

Ruijie Reyee RG-EW3000GX Wi-Fi Router

ReyeeOS 1.308 Configuration Guide



Document Version: V1.1 Date: 2024-09-30 Copyright © 2024 Ruijie Networks

Copyright

Copyright © 2024 Ruijie Networks

All rights are reserved in this document and this statement.

Any reproduction, excerption, backup, modification, transmission, translation, or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

Reyce and other Ruijie networks logos are trademarks of Ruijie Networks.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

Disclaimer

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

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

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

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

Preface

Technical Support

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

Conventions

1. GUI Symbols

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

2. Signs

The signs used in this document are described as follows:

💋 Danger

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

Warning

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

🛕 Caution

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

🚺 Note

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

Specification

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

3. Note

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

Contents

PrefaceI
1 Change Description1
1.1 ReyeeOS 1.3081
1.1.1 Hardware Change1
1.1.2 Software Feature Change1
2 Quick Setup (As a Primary Router)
2.1 Getting Started3
2.2 Connecting to the Router
2.3 Logging In4
2.4 Configuration Steps5
2.4.1 Configuring the Internet Connection Type5
2.4.2 Configuring a Wi-Fi Network9
2.4.3 Configuring IoT Wi-Fi12
3 Quick Setup (As a Secondary Router)14
3.1 Getting Started14
3.2 Connecting to Primary Router14
3.2.1 Wired Connection14
3.2.2 Wireless Connection15
3.3 Verification and Testing27
3.4 Manage the Device after Successful Setup27
4 Wi-Fi Network Settings
4.1 Changing the SSID and Password29
4.2 Enabling Band Steering

4.3 Hiding the SSID	
4.3.1 Overview	
4.3.2 Getting Started	
4.3.3 Configuration Steps	
4.4 Adding Wi-Fi Networks	31
4.4.1 Adding Game Wi-Fi Network	
4.4.2 Adding Other Types of Wi-Fi Networks	
4.5 Configuring the Wi-Fi Blocklist or Allowlist	
4.5.1 Overview	
4.5.2 Configuration Steps	
4.6 Optimizing the Wi-Fi Network	
4.6.1 Overview	
4.6.2 Getting Started	
4.6.3 Configuration Steps	
4.7 Configuring the Healthy Mode	40
4.8 Enabling Roaming Optimization	41
5 Configuring Work Mode	42
5.1 Access Point	42
5.2 Wireless Repeater	43
5.3 WISP	45
6 Configuring Network Settings	49
6.1 Configuring Internet Connection Types	49
6.2 Configuring WAN Settings	49
6.3 Changing the Address of a LAN Port	57

6.4 Connecting to IPTV	8
6.4.1 Getting Started58	8
6.4.2 IPTV Configuration Steps (VLAN Type)58	8
6.4.3 IPTV Configuration Steps (IGMP Type)59	9
6.5 Configuring Wi-Fi/IGMP	0
6.5.1 Overview	0
6.5.2 Configuration Steps	0
6.6 Configuring IPv6	0
6.6.1 Configuring the IPv6 of the WAN Port6	1
6.6.2 Configuring the IPv6 of the LAN Port6	1
6.7 Configuring Auto Bandwidth Control	3
6.8 Enabling Parental Control	5
6.8.1 Setting the Internet Block Periods6	7
6.8.2 Disabling Parental Control	8
6.9 Configuring DHCP Server	9
6.9.1 Overview	9
6.9.2 Configuration Steps69	9
6.10 Configuring DNS Server	1
6.10.1 Local DNS Server	1
6.10.2 Configuring DNS Proxy72	2
6.11 Configuring Port Mapping7	3
6.11.1 Overview	3
6.11.2 Getting Started73	3
6.11.3 Configuration Steps73	3

6.11.4 Verification and Testing75
6.11.5 Solution to a Test Failure75
6.11.6 DMZ Configuration Steps75
6.12 Configuring DDNS76
6.12.1 Overview
6.12.2 Getting Started76
6.12.3 Configuration Steps76
6.13 Configuring Connectivity Detection77
6.14 Enabling CWMP78
6.15 Configuring APR Binding
6.15.1 Overview
6.15.2 Configuration Steps79
6.16 Configuring Static Routing
6.17 Policy-based Routing
6.18 Enabling Smart Flow Control
6.19 Enabling Port-Based Flow Control85
6.20 Enabling Hardware Acceleration
6.21 Enabling Reyee Mesh87
6.22 Configuring Reyee Mesh 3.087
6.22.1 Parallel Networking88
6.22.2 AP Networking
6.23 Configuring UpnP91
6.23.1 Overview
6.23.2 Configuration Steps91

6.24 Enabling Wi-Fi Switch	
6.25 Switching to AP Mode	92
6.26 Configuring PPTP VPN	93
6.26.1 Overview	93
6.26.2 Configuring PPTP Server	93
6.26.3 Configuring PPTP Client	95
6.27 Configuring OpenVPN	96
6.27.1 Overview	96
6.27.2 Configuring OpenVPN (Server Mode)	96
6.27.3 Configuring OpenVPN (Client Mode)	100
6.27.4 Typical Configuration Example	101
6.27.5 Configuring Auto NAT66	
6.28 Other Settings	
6.28 Other Settings7 System Settings	
	108
7 System Settings	108
7 System Settings 7.1 Switching to PC View	108 108 108
 7 System Settings 7.1 Switching to PC View 7.2 Configuring the Login Password 	
 7 System Settings 7.1 Switching to PC View 7.2 Configuring the Login Password 7.3 Remote Access 	
 7 System Settings 7.1 Switching to PC View 7.2 Configuring the Login Password 7.3 Remote Access 7.4 Restoring Factory Settings 	
 7 System Settings 7.1 Switching to PC View 7.2 Configuring the Login Password 7.3 Remote Access 7.4 Restoring Factory Settings 7.5 Configuring System Time 	
 7 System Settings 7.1 Switching to PC View 7.2 Configuring the Login Password 7.3 Remote Access	
 7 System Settings 7.1 Switching to PC View 7.2 Configuring the Login Password 7.3 Remote Access 7.4 Restoring Factory Settings 7.5 Configuring System Time 7.6 Configuring Scheduled Reboot 7.6.1 Getting Started 	

	7.9 Switching System Language113
	7.10 Enabling Alerts114
	7.11 Diagnosing Network Problems116
	7.12 Network Diagnosis Tools
	7.13 Configuring Backup and Import119
	7.14 Configuring Session Timeout Duration120
8	FAQs121
	8.1 How Do I Restore the Router to Factory Settings?
	8.2 What Should I Do If I Forgot the Password?121
	8.3 How Do I Manage the Router When Used As a Range Extender After Installation is
	Successful?
	8.4 What Should I Do If the System LED Keeps Flashing After the Router is Powered On?121

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-EW3000GX	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 <u>2.4.1</u> 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.

Add		
* Name		
Preferred Server	HTTP ~	
Protocol	ТСР 🗸	
External IP Address	Default: WAN IP address.	
* External Port/Range	Example: X or X-X (Range: 1-655.	
* Internal Server IP		
* Internal Port/Range	80	
	Cancel	ОК

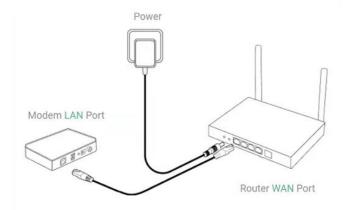
After the change: Port mapping now can be configured for a selected WAN interface. For details, see Section
 <u>6.11</u> Configuring Port Mapping.

Add		×
* Name		
Preferred Server	HTTP ~	
Protocol	тср 🗸	
External IP Address	WAN port O Enter/Select an IP WAN ✓	
• External Port/Range	Example: X or X-X (Range: 1-65535)	
* Internal Server IP		
* Internal Port/Range	80	
	Cancel	

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: <u>192.168.110.1</u>) or <u>https://192.168.110.1</u> 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.

C 🔺 Not secure)	Neps://192.168.110.1	A* 18 (
	٨	
	Your connection isn't private	
	Attackers might be trying to steal your information from 192.16 passwords, messages, or credit cards).	8.110.1 (for example,
	NET:ERR_CERT_AUTHORITY_INVALID	
	Hide advanced	Go back
	This server couldn't prove that it's 192.168.110.1 ; its security trusted by your computer's operating system. This may be c misconfiguration or an attacker intercepting your connection	aused by a
	Continue to 192.168.110.1 (unsafe)	

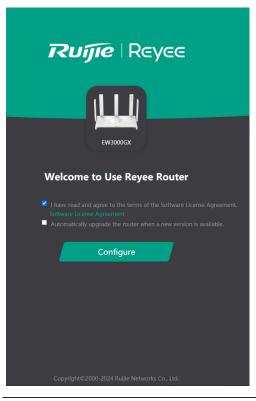
• If you forget your password and enter the incorrect password to log in, you will need to wait for 10 minutes after each 10 unsuccessful attempts.

Log In
Forgot Password? English V

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.

Internet		
Internet Cor	nnection Type:	DHCP Recommended C
DHCP		
\odot		
IP 192.168.111		
Subnet Mas 255.255.255		
Gateway 192.168.111		
DNS Server 192.168.111		
0	evious	Next

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

	ernet	
nternet Connection Type:	DHCP Recommende	d 😋
РРРОЕ		
Username		
Password		
Service Name		
(Optional) Provided by ISP		
Dotain the username and passw		

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

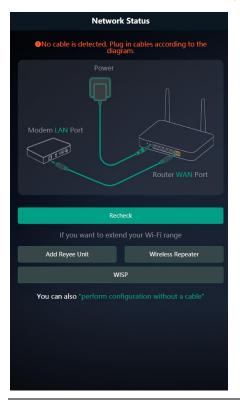
Internet		
nternet Connection Type:	DHCP Recommended C	
Static IP		
IP		
192.168.111.19		
Subnet Mask		
255.255.255.0		
Gateway		
192.168.111.1		
DNS Server		
192.168.111.1		

- 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.

Inte	ernet	Internet	
Internet Connection Type:	DHCP Recommended C	DHCP Reco Internet Connection Type:	mmended 🕃
L2TP	~	L2TP	
IP Type DHCP Static IP		IP Type DHCP Static IP	
* Username		* Username	
		Username	
* Password		* Password	
	***	Password	
* Server IP/Domain Name		* Server IP/Domain Name	
		Server IP/Domain Name	
		* IP	
		192.168.111.19	
		* Subnet Mask	
		255.255.255.0	
		* Gateway	
		192.168.111.1	
		DNS Server	
		192.168.111.1	
Previous	Next	Previous	Vext

1 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.

Wi-Fi Settings	
Dual-Band Single SSID A shared SSID for both the 2.4 GHz and 5 GHz Wi-Fi networks.	
2.4G Wi-Fi Large Coverage & Slow Rate	
* SSID @Ruijie-s9976	
Do you want to use the Wi-Fi password as the manage password?	gement Cancel
SG WI-FI Small Coverage & Fast Rate * SSID	
@Ruijie-s9976_5G Security	
WPA/WPA2-PSK	
Previous Next	**

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

Wi-Fi Settings	
Dual-Band Single SSID A shared SSID for both the 2.4 GHz and 5 GHz Wi-Fi networks.	
2.4G Wi-Fi	
Large Coverage & Slow Rate	
* SSID	
@Ruijie-s9976	
Security	
WPA/WPA2-PSK	
* Wi-Fi Password	
5G Wi-Fi	
Small Coverage & Fast Rate	
* SSID	
@Ruijie-s9976_5G	
Security	
WPA/WPA2-PSK	
AUCEN I	
Previous Next	

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

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

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, 5G Wi-Fi, and Game Wi-Fi networks. Set an SSID for the 2.4G Wi-Fi, 5G Wi-Fi and Game Wi-Fi networks, 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.

