

Ruijie Reyee Home Wi-Fi Router

Implementation Cookbook



Document Version: V1.5 Date: 2024-02-02 Copyright © 2024 Ruijie Networks

Copyright

Copyright © 2024 Ruijie Networks

All rights are reserved in this document and this statement.

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



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

Disclaimer

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

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

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

Preface

Technical Support

- The official website of Ruijie Reyee: https://www.ruijienetworks.com/products/reyee
- Technical Support Website: <u>https://www.ruijienetworks.com/support</u>
- Case Portal: <u>https://www.ruijienetworks.com/support/caseportal</u>
- Community: <u>https://community.ruijienetworks.com</u>
- Technical Support Email: <u>service_rj@ruijienetworks.com</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	Select System > Time.	

2. Signs

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

Warning

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

🛕 Note

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

Instruction

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

Specification

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

3. Instruction

This manual is used to guide users to understand the product, install the product, and complete the configuration.

- The example of the port type may be different from the actual situation. Please proceed with configuration according to the port type supported by the product.
- The example of display information may contain the content of other product series (such as model and description). Please refer to the actual display information.
- The routers and router product icons involved in this manual represent common routers and layer-3 switches running routing protocols.

Contents	
----------	--

Preface I
1 Introduction to Reyee Products
1.1 Product List
1.2 LED2
1.3 Button
2 Reyee Login
2.1 Connecting to the Router
2.2 Logging In
3 Reyee Quick Start 10
3.1 Internet Access Modes10
3.2 Primary Router Mode10
3.2.1 Getting Started10
3.2.2 Configuration Steps11
3.2.3 Verification and Testing13
3.2.4 Forgetting the PPPoE Account13
3.3 Secondary Router Mode14
3.3.1 Getting Started14
3.3.2 Configuration Steps14
3.3.3 Verification and Testing21
4 Reyee Wi-Fi Network Settings
4.1 Changing the SSID and Password22
4.2 Hiding the SSID23
4.2.1 Overview

4.2.2 Getting Started	23
4.2.3 Configuration Steps	23
4.3 Adding a Wi-Fi Network	24
4.3.1 Overview	24
4.3.2 Configuration Steps	25
4.3.3 Verification and Testing	25
4.4 Configuring a Wi-Fi Blacklist or Whitelist	25
4.4.1 Overview	25
4.4.2 Configuration Steps	25
4.5 Optimizing the Wi-Fi Network	
4.5.1 Overview	
4.5.2 Getting Started	
4.5.3 Configuration Steps	
4.6 Configuring the Healthy Mode	31
4.7 Enabling Roaming Optimization	
5 Reyee Networks Settings	
5.1 Configuring Internet Connection Type	
5.2 Changing the Address of a LAN Port	
5.3 Changing the MAC Address	34
5.4 Changing the MTU	35
5.5 Configuring the Repeater Mode	
5.5.1 Wired Repeater	
5.5.2 Wireless Repeater	
5.5.3 WISP	

5.6 Controlling the Internet Access Time Range		
5.7 Configuring XPress	40	
5.8 Configuring Port Mapping	41	
5.8.1 Overview	41	
5.8.2 Getting Started	41	
5.8.3 Configuration Steps	41	
5.8.4 Verification and Testing	42	
5.8.5 Solution to a Test Failure	42	
5.8.6 DMZ Configuration Steps	42	
5.9 Configuring the DHCP Server	43	
5.9.1 Overview	43	
5.9.2 Configuration Steps	43	
5.10 Configuring DNS	46	
5.11 Configuring DDNS	47	
5.11.1 Overview	47	
5.11.2 Getting Started	47	
5.11.3 Configuration Steps	47	
5.12 Configuring APR Binding and ARP Guard	47	
5.12.1 Overview	47	
5.12.2 Configuration Steps	47	
5.13 Configuring Static Routing	48	
5.14 Policy-based Routing	50	
5.15 Connecting to IPTV	53	
5.15.1 Getting Started	53	

5.15.2 IPTV Configuration Steps (VLAN Type)	53
5.15.3 IPTV Configuration Steps (IGMP Type)	54
5.16 Configuring Wi-Fi/IGMP	55
5.16.1 Overview	55
5.16.2 Configuration Steps	55
5.17 Configuring IPv6	56
5.17.1 Configuring the IPv6 of the WAN Port	56
5.17.2 Configuring the IPv6 of the LAN Port	56
5.18 Enabling Smart Flow Control	57
5.19 Configuring Firewall	58
5.20 Enabling Wi-Fi Switch	59
5.21 Configuring UPnP	60
5.21.1 Overview	60
5.21.2 Configuration Steps	60
5.22 Configuring PPTP VPN	60
5.22.1 Overview	60
5.22.2 Configuring PPTP Server	60
5.22.3 Configuring the PPTP Client	62
5.23 Configuring OpenVPN	63
5.23.1 Overview	63
5.23.2 Configuring OpenVPN (Server Mode)	64
5.23.3 Configuring OpenVPN (Client Mode)	67
5.23.4 Typical Configuration Example	68
5.24 Configuring Connectivity Detection	75

	5.25 Enabling CWMP	76
	5.25.1 Overview	76
	5.25.2 Configuration Steps	76
	5.26 Enabling Reyee Mesh	77
	5.27 Enabling Hardware Acceleration	78
	5.28 Configuring Console Booster	79
	5.29 Configuring AP Networking	79
	5.30 Configuring Reyee Mesh 3.0	80
	5.30.1 Configuration Steps	80
	5.31 Diagnosing Network Problems	84
6	Reyee System Settings	85
	6.1 Switching to the PC View	85
	6.2 Configuring the Login Password	85
	6.3 Remote Access	86
	6.4 Restoring Factory Settings	87
	6.5 Configuring the System Time	87
	6.6 Configuring Scheduled Reboot	88
	6.6.1 Getting Started	88
	6.6.2 Configuration Steps	88
	6.7 Performing Online Upgrade and Displaying the System Version	89
	6.8 Enabling or Disabling the LED	90
	6.9 Switching the System Language	90
	6.10 Network Diagnosis Tools	91
	6.10.1 Network Test Tool	91

6.10.2 Packet Obtaining Tool91
6.11 Configuring Backup and Import92
6.12 Configuring the Session Timeout93
7 Reyee FAQ
7.1 Reyee Password FAQ (Collection)94
7.2 Reyee Wireless Repeater FAQ (Collection)94
7.3 Reyee Parental Control FAQ (Collection)94
7.4 Reyee Mesh FAQ (Collection)94
7.5 Reyee Self-Organizing Network (SON) FAQ (Collection)94
7.6 Reyee series Devices Parameters Tables94
7.7 Reyee Parameter Consultation FAQ (Collection)94
8 Appendix: Monitoring of Reyee Mesh Wi-Fi Routers
8.1 Overview
8.2 Endpoints95
8.3 Internet

1 Introduction to Reyee Products

Reyee EW series products are gigabit dual-band Wi-Fi 6 wireless routers designed for large flat space, villas, small shops, SOHO, and other scenarios. It is designed to meet the needs of high-quality next-generation Wi-Fi services. Reyee EW series products support various local and remote management platforms, such as web and Ruijie Cloud App. This wireless router also provides multiple home-care-based function, including the parental control mode, health mode, and Xpress mode, and is exclusively designed for Smart Life Kit System, meeting needs of all household scenarios.



1.1 Product List

Model	Reyee Mesh	Wi-Fi Standards	Maximum Wi-Fi Rate	МІМО	Recommended Users
EW300 PRO	Not supported	Wi-Fi 4 (802.11n)	2.4 GHz: 300 Mbps	2.4 GHz: 2×2	8
EW300N	Not supported	Wi-Fi 4 (802.11n)	2.4 GHz: 300 Mbps	2.4 GHz: 2x2	8
5144000	Quantation	Wi-Fi 5 (802.11ac)	2.4 GHz: 300 Mbps	2.4 GHz: 2×2	2.4 GHz: 8
EVV1200	Supported		5 GHz: 867 Mbps	5 GHz: 2×2	5 GHz: 16
	Supported	Wi-Fi 5 (802.11ac)	2.4 GHz: 400 Mbps	2.4 GHz: 2×2	2.4 GHz: 8
	Supported		5 GHz: 867 Mbps	5 GHz: 2×2	5 GHz: 24
EW1800GX	Supported	W/i Ei 6 (802 11ox)	2.4 GHz: 573 Mbps	2.4 GHz: 2×2	2.4 GHz: 12
PRO	Supported	WI-FT0 (002.11ax)	5 GHz: 1200 Mbps	5 GHz: 2×2	5 GHz: 36
EW3200GX	Cupported		2.4 GHz: 800 Mbps	2.4 GHz: 4×4	2.4 GHz: 12
PRO	Supported	vvi-F1 6 (802.11ax)	5 GHz: 2400 Mbps	5 GHz: 4×4	5 GHz: 48

1

Model	Reyee Mesh	Wi-Fi Standards	Maximum Wi-Fi Rate	МІМО	Recommended Users
M18	Supported	Wi-Fi 6 (802.11ax)	2.4 GHz: 574 Mbps 5 GHz: 1201 Mbps	2.4 GHz: 2×2 5 GHz: 2×2	2.4 GHz: 12 5 GHz: 36
M32	Supported	Wi-Fi 6 (802.11ax)	2.4 GHz: 800 Mbps 5 GHz: 2402 Mbps	2.4 GHz: 4×4 5 GHz: 4×4	2.4 GHz: 12 5 GHz: 48
EW3000GX PRO	Supported	Wi-Fi 6 (802.11ax)	2.4 GHz: 573 Mbps 5 GHz: 2401 Mbps	2.4 GHz: 2×2 5 GHz: 2×2	2.4 GHz: 12 5 GHz: 48
EW1300G	Supported	Wi-Fi 5 (802.11ac)	2.4GHz: 400 Mbps 5GHz: 867 Mbps	2.4 GHz: 2×2 5 GHz: 2×2	2.4 GHz: 8 5 GHz: 24

1.2 LED

(a) EW300 PRO System LED

Status	Description
Off	The router is not powered on.
Solid on	The router is running normally.
Fast blinking (on for 62 ms, off for 62 ms)	The router is starting up or powered off.
Slow blinking (on for 250 ms, off for 250 ms)	The Internet is unreachable.
East blinking twice	The router is restored to factory settings.
	The firmware is upgraded.
Slow blinking once and fast blinking three times	The firmware is faulty.

(b) EW300N System LED

Description	Status	
The router is starting up.	Blinking green	
The router is connected to the Internet.	Solid green	

The router is not connected to the Internet.	Solid red
The router is resetting.	Blinking green
The router is upgrading.	Blinking green
The router is rebooting.	Blinking green

(c) EW1200

LED	Status	Description
	Off	The router is not powered on.
	Solid on	The router is running normally.
System Status LED	Slow blinking (one interval of 1.75 seconds: on for 250 ms, off for 250 ms)	The router is initialized.The router does not access the Internet.
	Fast blinking (on for 62.5 ms, off for 62.5 ms)	 The router is restored to factory settings. The router restarts. The router is initialized. The firmware is upgraded.
Wi-Filed	Solid on	Reyee mesh router is sunning normally.
	Slow blinking	Reyee mesh router is being paired or the repeater stops.
	Off	The port is not connected or the cable is disconnected.
	Solid on	The port is connected normally.

