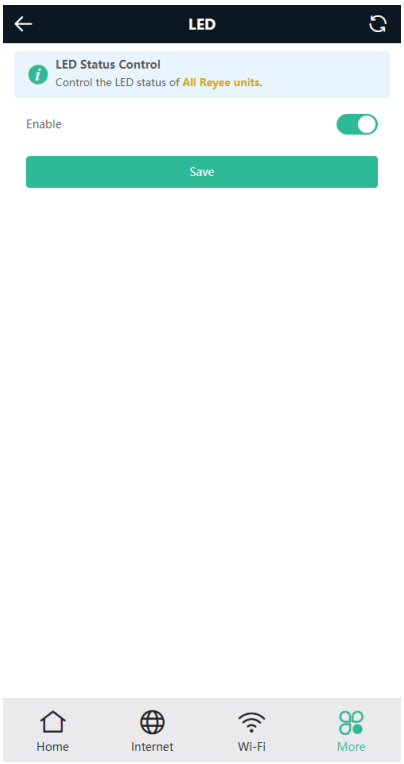
If no new version is detected and online upgrade cannot be performed, check whether the DNS is correctly obtained or go to **More** > **Advanced** > **Local DNS** to set the DNS server for the router.



7.8 Turning On/Off the Indicator

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

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

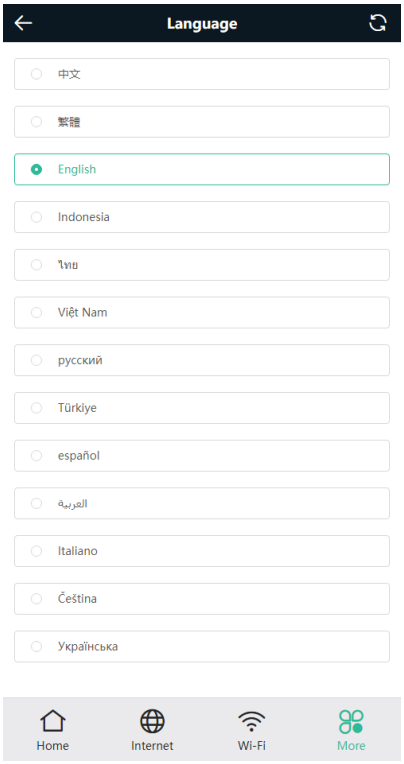


7.9 Switching System Language

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

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

Click a required language to switch the system language.