🚺 Note

A separate password can be set for the Game Wi-Fi network on the web interface.

- 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.

Game Wi-Fi	
A dedicated game Wi-Fi network for enhancing ga	ming experience.
* SSID	
@Ruijie-s9976_Game	
Security	
WPA/WPA2-PSK	
* Wi-Fi Password	
Enter 8-63 characters.	
Management Password	
Same as Wi-Fi Password	
Management Password:	
Country/Region/Time Zone	~
* Country/Region	
United States (US)	
* Time Zone	
(GMT-5:00)America/New_York	
Previous	Next

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

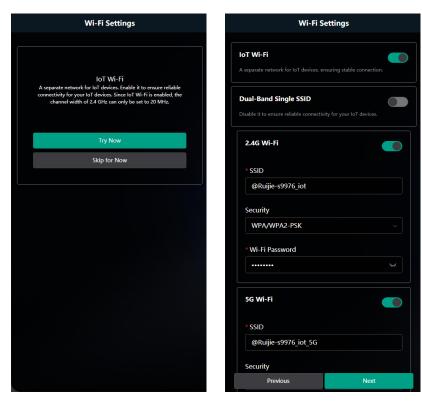
2.4.3 Configuring IoT Wi-Fi

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

1 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.

Finish
Setup successful. Reconnect to your Wi-Fi network to enjoy the Internet.
Management Password: 111111111
SSID: @Ruijie-59976 2.46 Wi-Fi Password: 11111111 SSID: @Ruijie-59976_56 56 Wi-Fi Password: 11111111
SSID: @Ruijie-s9976_Game Game Wi-Fi Password: 111111111
Scan the QR code to download the app. • Quick and easy setup • Infuitive management • Intelligent fault diagnosis

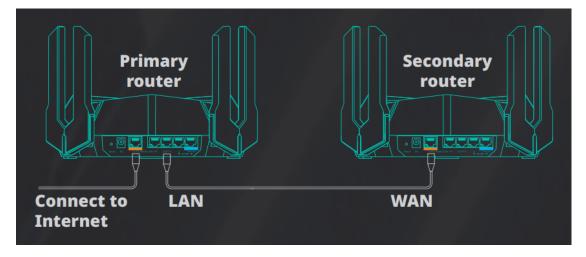
3 Quick Setup (As a Secondary Router)

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.

A 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 <u>2.2</u> Connecting to the <u>Router</u> and <u>2.3</u> Logging In.

Click Configure.

	Network S	itatus
Ruíjie Reyce	•No cable is detected. Plug in diagram	n cables according to the n.
- · ·	Power	
EW3000GX	Modem LAN Port	
Welcome to Use Reyee Router		Router WAN Port
I have read and agree to the terms of the Software License Agreement. Software License Agreement	Rechec	k.
Automatically upgrade the router when a new version is available.	If you want to extend	your Wi-Fi range
Configure	Add Reyee Unit	Wireless Repeater
	WISP	
	You can also *perform config	uration without a cable"
Copyright©2000-2024 Ruijie Networks Co., Ltd.		

- 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.

← Scan	Repeater Mode ~	Enter Pass	word (1/4)
Q SSID Filtering	G		
5G @Ruijie-s0356		Primary Router Wi-Fi passwo	ord
sg @Ruijie-s0356_Game		Primary Router SSID	
2.4G @Ruijie-s0356		@Ruijie-s0356	
2.4G 1		* Password Ruijie123	•
24G @Ruijie-s0848		Kujie 123	
Other Networks		Please ensure that the pass	word entered is correct.
		Previous	Next

(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.

Set Wi-Fi (2/	/4)
Local Router Wi-Fi	
Same as Primary Router Wi-Fi	
* SSID (2.4G)	
Do you want to use the Wi-Fi passwo password?	ord as the management OK Cancel
Same as Wi-Fi Password	
Sume as within assistera	
* Management Password	

- (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.

Set Wi-Fi (2/4)		
Local Router Wi-Fi		
Same as Primary Router Wi-Fi		
* SSID (2.4G)		
* SSID (5G)		
Wi-Fi Password		
Management Password		
Same as Wi-Fi Password		
Strong		
Previous Next		

(4) Configuring IoT Wi-Fi

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

1 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.

loT Wi-Fi (3/4)	loT Wi-Fi (3/4)
loT Wi-Fi	IoT WI-FI A separate network for IoT devices, ensuring stable connection.
A separate network for IoT devices. Enable it to ensure reliable connectivity for your IoT devices.	Dual-Band Single SSID Disable it to ensure reliable connectivity for your IoT devices.
Try Now	
Skip for Now	2.4G Wi-Fi
	* SSID
	@Ruijie-s0356_iot
	Security
	WPA/WPA2-PSK v
	* Wi-Fi Password
	5G Wi-Fi
	* SSID
	@Ruijie-s0356_iot_5G
	Previous Next

(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.

Set Country/F	Region (4/4)
Country/Region/Time Zon	0
Country/Region/Time 201	
* Country/Region	
United States (US)	
* Time Zone	
(GMT-5:00)America/New_	York 🗸 🗸
Previous	News
	Next

(6) Click Next.

Wireless Repeating Result
Finish Connect to the Wi-Fi network again.
Management URL: 10.44.77.254 Management Password: Ruijie123
SSID: @Ruijie-s0356 24G Wi-Fi Password: Ruijie123 SSID: @Ruijie-s0356 56 Wi-Fi Password: Ruijie123
SSID: @Ruijie-s0356_iot lot 2.4G Wi-Fi Password: Ruijie123 SSID: @Ruijie-s0356_iot_5G lot 5G

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.

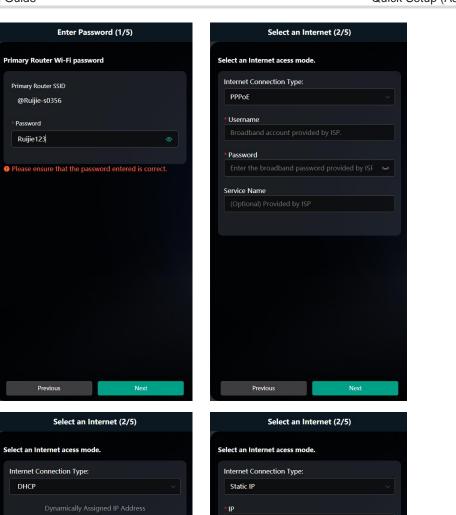
Network S	tatus	← Scan	Repeater Mode ~
ONO cable is detected. Plug in diagram	cables according to the	Q SSID Filtering	S
Power		5G @Ruijie-s0356	
	Λ	^{5G} @Ruijie-s0356_Game	
T T		2.46 @Ruijie-s0356	
		2:46 1	
A THE		2.4G @Ruijie-s0848	
	Router WAN Port	2.4G ruijie-office	
		2.4G ruijie-guest	
Rechect	¢	2.4G rj-network	
If you want to extend	your Wi-Fi range	Other Networks	
Add Reyee Unit	Wireless Repeater		
WISP			
You can also "perform configu	uration without a cable"		

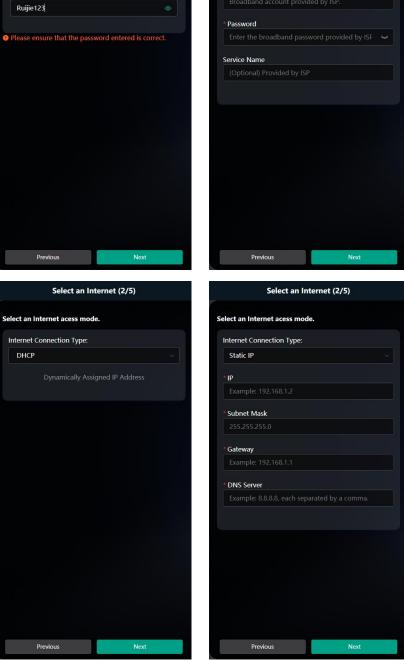
- (2) Enter the password of the primary router Wi-Fi, and select an Internet access mode. For details, see <u>2.4.1</u> <u>Configuring the Internet Connection Type</u>.
 - o Select DHCP and the extender will automatically obtain an IP address.
 - o If the primary router cannot assign IP addresses, select Static IP.
 - o In the PPPoE mode, a username, a password, and possibly a service name are needed.
 - o 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.

Primary Router SSID

@Ruijie-s0356

Password





Select an Internet (2/5)	Select an Internet (2/5)
elect an Internet acess mode.	Select an Internet acess mode.
Internet Connection Type:	Internet Connection Type:
L2TP	✓ L2TP
IP Type DHCP Static IP	IP Type DHCP Static IP
* Username	* Username
	Username
* Password	* Password
	Password 😽
*Server IP/Domain Name	* Server IP/Domain Name
	Server IP/Domain Name
	хIb
	Example: 192.168.1.2
	* Subnet Mask
	255.255.0
	* Gateway
	Example: 192.168.1.1
	DNS Server
	Example: 8.8.8.8, each separated by a comma.
Previous Next	Previous Next

Click $\ensuremath{\textit{Next}}.$ Verify the Internet settings. Then, click $\ensuremath{\textit{OK}}.$

Select an II	nternet (2/5)	
Select an Internet acess mo	de.		
Internet Connection Type:			
DHCP			
Verify that the following config information provided by your	- ISP. Any inc	onsistency may	
result in an inability to access Internet: DHCP	the Internet		
	OK	Return to modify	

(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.

Set Wi-	Fi (3/5)
Local Router Wi-Fi	
Same as Primary Router Wi-Fi	
* SSID (2.4G)	
Do you want to use the Wi-Fi passw	
	Next

- 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.

Set Wi-Fi (3/5)			
Local Router Wi-Fi			
Same as Primary Router Wi-Fi			
* SSID (2.4G)			
* SSID (5G)			
Wi-Fi Password			
Management Password			
Same as Wi-Fi Password			
	Strong		
Previous	Next		

(4) Configuring IoT Wi-Fi

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



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.

loT Wi-Fi (4/5)	loT Wi-Fi (4/5)
loT Wi-Fi	IoT WI-FI A separate network for IoT devices, ensuring stable connection.
A separate network for IoT devices. Enable it to ensure reliable connectivity for your IoT devices.	Dual-Band Single SSID Disable it to ensure reliable connectivity for your IoT devices.
Try Now Skip for Now	2.4G Wi-Fi
	* SSID @Ruijie-s0356_iot Security
	WPA/WPA2-PSK * WI-FI Password
	5G Wi-Fi ^SSID @Ruijie-s0356_iot_5G
	Previous Next WPA/WPA2-PSK

(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.

Set Country/	/Region (5/5)	
Country/Region/Time Zo	ne	
country, neglon, nine 20		
* Country/Region		
United States (US)		
* Time Zone		
(GMT-5:00)America/New	York v	
Previous	Next	

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

Wireless Repeating Result
Finish Connect to the Wi-Fi network again.
Management URL: 10.44.77.254 Management Password: Ruijie123
SSID: @Ruijie-s0356 2.4G Wi-Fi Password: Ruijie123 SSID: @Ruijie-s0356 56 Wi-Fi Password: Ruijie123
SSID: @Ruijie-s0356_iot lot 2.4G Wi-Fi Password: Ruijie123 SSID: @Ruijie-s0356_iot_5G lot 5G

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

• 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 <u>https://reyee.ruijie.com</u> or reach out to customer service by emailing <u>service_rj@ruijienetworks.com</u>.

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.