(d) EW1200G PRO

LED	Status	Description
	Off	The router is not powered on.
	Solid on	The router is running normally.
	Fast blinking	The router is restored to factory settings. The router restarts.
System Status LED	Slow blinking (one interval of 1.75 seconds: on for 250 ms , off for 250 ms)	The router is initialized. The router does not access the Internet.
	Slow blinking (alternately on for 40 ms and off for 150 ms)	Reyee mesh router is being paired or the repeater stops.

LED	Status	Description
Port LED -	Off	The port is not connected or the cable is disconnected.
	Solid on	The port is connected normally.
	Blinking	Data is being transmitted.

(e) EW1800GX and EW3200GX PRO

LED	Color/Status		Description
Mesh LED	Green	Blinking	The router is being paired.
		Solid on	The router is paired and Wi-Fi signals are normal.
	Orange	Solid on	The router is paired but Wi-Fi signals are weak.
	Red	Solid on	Device pairing is disconnected.
System Status LED	Blue	Solid on	The router is running normally.
		Fast blinking (on for 62.5 ms, off for 62.5 ms)	The router is restored to factory settings. The router restarts. The firmware is upgraded.
		Slow blinking (one interval of 1.75 seconds: on for 250 ms , off for 250 ms)	The router is initialized. The router does not access the Internet.

(f) M18 and M32

LED	Status	Description
Reyee Mesh Indicator	Blinking white	The device is being paired
	Four bars are solid white	The Mesh network signal is excellent.
	Three bars are solid white	The Mesh network signal is good
	Two bars are solid white	The Mesh network signal is average.
	One bar is solid white	The Mesh network signal is poor.
	Off	The Mesh network is disconnected or not set up.

LED	Status	Description
System Status Indicator (Reyee Mesh Button)	Solid blue	The device is working normally and can access the Internet.
	Solid orange	The device does not access the Internet.
	Blinking blue	The device is starting up or restoring the factory settings.

(g) EW3000GX PRO

LED	Color/Status		Description
	Solid on		Mesh pairing succeeds.
Reyee Mesh Indicator	Off		Mesh pairing is not performed./Mesh network is disconnected.
	Blinking		Mesh pairing is in progress.
Green System Status Indicator Orange	Green	Solid on	The router is functioning properly or is connected to the Internet.
		Blinking	The router is starting up, being reset, or upgrading.
	Orange	Solid on	The signal strength of the mesh link is low (secondary router).
	Red	Solid on	The router is not connected to the Internet.

(h) EW3000GX PRO

LED	Color/Status		Description
	Solid on		Mesh pairing succeeds.
Reyee Mesh Indicator	Off		Mesh pairing is not performed./Mesh network is disconnected.
	Blinking		Mesh pairing is in progress.
System Status Indicator Orange	Green	Solid on	The router is connected to the Internet, or to the primary route, with an RSSI > -78dBm.
		Blinking	The router is starting up, being reset, or upgrading.
	Solid on	The mesh connection is weak, with an RSSI \leq -78dBm.	

LED	Color/Stat	us	Description
	Red	Solid on	The router is not connected to the Internet, or to the primary router when used as a secondary router.

1.3 Button

(a) EW300 PRO

Button	Function	Operation
Reset Reset	Press the button for over 3 seconds until the LED starts to blink.	
	Release the button. Then the router is reset.	

(b) EW1200 and EW1200G PRO

Button	Function	Operation
Pairing/Reset	Pair	Press the button for 1 second to pair the router.
	Reset	Press the button for over 10 seconds until the LED starts to blink. Release the button. Then the router is reset.

(c) EW1800GX and EW3200GX PRO

Button	Function	Operation
Reyee Mesh Button	Pair	Press the button for 1 second to pair the router.
Reset Button	Reset	Press the button for over 10 seconds until the LED starts to blink. Release the button. Then the router is reset.

(d) M18 and M32

Button	Function	Operation
Reyee Mesh Button	Pair	Press the button for 1 second to pair the router.
Reset Button	Reset	Press the button for over 10 seconds until the LED starts to blink. Release the button. Then the router is reset.

(e) EW3000GX PRO

Button	Function	Operation
Reyee Mesh Button	Pair	Press the button for 1 second to pair the router.
Reset Button	Reset	Press the button for over 10 seconds until System Status Indicator starts to blink. Release the button. Then the router is reset.

(f) EW1300G

Button	Function	Operation
Reyee Mesh Button	Pair	Press the button for 1 second to pair the router.
Reset Button	Reset	Press the button for over 10 seconds until the LED starts to blink. Release the button. Then the router is reset.

2 Reyee Login

2.1 Connecting to the Router

You can open the management page and complete Internet access configuration only after connecting a PC or a mobile phone to the router. You can connect a PC to the router in either of the following ways, and connect a mobile phone to the router in wireless connection mode.

Wired connection

Connect a local area network (LAN) port of the router to the network port of the PC, and configure **Obtain an IP address automatically** on the PC. The EW300 is used as an example. The following figure shows the connection between the router and laptop.



Wireless connection

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

2.2 Logging In

When a PC or a mobile phone connects to a router in initial state, the configuration wizard page appears. If the configuration page does not appear, enter the device IP address into the address bar of the browser to navigate to the login page, and then enter the password for login.

 Table 2-1
 Default Configuration

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

If you forget the IP address or password, hold down the **Reset** button for more than 5 seconds to restore factory settings. Then you can use the default IP address and password to log in.

A Note

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

If the router in 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 1 minute later.

3 Reyee Quick Start

3.1 Internet Access Modes

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

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

Secondary Router Mode: On an available network, the device can be connected to the primary router through either the wired or wireless connection to expand the Wi-Fi coverage and increase the number of LAN ports and wireless access devices. The wireless repeater mode includes the repeater mode and wireless Internet service provider (WISP) mode.

Instruction

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

3.2 Primary Router Mode

3.2.1 Getting Started

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



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

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

3.2.2 Configuration Steps

1. Configuring an Internet Connection Mode

Click Configure and select the Internet connection mode confirmed by the carrier.

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

A Note

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

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



2. Configuring a Wi-Fi Network

(1) Setting the SSID and Wi-Fi password: The 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 64 characters, which can contain uppercase and lowercase letters, digits, and English characters. It cannot contain special characters such as single quotation marks ('), double quotation marks ('), or spaces.

- (2) Setting the management password: The password is used for logging in to the management page. The management password must be a string of 8 to 64 characters and contain at least three types among uppercase letters, lowercase letters, digits, and English characters. It cannot contain admin, Chinese characters, spaces, or question marks (?). You can select **Same as Wi-Fi Password**.
- (3) Enabling the Wi-Fi 6: Wi-Fi 6 can provide a faster and more stable network for Wi-Fi 6-capable clients. You are advised to enable this function.

A Caution

Only EW1800GX-PRO and EW3200GX-PRO support Wi-Fi 6.

- (4) Setting the country or region: A Wi-Fi channel may vary according to the country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.
- (5) Setting the time: The network time server is enabled by default to provide the time service. You are advised to select the actual time zone.
- (6) Overriding the configuration: Click **Override**. The Wi-Fi network will restart. You need to enter the new Wi-Fi password to connect to the new Wi-Fi network.

Wizard	Wizard
Wi-Fi Settings	@Ruijie-sFC86_5G
Dual-Band Single SSID	Wi-Fi Password
* SSID (2.4G) Large Coverage & Slow Rate	
@Ruijie-sFC86	Management Password
* SSID (5G) Small Coverage & Fast Rate	* Management Password
@Ruijie-sFC86_5G	(Please remember the password.)
* Wi-Fi Password	The password is 8-31 characters long.
Please enter a Password.	Country/Region/Time Zone
Management Password Same as Wi-Fi Password	* Country/Region
* Management Password	China (CN) 🗸
(Please remember the password.)	* Time Zone
The password is 8-31 characters long.	(GMT+8:00)Asia/Shanghai v
Previous Override	Previous Override



3.2.3 Verification and Testing

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



3.2.4 Forgetting the PPPoE Account

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

-	Internet	S	Obtain PPPoE Account from Old F	Router
iternet:		Online (DHCP)	Old Router	New Router
PPPoE	DHCP	Static IP		
* Username		Provided by ISP		
Please enter a Pl	PPoE username.			
* Password	Obtain Accou	unt from Old Device		• • • • • •
Password		***	Steps:	
Service Name			1. Transmit Power on the old router a	nd new router.
(Optional) Provid	ded by ISP		Connect one end of a cable to the connect the other end to the LAN po	WAN port of the old rt of the new router.
			3. Click "Obtain".	
	Save		Obtain	

3.3 Secondary Router Mode

3.3.1 Getting Started

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

3.3.2 Configuration Steps

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

1 Note

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

2. Wireless Connection by using the Reyee Mesh function

- (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.

3. Wireless Connection by Web configuration

4. Wireless Repeater Mode

(1) Click **Wireless Repeater**, select **Country/Region** and **SSID** of the primary router, and enter the Wi-Fi password to connect to the primary router.



<	Country/Region	
	Country/Region	
	Country/Region	
	China (CN) ~	
	Time Zone	
	(GMT+8:00)PRC ~	
	Next	

Image: Solution of Solu	\leftarrow	Wireless Repeating	
so @Ruijie:s49FD_5G			G
so method with the solution of		5G @Ruijie-s49FD_5G	≙ (
so so so so so so so so so so so so so s		5G	∂ ≈
50 fmmm mt 50 fmmm fmmm <		56	A 🛜
50 50 <th></th> <td>56 harris ht</td> <td>((;-</td>		56 harris ht	((;-
50 50 <th></th> <td>5G</td> <td>A 🛜</td>		5G	A 🛜
50 50 <th></th> <td>5G 111112</td> <td>A 🛜</td>		5G 111112	A 🛜
50 51 9 </td <th></th> <td>56</td> <td>A 🛜</td>		56	A 🛜
SG SG <th></th> <td>56</td> <td>((i•</td>		56	((i•
56 56 56 56 56 56 56 56 56 56 56 57 Wireless Repeating Wireless Repeating Wireless Repeating Wireless Repeating Wireless Repeating Primary Router SSID @Ruijie-s49FD_5G * Password Image: Image: Image State St		5G C	A 🛜
50 Image: Second control of the second con		5G W	((:-
Wireless Repeating Confirm SSID and Wi-Fi Key: * Primary Router SSID @Ruijie-s49FD_5G * Password 		560	A 🛜
Wireless Repeating Confirm SSID and Wi-Fi Key: * Primary Router SSID @Ruijie-s49FD_5G * Password *******			-
Confirm SSID and Wi-Fi Key: * Primary Router SSID @Ruijie-s49FD_5G * Password ************************************		Wireless Repeating	
* Primary Router SSID @Ruijie=s49FD_5G * Password		Confirm SSID and Wi-Fi Key:	
@Ruijie-s49FD_5G * Password ******		* Primary Router SSID	
* Password		@Ruijie-s49FD_5G	
		* Password	
			يمتدر
		Next	
Next			

(2) Set the SSID and password and save the settings. Then settings of the Wi-Fi network are reset.