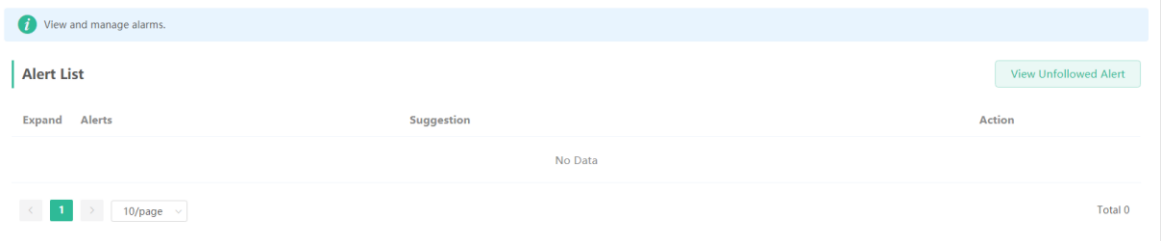


7.10 Enabling Alerts

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

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

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



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

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

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

Table 7-1 Alerts and Suggested Action

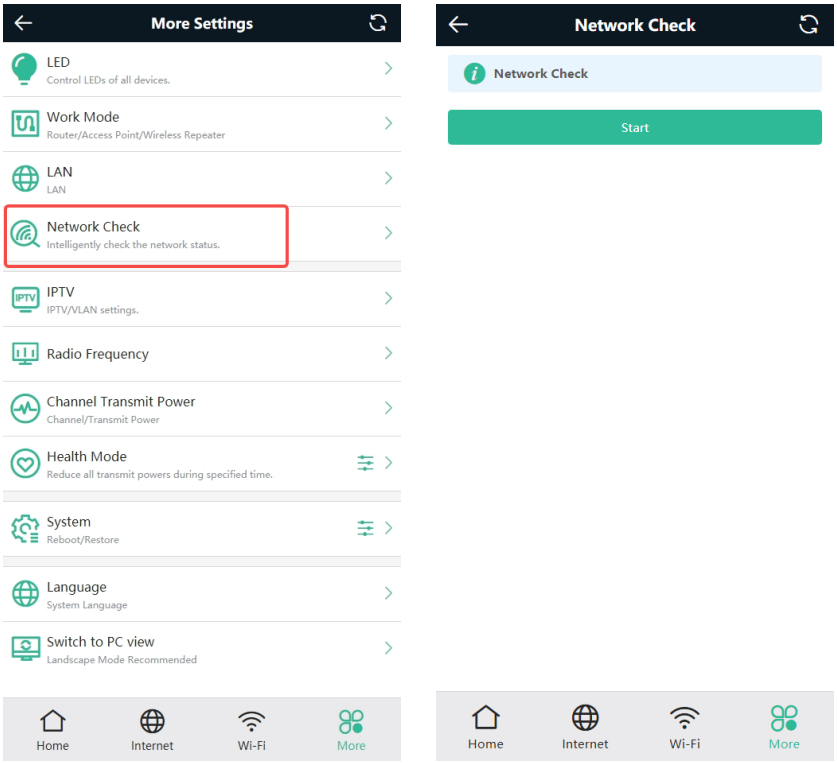
Alerts	Suggested Action
The WAN port has no link.	Please check whether a cable is plugged into the WAN port.
The port is operating at 10Mbps.	Please check the peer port settings, unplug and re-plug the cable, or replace the cable.
There is more than one DHCP server in the LAN network.	Please disable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

7.11 Diagnosing Network Problems

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

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

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



7.12 Network Diagnosis Tools

1. Network Test Tool

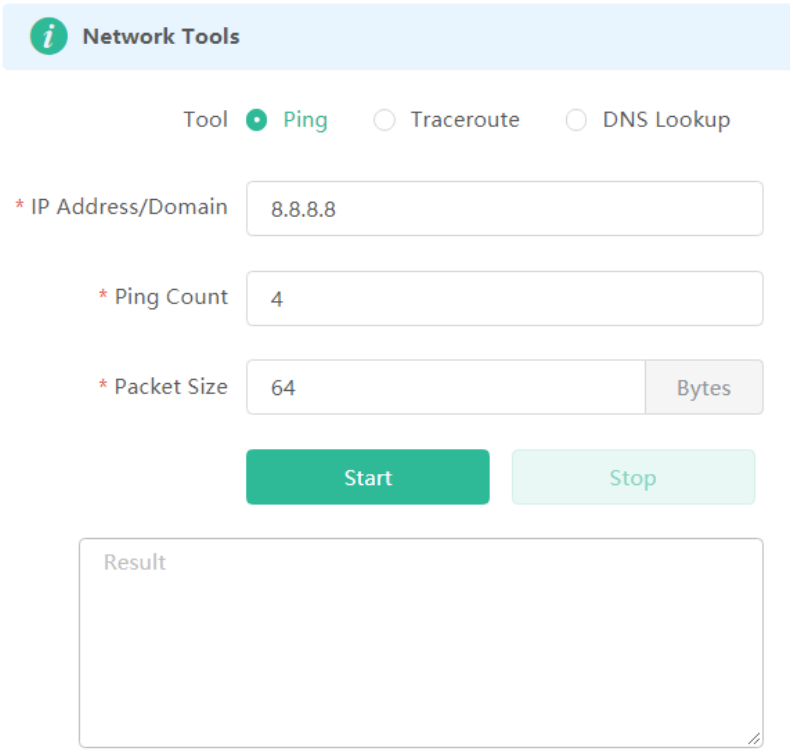
Smartphone View: Choose **More** > **System** > **Network Tools**.