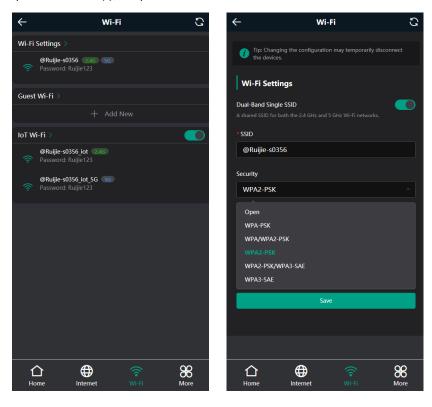
A Caution

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

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

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

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



4.2 Enabling Band Steering

🛕 Caution

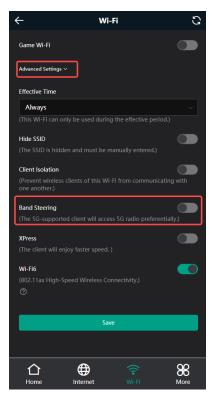
Before enabling the band steering, you must enable the dual-band integration. Because the client can automatically choose to steer to either band only when the 2.4G and 5G bands use the same SSID.

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, 5G Wi-Fi and Game Wi-Fi will be hidden.

🛕 Caution

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

← Wi-Fi ପି	େ Wi-Fi ପ
Wi-Fi Settings >	Game Wi-Fi
@Ruijie-s0356 246 56 중 Password: Ruijie123	Advanced Settings ~
Guest Wi-Fi >	Effective Time
+ Add New	Always v (This Wi-Fi can only be used during the effective period.)
loT Wi-Fi >	Hide SSID
ORuijie-s0356_iot ZaG Password: Ruijie123	(The SSID is hidden and must be manually entered.)
	Client Isolation
Password: Ruijie123	(Prevent wireless clients of this Wi-Fi from communicating with one another.)
	Band Steering
	(The 5G-supported client will access 5G radio preferentially.)
	XPress
	(The client will enjoy faster speed.)
	Wi-Fi6
	(802.11ax High-Speed Wireless Connectivity.)
	0
	Save
Internet Internet Internet Nore	Internet Internet Sec Sec Home Internet Wi-Fi More

1 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, Game Wi-Fi, Guest Wi-Fi and Smart Home Wi-Fi networks.

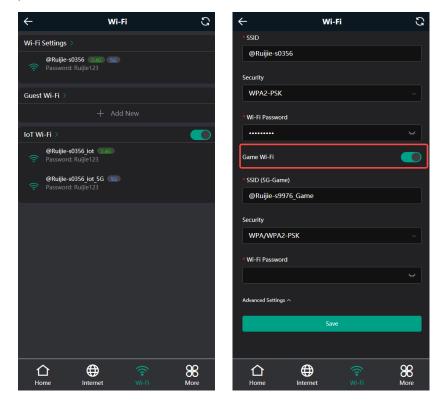
Smartphone View: Choose Wi-Fi > Wi-Fi Settings.

Click the target Wi-Fi network.

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

4.4.1 Adding Game Wi-Fi Network

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



4.4.2 Adding Other Types of Wi-Fi Networks

1. Overview

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

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

2. Configuration Steps

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

← Wi-Fi ଅ	← Wi-Fi C
Wi-Fi Settings >	Tip: Changing the configuration may temporarily disconnect
@Ruijie-s0356 246 56 Password: Ruijie123	 inp: Changing the configuration may temporarily disconnect the devices.
	Guest Wi-Fi
Guest Wi-Fi >	Enable
+ Add New	Dual-Band Single SSID
loT Wi-Fi >	A shared SSID for both the 2.4 GHz and 5 GHz Wi-Fi networks.
@Ruijie-s0356_iot 2243 Password: Ruijie123	* SSID
@Ruijie-s0356 iot 5G 56	@Ruijie-guest-9976
Password: Ruijie123	Security
	WPA/WPA2-PSK v
	* Wi-Fi Password
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
	Speed Limit
	Advanced Settings ^
	Save
Home Internet WI-Fi More	Home Internet WI-Fi More
mone mone more	Home Mole Mole

- **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**.

• Wi-Fi6: You can enable Wi-Fi6 to enjoy high-speed Internet access.

# 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.

#### A 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.

© %    ⊗ ● 0	) 10 🕸 🔌 27% 🔲 I 11:02	🖾 👘 🕲 💊	関 🎯 岩 🎗 27% 💷 11:03	a %al 🛪 🖬	
← WLAN	?	← EW1800G	X PRO	← EW1800GX	PRO
WLAN		Privacy	Use randomized >	Privacy	Use device MAC
Network acceleration	Off >	Advanced settings		Advanced settings	
More settings	2	Proxy	None >	Proxy	None
CONNECTED		IP settings	Dynamic >		
EW1800GX PRO Connected (good quality)	(((-	ir settings	Dynamic 7	IP settings	Dynamic
AVAILABLE	EW180				
RuiJie-ChengDu	Forget				
Saved, encrypted (available)	Modify network				
R6 Saved (no Internet access)	লি				
Meituan-City Encrypted	<b></b>			Privacy	
CTTC Encrypted	()			Use randomized M	
HUAWEI_H112_8915 Encrypted	6 🗟			Use device MAC	0
HUAWEI_H112_8915_5G	6 7	CANCEL	SAVE	CAI	NCEL

Ruijie	R∈y	'EE					
Basics							
😤 WLAN		Only	Add				
Wi-Fi Blocklist/Allowlis	ר	Block	* MAC	Example: 00:11:22:33:44:55		+ Add	
Radio Frequency		Up to	Remark				
🖾 Work Mode							
⊘ Security					Cancel OK		
🗐 VPN			10/page 🗸				
台 Advanced							
Oiagnostics							
🗄 System							
«Collapse							

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

Ruijie Rey	/⊂⊂	nterne 🎅 Wi-Fi 📑 More	English ~ 🎇 😭 🛞
Basics	All devices except blocklisted devices can connected the second devices can connected the second devices can connected the second devices can be set of the second devices can be second devices can be set of the second devices can be seco	nect to the Wi-Fi network.	
হি WLAN ^	Only allowlisted devices can connect to the Wi	i-Fi network.	
<b>Wi-Fi</b> Blocklist/Allowlist	Blocked Device List		+ Add 👜 Batch Delete
Radio Frequency	Up to <b>64</b> devices can be added.		
🖾 Work Mode	MAC	Remark	Action
⊘ Security 👋	11:22:43:23:56:23		Edi Delete
₩ VPN ×	< 1 > 10/page >		Total 1
🗄 Advanced 🛛 👋			
Diagnostics			
:⊪- System ∨			
Collapse			

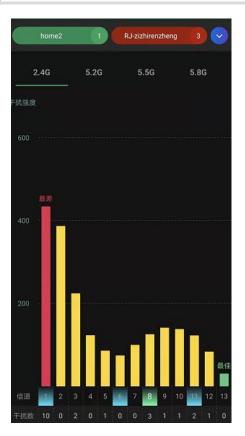
# 4.6 Optimizing the Wi-Fi Network

## 4.6.1 Overview

The device detects the surrounding wireless environment and selects the appropriate configuration upon poweron. 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 <u>7.6</u> <u>Configuring Scheduled Reboot</u>. 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.

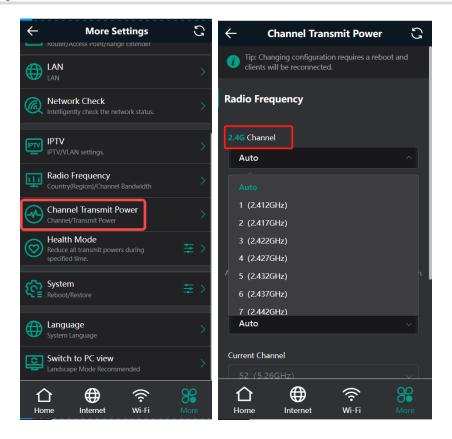
Choose the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. Excess clients connected to a channel can bring stronger wireless interference.

#### 1 Note

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

## A 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.

← More Settings 🗘	🔶 Radio Frequency ପ୍ରି
Configure Internet access time.	Tip: Changing the configuration may temporarily disconnect the devices.
Control LEDs of all devices.	Radio Frequency
Wizard	Country/Region
Internet/Wi-Fi/Scan QR Code	United States (US)
Work Mode >	2.4G Bandwidth
LAN >	Auto ~
Network Check         >           Intelligently check the network status.         >	5G Bandwidth
IPTV IPTV/VLAN settings.	Auto ~
Radio Frequency Country(Region)/Channel Bandwidth	Save
Channel Transmit Power > Channel/Transmit Power	
Reduce all transmit powers during	
Home Internet Wi-Fi More	Home Internet Wi-Fi More

• Optimizing the transmit power

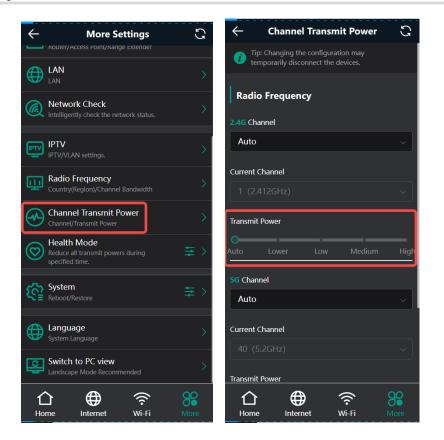
Smartphone View: Choose More > Channel Transmit Power.

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

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

#### 🛕 Caution

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



# 4.7 Configuring the Healthy Mode

Smartphone View: Choose More > Healthy Mode.

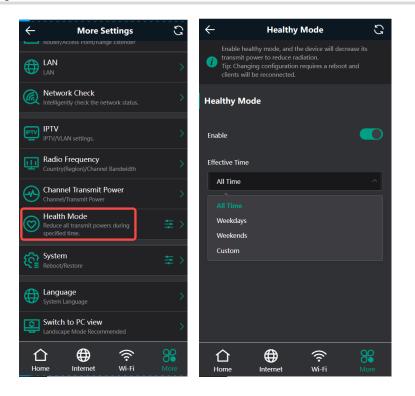
PC View: Choose More > WLAN > Wi-Fi > Healthy Mode.

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

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

#### 🚺 Note

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



# 4.8 Enabling Roaming Optimization

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

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

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

Wi-Fi Settings	Guest Wi-Fi	loT Wi-Fi	Health Mode	Roaming Optimization	Wi-Fi/IGMP
Roaming	Optimization				
	Enable 🗾				
		Save			
		Save			

# **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.

The router is curr	ently in Router mode.		
Router	• Access Point	Wireless Repeater	WISP
		s connected to the primary router t of this router to the LAN port of	
Access Poin	ıt		
	Check		

The router is currently in Rou	ter mode.			
Router     Acc	cess Point	Wireless Repeater	• WISP	
		ected to the primary router WAN port of this router to t		age. ry router using an Ethernet cable.
Access Point				
Status	Cable Plugged			
	IP Address: 10.48.40	.11		
* Local Router SSID(2.4G)	@Ruijie-s9976			
* Local Router SSID(5G)	@Ruijie-s9976_50	j		
Password	•••••			
	Save			

# 5.2 Wireless Repeater

Smartphone View: Choose More > Work Mode.

PC View: Choose More > Work Mode.

#### 1 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.

The router is cu	urrently in Router mode.
Router	Access Point     Wireless Repeater     WISP
	is mode, this router can be connected to the primary router with an Ethernet cable to extend the Wi-Fi coverage. ct a 5G Wi-Fi network of the primary router for better Internet experience.
Wireless	Repeater
— Prima	ry Router
	* SSID Select

		×
5G Wi-Fi List Click to	select the Wi-Fi of the	primary router.
Q SSID Filtering	5G 🗸 Re-scan	
SSID	RSSI	Security
@Ruijie-s0356	Low	Security
@Ruijie-s0356_Game	Low	Security
1	Medium	Open
rj-network	Medium	Security
ruijie-guest	Medium	Open
Ruijie-Partner	Medium	Security
Ruijie-Partner	Medium	Security
rj-network	Medium	Security

- (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.