	Wireless Re	epeating
Ne	ew SSID and Wi-Fi Key:	
s	SSID (2.4G)	
	@Ruijie-WirelessRepeater	
*	* SSID (5G)	
	@Ruijie-WirelessRepeater5G	
	* Wi-Fi Password	
	•••••	> ₇₄ 4
Ma	anagement Parculard	Sama as Wi Ei Dassword
Ma	shagement Password	Same as with Password
*	Management Password	
	(Please	e remember the password.)
		nr.
	Mediu	m
	Next	



In wireless repeater mode, only Wi-Fi signals are extended and the DHCP function is disabled. 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 a WAN cable is installed, the device automatically switches to the wired repeater mode.

Power Power Modem LAN Port Norder LAN Port Recherk If you want to extend your Wi-Fi range Mesh Networking Wireless Repeater Mush		Wizard
Power Wodem LAN Port Modem LAN Port Router WAN Port Router WAN Port If you want to extend your Wi-Fir range Mesh Networking Wreless Repeater WISP	ØN	vo cable is detected. Please plug in cables according to the diagram.
Recheck If you want to extend your Wi-Fi range Mesh Networking Wireless Repeater WisP	Me	lodem LAN Port
If you want to extend your Wi-Fi range Mesh Networking WisP		Recheck
Mesh Networking Wireless Repeater WiSP		If you want to extend your Wi-Fi range
WSP		Mesh Networking Wireless Repeater
		WISP

5. Wireless ISP Mode

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

-			wis	P	
ernet:					
	PPPoE		DHC	Р	
2 168 111 10					
net Mask					
5.255.255.0					
vay					
.168.111.1					
92.168.111.1					
			Nex	t	
			WISI	•	
		Q ssid			C
		SG @R	uijie-s49FD_5G		A 🛜
					(li.
					((:-
		51			((i-
		sr			A 🛜
		5G			A 🛜
		56			
		,			~
		5G			1
					((r-
		5G			A 🛜
		5G			A 🛜
		5G			(()-
			1.400		
			Wireless R	epeating	
		Confirm S	SID and Wi-Fi Key:		
		Primary @Ruiji	Router SSID e-s49FD 5G		
		* D	-		
		* Passwo	•••		374
			Nex	t	

(2) Set the SSID and password and save the settings. Then settings of the Wi-Fi network are reset.

←	Wireless Repeating
	ocal Router Wi-Fi
	New Wi-Fi Same as Primary Router Wi-Fi
	* SSID (2.4G)
	@Ruijie-s49FD_5G_plus
	* SSID (5G)
	@Ruijie-s49FD_5G_plus_5G
	* Wi-Fi Password
	······
'	Management Password Same as Wi-Fi Password
	* Management Password
	(riease remember the password)
	High
	Ned
	HEM .
←	Wireless Repeating
	ocal Router Wi-Fi
	New Wi-Fi
	* SSID (2.4G)
	@Ruljle-s49FD_5G_plus
	* SSID (5G)
	Pairing
	Please wait for 1 to 2 minutes.
	Management Password Same as Wi-Fi Password
	* Management Password (Please remember the password)
	High I
	Neat
÷	Wireless Repeating Result
	Finish
	discover the SSID, please try again.
	SSID (2.4G):
	@Ruijie-s49FD_5G_plus SSID (5G):
	@Ruijie-s49FD_5G_plus_5G
	WI-FI PASSWUIG:
	Admin URL: ruiyi.cn
	Admin Password:RUUIE123.

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

connected to the secondary router are assigned by the secondary router. When the device connects to the Internet in wireless connection mode, the wired WAN port becomes the LAN port and is used by clients.

6. Mesh Networking

🛕 Caution

This function is not supported by the EW300 PRO.

(1) Click Mesh Networking, then click the Next button after accessing the Mesh Networking page. According to mesh networking steps on this page, press the Mesh Networking button on the primary and second routers.

Wizard				
	No cable is detected. Please plug in cables according to the diagram.			
	Power Modem LAN Port Router WAN Port			
	If you want to extend your Wi-Fi range			
	Mesh Networking Wireless Repeater			
	WISP			



🛕 Caution

The EW1200G PRO and EW1200 do not have the **Mesh Networking** button, press the **Reset** button for less than 2s.

(2) After the page indicating that the mesh networking is succeeded is displayed, you can view that one new repeater is connected to the primary router.



3.3.3 Verification and Testing

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

4 Reyee Wi-Fi Network Settings

4.1 Changing the SSID and Password

PC view: Choose Wi-Fi > Wi-Fi Settings.

Mobile Phone: Choose **Wi-Fi > Wi-Fi Settings**. Click the target Wi-Fi network, change the SSID and password of the Wi-Fi network, and click **Save**.

A Note

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

1 Home	8 Clients	Internet	(r Wi-Fi	-o- -o- More
Wi- Dual	Fi Settings -Band Single SSID			
* (SSID (2.4G) @Ruijie-sFC86	Large Cov	verage & Slow	/ Rate
* S	SID (5G) @Ruijie-sFC86_5G	Small Co	overage & Fast	t Rate
Wi	-Fi Password		(
		Save		

\leftarrow	Wi-Fi	S	\leftarrow	Wi-Fi	C
Wi-Fi Settings			2.4G Wi-Fi		
2.4G home2		Secured >	Large Coverage, Lov	v Speed	
	+ Add Wi-Fi		* SSID	home2	
Guest Wi-Fi			* Wi-Fi		•
2.46 123		Open >	Password		
	+ Add Wi-Fi		Hide SSID Clients will not find t	his SSID by scanning.	
Smart Wi-Fi					
	+ Add Wi-Fi			Save	

4.2 Hiding the SSID

4.2.1 Overview

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

4.2.2 Getting Started

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

4.2.3 Configuration Steps

Choose More> Wireless> Wi-Fi > Wi-Fi Settings > Expand.

Enable Hide SSID and click Save.

A Note

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

Wi-Fi Settings Gu	uest Wi-Fi	Smart Wi-Fi	Healthy Mode
<i>i</i> Tip: Changing c	onfiguration r	equires a reboot a	nd clients will be reconnected.
Wi-Fi Settings			
* SSID(2.4G)	@Ruijie-	s0848	
Security	Open		~
		Collapse	
Wireless Schedule	All Time		\sim
Hide SSID	(Th	e SSID is hidden a	and must be manually entered.)
AP Isolation	(Th	e client joining th	is Wi-Fi network will be isolated.)
XPress	(Th	e client will exper	ience faster speed.)
	Sé	ave	

Instruction

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

4.3 Adding a Wi-Fi Network

4.3.1 Overview

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

- Master Wi-Fi: The master Wi-Fi network is listed in the first line of the page and is enabled by default.
- Guest Wi-Fi: The guest 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 through Wi-Fi, but cannot access each other, improving security.

The guest Wi-Fi network can be disabled as scheduled. You can configure the guest Wi-Fi network to be disabled 1 hour later. When the time expires, the guest Wi-Fi network is disabled.

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

4.3.2 Configuration Steps

Mobile phone view: Choose Wi-Fi > Wi-Fi Settings.

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

PC view: Choose More > Wireless> Wi-Fi > Wi-Fi Settings/Guest Wi-Fi/Smart Wi-Fi.

÷	Wi-Fi	G	\leftarrow	Wi-Fi	G
Wi-Fi Settings			Guest Wi-Fi		
2.46 @Ruijie-s0848	8 Add Wi-Fi	Secured >	* SSID	SSID	
Guest Wi-Fi			Wi-Fi Password		
+	Add Wi-Fi		Hide SSID Clients will not find	this SSID by scanning.	
Smart Wi-Fi				Save	
+	Add Wi-Fi			<u> </u>	

4.3.3 Verification and Testing

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

Guest Wi-Fi			D	
(2.4G	123	Open	>

4.4 Configuring a Wi-Fi Blacklist or Whitelist

4.4.1 Overview

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

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

4.4.2 Configuration Steps

Mobile phone view: Choose More > Switch to PC view > More > Wireless > Blacklist/Whitelist.

PC view: Choose **More** > **Wireless** > **Blacklist/Whitelist**.

\leftarrow	More Setti	S	
Ē	Country(Region)/Channel	>	
	Channel Transmit Power Country(Region)/Transmit Power/Roaming Sensitivity Level		
ᡛ ᠽᠯ	XPress XPress helps you to get a faster ne	twork speed.	>
\bigcirc	Healthy Mode LED/Healthy Mode	⇒>	
ঞ্জি	System Reboot/Restore		⇒≻
	Language System Language		>
្ន	Switch to PC view Landscape Mode Recommended		>
	•		8
Hon	internet	VVI-FI	wore

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

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

🛕 Note

The blacklist prevents some devices from connecting to the Wi-Fi network. Exercise caution when performing this operation.
o ali st.	As except blacklis	ted STAs are allowe	d to access Wi-Fi.
Only t	the whitelisted ST	As are allowed to ac	ccess Wi-Fi.
Block	ed WLAN Clie	ents + Add	Delete Selected
Up to	30 members can	be added.	
	MAC	Remark	Action
		No Data	
< 1) > 10/pa	ge 🗸	Total 0
dd			×
MAC			
Exam	nple: 00:11:22:	33:44:55	
lease ent	er a MAC address.		
Rain(DS (30:0d:9e:3e:	7e:be)	
PC-3	e7ebe (52:54:00	:3e:7e:be)	
ELZ-/	AN10 (82:26:75:	da:ce:73)	
Hone	or_10-a96f220e7	/3c0a3f9 (c8:c2:fa	:be:55:5d)
TIONS			
none		Cancel	
Hone		Cancel	_

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

O All ST/	As except blacklisted	d STAs are allov	ved to access Wi-Fi.
Only t	he whitelisted STAs	are allowed to	access Wi-Fi.
Blocke	ed WLAN Clien	ts + Add	Delete Selected
Up to	30 members can be	added.	
	MAC	Remark	Action
F	2:36:1D:EB:20:6 D	test	Edit Delete
< 1	> 10/page	~	Total 1

4.5 Optimizing the Wi-Fi Network

4.5.1 Overview

The device detects the surrounding wireless environment and selects the appropriate configuration upon poweron. However, network freezing caused by wireless environment changes cannot be avoided. Restarting the router is a convenient and effective method to cope with network freezing. The router supports scheduled restart. For details, see <u>6.6</u> <u>Configuring Scheduled Reboot</u>. You can also analyze the wireless environment around the router and select appropriate parameters.