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

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

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

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



2. Packet Capture Tool

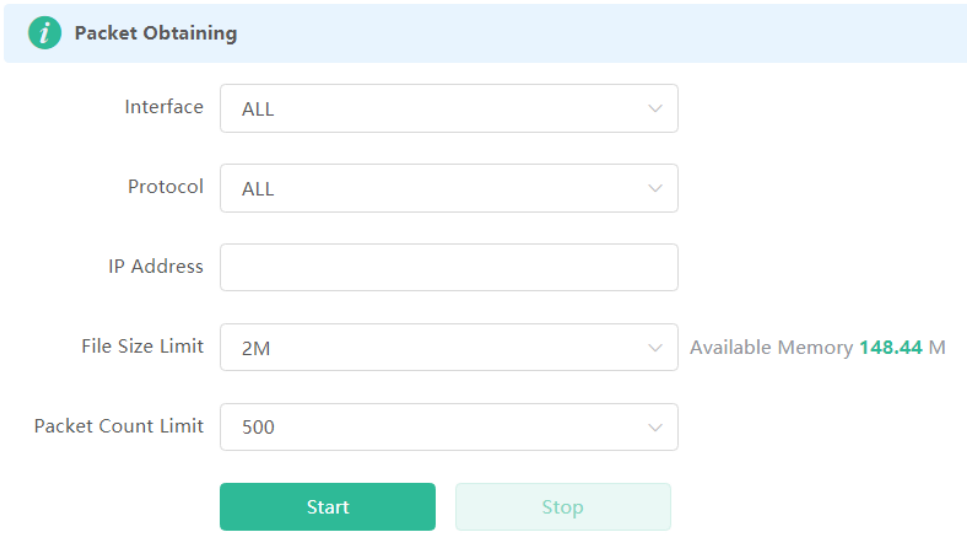
Smartphone View: Choose **More** > **Switch to PC view** > **More** > **Diagnostics** > **Packet Obtaining.**

PC View: Choose **More** > **Diagnostics** > **Packet Obtaining**

Set the interface, protocol, and IP address whose packets need to be captured, file size limit, and packet count limit to limit the volume of packets captured. Click **Start**. Packet Obtaining can be stopped at any time and a link to the generated file is generated. You can use Wireshark and other analysis software to open and view the file.

Caution

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



Note

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

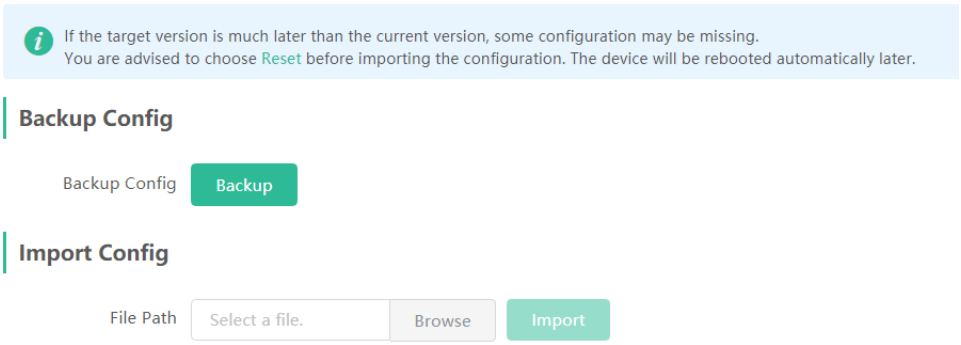
7.13 Configuring Backup and Import

Smartphone View: Choose **More** > **Switch to PC view** > **More** > **System** > **Management**. >**Backup & Import**

PC View: Choose **More** > **System** > **Management**. >**Backup & Import**

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

Configure import: Click **Browse**, select a configuration file backup on the local PC, and click **Import** to import the configuration file. The device will restart.

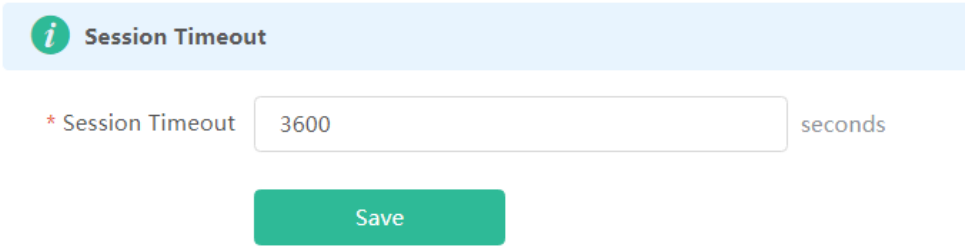


7.14 Configuring Session Timeout Duration

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

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

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



8 FAQs

8.1 How Do I Restore the Router to Factory Settings?

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

8.2 What Should I Do If I Forgot the Password?

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

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

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

If you are unable to access the router's web interface using the default IP address, you can use the alternative methods specified in 3.4 Manage the Device after Successful.

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

Restore the router to factory settings and power on it again.

If the system LED still fails to turn solid on, you can contact us through the following channels:

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