The router is current	ntly in Router mode.		
Router	Access Point	Wireless Repeater	• WISP
	5G Wi-Fi network of the pri	nected to the primary router with a mary router for better Internet exp	In Ethernet cable to extend the Wi-Fi coverage. erience.
— Primary F			
*	SSID @Ruijie-s0356	Select	
* Wi-Fi Pass	word		
— Local Roı	ıter		
Local Router	Wi-Fi 🔵 New Wi-Fi	Same as Primary Router Wi-F	
	Save	-	

 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.

The router is currently in	Router mode.			
Router	Access Point	Wireless Repeat	er 🚺 🔍 WIS	Ρ
		lected to the primary route nary router for better Inter		le to extend the Wi-Fi coverage.
Wireless Repeat	er			
— Primary Route	r			
* SSID	@Ruijie-s0356 _S ,	elect		
* Wi-Fi Password	•••••			
— Local Router				
Local Router Wi-Fi	💿 New Wi-Fi 🌘	Same as Primary Rout	er Wi-Fi	
* SSID(2.4G)	@Ruijie-s0356_p	lus		
* SSID(5G)	@Ruijie-s0356_p	lus_5G		
Wi-Fi Password	A blank value ind	licates no encryption.		
	Save			

#### 🛕 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**.

The router is curr	ently in <mark>Rout</mark>	er mode.		
Router	Acce	ess Point	Wireless Repeater	• Wisp
<ul> <li>In WISF</li> <li>WISP a</li> </ul>	P mode, this ro llows users to	outer acts as a clien create a personal \	t device, connecting to anoth VLAN in public spaces such as	er wireless network. Select the Internet connection type (DHCP, PPPoE or Static IP) and connect to the target SSID. cafes, hotels, airports or restaurants.
WAN				
1	* Internet	DHCP		
	Internet	DHCP		
		Next		
		Next		

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

Router     Access Point     Wireless Repeater     WISP     In WISP mode, this router acts as a client device, connecting to another wireless network. Select the Internet connection type (DHCP, PPPoE or Static IP) and     WiSP allows users to create a personal WLAN in public spaces such as cafes, hotels, airports or restaurants.      Wireless Repeater     Primary Router	d connect to the target SSID.
<ul> <li>WISP allows users to create a personal WLAN in public spaces such as cafes, hotels, airports or restaurants.</li> <li>Wireless Repeater</li> </ul>	d connect to the target SSID.
Wireless Repeater	
Trindi y Koutei	
* SSID Select	
Previous	
×	
5G Wi-Fi List Click to select the Wi-Fi of the primary router.	
○ SSID Filtering 5G ∨ Re-scan	
SSID RSSI Security	
@Ruijie-s0356_Game High Security	
@Ruijie-s0356 Low Security	
1 Medium Open	
Ruijie-Partner Medium Security	
ruijie-guest Medium Open	
Ruijie-Partner Medium Security	
ruijie-office Medium Security	

- (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.

The router is currently i	in Router mode.				
Router	Access Point	Wireless Repeater	• WISP		
<ul> <li>In WISP mode</li> <li>WISP allows up</li> </ul>	e, this router acts as a clie users to create a persona	ent device, connecting to another WLAN in public spaces such as ca	vireless network. Select the Internet conne fes, hotels, airports or restaurants.	ection type (DHCP, PPPoE or Static IP) and connect to	the target SSID.
Wireless Repea	ater				
— Primary Rout	ter —				
* SSIC	@Ruijie-s0356 _{Sel}	ect			
* Wi-Fi Password					
Local Router  Local Router Wi-F		Same as Primary Router Wi-Fi			
	Previous	Save			

 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.

e router is currently in	Router mode.				
	Access Point	Wireless Repeater	• WISP		
<ul> <li>In WISP mode,</li> </ul>	, this router acts as a cl	ient device, connecting to anothe	r wireless network. Select the l	nternet connection type (DHCP, P	PPoE or Static IP) and connect to the targe
<ul> <li>WISP allows us</li> </ul>	sers to create a persona	al WLAN in public spaces such as	cafes, hotels, airports or restau	irants.	
Wireless Repea	ter				
<ul> <li>Primary Route</li> </ul>	er				
* SSID	@Ruijie-s0356 Se	lect			
where the second					
* Wi-Fi Password	•••••				
– Local Router					
Local Router Wi-Fi	💿 New Wi-Fi 🏾	Same as Primary Router Wi-I	FI		
* SSID(2.4G)	@Ruijie-s0356_pl	us			
* SSID(5G)	@Ruijie-s0356_pl	us_5G			
Wi-Fi Password	A blank value ind				
	Previous	Save			

(4) Click Save.

#### A 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.

Router     Access Point     Wireless Repeater	A JAILED	
<ul> <li>In WISP mode, this router acts as a client device, connecting to another w</li> <li>WISP allows users to create a personal WLAN in public spaces such as caf</li> </ul>	×	tic IP) and connect to the target SSID.
Wireless Repeater	Finish	
- Primary Router		
SSID @Ruijie-s0356 Select		
- Local Router		
	@Ruijie-s0356 2.4G	
Local Router Wi-Fi 🛛 New Wi-Fi 🕘 Same as Primary Router Wi-Fi		
	Ruijie123	
	@Ruijie-s0356 5G	
	Ruijie123	

# 6 Configuring Network Settings

# 6.1 Configuring Internet Connection Types

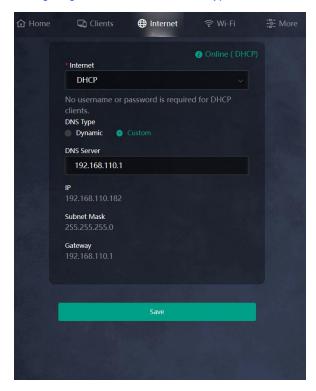
#### 🛕 Caution

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 <u>2.4.1</u> <u>Configuring the Internet Connection Type</u>.



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

Basics	^	🥡 wan		
WAN		Single Line Dual-L	Line	
LAN		0	Online ( DHCP)	
IPTV		* Interne	et DHCP	
IPv6		DNS Typ	pe 🧿 Dynamic 🛛 🔵 Custom	
হি WLAN		DNS Servi	<b>er</b> 192.168.111.1	
Work Mode				
Security			IP 192.168.111.19	
型 VPN		Subnet Ma	sk 255.255.255.0	
🗄 Advanced		Gatewa	ay 192.168.111.1	
Diagnostics		Adva		
System			Save	

- 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.

Single Line Dual-Line	
🕧 Or	nline ( DHCP)
* Internet	L2TP v
	Select this type if your ISP provides L2TP VPN server information and an account. Some ISPs also provide specific IP parameters.
IP Туре	DHCP Static IP
* Username	
* Password	Password 😽
* Server IP/Domain Name	Server IP/Domain Name

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.

* Internet	L2TP	×
	Select this type if your ISP provide	es L2TP VPN server information and an account. Some ISPs also provide specific IP parameters.
ІР Туре	DHCP     Static IP	
* Username		
* Password	Password	*
* Server IP/Domain Name	Server IP/Domain Name	
* Ib	192.168.111.19	
* Subnet Mask	255.255.255.0	
* Gateway	192.168.111.1	
* DNS Server	192.168.111.1	

#### 2. Changing the MAC Address

#### 🛕 Caution

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

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

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

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

#### 🛕 Caution

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

Single WAN	Dual-W	AN				
	() Online (DHCP)					
* Internet Conne	ction Type	ОНСР ~				
	DNS Type	Dynamic Sustom				
D	NS Server	192.168.110.1				
	IP	192.168.110.152				
Sul	onet Mask	255.255.255.0				
	Gateway	192.168.110.1				
	* MTU	1500				
	* MAC	00:d0:f8:15:08:48				
802.1Q Tag						
Р	rivate Line	• • •				
		Save				

#### 3. Modifying MTU

#### A 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.

Single WAN	Dual-W	AN				
	() Online (DHCP)					
* Internet Connec	tion Type	DHCP ~				
I	DNS Type	Dynamic Ocustom				
DI	NS Server	192.168.110.1				
	IP	192.168.110.152				
Sub	onet Mask	255.255.255.0				
	Gateway	192.168.110.1				
	Advance	ed Settings ~				
	* MTU	1500				
	* MAC	00:d0:f8:15:08:48				
80	02.1Q Tag	0				
Pr	ivate Line	0				
		Save				

## 4. Configuring a Private Line

## A Caution

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

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

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

Single WAN Dual-W	AN
0 0	nline (DHCP)
* Internet Connection Type	ОНСР 🗸
DNS Type	Oynamic Custom
DNS Server	192.168.110.1
IP	192.168.110.152
Subnet Mask	255.255.255.0
Gateway	192.168.110.1
Advance	ed Settings A
* MTU	1500
* MAC	00:d0:f8:15:08:48
802.1Q Tag	
Private Line	0
	Save

#### 5. Configuring the VLAN Tag

#### 🛕 Caution

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

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

<b>()</b> O	nline ( DHCP)		
* Internet	DHCP		
DNS Type	o Dynamic 🌒	Custom	
DNS Server	192.168.111.1		
IP	192.168.111.19		
Subnet Mask	255.255.255.0		
Gateway	192.168.111.1		
Advance	ed Settings ^		
* MTU	1500		
* MAC	0a 70	5	
802.1Q Tag			
* VLAN ID	Range: 2-232 or	234-4090.	
Private Line	0		
	Save		

#### 6. Configuring LCP Parameters

#### A 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.

Advanced	d Settings ^
* LCP Echo Failure Count	6
* LCP Echo Interval	30
	Save

## 7. Configuring Load Balancing Settings

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

	Dual-WAN	
WAN WAN1	Load Settings	
Load Balancir	ng Settings	
	node: The traffic will be spread across r ill be routed over WAN and 40% over '	multiple links according to the weight of each
2. Primary &		over the primary interface. Once the primary in
Load Mo	de Balanced	
Balancing Poli	cy Based on Link	Ţ,
Balancing Poli	Cy Based on Link	
Balancing Poli	If your feil to come calling heading on Based on Src IP.	
	Based on Src IP.	

Table 6-1	Description	of Load-ba	lancing	Mode
-----------	-------------	------------	---------	------

Load Mode	Description
Balanced	Traffic is allocated in proportion to the weight of each WAN port. The higher the weight is, the more traffic is allocated. The weight of each WAN port must be specified in this mode. For example, if the weights of WAN and WAN1 ports in the dual-line mode are set to 3 and 2 respectively, then traffic will be allocated at 3:2, with 60% traffic routed to WAN port, and 40% traffic routed to WAN1 port.

Load Mode	Description
Primary & secondary	When the primary interface is normal, all the traffic will be routed to the primary interface. If the primary interface fails, traffic is automatically routed to the secondary interface. In this mode, each WAN port must be specified as a primary or secondary interface. If there are multiple primary or secondary interfaces, a weight must be set for each interface (same as the balanced mode).