4.5.2 Getting Started

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



4.5.3 Configuration Steps

• Optimizing the radio channel

Mobile phone view: Choose **More** > **Channel Transmit Power**.

PC view: Choose More > Wireless > Radio Frequency.

Select 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 may result in stronger wireless interference.

1 Instruction

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

A Note

Settings of settings of the Wi-Fi network are reset after the radio channel is changed. Therefore, exercise caution when performing this operation.

\leftarrow	More Settings	S
V	Network Schedule Configure Internet access time and application	>
$\langle \bullet \rangle$	Wizard Internet/Wi-Fi/Scan QR Code	>
ហ	Repeater Mode Router/Wired Repeater/Wireless Repeater	>
Q	Network Check Check the current network status smartly.	>
Ş	Roaming Optimization Roaming Sensitivity Level	>
ш	Country(Region)/Channel Width	>
	Channel Transmit Power Country(Region)/Transmit Power/Roaming Sensitivity Level	>
*	XPress	>
		88
Hon	ne Internet Wi-Fi	More

÷	Channel Transmit Power	S
0	Tip: Changing configuration requires a reboot and clients will be reconnected.	
Radi	o Frequency	
2.4G Ch	annel	
Auto		~
Auto		
1 (2	2.412GHz〉	
['] 2 (2	2.417GHz)	1

• Optimizing the channel width

Mobile phone view: Choose More> Country(Region)/Channel Width.

PC view: Choose More > Wireless > Radio Frequency.

If the interference is severe, select a lower channel width to avoid network freezing. The router supports 20 MHz and 40 MHz channel width. You are advised to select 20 MHz channel width. After changing the channel width, click **Save** to make the configuration take effect immediately.

🛕 Note

After the change, settings of settings of the Wi-Fi network are reset, and clients need to reconnect to the Wi-Fi network. Therefore, exercise caution when performing this operation.

Radio Frequency	
Country/Region	
United States (US)	~
2.4G Channel Width	
Auto	^
Auto	
20MHz	
40MHz	

• Optimizing the transmit power

Mobile phone view: Choose More > Channel Transmit Power.

PC view: Choose More > Wireless > 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 in centralized mode, a lower transmit power is recommended.

🛕 Note

After the change, settings of settings of the Wi-Fi network are reset, and clients need to reconnect to the Wi-Fi network. Therefore, exercise caution when performing this operation.

Radio	Frequency			
2.4G Cha	nnel			
Auto				~
Transmit	Power			
O Auto	Lower	Low	Medium	High
_				

• (Optional) Configuring the roaming sensitivity

Mobile phone view: Choose **More** > **Roaming Optimization**.

PC view: Choose More > Wireless > Radio Frequency.

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

A low sensitivity is recommended.

A Note

After the change, settings of settings of the Wi-Fi network are reset, and clients need to reconnect to the Wi-Fi network.

A high sensitivity may cause Wi-Fi network disconnection. Therefore, exercise caution when performing this operation.

\leftarrow	F	Roaming O	ptimization		S
	Roaming sens and switches t better signal.	itivity is the rate o the nearest a	e at which your c vailable access p	levice selects oint, offering	а
Roan	ning Opti	mization			
2.4G Roa	aming Sensit	ivity ⑦			
0					
Low	20%	40%	60%	80%	High
5G Roan	ning Sensitiv	ity 🕐			
0					
Low	20%	40%	60%	80%	High
		Sa	ave		
\triangle	1	\oplus	((:	8	
Hon	ne	Internet	Wi-Fi	Μ	lore

4.6 Configuring the Healthy Mode

Mobile phone view: Choose More > Healthy Mode > Healthy Mode.

PC view: Choose More > Wireless > Wi-Fi > Healthy Mode.

Click **Enable** to enable the healthy mode. You are allowed to set the validity time 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 freezing. You are advised to disable it.

Instruction

All Ruijie wireless routers have undergone stringent radiation detection and evaluation, and comply with IEC/EN62311, EN 50385, and other standards. Wi-Fi networks will not affect human health, and you can use Ruijie wireless routers safely.

	Healthy Mode	C
0	Enable healthy mode, and the device will decrease its transmit power to reduce radiation. Tip: Changing configuration requires a reboot and clients will be reconnected.	0
Hea	Ithy Mode	
Enable		
Enable)	
Enable	s Schedule	

4.7 Enabling Roaming Optimization

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

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

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



5 Reyee Networks Settings

5.1 Configuring Internet Connection Type

Mobile phone view: Choose More > Switch to PC view > More > Basics > WAN.

PC view: Choose More > Basics > WAN.

The router supports three Internet connection modes: PPPoE, DHCP, and static IP address. For details, see <u>3.2.1 Getting Started</u>.

<i>i</i> Configure WAN settings.				
* Internet	DHCP]		
	PPPoE	or DHCP clients.		
IP	DHCP			
	Static IP			
Subnet Mask	233.233.233.0			
Gateway	172.20.141.1			
DNS Server	172.30.44.20 192.168.5.28			
	Advanced Settings			
	Save			

5.2 Changing the Address of a LAN Port

Mobile phone view: Choose More > Switch to PC view > More > Basics > LAN.

PC view: Choose More > Basics > LAN.

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

🛕 Note

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

LAN Settings	DHCP	Clients	Static IP Addresse	s D	NS Proxy
LAN Sett The LAN 1 192.168.1	tings port is co 110.1 to	onfigured with 1 92.168.111 .	n An address conflic 1 to ensure network	t occurs . connecti	. The IP add on.
	* IP (192.168.11	1.1		
* Subnet	Mask	255.255.25	5.0		
Re	emark	Remark			
*	MAC	00:d0:f8:15	:08:49		

5.3 Changing the MAC Address

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

Mobile phone view: Choose More > Switch to PC view > More > Basics > WAN.

PC view: Choose More > Basics > WAN.

Click Advanced Settings.

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

To change the MAC address of the LAN port, choose **Basics** > LAN.

A Note

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

Figure 5-1	WAN Port Settings		
	i Configure WA	N settings.	
	* Internet	DHCP ~	
		No username or password is required for DHCP client	ts.
	IP	172.26.1.118	
	Subnet Mask	255.255.255.0	
	Gateway	172.26.1.1	
	DNS Server	192.168.58.94 192.168.58.110	
		Advanced Settings	
	* MTU	1500	
	* MAC	00:d0:f8:15:08:48	
	802.1Q Tag		
		Save	

5.4 Changing the MTU

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

Mobile phone view: Choose More > Switch to PC view > More > Basics > WAN > Advanced Settings.

PC view: Choose More > Basics > WAN > Advanced Settings.

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

() Configure WAI	N settings.	
* Internet	DHCP v	
	No username or password is required for DHCP clients.	
IP	172.20.141.106	
Subnet Mask	255.255.255.0	
Gateway	172.20.141.1	
DNS Server	172.30.44.20 192.168.5.28	
	Advanced Settings	
* MTU	1500	
* MAC	30:0d:9e:c6:fc:86	
802.1Q Tag		
	Save	

5.5 Configuring the Repeater Mode

🛕 Caution

Only the EW1200G-PRO and EW300-PRO support the WISP mode.

5.5.1 Wired Repeater

The wired repeater mode is available when the network cable provides reliable transmission over a more stable Wi-Fi network with less interference. You are advised to use the wired repeater mode. Ensure that the primary router can access the Internet with the DHCP server enabled. Otherwise, the configuration will take ineffective.

Choose More > Switch to PC view > More > Basics > Repeater/WISP.

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

🛕 Note

Ensure that the primary router can access the Internet with the DHCP server enabled. After the configuration is saved, settings of the Wi-Fi network are reset, and clients need to reconnect to the Wi-Fi network.

Figure 5-2 Wired Repeater Settings (1/2)

O Router	• Wired Repeater	O Wireless Repeater	O WISP
This mode allow secondary route Cable Connection primary router.	ws you to establish a wired o er, extending network cover on: Please connect the WAN	connection between a primary rou age. I port of the local router to the LA	ter and a N port of the
Wired Repeate	r		
	Check		
gure 5-3 Wired Re	epeater Settings (2/2)		
Wired Repeater			
Wired Repeater	Cable Plugged		
Wired Repeater Status	Cable Plugged IP Address: 172.26.1.118		
* Local Router SSID	Cable Plugged IP Address: 172.26.1.118 home2		
Wired Repeater Status * Local Router SSID Password	Cable Plugged IP Address: 172.26.1.118 home2		
Wired Repeater Status * Local Router SSID Password	Cable Plugged IP Address: 172.26.1.118 home2	©	

5.5.2 Wireless Repeater

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



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

Choose More > Switch to PC view > More > Basics > Repeater/WISP.

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

The de	vice is working) in Router n	node. The foll	owing th	iree modes ar	e available:	
O Ro	outer	O Wired F	\epeater	0	Wireless Rep	eater	O WISP
1	 This mode secondary The local ro It is recommendation Please unplug 	allows you to router, extend outer will work mended to sel the cable to a	establish a wir ling network co c as a secondar ect a 5G Wi-Fi avoid loops.	eless cor overage. ry router. of the pr	inection betwe	en a primary	router and a
Wir	eless Repe	ater					
ŀ	rimary Rou	ter					
	* SSII	D Select					

- (2) Select the Wi-Fi signal of the primary router and enter its Wi-Fi password. You can configure a new Wi-Fi network or use the same Wi-Fi network as that of the primary router.
 - If you select Same as Primary Router Wi-Fi, Wi-Fi settings of the primary router are automatically synchronized to the current router. In most cases, clients merge Wi-Fi signals with the same SSID into one Wi-Fi signal, and they can search out only the Wi-Fi signal of the primary router.
 - If you select **New Wi-Fi**, you can set the local SSID and password. Clients will search out a Wi-Fi signal that is different from the Wi-Fi signal of the primary router.

A Note

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

Figure 5-4 Selecting the Wi-Fi Signal of the Primary Router and Connecting to the Wi-Fi Network

SSID	2.4G	✓ Re-scar	n		Primary Router
SSID WiFi_77FC	BSSSID	Security	Channel	RSSI High	* SSID xiaoxi Select
xiaoxi	50:64:2b:0e:77:fd	WPA2PSK	3	-28 dBm High	* WI-Fi Password
NLS-PRO-140	02:0d:9e:85:bb:1 1	WPA2PSK	10	-49 dBm High	Local Router Wi-Fi O New Wi-Fi O Same as Primary Router Wi
ruijie-802.1x	06:05:88:c6:65:c8	WPA2PSK	1	-57 dBm High	* SSID(2.4G) xiaoxi_plus
22222	46:0d:9e:e7:e9:18	WPAPSK	11	-64 dBm Medium	Wi-Fi Password A blank value indicates no encryption.