# 6.3 Changing the Address of a LAN Port

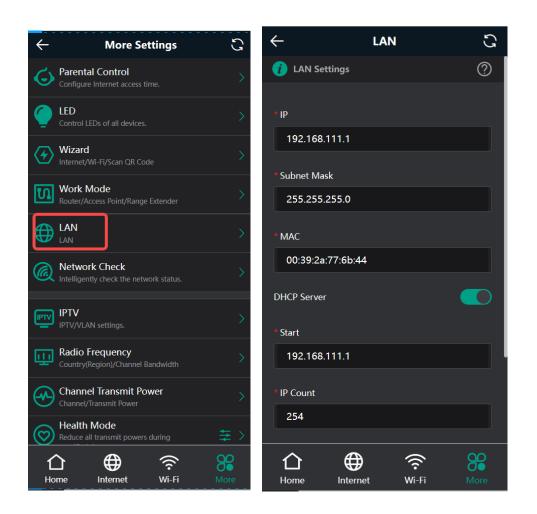
Smartphone View: Choose More > LAN.

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

#### A 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.

Basics	*	IPTV/VLAN IPTV/IGMP	
WAN		IPTV Provide Internet access and IPTV convices through only one Ethernet cable	
LAN		Provide Internet access and IPTV services through only one Ethernet cable.	
IPTV		IPTV/VLAN	
IPv6		IPTV 🛑	
🗇 WLAN		IPTV Port Connect the default or configured IPTV port.	
Work Mode			
Security		LAN1 LAN2 IPTV LAN4 WAN DC	
VPN		VLAN	
🗄 Advanced		* IPTV VLAN ID Range: 2-232 or 234-4090.	
Diagnostics		Range. 2-252 01-254-4090.	
:== :== :==	~	Save	

## 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.

IPTV/VLAN	IPTV/IGMP	
<i>i</i> ) iptv/i	GMP ( For FPT Service Provider)	
IPTV/IGM	IP	
	Enable	
	Save	
	Save	

# 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 WIFI/IGMP for 2.4G wireless clients.

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

Basics		Wi-Fi Settings	Guest Wi-Fi	loT Wi-Fi	Health Mode	Roaming Optimization	Wi-Fi/IGMP
ଙ୍କ WLAN		🥡 Wi-Fi/IGN	ЛР				
		Wi-Fi/IGMP					
Blocklist/Allowlis	t	M2U (2	24(3)				
Radio Frequency		iiilo (i					
Mork Mode		M2U	(5G)				
Security				Save			
s VPN							
🖶 Advanced							
@ Diagnostics							

# 6.6 Configuring IPv6

#### A 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.

Basics	^	IPv6 When IPv6 is enabled. The MTU on the interface for sending IPv6 packets must be greater than 1280 bytes.
WAN		
LAN		Enable
IPTV		WAN Settings LAN Settings DHCPv6 Clients
IPv6		WAN_V6
হু WLAN		* Internet Connection Type DHCP V
Mork Mode		DNS Type 💿 Dynamic 💿 Custom
Security		DNS Server
孠 VPN		IPv6
🔁 Advanced		
Diagnostics		IPv6 Prefix
: System		Gateway
		NAT66
		Advanced Settings ~
		Save

## 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.

<b>IPv6</b> When IPv6 is enabled. The MTU on the interface for sending IPv6 packets must be greater than 1280 bytes.					
Enable 🦲					
WAN Settings LAN	Settings DHCPv6 Clients				
IPv6 Assignment	Auto	0			
IPv6/Prefix Length	0:0::2				
Subnet Prefix Name	Default ~	0			
Subnet Prefix Length	64	0			
Subnet ID	0	0			
* Lease Time(min)	120	0			
DNS Server	Example: 0:0::2, each separated by a comma.				
	Save				

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

<i>IPv6</i> When IPv6 is enabled. The MTU on the interface for sending IPv6 packets must be greater than 1280 bytes.					
E	Enable 🗾				
WAN Settings	LAN Settings	DHCPv6 Clients			
	5 Clients clients are listed on 1	this page.			
DHCPv6 Clients				Search by DUID	Q
No.	Hostname	IPv6	Remaining Lease Time(	min) DU	liD
No Data					
	10/page ~				Total 0

# 6.7 Configuring Auto Bandwidth Control

### A Caution

This feature is supported in router mode.

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

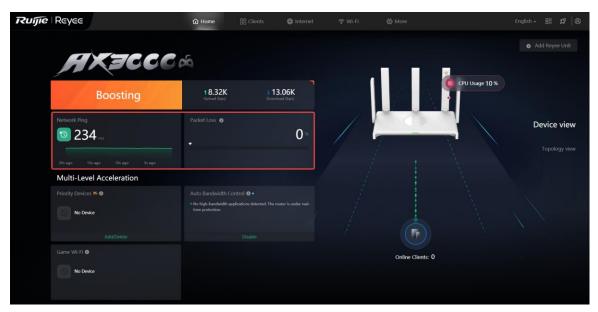
#### PC View: Home page > Auto Bandwidth Control

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

Ruíjie Reyce		🚹 Home	믑 Clients	Internet	💎 Wi-Fi	🛞 More		English • 🗄 💋 🛛 🛞
AX	JCCC	ā						<ul> <li>Add Reyee Unit</li> </ul>
Nc	ormal	<b>1140.00</b> Upteed (bpc)	Sources	8.00 ad (bps)			CPU Usage 2 %	
Network Ping <b>132</b> ms		Packet Loss 🛛		0%		ÍI	Dream	Device view
Multi-Level Acce	leration							
Priority Devices 14 @		Auto Bandwidth Cont	trol 🕢 - Enable					
						Online Clients: 0		
No Device								

#### 1. Viewing Network Latency

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



### 2. Configuring Designated Devices

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

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

Ruíjie Reyce	1 Home		⊕ Internet			
HXJCCC	6					
Boosting	110.00K Upload (bps)	I 15 Downlor	.83K ad (bps)			CPU Usage 12 %
Network Fing D229 ===	Packet Loss 💿		0*	17	-	Device view
201: ago 15: ago 10: ago 5: ago Multi-Level Acceleration						
Priority Devices 14 0	Auto Bandwidth Conf No high-bandwidth appli time protection.					
Add/Delete						
Game Ve-F-I 🔮					Online Clients: 0	

### 3. Viewing Auto Bandwidth Control Device Details

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

Ruíjie Reyec	Home	BB Clients	Internet	ଙ୍କ Wi-Fi 🛛 🖉	향 More	English • 🔠 💋 🛛 🛞
AXECCO	Ŕ			. 1		
Boosting	112.89K Upload (bps)	1 Down	8.82K flored (bps)		(0) CPU Usage 11 %	
Network Ping 236 ms 20s ago 10s ago 5s ago	Packet Loss 🕢		0 %	1/1	-	Device view Topology view
Multi-Level Acceleration						
Priority Devices 14 0	Auto Bandwidth Cor • No high-bandwidth app time protection.		router is under real-			
Game Wi-Fi ❶					Online Clients: 0	

### 4. Disabling Auto Bandwidth Control

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

Rujje Reyee		et 🎓 Wi-Fi 🚳	More	English • 🗄 🕫 🖗
AXJCCC	6			
Boosting	110.92K 15.28K Upload (bps) Download (bps)		CPU Usage 9 %	
Network Ping			0	Device view
<b>100</b> 236	<b>.</b> 0∗			
20s ago 15s ago 10s ago 5s ago				
Multi-Level Acceleration				
Priority Devices 💆 💿				
No Device	<ul> <li>No high-bandwidth applications detected. The router is under real time protection.</li> </ul>			
Add/Delete	Disable			
Game Wi-Fi <b>O</b>			Online Clients: 0	
No Device				

# 6.8 Enabling Parental Control

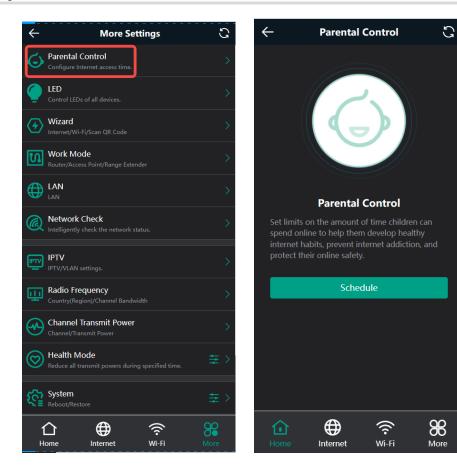
Smartphone View: Choose More> Parental Control.

PC View: Choose Clients > Manage Blocking Schedules.

### A Caution

This function is supported only in router mode.

Select a client and click **Schedule**. You can set the Internet block periods.



$\leftarrow$	← Parental Control					
╘	ET-ALOO 🖉	Allowe	÷			
	e Block Time Ø		+			
for the second s	Internet	((∩ Wi-Fi	Hore More			

## 6.8.1 Setting the Internet Block Periods

### 1. Setting the Internet Block Rules

Click Tap here to set to set the Internet block periods. In the block periods, the client cannot access the Internet.

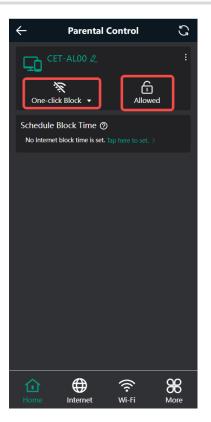
You can select certain days of the week or customize the Internet block periods.

$\leftarrow$	Parental Co	ontrol	S	÷	Schedule B	Block Time	S
	Cet-aloo 🖉		:	i Set a the In	schedule to pre ternet during t	event clients to acc he specified time.	ess
	У.	6		Repeat			ct >
One-o	click Block 🔻	Allowed		Start Time	© 15:45	5	>
	e Block Time ⑦ net block time is se. Taj	hore to set		End Time			>
No men	let block time is set. Tap	5 here to set. 7		Ca	incel	Save	
ŵ	<b>(</b>	<u> </u>	<del>36</del>	<u>ن</u>	<b>(</b>	(,	88
Home	Internet		More		Internet	Wi-Fi	More

### 2. Blocking Internet Access Temporarily

- Click **One-click Block** and select a period to block the client from accessing the Internet temporarily.
- Click **Allowed** to lift all Internet access restrictions imposed on the client on the current day. The lifting operation is valid only on the current day. The restrictions will be resumed the next day.

### Configuration Guide



# 6.8.2 Disabling Parental Control

To disable parental control, click **Delete** in the upper right corner to lift the restrictions on the client.

÷	Parental	Control	G
One	CET-ALOO 🖉	Ledi De Allowe	
	ule Block Time ( ernet block time is set		, ,
<u>ہ</u>	<b>A</b>	<u>_</u>	<u>9</u> 2
Home	Internet	ົ Wi-Fi	00 More

# 6.9 Configuring DHCP Server

### A Caution

This feature is supported in router mode.

### 6.9.1 Overview

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

## 6.9.2 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.

Basics	LAN Settings DHCI	P Clients Static IP Addresses DHCP Option DNS Proxy	
WAN	i LAN Settings	0	
LAN IPTV	* Ib	192,168.111.1	
IPv6 Address	* Subnet Mask	255.255.255.0	
হি WLAN	*MAC	00:39:2a:77:6b:44	
🖾 Work Mode	DHCP Server		
Security	* Start	192.168.111.1	
VPN	* IP Count	254	
<ul> <li>Advanced</li> <li>Diagnostics</li> </ul>	* Lease Time(Min)	120	
System		Save	
Collapse			

### 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.

Basics	LAN Settings	DHCP Clients	Static IP Addresses	DHCP Option [	ONS Proxy	
WAN	🥡 View D	HCP clients.				0
LAN	DHCP Cli	ents			ରୁ ତି Refresh	+ Batch Convert
IPv6 Address	No.	Hostname		МАС	Remaining Lease Time(min)	Status
ି WLAN		DESKTOP-1JM66E2	192.168.111.170	70:b5:e8:76:f5:e9	) 102	
Work Mode		10/page V				Total 1
🛇 Security		To page				
፼ VPN						
🗄 Advanced						
@ Diagnostics						
:E: System						
«Collapse						

### 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.

LAN Set	ttings	DHCP Clients	Static IP Addresses	DHCP Option	DNS Proxy	
1	View DH0	CP clients.				0
рнс	P Clier	nts	Search b	by Hostname/IP/MA	ୁ ି Refresh	+ Batch Convert
	No.	Hostname	IP	MAC	Remaining Lease Time(min)	Status
	1	DESKTOP-1JM66E2	192.168.111.170	70:b5:e8:76:f5:e	9 102	Convert to Static IP
	1 >	10/page V				Total 1

### 4. Configuring DHCP Option

 $\label{eq:startphone} Smartphone \ View: \ Choose \ More > Switch \ to \ PC \ view > More > Basics > LAN > DHCP \ Option.$ 

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.