5.5.3 WISP

(2)

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

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

Click WISP, select an Internet connection mode, and click Next.

WAN		
* Internet	DHCP	~
No username o	or password is required for DHCP clients.	
	Next	
Click Select, select a Wi-Fi signal, and	d click Save .	
A Note		
After you click Save, settings of setting	gs of the Wi-Fi network are reset. You need to conn	ect to the new

5.6 Controlling the Internet Access Time Range

Mobile phone view: Choose **More** > **Network Schedule**. Select a client and click **Schedule**. Click **Add** and set the time range in which Internet access is blocked. In the specified time range, the client is prevented from accessing the Internet.

Wi-Fi network. Exercise caution when performing this operation. Remember the SSID and password.

PC view: Choose Clients > Add Blocked Time.

Select a client and click Add Blocked Time.

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

Add Rule		×
Blocked Time	All Time \checkmark	
Remark	nova_7_5G-812eb95e638f7ba	
	Cancel	ОК

Reyee Networks Settings

\leftarrow	Network Schedule	G	← Network Schedule C	← Schedule Block Time	S
8 Ra	ainOS Wired	Schedule	Set a schedule to restrict the network surfing time for children, preventing Internet addiction.	Set a schedule to prevent clients to access the Internet during the specified time.	
8	C-3e7ebe Wired	Schedule	Scheduled Blocked Time	Schedule Select	>
8 MI	15-xiaomi5-c 2.46 01-12 00:00	Schedule	No Data Available	Start Time 🕓 15:55	>
8 EL ?	.Z-AN10 2.4G 01-12 00:52	Schedule	Add	End Time S End Time	>
8 *	2.4G 01-12 01:06	Schedule			
su ⊗ Su ₹	en-woGT-da-shi-tan- io-ban 2.46 01-12 02:23	Schedule			
	÷	86	☆ ⊕ 중 %	Cancel Save	

5.7 Configuring XPress

Mobile phone view: Choose **More** > **XPress**.

PC view: Choose More >Wireless > Wi-Fi > Wi-Fi Setting > Expand > XPress.

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



In the PC view, enable **XPress** as follows.

Wi-Fi Settings	
* SSID(2.4G)	home2
Security	WPA_WPA2-PSK

Security	WPA_WPA2-	-PSK	~	
* Wi-Fi Password	•••••		**	
		Collapse		
/ireless Schedule	All Time		~	
Hide SSID	(The S	SID is hidden and	must be r	manually entered.)
AP Isolation	(The cl	lient joining this V	Vi-Fi netw	ork will be isolated.)
XPress	(The cl	lient will experien	ce faster s	peed.)
	Save			

5.8 Configuring Port Mapping

5.8.1 Overview

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

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

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

All packets are forwarded from the Internet to DMZ hosts to provide the Internet access service.

5.8.2 Getting Started

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

5.8.3 Configuration Steps

Mobile phone view: Choose More > Switch to PC view > More > Advanced > Port Mapping.

PC view: Choose More > Advanced > Port Mapping.

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

Name: Enter a name for ease of maintenance.

Preferred Server: Select a service to be mapped, such as HTTP or FTP. The device will automatically fill in the internal port number of the service. If the service is uncertain, 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 must be consistent with that on the client.

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

Internal IP Address: Enter the LAN IP address used by an extranet terminal to access the device, such as the IP address of an IP camera.

Internal Port/Range: Enter the port number used by an application, such as port 8080 used by the web service.

		Add	
Port Mapping NAT-DMZ		* Name	test
	0		
Port Mapping	(?)	Preferred Server	HTTP ~
Port Mapping List + Add	J Delete Selected	Protocol	TCP ~
Up to 50 entries can be added.		External IP Address	172.26.1.118
Extern	al I	* External Port/Range	Example: X or X-X (Range: 1-6553!
Name Protocol IP	Port		Please enter an external port.
Addres	ss /	* Internal IP Address	Example: 1.1.1.1
			Please enter an internal IP address.
	No Data	* Internal Port/Range	Example: X or X-X (Range: 1-6553!
			Please enter an internal port.
< 1 > 10/page <	Total 0		Cancel OK

5.8.4 Verification and Testing

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

5.8.5 Solution to a Test Failure

- (1) Use a new external port number and perform a test again. The test often fails on the ports blocked by firewalls of some ISPs.
- (2) Enable the remote access permission on a server. The common cause is that remote access is disabled on the server by default. As a result, intranet access is successful but the access across different network segments fails.
- (3) Enable the DMZ service. For details, see <u>5.8.6 DMZ Configuration Steps</u>. The common cause is that port configuration is incorrect or incomplete.

5.8.6 DMZ Configuration Steps

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

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

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

Port Mapping	NAT-DMZ
i NAT-DMZ	
Enab	le 🚺
* Dest IP Addre	ss Example: 1.1.1.1
	Please enter a destination IP address. Save

5.9 Configuring the DHCP Server

5.9.1 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 may occur. In this case, you need to disable the DHCP server function and enable the DHCP service on one router only. Otherwise, some devices may be disconnected from the network.

5.9.2 Configuration Steps

1. Configuring the DHCP Server Function

Mobile phone view: Choose More > Switch to PC view > More > Basics > LAN > LAN Settings.

PC view: Choose More > Basics > LAN > LAN Settings.

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

🛕 Note

If the DHCP server function is disabled on all routers on the network, clients cannot automatically obtain IP addresses. In this case, 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. When a client keeps connected, the lease is automatically renewed. If a lease is not renewed due to client disconnection or network instability, the IP address will be reclaimed after the lease time expires. After the client is re-connected, the client requests an IP address again. The default lease time is 30 minutes.

LAN Settings DHC	P Clients	Static IP Addresses	DNS Proxy	
<i>LAN Settings</i> <i>The LAN port is a to ensure networ</i>	configured wit k connection.	h An address conflict occu	rs. . The IP address	of the LAN port
* IP	192.168.1	11.1		
* Subnet Mask	255.255.25	55.0		
Remark	Remark			
* MAC	00:d0:f8:1	5:08:49		
DHCP Server				
* Start	192.168.1	11.1		
* IP Count	254			
* Lease Time(Min)	30			
	Sav	/e		
LAN Settings DHO	CP Clients	Static IP Addresses	DNS Proxy	
i LAN Settings				
* IP	192.168.	110.1		
* Subnet Mask	255.255.2	255.0		
* MAC	ec:b9:70:	f2:41:a1		
DHCP Server				
* Start	192.168.	110.1		
* IP Count	254			
* Lease Time(Min)	30			
	Si	ave		

2. Displaying Online DHCP Clients

Mobile phone view: Choose More > Switch to PC view > More > LAN > DHCP Clients.

PC view: Choose More > LAN > DHCP Clients.

Check information about an online client. Click **Convert to Static IP** and click **OK**. Then the client obtains the IP address each time when it connects to the router.

LAN Se	ttings	DHCP Clients	Static IP Addresses	DNS Proxy		
0	View DH	CP clients.				0
DHC	CP Clie	nts		Search by Hostname/IP/MAC	Q C Refresh	+ Batch Convert
Up t	o 300 IF	P-MAC bindings can be	added.			
	No.	Hostname	IP	MAC	Remaining Lease Time(Min)	Status
	1	RainOS	192.168.111.18	30:0d:9e:3c:d6:be	24	Convert to Static IP
	2	PC-3CD6BE	192.168.111.53	52:54:00:3c:d6:be	17	Convert to Static IP
	3	*	192.168.111.176	f2:36:1d:eb:20:6d	22	Convert to Static IP
	1	10/page 🗸				Total 3

3. Displaying the DHCP Static IP Address Table

Mobile phone view: Choose More > Switch to PC view > More > LAN > Static IP Addresses.

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

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

LAN Settings	DHCP Clients	Static IP Addresses	DNS Proxy	
i Static IP	Address List			0
Static IP A	ddress List		Search by IP/MAC Q	+ Add 🗇 Delete Selected
Up to 300 e	ntries can be added.			
No.		IP	МАС	Action
			No Data	
< 1	10/page \vee			Total 0

Add	~
* IP	
Example: 1.1.1.1	
* MAC	
Example: 00:11:22:33:44:55	
Cancel	
ОК	

5.10 Configuring DNS

The domain name system (DNS) proxy configuration is optional. The device obtains the DNS server address from the uplink device by default.

Mobile phone view: Choose More > Switch to PC view > More > LAN > DNS Proxy.

PC view: Choose More > LAN > DNS Proxy.

DNS Proxy: The function is disabled by default and the DNS configuration delivered by a carrier is used. If the DNS configuration is incorrect, 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. When the DNS proxy function is enabled, you can enter the IP address of the DNS server. The available DNS service varies depending on the region. You can consult the local ISP.

LAN Settings	DHCP Clients	Static IP Addresses	DNS Proxy
<i>i</i> DNS prox	y is not required. The	e device will obtain the DN	NS server address from the uplink device by default.
E	nable 🚺		
* DNS S	Server Please en	ter a DNS server addres	S.
	Sa	ve	

5.11 Configuring DDNS

5.11.1 Overview

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

5.11.2 Getting Started

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

5.11.3 Configuration Steps

Mobile phone view: Choose More > Switch to PC view > More > Advanced > Dynamic DNS > Dynamic DNS.

PC view: Choose More > Advanced > Dynamic DNS > Dynamic DNS.

Peanut Shell NAT is a more advanced version of DDNS and can be used when an intranet IP address is configured for the WAN port. Peanut Shell NAT is recommended. Click **Enable** and then click **Save**. The service status and QR code for login appear in the lower part of the page. Scan the QR code to log in by using WeChat or PeanutHull app (the QR code shown in the figure below is unavailable. Scan the QR code displayed on your device).

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

Peanut Shell NAT	Dynamic DNS	No-IP DNS	DynDNS	Peanut She	II NAT	Dynamic DNS	No-IP DNS	DynDNS	
it is recommend	N AT nded to use WeChat	or Peanut Shell to	scan the QR code.	i by It is HTT	namic DNS recommend IPS mapping	led to use Peanut S J.	hell for NAT, includ	ing TCP, UDP, H1	TP and
Enabi	le Save			,	* Username * Password				
Scan to Logi					Link Status	Log In	Delete		
	∎if ∰				Domain	-			

5.12 Configuring APR Binding and ARP Guard

5.12.1 Overview

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

5.12.2 Configuration Steps

(1) Binding ARP information

Mobile phone view: Choose More > Switch to PC view > More > Security> ARP List

PC view: Choose More > Security> ARP List

ARP binding means binding of IP addresses and MAC addresses on the LAN.