LAN Settings	DHCP Clients	Static IP Addresses	DHCP Option	DNS Proxy
<i>i</i> DHCP O	•	lied to all LAN ports.		
DNS S	Example:	8.8.8.8, Separate multipl	e DNS serv	
	S	ave		

# 6.10 Configuring DNS Server

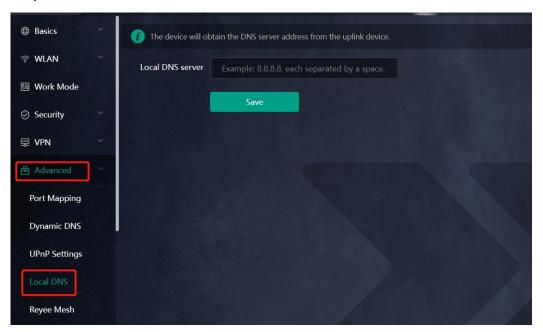
## 6.10.1 Local DNS Server

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

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

PC View: Choose More > Advanced > Local DNS server

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



# 6.10.2 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.

Basics	^	LAN Settings	DHCP Clients	Static IP Addresses	DHCP Option	DNS Proxy
WAN		DNS prox	y is not mandatory.	The device will obtain the I	ONS server address fro	om the uplink device by default.
LAN			nable 🔵			
ΙΡΤν		* DNS S	ionur Es i			
IPv6 Address		DNSS	Enter a l			
ବ୍ଲ WLAN			Si	ave		
🔟 Work Mode						
⊘ Security						

# 6.11 Configuring Port Mapping

#### A Caution

This feature is supported in router mode.

## 6.11.1 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.

## 6.11.2 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.

### 6.11.3 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.

Basics	~	Port Mapping NAT-D	MZ					
ଙ୍କ WLAN	~	i Port Mapping						0
M Work Mode		Port Mapping List					+ Add	🗊 Batch Delete
Security	~							
题 VPN	~	Up to <b>50</b> entries can be	e added.					5.
🖶 Advanced	^	Name	Protocol	External IP Address	External Port	Internal Server IP	Internal Port	Action
Port Mapping					No Data			
Dynamic DNS		< <u>1</u> > 10/p.	age 🗸					Total 0
UPnP Settings								
Local DNS								
Reyee Mesh								
Reyee Mesh 3.0								
AP Networking				4	and the second			

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.

Add		×
* Name		
Preferred Server	HTTP	
Protocol	тср	~
External IP Address	WAN port O Enter/Select a WAN	n IP V
External Port/Range	Example: X or X-X (Range: 1-6553	35)
* Internal Server IP	Example: 1.1.1.1	
Internal Port/Range	80	
	Cancel	ОК

## 6.11.4 Verification and Testing

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

## 6.11.5 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 <u>6.11.6 DMZ Configuration Steps</u>. The common cause is that port configuration is incorrect or incomplete.

## 6.11.6 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.

Basics	~	Port Mapping NAT-DMZ
ବ୍ଟ WLAN		i) NAT-DMZ
Work Mode		Enable
🔄 Security		
櫽 VPN		* Dest IP Address Example: 1.1.1.1
🗄 Advanced		Save
Port Mapping	]	
Dynamic DNS		
UPnP Settings		

# 6.12 Configuring DDNS

### 6.12.1 Overview

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

## 6.12.2 Getting Started

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

## 6.12.3 Configuration Steps

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

PC View: Choose More > Advanced > Dynamic DNS

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

፼ VPN ∽	No-IP DDNS DynD	NS		
🔁 Advanced 🛛 ^	no-IP DDNS			
Port Mapping				
Dynamic DNS	* Service Interface	WAN		
UPnP Settings	* Username			
Local DNS	* Password			
Reyee Mesh	Domain			0
Reyee Mesh 3.0				
AP Networking		Log In	Delete	
Link Aggregation	Link Status			
Routing	Domain -			

# 6.13 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.

i Connectivity De	etection		
* Keepalive Interval	120		seconds
* Probe Interval	5		seconds
* URL List	http://www.amazon.cor	Add	
	http://www.google.co	Delete	
	http://www.yahoo.co	Delete	
	http://wikipedia.org	Delete	
	http://www.msn.com	Delete	
	Save		

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

# 6.14 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.

neyee mesn		
Reyee Mesh 3.0	() СШМР	
AP Networking	СММР	
Link Aggregation	* Inform Interval	600
Routing	* ACS Address	http://127.0.0.1:8080/acs
Game Port Guarantee		
Flow Control	* ACS Account	0
Hardware Acceleration	* ACS Password	O
Port Settings	STUN	
Connectivity detection	* STUN Service Address	127.0.0.1
Wi-Fi Switch	* STUN Server Port	0
СШМР		
Other Settings	* STUN Server Account	0
Q Diagnostics	* STUN Server Password	0
🗄 System		Save
«Collapse		

# 6.15 Configuring APR Binding

### A Caution

This feature is supported in router mode.

# 6.15.1 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.

# 6.15.2 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.

Basics	i The device l	earns IP-MAC mapping of a	II devices connected to its interfa	aces. You can bind or filter the MAC ac	ldress.
ଙ୍କ WLAN					
🕼 Work Mode	ARP List		y IP/MAC Q	+ Add   ∅ Batch Bind	面 Batch Delete
Security	Up to 64 IP-M.	AC bindings can be added.			
	No.	MAC	IP	Туре	Action
🕎 VPN		70:b5:e8:76:f5:e9	192.168.111.170		
🗄 Advanced	2	ec:b9:70:13:db:e5	192.168.110.1		
Ø Diagnostics	Total 2 10/page		Go to page 1		
System					

# 6.16 Configuring Static Routing

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

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

## 🛕 Caution

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

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

₽ VPN × PBR S				
🖻 Advanced ^	ntic Routing			
Port Mapping	en a packet arrives, the device checks th stination network then it will forward the	e destination field and compare packet from the specified interf	is it against the routing face.	table. If it finds a match for (
Dynamic DNS Static F	Route List			+ Add 👘 Batch Dele
UPnP Settings	100 entries can be added.			
Local DNS				
Reyee Mesh	Dest IP Address Subnet Mask	Outbound Interface	Next Hop I	Reachable Action
Reyee Mesh 3.0				
AP Networking	10/page			Tot
Link Aggregation	. of log 2			
Routing				
Game Port Guarantee				
Flow Control				
Hardware Acceleration				
«Collapse				
Add				
* Dest IP Addres	s			
* Subnet Mas	k 255.255.255.0			
* Outbound Interfac	e Select			
t Nort Ho	_ [			
* Next Ho	p			
		Cancel	ОК	

### Table 6-2 Description of Static Routing Configuration

Parameter	Description
Dest IP Address	The destination network of the packet. The destination IP address of the packet is matched based on the destination IP address and subnet mask.
Subnet Mask	The subnet mask of the destination network. The destination IP address of the packet is matched based on the destination IP address and subnet mask.
Outbound Interface	Interface over which packets are forwarded.

Parameter	Description
	The IP address of the next-hop router to which the packet will be sent. If the
Next Hop	outbound interface is a PPPoE interface, there is no need to configure the next-
	hop IP address.

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

PBR						
0	Static Routing When a packet arrives, the destination network the				outing table. If it finds	a match for
Stat	tic Route List				+ Add	面 Batch Delete
Up	to <b>100</b> entries can be ac	lded.				
	Dest IP Address	Subnet Mask	Outbound The route is unrea	Next Hop achable. Initiate a Ping te	Reachable st from the outbound in	Action terface to the next hop.
	192.168.2.0	255.255.255.0	WAN	172.168.1.1	No 🕥	Edit Delete
K	1 2 10/page					Total 1

# 6.17 Policy-based Routing

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

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

#### 1. Overview

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

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

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

# 2. Configuration Steps

Click Add to add a PBR rule.

፼ VPN →	R Static Routing
🗄 Advanced 🔷 🚽	PBR
Port Mapping	Route Priority: PBR > Static Routing > ISP Routing.     Description PBR is more flexible than destination-based routing.
Dynamic DNS	PBR List + Add 🖻 Batch Delete
UPnP Settings	
Local DNS	Up to <b>30</b> entries can be added.
Reyee Mesh	■ Protocol Src IP Dest IP Src Port Dest Port Outbound ■ Name Type Address Address Range Range Interface
Reyee Mesh 3.0	
AP Networking	< 1 → 10/page → Total 0
Link Aggregation	
Routing	
Game Port Guarantee	
Flow Control	
Hardware Acceleration <u>«Collapse</u>	
Add PBR	×
* Name	
Protocol Type	IP ~
Src IP/IP Range	All IP Addresses
Dest IP/IP Range	All IP Addresses
Outbound Interface	WAN ~
Status	
	Cancel

## Table 6-3 Description of Policy-based Routing

Parameter	Description
Name	The name of the PBR rule, as the identifier of the PBR route. The name must be unique.
Protocol Type	The protocol for the PBR route to take effect, which can be IP, ICMP, UDP, TCP, or a custom protocol type as needed.

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

#### 1 Note

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

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

I VPN V	PBR	Static Rou	ıting								
Advanced ^	1			tic Routing > flexible than d		used routing.					0
Dynamic DNS	PBR	List							+ Ac	ld 🛅 🕅	Batch Delete
UPnP Settings	Up to	o 30 entrie	s can be adde	ed.							
Local DNS											
Reyee Mesh		Name	Protocol Type	Src IP Address	Dest IP Address	Src Port Range	Dest Port Range	Outbou nd Interfac	Status	Match Order	Action
Reyee Mesh 3.0											
AP Networking		test2	IP	2.2.2.2	3.3.3.3			WAN			
Link Aggregation											
Routing		test1	IP	All IP Addresse s	All IP Addresse s			WAN			
Game Port Guarantee											
Flow Control		1	10/page								Total 2
Hardware Acceleration <u>«Collapse</u>				6							

# 6.18 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.

፼ VPN ✓	Smart Flow Control	Custom Policy	
🗄 Advanced 🔷 🔿	Smart Flow Co	natral	
Port Mapping		ust the network speed to ensure that each user shares the network fairly.	0
Dynamic DNS	Enable	If you want to test the WAN rate, disable smart flow control first.	
UPnP Settings	WAN Bandwidth	Up 2500 Mbps * Down 2500 Mbps	
Local DNS		Save	
Reyee Mesh			
Reyee Mesh 3.0			
AP Networking Link Aggregation			
Routing			
Game Port Guarantee			
Hardware Acceleration <u> «Collapse</u>			

### 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.

Smart Flow	Control Custom Policy								
	stom Policy cate bandwidth to the specified	d IP address or range. The priority	y is sorted as follows: Cust	om Policy > Smart Flow Control.					?
Policy	List						Add	前 Batch Del	ete
Up to 3	o entries can be added.								
•	Policy Name	IP / IP Range	Bandwidth Type	Uplink Rate	Downlink Rate	Interface	Status	Effectiv e State	A
				No Data					
					X				

# 6.19 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.

### Configuration Guide

n	eyee mesh 5.0	
A	AP Networking	Port Flow Control Port Flow Control can mitigate the data congestion caused by ports at different speeds and improve the network speed.
L	ink Aggregation	Enable 💽
R	Routing	Save
G	Game Port Guarantee	
F	low Control	
F	lardware Acceleration	
	Port Settings	
C	Connectivity detection	
v	Vi-Fi Switch	
с	CWMP	
с	Other Settings	
Q	Diagnostics 🛛 🗸	
	System 💛	
	«Collapse	

# 6.20 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 ratelimited. You are advised to enable hardware acceleration when doing speed measurement.

neyee wesh b.u	
AP Networking	Hardware Acceleration After Hardware Acceleration is enabled, the Internet access speed will be improved and clients will not be rate-limited.
Link Aggregation	Enable
Routing	Save
Game Port Guarantee	
Flow Control	
Hardware Acceleration	
Port Settings	
Connectivity detection	
Wi-Fi Switch	
С₩МР	
Other Settings	
@ Diagnostics	
System	
«Collapse	

### 🛕 Caution

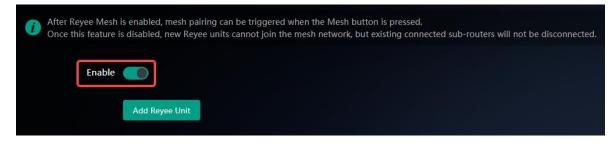
After hardware acceleration is enabled, IPv6 and smart flow control will be disabled.