ARP	Guard Ena	2 ble Only the devices	configured with IP-MAC	binding are allowed to a	ccess the Internet.	
ARP	List	Sear	ch by IP/MAC	Q + Add	Ø Bind Selected	Delete Selected
Up to	o 64 IP-M/	AC bindings can be added.				
	No.	MAC	IP	Туре	2	Action
	1	f2:36:1d:eb:20:6d	192.168.111.176	Dynam	ic	1 Ø Bind
	2	30:0d:9e:7e:13:a1	172.26.1.1	Dynam	ic	
	3	52:54:00:3c:d6:be	192.168.111.53	Dynam	ic	∂ Bind
otal 3	10/page	, √ < <mark>1</mark> > G	io to page 1			

(2) Enabling ARP guard

Enable **ARP Guard** and then click **OK.** After ARP guard is enabled, only clients whose IP address and MAC address are bound are allowed to access the Internet.

🛕 Note

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

5.13 Configuring Static Routing

Note

Only EW3000GX PRO supports this function.

Smartphone View: Choose More > Switch to PC view > More > Advanced > Routing > Static Routing.
PC View: Choose More > Badvanced > 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 🗸	DDD Chat's Daviding					
🔁 Advanced 🛛 ^	Static Routing					
Port Mapping	When a packet arrivition destination network	ves, the device checks the c then it will forward the	e destination field and comp packet from the specified in	pares it against the ro sterface.	outing table. If it finds	a match for
Dynamic DNS	Static Route List				+ Add	fill Batch Delete
UPnP Settings						E buttin belete
Local DNS	Op to Too entries can	be added.				
Reyee Mesh	Dest IP Addres	s Subnet Mask	Outbound Interface	Next Hop	Reachable	Action
Reyee Mesh 3.0						
AP Networking	< 1 → 10/r	age 🗸				Total
Link Aggregation						
Routing						
Game Port Guarantee						
Flow Control						
Hardware Acceleration «Collapse					1 Strake	
Add				>	<	
* Dest IP	Address					
* Subn	net Mask 25	5.255.255.0				
* Outbound I	nterface Se	lect				
* N	lext Hop					
			Cancel	ОК		

Table 5-1 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
Next Hop	The IP address of the next-hop router to which the packet will be sent. If the outbound interface is a PPPoE interface, there is no need to configure the next-hop IP address.

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

PBR						
0	Static Routing When a packet arrives, th destination network ther	ne device checks the de n it will forward the pae	estination field and co cket from the specified	mpares it against the ro I interface.	outing table. If it finds	a match for
Stat	tic Route List				+ Add	볩 Batch Delete
Up	to 100 entries can be ad	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 nterface to the next hop.
	192.168.2.0	255.255.255.0	WAN	172.168.1.1	No 🥹	Edit Delete
	1 2 10/page					Total 1

5.14 Policy-based Routing

 Note 	;					
Only EW3	3000GX PR	O supports	this function.			
				 合		

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

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

1. Overview

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

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

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

2. Configuration Steps

PC View: Choose Advanced > Routing > PBR.

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

?
ete
on
tal 0
e

Add PBR					
* Name					
Protocol Type	IP				
Src IP/IP Range	All IP Addresses				
Dest IP/IP Range	All IP Addresses				
Outbound Interface	WAN				
Status					
		C	Cancel	OK	

Parameter	Description
Name	The name of the PBR rule, as the identifier of the PBR route. The name must be unique.
Protocol Type	The protocol for the PBR route to take effect, which can be IP, ICMP, UDP, TCP, or a custom protocol type as needed.
Protocol Number	When the protocol type is Custom, the protocol number is required.
Src IP/IP Range	 The source IP/IP range to which the PBR rule matches. By default, All IP is selected. All IP: Matches all source IP addresses. Custom: Matches source IP addresses in the specified range.
Custom Src IP	The source IP address or range is required when the matching source IP/IP range is Custom.
Dest IP/IP Range	 The destination IP/IP range to which the PBR rule matches. By default, All IP is selected. All IP: Matches all destination IP addresses. Custom: Matches destination IP addresses in the specified range.
Custom Dest IP	The destination IP address or range is required when the matching destination IP/IP range is Custom.
Src Port Range	This field is displayed only when the protocol type is TCP or UDP. The value in this field is the source port range matching the PBR route.
Dest Port Range	This field is displayed only when the protocol type is TCP or UDP. The value in this field is the destination port range matching the PBR route.
Outbound Interface	Interface over which packets hit the PBR rule are forwarded.
Status	You can enable or disable the toggle switch next to Status to enable or disable the PBR rule.

Table 5-2	Description of Policy-based Routin	na
	Description of Folloy based Routh	۰y

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.

₩ VPN ×	PBR	Static Rou	ıting								
🗄 Advanced 🔷 🔿		200									
Port Mapping	1	Route Priori Description	ty: PBR > Stat PBR is more f	tic Routing > lexible than d	ISP Routing. lestination-ba	ised routing.					0
Dynamic DNS	PBR	List							+ Ad	d 🖻	Batch Delete
UPnP Settings	Unite	30 entrie	s can be adde	d							
Local DNS	opic	, Jo chuic		u.							
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			

5.15 Connecting to IPTV

Internet Protocol Television (IPTV) is provided by ISPs.

5.15.1 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 VLAN type is used, confirm the VLAN ID. If the IPTV type is unknown, contact your local ISP.

5.15.2 IPTV Configuration Steps (VLAN Type)

Mobile phone view: Choose More > Switch to PC view > More > Basics > IPTV/VLAN

PC view: Choose More > Basics > IPTV/VLAN

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

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

After the configuration, confirm that the IPTV STB is connected to the specified port properly. In the following figure, the IPTV STB is connected to LAN3.

🛕 Note

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

iPTV/VLAN set	tings.	
IPTV/VLAN		
* Mode	Custom	~
* LAN1	Internet	\sim
* LAN2	Internet	\sim
* LAN3	Internet	~
Internet VLAN	802.1Q Tag	
	Save	

5.15.3 IPTV Configuration Steps (IGMP Type)

Mobile phone view: Choose More > Switch to PC view > More > Basics > IPTV.

PC view: Choose More > Switch to PC view > More > Basics > IPTV.

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

IPTV/VLAN	IPTV/IGMP
iptv/i	GMP (for Vietnam FPT ISP)
IPTV/IGM	1P
	Enable
	Save
A Caution	

The EW1200 does not support the IGMP type.

5.16 Configuring Wi-Fi/IGMP

5.16.1 Overview

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

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

5.16.2 Configuration Steps

Mobile phone view: Choose More > Switch to PC view > More > Basics > IPTV> Wi-Fi/IGMP.

PC view: Choose More > Basics > IPTV> Wi-Fi/IGMP.

Note	
Select the method to configure EW3000GX PRO:	
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.

ClickM2U(5G) to enable WIFI/IGMP for 5G wireless clients.

R	Ruíji	e i Reyee	1 Home	Clients	Internet	-B- -B- More		88	
Basics WAN	Ŷ	IPTV/VLAN IPTV/IGMP	WIFI/IGMP						
LAN		🚺 WIFI/IGMP							
IPTV		WIFI/IGMP							
IPv6 Address		M2U (2.4G)							
🗇 WLAN	~	M2U (5G)							
Mork Mode			Save						
Security	~								
S VPN	×								
🗄 Advanced	×								
Diagnostics Diagno	×								
System	×								6
									Ai
«Collapse									

5.17 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 Address

PC View: More > Basics > IPv6 Address

5.17.1 Configuring the IPv6 of the WAN Port

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

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

🛕 Caution

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



5.17.2 Configuring the IPv6 of the LAN Port

Click LAN Settings.

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

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

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

	R	uíjie I #Reye	e	1 Home	Clients) Internet	(îr Wi-Fi	-0- More		80	8
Basics	^	IPv6 Address									
WAN		1. When IPv6 is e	nabled, the MTU of IPv4 WAN por	t is The MTU of IPv4	WAN port must be great	er than 1280.					
LAN		Enable									
IPTV		WAN Settings LAN	Settings DHCPv6 Clients								
IPv6 Address		10 ()									
🗇 WLAN		IPv6 Assignment	Auto		0						
Work Mode		IPv6 Address/Prefix									
Security	~	Length									
			Advanced Settings \wedge								
A		Subnet Prefix Name	Default		0						
H Advanced		Subnet Prefix Length	64		0						
② Diagnostics											
😤 System	Ň	Subnet ID	0		0						
		* Lease Time(Min)	120		0						
		DNS Server	Example: 0:0::2, each separate	d by a comma.							
			Save								e
- 6 - 6											
Collapse											

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

ī	ZUÍJIÓ	e ⊨ ≋Reyee	1 Home	Clients	Internet		-B- -B- More	English 🗸 🕌 🧍		
Basics	~									1
WAN		IPv6 Address 1. When IPv6 is enabled, the N	TU of IPv4 WAN port is	The MTU of IPv4 W	AN port must be grea	ter than 1280.				
LAN		Enable								
IPTV		WAN Settings LAN Settings	DHCPv6 Clients							
IPv6 Address		DHCPv6 Clients								
🗇 WLAN	~	You can view the DHCPv6 clier	ts information on this	oage.						
Work Mode		DHCPv6 Clients						Search by DUID	Q	
⊘ Security	~	No. Hostnam	2	IP	v6 Address	R	emaining Lease Time(min)	DUID		
🐺 VPN	~					No Data				
🗄 Advanced	×	< 1 > 10/page >							Total 0	
Diagnostics Diagno	~									
:a: System	~									
«Collapse										

5.18 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.

A Caution

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

Ruijie	[∣] ≋R∈y∈∈	1 Home	Clients	Internet	(investigation of the weight o	-B- -B- More	English ~	8-0 200	۵	8
VPN V	Smart Flow Control	Custom Policy								
🖹 Advanced 🗠	Smart Flow Con	itrol								2
Port Mapping	Intelligently adjus	t the network speed to e	nsure that each us	ser shares the networ	rk fairly.				(?)
Dynamic DNS	Enable	If you want to	test the WAN ra	ate, disable smart f	flow control first.					
UPnP Settings	WAN Bandwidth	* Up 1000 M	1bps * Down	1000 Mbps						
Local DNS		Save								
Reyee Mesh										
Reyee Mesh 3.0										
AP Networking										
Flow Control										
Hardware Acceleration										
« Collapse										

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.

Ruíjie	[∣] ≋R∈y∈∈	1 Home	Clients	Internet	🛜 Wi-Fi	More	English ~ 🖁	8 8
ም VPN ~	Smart Flow Control	Custom Policy						
🖻 Advanced 🗠	Custom Policy Allocate bandwid	th to the specified IP ad	dress or range. The j	priority is sorted as fo	Ilows: Custom Po	licy > Smart Flow Control.		?
Dynamic DNS	Policy List						+ Add	Batch Delete
UPnP Settings	Up to 30 entries can	be added.						
Local DNS	Policy	Name	IP / IP Range	Bandwi Type	dth	Uplink Rate	Downlink Rate	Interfac
Reyee Mesh Reyee Mesh 3.0						No Data		
AP Networking								
Flow Control								
Hardware Acceleration «Collapse								2

5.19 Configuring Firewall

A 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.