# 6.21 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

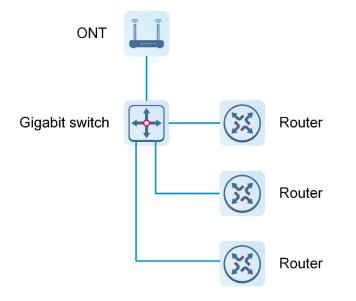
When Reyee Mesh is disabled, bridged mesh repeaters will not be disconnected.

# 6.22 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

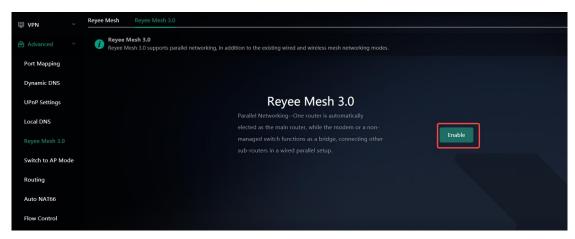
Connect the routers as indicated in the following figure:



### 6.22.1 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.



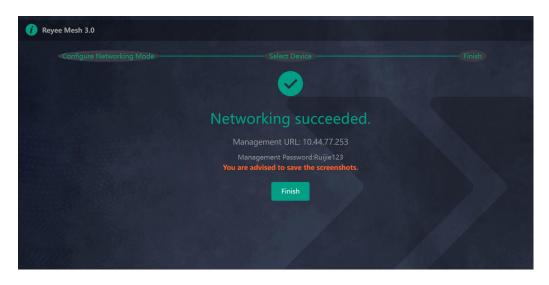
(2) Choose Parallel Networking, and click Next.

	AP Networking	
Advantage: All management		
	the bandwidth usage is high.	
Disadvantage: The latency is high	Disadvantage: Some management	
and the bandwidth usage is low.		
N	ext	

(3) Check routers for the networking.

0	Reyee M	Vlesh 3.0							
								Finish	
Sele	ect the ta	rget device.							
		Hostname		SN	Model	Networking Mode	M	AC	Software Ver
		Ruijie	M	ж		Parallel Networking	3	с	ReyeeOS 1.
	0	Reyee		1			1	4	ReyeeOS 1.
		Ruijie	M	IG		Parallel Networking	3	A	ReyeeOS 1.
		Ruijie	_	9			F	9	ReyeeOS 1.
					Previous	Next			

(4) Click Next.



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

rent Mode:Parallel Network	ing Add Device			
		N	o Data	
	htt	p://10.44.77.253 Redirectin	g 1s	

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

## 6.22.2 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.

₩ VPN ×	Reyee Mesh 3.0	
	Reyee Mesh 3.0 Reyee Mesh 3.0 supports parallel networking, in addition to the existing wired and wireless mesh networking modes.	
Port Mapping		
Dynamic DNS		
UPnP Settings	Reyee Mesh 3.0	
Local DNS	Parallel NetworkingOne router is automatically elected as the main router, while the modem or a non-	Enable
	managed switch functions as a bridge, connecting other sub-routers in a wired parallel setup.	
Switch to AP Mode		
Routing		
Auto NAT66		
Flow Control		

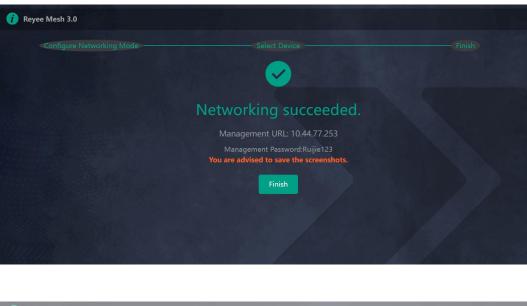
(2) Choose AP networking, and click Next.

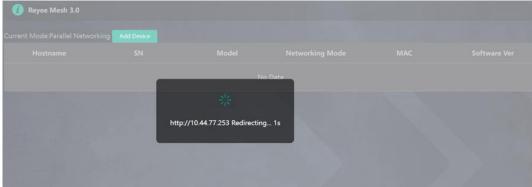
Select	Device	
Parallel Networking		
Advantage: All management	Advantage: The latency is low and	
	the bandwidth usage is high.	
Disadvantage: The latency is high	Disadvantage: Some management	
and the bandwidth usage is low.		
	ext	

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

							- Finisl	
elect the tar	get device.							
	Hostname	s	N	Model	Networking Mode	MAC		Software Ve
	Ruijie	MA	DT		Parallel Networking	3(	с	ReyeeOS 1
	Ruijie	G	5	E		F	, ,	ReyeeOS 1
•	Ruijie	MA	NG		Parallel Networking	3(	٩	ReyeeOS 1
	Reyee	м	21			1	•	ReyeeOS 1
				Previous	Back			
				Previous	Back			

(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.

# 6.23 Configuring UpnP

### A Caution

This feature is supported in router mode.

### 6.23.1 Overview

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

## 6.23.2 Configuration Steps

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

PC View: Choose More > Advanced > UPnP Settings.

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

<ul> <li>♥ WLAN</li> <li>♥ Work Mode</li> <li>♥ Security</li> <li>♥ VPN</li> <li>♥ Advanced</li> </ul>	UPnP Settings UPnP (Universal Plu Enable	g and Play) UPnP is a nev	v Internet protocol aimed at impr	oving communication betwe	een devices. Ø
Port Mapping	Protocol	Арр	Client IP Address	Internal Port	External Port
Dynamic DNS					
UPnP Settings					
Local DNS					
Reyee Mesh					
Reyee Mesh 3.0					
AP Networking					
Link Aggregation					
Routing «Collapse				Carl State	

# 6.24 Enabling Wi-Fi Switch

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

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

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

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

neyee mesh 5.0	
AP Networking	Wi-Fi Switch  I takes 30 seconds to activate settings after the Wi-Fi switch is turned on. The Wi-Fi function is disabled on the device after the Wi-Fi switch is turned off.
Link Aggregation	
Routing	Wi-Fi Switch
Game Port Guarantee	Save
Flow Control	
Hardware Acceleration	
Port Settings	
Connectivity detection	
Wi-Fi Switch	
СWMP	
Other Settings	
@ Diagnostics	
System	
«Collapse	

# 6.25 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

₽ VPN ×	Switch to AF Switch the rou	• Mode uter found on the local net	work to AP mode with a	single click.			
🗄 Advanced 🛛 ^	Model	IP	Work Mode	МАС		Software Ver	
Port Mapping	EW3000GX	192.168.110.1	ROUTER	0A: :76	MA /ZH	ReyeeOS 1.	
Dynamic DNS		10/page 🗸			10000		Total 1
UPnP Settings							
Local DNS	Switch To AP N	Mode					
Reyee Mesh 3.0							
Switch to AP Mode							
Routing							é

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

# 6.26 Configuring PPTP VPN

## 6.26.1 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.

### 6.26.2 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.

PPTP Settings Online	User	
<i>i</i> PPTP Settings		
Enable		
РРТР Туре	Server Client	
* Local Tunnel IP	Example: 1.1.1.1	
* VPN Subnet/Netmask	Example: 1.1.1.2-1.1.1.100	0
* DNS Server	Example: 1.1.1.1	
МРРЕ	Disable Enable	
* PPP Hello Interval	10	seconds
	Save	

(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.

Account			Username/Passwo		+ Add	面 Batch Delete
Up to 8 e	ntries can be added.					
	Username	Password	Network Mode	Status		Action
			No Data			
< 1	10/page					Total 0

Add User			×
* Username	Enter a username.		
* Password	Enter a password.		٢
Network Mode	PC to Router		]
Status			
		Cancel	ОК

## 6.26.3 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.

PPTP Settings Online	User	
PPTP Settings		
Enable	•	
РРТР Туре	Server O Client	
* Username	Username of PPTP user	
* Password	Password of PPTP user	•
Interface	WAN	
Tunnel IP	O Dynamic O Static	
*Service Address	IP/Domain	
* Peer Subnet	Example: 192.168.110.0/24	
МРРЕ	• Disable • Enable	
Work Mode	NAT  Router	
* PPP Hello Interval	10	
	Save	

# 6.27 Configuring OpenVPN

## 6.27.1 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.

## 6.27.2 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

OpenVPN	Online User		and the state of the state
🕧 Open	VPN		
	Enable 🧲	D	
Ope	enVPN Type 🏮	Server 🔵 Client	
	Service Mode	Certificate	
	Service Type	тср	
<b>∳</b> s	ervice Address	IP/Domain	
	• Service Port	11940	1-65535
* VPN Su	ibnet/Netmask	10.80.12.0/24	0
	Client Access	Home Network Only	
		- Grpans	
		Save	
Cor	nfiguration File	Export	
	CA Certificate	Export	

(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.

		Collapse			
TLS Authentication (					
Allow Data Compression	Yes		0		
Cipher	AES-128-CBC		8		
Deliver DNS	Example: 1.1.1.1		• +		
Authentication	SHA256				

(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 6-4 Configuration Items of OpenVPN Server Mo
----------------------------------------------------

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

Item	Description
	<ul> <li>server.</li> <li>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.</li> </ul>
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.

Account				+ Add
Up to 8 entr	ies can be added.			
	Username	Password	Status	Action
		No Data		
< 1 >	10/page 🗸			Total 0

Add User			×
* Username			]
* Password	Enter a password.		٥
Status			
		Cancel	ОК

## 6.27.3 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.

OpenVPN Online User		
🥡 OpenVPN		
Enable		
OpenVPN Type 🌑	Server 🧿 Client	
Service Mode	Account & Certificate ~	
* Username	Username of OpenVpn user	9
* Password	Password of OpenVpn user	9
* Client Config	.ovpn Browse	
	Save	

Parameter	Description
	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.
Server Mode	• <b>Certificate mode</b> : 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.
Licername and peopulard	Enter the username and password configured on the server.
Username and password	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.

# 6.27.4 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.

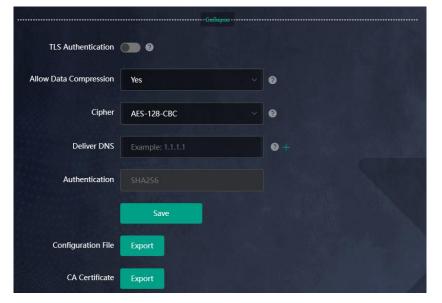
If the router does not have a public IP address, contact the ISP to obtain a public IP address.

OpenVPN Online User				751.46 2.4
🥡 OpenVPN				
Enable 🧲	•			
OpenVPN Type 🏼 💿	Server 🔵 Client			
Service Mode	Certificate			
Service Type	ТСР			
* Service Address	192.168.50.94			
* Service Port	11940			
* VPN Subnet/Netmask	10.80.12.0/24		0	
Client Access	Home Network Only			
	Save	aparel .		

- (2) Click **Save**. The OpenVPN settings are saved.
- (3) The following table describes the OpenVPN server configuration.

Parameter	Description		
Service Mode	<ul> <li>Account: Authentication based on password.</li> <li>Certificate: Authentication based on client certificate.</li> <li>Account &amp; Certificate: Authentication based on password and client certificate.</li> </ul>		
Service Type	Use the default value unless there are specific requirements. Both <b>UDP</b> and <b>TCP</b> 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 <b>TCP</b> .		
Service Address	The IP address of the WAN port is automatically populated.		
Service Port	Indicates the port for OpenVPN service. Use the default value unless there are specific requirements.		
VPN Subnet/Netmask	Indicates the network segment of the OpenVPN address pool. The first available IP address in the address pool is reserved for the server, while other addresses can be allocated to clients. For example, if this parameter is set to <b>10.80.12.0/24</b> , then the virtual IP address of the VPN server is 10.80.12.1.		
Client Access	<ul> <li>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.</li> <li>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.</li> </ul>		

(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 (<u>https://openvpn.net</u>).



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

OpenVPN	Connect		- ×
≡	Impor	t Profile	Ð
	URL	FILE	
		ipload .OVPN pro one profile at a	
	~	~	
	.01		
		·	
	BR	OWSE	

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

penVPN Connect - ×				
<	Impor	rted Pro	file	
Profile N	ame			
192.16	8.50.94 [2023	0614_clie	nt]	
Server H	ostname (locked)			
192.16	8.50.94			
	PROFILES	1	CONNECT	

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

OpenVPN Connect				
≡	Profiles	10		
CONNEC	CTED			
	OpenVPN Profile 192.168.50.94 [20230614_client]			
CONNEC	CTION STATS			
5.3KB/s				
0B/s				
BYTES IN 0 KB/S	BYTES 0 313 B/S	UT		
DURATION 00:00:12				
YOU	•	Ð		

(5) Check the obtained virtual IP addresses.

OpenVPN Connect	Drefiles	– × •
=	Profiles	Ð
OB/s		
	1 BYTES 2.47 K	
DURATION 00:00:17	PACKET RECEIVED <b>0 sec ago</b>	
YOU		
YOUR PRIVATE IP 10.80.12.2		
SERVER		
192.168.50.94		
SERVER PUBLIC IP 192.168.50.94		
PORT 11940	VPN PROTOCOL TCPv4	
		0

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

enVPN C	Inline User				
🧿 Online U	ser				
1	Username	Server/Client	Status	Real IP Address	Virtual IP Address

## 6.27.5 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.

<i>i</i> Auto NAT66						
	Enable 🗾	]				
		Save				

# 6.28 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.

i Other Settings		
Enable Advanced Firewall	• •	
Disable ICMPv6 Error Messages		
	Save	

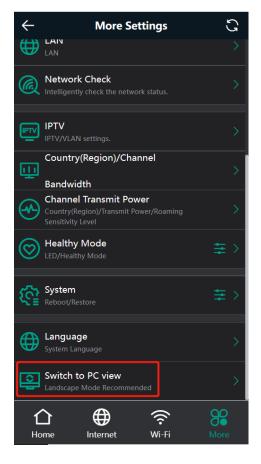
# **7** System Settings

# 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).

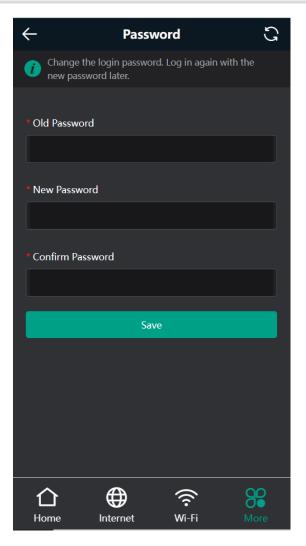


# 7.2 Configuring the Login Password

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.

## A 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 <u>7.2</u> Configuring the Login Password to configure a strong and secure device management password.

@ n :	~	
Basics		Login Password Session Timeout Remote Access
ଙ୍କ WLAN		Remote Access     Allow others to log in to the device through URL link
🔟 Work Mode		Allow others to log in to the device through UKL link
🛇 Security		Enable 🗾
孁 VPN		Login URL http://192.168.110.143
🗄 Advanced		Save
Diagnostics		
:#: System		
System Time		
Login		
Management		
Upgrade		
LED		
Reboot 《Collapse		

# 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.

#### A Caution

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

## I 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.

🥡 Restoring a router to	factory default settings will clear the current settings of the router. If you want to keep the current settings, click Backup Config to back up the configuration file first.	
Keep Config		
Reset		

# 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.

H Dasics				
ଙ୍କ WLAN	~	(i) Configure and vie	w system time	
🕼 Work Mode		Current Time	2023-06-26 03:55:44	Edit
Security	~	* Time Zone	(GMT-5:00)America/No	ew_York 🗸
₩ VPN	~	* NTP Server	0.cn.pool.ntp.org	Add
🗄 Advanced	~		1.cn.pool.ntp.org	Delete
@ Diagnostics	~			
	^		cn.pool.ntp.org	Delete
			pool.ntp.org	Delete
Login			asia.pool.ntp.org	Delete
Management	t		europe.pool.ntp.org	Delete
Upgrade			ntp1.aliyun.com	Delete
LED				
Reboot			Save	
«Collapse	e			

# 7.6 Configuring Scheduled Reboot

## 7.6.1 Getting Started

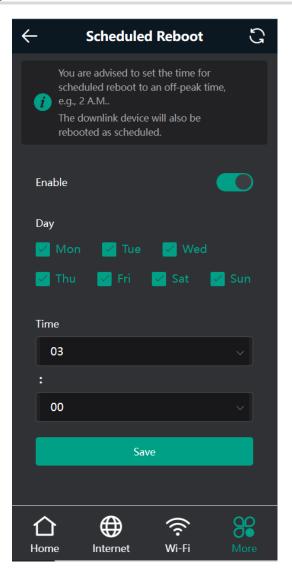
Confirm that the system time is accurate to avoid network interruption caused by device reboot at the wrong time. For details, see <u>7.5</u> Configuring System Time.

## 7.6.2 Configuration Steps

Smartphone View: Choose More > System > Scheduled Reboot.

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

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



# 7.7 Performing Online Upgrade and Displaying the System Version

Smartphone View: Choose More > System >Online Upgrade.

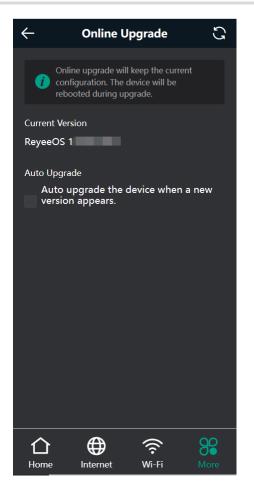
PC View: Choose More > System > Upgrade > Online Upgrade.

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.

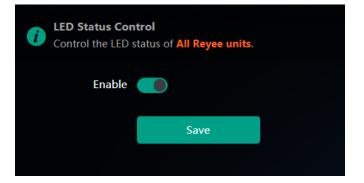
If no new version is detected and online upgrade cannot be performed, check whether the DNS is correctly obtained or go to **More** > **Advanced** > **Local DNS** to set the DNS server for the router.



# 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

glish ~

in the upper right corner of the page.

Click a required language to switch the system language.

←		Lang	uage	S
	中文			
	繁體			
•				
	Indonesia			
	ไทย			
	Việt Nam			
	русский			
	Türkiye			
	español			
	العربية			
	Italiano			
	Čeština			
и Н	<b>À</b> Iome	Haternet	( Wi-Fi	More

# 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.

Basics     Basics     Basics     Basics     Basics     Compared to the second	View and ma	nage alarms.		
ଙ୍କ WLAN	Alert List			View Unfollowed Alert
🕼 Work Mode				
😔 Security	× Expand Alerts		Suggestion	Action
孁 VPN				
🗄 Advanced	× (1)	10/page v		Total 0
Diagnostics     Diagno				
Network Check				
Alerts				
Network Tools				
Packet Obtaining				
-9 -9- System				
«Collapse				

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.

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.

Alerts	Suggested Action
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.

Basics		🥡 Network Check		
ବ୍ଚ WLAN				
		Start		
Work Mode				
Security				
👳 VPN				
A				
🗄 Advanced				
Diagnostics     Diagno				
Network Check				
Alerts				
Aicits				
Network Tools				
Packet Obtaining	g			
System	~			

# 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.

Basics ~	i Network Tools			0
়ি WLAN ৺	ТооІ	💿 Ping 💿 Traceroute	DNS Lookup	
Work Mode				
	* IP Address/Domain	8.8.8.8		
Security				
፼ VPN ∽	* Ping Count	4		
🗄 Advanced 🛛 👋	* Packet Size	64	Bytes	
Q Diagnostics     ^		Chert		
~		Start	Stop	
Network Check				
Alerts				
Network Tools				
Packet Obtaining				
÷esse System ∨				
«Collapse		C S		

## 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.

	1	08	and the second				
) Bas	ics		i Packet Obtainin	9			0
ଙ୍କ WL	AN		Interface	ALL			
🕼 Wo	rk Mode						
🕝 Sec	urity		Protocol	ALL			
🛒 VPI	N		IP Address				
🗄 Adv	vanced		File Size Limit	2М		Available Memory 284.58 M	
			Packet Count Limit	500			
Netw	vork Check						
Alert	s			Start	Stop		
Netw	vork Tools						
	et Obtaininç						
쁢 Sys	tem						
*	Collapse				Santan Santa		and the second

## 🛕 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.

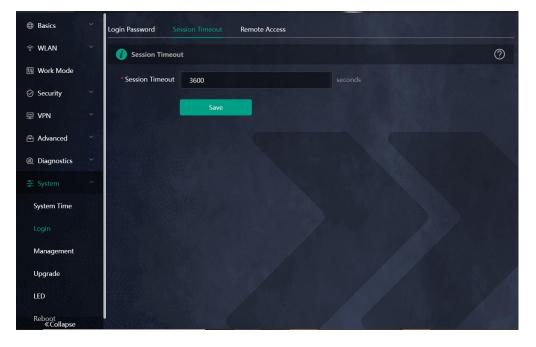
Basics ×	Backup & Import Reset	
	If the target version is much later than the current version, some configuration may be missing.	0
Mork Mode	You are advised to choose Reset before importing the configuration. The device will be rebooted automatically later.	Ŭ
⊘ Security ×	Backup Config	
፼ VPN [∨]	Backup Config Backup	
🗄 Advanced 🛛 👻	Import Config	
@ Diagnostics	File Path Select a file. Browse Import	
System ^		
System Time		
Login		
Management		
Upgrade		
LED		
Reboot «Collapse		

# 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:
  - o 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 <u>3.4</u> 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: <u>https://reyee.ruijie.com/en-global/rita</u>
- Community: <u>https://community.ruijienetworks.com</u>
- Service hotline: <u>https://www.ruijienetworks.com/support/hotline</u>