Ruíjie	Reyee	1 Home	Clients	Internet	(îr Wi-Fi	-B- More	English ~		8
Reyee Mesh 3.0	 Other Settings 								
AP Networking	Enable Advanced	0							
Flow Control	Firewall								
Hardware Acceleration	Disable ICMPv6 Error								
Port Settings	Messages								
Connectivity detection		Save							
CWMP									
Other Settings									
Ø Diagnostics									
:e: System									(? Ai
« Collapse									

5.20 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.

Ruíjie	∣ ≋R∈y∈∈	1 Home	Clients	Internet	(r Wi-Fi	-o- -o- More	English ~	0/0 82	٩	8
Reyee Mesh 3.0	Wi-Fi Switch It takes 30 seconds to act	tivate settings afte	er the Wi-Fi switch	is turned on. The W	i-Fi function is disab	oled on the device	after the Wi-Fi switch is turned off.			
AP Networking Flow Control	Wi-Fi Switch 🚺									
Hardware Acceleration		Save								
Port Settings										
Connectivity detection										
Wi-Fi Switch										
Other Settings										
Oiagnostics										
-a- -a- System										
«Collapse										

5.21 Configuring UPnP

5.21.1 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 more fast or stably. Common applications that support UPnP include MSN Messenger, Xunlei, BT, and PPLive.

5.21.2 Configuration Steps

Mobile phone view: Choose More > Switch to PC view > More > Advanced > UPnP Settings.

PC view: Choose More > Advanced > UPnP Settings.

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

i	UPnP Settings UPnP (Universal Plug and Play) is	s a new Internet protocol	aimed at improving communicatior	n between devices. 🗿	
UP	Enable				
	Protocol	Арр	Client IP Address	Internal Port	External Port
			No UPnP Device		

5.22 Configuring PPTP VPN

🛕 Caution

The EW1800GX PRO and EW3200GX PRO support this function. The EW1200G PRO only supports the PPTP client.

5.22.1 Overview

The device supports the 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.

5.22.2 Configuring PPTP Server

Mobile phone view: Choose More > Switch to PC view-> More-> VPN > PPTP.

PC view: Choose More-> VPN > PPTP.

(1) Click Enable to enable PPTP and select Server.

Local Address: Enter the local address. It is used as the local virtual IP address of the VPN tunnel for the client to access the server after dial-up.

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

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

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

Click Save. The device will receive and process VPN requests.

PPTP Settings Tunnel	List				
i PPTP Settings					?
Enable					
РРТР Туре	● Server 🔿 (Client			
* Local Address	Example: 1.1.1.1				
* IP Range	Example: 1.1.1.2	-1.1.1.100	0		
* DNS Server	Example: 1.1.1.1				
* PPP Hello Interval	10		second	S	
	Save				
VPN Client List			+	Add	Delete Selected
Up to 32 entries can be	added.				
Username	Password	Network Mode	Peer Subnet	Stat	us Action

(2) Add a PPTP user.

Click + Add to enter a username and a password for authentication during client dial-up.

Select the network connection mode. **PC to Router** indicates dial-up from a PC to a router. **Router to Router** indicates dial-up from one router to the other router.

Enable Status and click OK.

Add User		×
* Username	Please enter a username.	
* Password	Please enter a password.	\odot
Network Mode	PC to Router \sim	
Status		
	Cancel	ÖK

5.22.3 Configuring the PPTP Client

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

PC view: Choose **More**-> **PPTP**.

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

Tunnel IP: Enter the virtual IP address used to create a 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, which does not cause conflicts.

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

Peer Subnet: Enter the destination network segment of the server, which must be different from that of the client.

Work Mode: The NAT mode only allows a 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. The device will send VPN tunnel requests to the WAN port.
PPTP Settings Tunnel	List	
<i>i</i> PPTP Settings		
Enable		
РРТР Туре	O Server O Client	
* Username	Username of PPTP user	
* Password	Password of PPTP user	\odot
Interface	WAN ~	
Tunnel IP	• Dynamic O Static	
* Server Address	IP/Domain	
* Peer Subnet	Example: 192.168.110.0/24	
Work Mode	NAT OROuter	
* PPP Hello Interval	10	seconds
	Save	

5.23 Configuring OpenVPN

5.23.1 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, mobile phones, 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.

5.23.2 Configuring OpenVPN (Server Mode)

Mobile Phone View: Choose More > Switch to PC view-> More->

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 5-5 Configuring OpenVPN Server

Ruíj	īe	≋R∈у∈с 1	ome Clien) 🕀 ts Internet	ି Wi-Fi
Basics	~				
WLAN	~				
Work Mode		() OpenVPN			
Security	~	Enable 🧲	D		
🛒 VPN	^	OpenVPN Type 🧿	Server O Clie	nt	
PPTP		Service Mode	Certificate	~	
OpenVPN					
🗄 Advanced	\sim	Service Type	TCP	~	
Ø Diagnostics	~	* Service Address	192.168.50.94	C	
:== System	~	* Service Port	192.168.50.94 (WAN)	1-65535
		* VPN Subnet/Netmask	10.80.12.0/24		0
		Client Access	O Home Network	Only O Internet ar	nd Home Network
				Expand	
			Save		
« Collapse					

(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	~	0
Deliver DNS	Example: 1.1.1.1		• +
Authentication	SHA2		

- (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 5-3	Configuration Items of OpenVPN Server Mod	de
	Configuration Refile of Open II in Certer Met	40

Item	Description
Server Mode	The device supports Account, Certificate and Account & Certificate authentication modes:
	 Account mode. The confect account name, password, and CA certificate are required to connect to the server. The configuration is simple. Certificate mode: The client needs the correct CA certificate, client certificate,
	and pre-shared key to connect to the server.
	 Account & Certificate mode: The client needs the correct account name, password, CA certificate, client certificate, and pre-shared key to connect to the server. This mode is suitable for scenarios with high security requirements.
	All communication on OpenVPN is based on a single IP port, using UDP or TCP 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.
	The port used by the OpenVPN service process. The official port assigned to
Service Port	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	The IP address pool delivered to VPN clients, in the form of a network segment.
Subnet/Netmask	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 will access	You can choose Home Network Only or Internet and Home Network

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

2. Adding OpenVPN clients

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

Enable **Status** and click OK.

VPN Clie	nt List	Use	ername/Password Q	+ Add	🖻 Batch Delete
Up to 30	entries can be added.				
	Username	Password	Status		Action
		No Data			
< 1	> 10/page ~				Total 0

Add User			×
* Username	Enter a username.		
* Password	Enter a password.		\bigcirc
Status			
		Cancel	OK

5.23.3 Configuring OpenVPN (Client Mode)

Mobile Phone 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 Tunnel List			
i OpenVPN			
Enable 🧲			
OpenVPN Type	Server O Client		
Server Mode	Account & Certificate	~	
* Username	Username of OpenVpn use	er	2
* Password	Password of OpenVpn use	er	9
* Client Config	.ovpn	Browse	
	Save		

Table 5-4 Configuration Items of OpenVPN Client Web Setting Configuration Mode

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

5.23.4 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



_ _ _ _ _ _ _ _ _

Device A as Server

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 Eweb management system of the device, 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.

Ruij	jie	Reyce 1	ome (Clients	Haternet	(r Wi-Fi
Basics	~					
🛜 WLAN	~					
Work Mode		() OpenVPN				
Security	~	Enable 🧲	D			
👳 VPN	^	OpenVPN Type 🧿	Server O	Client		
PPTP		Service Mode	Certificate		~	
OpenVPN						
Advanced	~	Service Type	TCP		~	
Ø Diagnostics	~	* Service Address	192.168.50.9	94	8]
:== System	~	* Service Port	192.168.50.	.94 (WAN)		1-65535
		* VPN Subnet/Netmask	10.80.12.0/2	24		0
		Client Access	O Home Netw	vork Only	Internet and	Home Network
					Expand	
			Save	e		
Collapse						

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

Parameter	Description
Service Mode	Account: Authentication based on password. Certificate: Authentication based on client certificate. Account & Certificate: Authentication based on password and client certificate.
Service Type	Use the default value unless there are specific requirements. Both UDP and TCP are supported. If the network connection between the two ends of an encrypted tunnel is poor, for example due to high latency or heavy packet loss, then select TCP .
Service Address	The IP address of the WAN port is automatically populated.

Parameter	Description
Service Port	Indicates the port for OpenVPN service. Use the default value unless there are specific requirements.
VPN Subnet/Netmask	Indicates the network segment of the OpenVPN address pool. The first available IP address in the address pool is reserved for the server, while other addresses can be allocated to clients. For example, if this parameter is set to 10.80.12.0/24 , then the virtual IP address of the VPN server is 10.80.12.1.
Client Access	Home Network Only: If this access mode is selected, then the client can only access resources on the server's internal network, but is unable to access the Internet through the server's network proxy. Internet and Home Network: If this access mode is selected, then the client not only can access resources on the server's internal network, but also can access the Internet through the server's network proxy.

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

Collapse

TLS Authentication		
Allow Data Compression	Yes 🗸	0
Cipher	AES-128-CBC V	0
Deliver DNS	Example: 1.1.1.1	0 +
Authentication	SHA256	
	Save	
Configuration File	Export	
CA Certificate	Export	

(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.

-		·					_
С		◇ 🏠 எ 🗟 ⊶ 192.168.1	10.1/cgi-bin/luci/;stok=28bd02	edfc370a711	dac592a9ba7d943/admin/alone/vpn/open_v ☆	\odot \mp	ź
sited 🕀 x preven	Fedora D ted this si	Docs 🚆 Fedora Magazine 🗋 Fedo te from opening a pop-up window.	ra Project 🗅 User Communitie	es 🗋 Red Ha	20230614_client.ovpn Completed — 4.2 KB	۵	
RU	jie	≋Reyee 1			20230612_client.ovpn Completed — 1.4 KB		
		* Service Port	11940	inciriici i	Show all downloads		
'S	\sim						
N	\sim	* VPN Subnet/Netmask	10.80.12.0/24		0		
: Mode		Client Access	Home Network Only	Internet and I	Home Network		
rity	\sim		Collar	200			
	^	TLS Authentication					
/PN		Allow Data Compression	Yes	~	0		
nced	~	Cipher	AES-128-CBC	~	0		

- 5. Configuring OpenVPN Client (Use Windows Client as an Example)
- (1) download the OpenVPN client (https://openvpn.net).

Connect to OpenVPN
Download our free and full-featured VPN client to connect to Cloud Connexa, Access Server or any OpenVPN protocol compatible server.
iOS
Download
Read the installation guide \rightarrow

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



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

< _	Im	porte	d Pro	file	
Profile Na	me				
192.168	8.50.94 [20	02306	4_clie	nt]	
Server Ho	ostname (lock	(ed)			
192.168	.50.94				

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

OpenVPN Co	onnect	- ×
≡	Profiles	10
CONNEC	TED	
	OpenVPN Profile 192.168.50.94 [20230614_client]	
CONNEC	TION STATS	
		Ī
0B/s		
BYTES IN 0 KB/S	U BYTES O 313 B/S	UT
DURATION 00:00:12	PACKET RECEIVED 1 sec ago	
YOU	•	Ð

Check the obtained virtual IP addresses.

OpenVPN Connect		– ×
≡	Profiles	Ð
	N	
0B/s		
BYTES IN 1.08 KB/S	† BYT 2.47	TES OUT 7 KB/S
DURATION 00:00:17	PACKET RECEIVED 0 sec ago	
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	
		Ð

(5) Log in to the Eweb management system of the device, and choose More > VPN > OpenVPN > Online User to find the connected client.

Basics	~						
🔶 WLAN	~	OpenVPN	Online User				
10 Work Mode		🧃 Onli	ne User				
UI WOR MODE			llearname	Server/Client	Statue	Peal ID Address	Virtual ID Address
Security	~		Usemane	Servenchent	Status	Real IP Address	Virtual IP Address
👳 VPN	^		openvpn	Server	OK	192.168.50.94	10.80.12.1
DDTD			client	Client	ОК	192.168.50.214	10.80.12.2
FFIF							
OpenVPN							
🗄 Advanced	~						

5.24 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 **Reachable Check Period**, **Unreachable Check Period** and **URL List** fields, and click **Save** to save the settings.

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

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

Ruíjie	≜Reyee	1 Home		Clients	Internet	(Wi-Fi	-B- More			
Local DNS	•									
Reyee Mesh	Connectivity de	rtection								
Reyee Mesh 3.0	* Reachable Check Period	120		seconds						
AP Networking	* Unreachable Check	5		seconds						
Flow Control	Period									
Hardware Acceleration	* URL List	http://www.amazon.con	Add							
Port Settings		http://www.google.cc	Delete							
Connectivity detection		http://www.yahoo.coi	Delete							
Wi-Fi Switch										
CWMP		http://wikipedia.org	Delete							
Other Settings		http://www.msn.com	Delete							
@ Diagnostics		Save								
📲 System										
«Collapse										

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

5.25 Enabling CWMP

PC View: Choose More > Advanced > CWMP

Mobile Phone View: Choose More > Switch to PC view > More > Advanced > CWMP

5.25.1 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.

5.25.2 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.

CWMP	
* Inform Interval	600
* ACS Address	http://127.0.0.1:8080/acs
* ACS Account	0
* ACS Password	0
STUN	
* STUN Server Address	127.0.0.1
* STUN Server Port	0
* STUN Server Account	0
* STUN Server Password	0
	Save

5.26 Enabling Reyee Mesh

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

PC View: Choose More > Advanced > 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.

5 Work Mode		
⊘ Security	~	 After Reyee Mesh is enabled, mesh pairing can be triggered through the button. After Reyee Mesh is disabled, the bridged slave router will still be connected.
VPN	~	Enable
🖶 Advanced	^	Save
Port Mapping		
Dynamic DNS		
UPnP Settings		
Local DNS		
Reyee Mesh		

Note

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

5.27 Enabling Hardware Acceleration

<u> </u>	Caution
This fe	eature is supported in router mode.
Smart	tphone 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.

Ruíjie	≋R∈y∈e	☆ Home	Clients	(Internet	(Wi-Fi	-B- More	English ~	88	8
Reyee Mesh 3.0	Hardware Accelerat After Hardware Accele	ion ration is enabled, the	e Internet access s	peed will be improve	ed and clients will n	ot be rate-limited.			
AP Networking Flow Control	Enable								
Hardware Acceleration		Save							
Port Settings Connectivity detection									
Wi-Fi Switch									
CWMP Other Settings									
Oiagnostics V									e
°a⊶ ∘o≕ System ∽ ≪Collapse									Ai

A Caution

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

5.28 Configuring Console Booster

1 Note	
Only EW30000	GX PRO supports this function.
Smartphone Vi	ew: Choose More > Switch to PC view > More > Advanced > Console Booster .
PC View: Choo	ose More > Advanced > Console Booster .
GearUP Conso the "Reyee Ro and control its	ble Booster is a brand new tool to optimize your console's network performance. By using either uter" or "GearUP Console Booster" app, you can easily and quickly bind your gaming console boost using your phone.
Image: Point of the second	(j) Console Booster
Port Mapping	Scan the QR code to download the Reyee Router app. Choose GearUP Console Booster on the home page.
Dynamic DNS	
UPnP Settings	
Local DNS Reyee Mesh	GearUP Console Booster GearUP Console Booster is a brand new tool to optimize your console's network performance! • Effectively reduce game latency and optimize NAT type.
	 compatible with mansurean consoles and optimized specifically for an common online games.



5.29 Configuring AP Networking

PC View: Choose More > Advanced > AP Networking
Smartphone View: Choose More > Switch to PC view > More > Advanced > AP Networking
Click Switch To AP Mode, switch the router found on the local network to AP mode with a single click.

Ruíjie	[≜] Reyee	1 Home	Clients) Internet	🛜 Wi-Fi	 More	English ~ 鼹	@ ®
VPN V	AP Networking	L						
🗎 Advanced	Switch the router	found on the local netwo	rk to AP mode with a	single click.				
Port Mapping	Model	IP	Work Mode	MAC		SN	Software Ver	
Dynamic DNS	M32	192.168.110.1	ROUTER	9C:2B:A6:F5:	1B:36	G1QHCVL003838	ReyeeOS 1.219.1821	
UPnP Settings	EW300N	192.168.110.1	ROUTER	02:D0:F8:15:	02:20	MACCEW3001001	ReyeeOS 1.300.2302	
Local DNS	EW3200GX	192.168.110.1	ROUTER	54:16:51:B7:	94:75	G1RH1VK14346C	ReyeeOS 1.223.2303	
Reyee Mesh	< 1 > 10	//page						Total 3
Reyee Mesh 3.0	Switch To AP Mod	le						
AP Networking								
Flow Control								
Hardware Acceleration								
«Collapse								

5.30 Configuring Reyee Mesh 3.0

5.30.1 Configuration Steps

PC View: Choose More > Advanced > Reyee Mesh 3.0 Mobile Phone View: Choose More > Switch to PC view > More > Advanced > Reyee Mesh 3.0 Connect the routers as indicated in the following figure:



1. Parallel Networking

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

(1) Click Enable to enable Reyee Mesh 3.0.

♥ VPN	😔 Security 🗸 🗸		
Advanced Port Mapping Dynamic DNS UPnP Settings Local DNS Reyee Mesh Reyee Mesh 3.0 AP Networking Flow Control	VPN V	7 Reyee Mesh 3.0	
Port Mapping Dynamic DNS UPnP Settings Local DNS Reyee Mesh Reyee Mesh 3.0 AP Networking Flow Control	🔁 Advanced		
Dynamic DNS AP Networking—The working mode of each UPnP Settings router is set to AP mode. The modem Local DNS Parallel Networking—A router is auto Reyee Mesh works as a gateway to connect to other Reyee Mesh 3.0 routers with the Ethernet cables. Flow Control Hardware Accoloration	Port Mapping	Reyee Mesh 3.0	
UPnP Settings router is set to AP mode. The modem router is auto selected as the master device. The modem router is auto selected as the master device. The modem routers with the Ethernet cables.	Dynamic DNS	AP NetworkingThe working mode of each	
Local DNS Parallel Networking—A router is auto Reyee Mesh Reyee Mesh 3.0 AP Networking Flow Control Hardware Accoloration «Collapse	UPnP Settings	router is set to AP mode. The modem works as the core node to forward packets. Enable	
Reyee Mesh selected as the master device. The modem Reyee Mesh 3.0 works as a gateway to connect to other AP Networking routers with the Ethernet cables. Flow Control Varduums Accoloration Varduums Accoloration Collapse	Local DNS	Parallel NetworkingA router is auto	
Reyee Mesh 3.0 routers with the Ethernet cables. AP Networking Flow Control Hardware Accoloration Collapse	Reyee Mesh	selected as the master device. The modem works as a gateway to connect to other	
AP Networking Flow Control Control Collapse	Reyee Mesh 3.0	routers with the Ethernet cables.	
Flow Control	AP Networking		
Acceleration «Collapse	Flow Control		
	Collapse	NR	

(2) Choose Parallel Networking, and click Next.

(3) Check routers for the networking.

💋 Modem	Networking					
	Configure Networking N	lode	Select Devic	e	Finis	h
elect the targ	get device.	-	12/27 0 27 41			
	Hostname	SN	Model	Networking Mode	MAC	Software Ver
2	Reyee	G1QHCVL003838	M32		9C:2B:A6:F5:1B:36	ReyeeOS 1.219.1726
n l	Reyee	G1RP2JM00031C	EW300-PRO		28:D0:F5:08:48:BB	ReyeeOS 1.219.1728

(4) Click Next.

Nodem Networking				
Configure Networking	Mode	Select	Device	- Finish
		Networking	succeeded.	
		Admin URL:	10.44.77.253	
		Admin Passw You are advised to :	vord:11111111 save the screenshots.	
		FI	nish	

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

Modem Networking					
Current Mode:Parallel Networking Add Device					
Hostname	SN	Model	Networking Mode	MAC	Software Ver
		No	o Data		
		214			
		http://10.44.77.253 Redirecting	16s		

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

2. AP Networking

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

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

🛇 Security 🗸	
™ VPN ∽	() Reyee Mesh 3.0
🔁 Advanced 🗠	
Port Mapping	Revee Mesh 3.0
Dynamic DNS	AP NetworkingThe working mode of each
UPnP Settings	router is set to AP mode. The modem Works as the core node to forward packets. Enable
Local DNS	Parallel NetworkingA router is auto
Reyee Mesh	selected as the master device. The modem works as a gateway to connect to other
Reyee Mesh 3.0	routers with the Ethernet cables.
AP Networking	
Flow Control	
Collapse	NR

(2) Choose AP networking, and click Next.

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

1 Modern Networking						
Configure Networking Mode						
Select the targ	jet device.					
V	Hostname	SN	Model	Networking Mode	MAC	Software Ver
X	Reyee	G1QHCVL003838	M32		9C:2B:A6:F5:1B:36	ReyeeOS 1.219.1726
	Reyee	G1RP2JM00031C	EW300-PRO		28:D0:F5:08:48:BB	ReyeeOS 1.219.1728
			- FIGNOUS	HLA.		

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

Configure Networking Mode Finish	D Modem Networking			
Control of the second	Config	ure Networking Mode	Select Device	Finish
Networking succeeded. Admin URL: 10.44.77.253 Admin Password: 1111111 You are advised to save the screenshots. Finish			0	
Admin URL: 10.44.77.253 Admin Password: 1111111 You are advised to save the creenshots. Finish			Networking succeeded.	
Admin Password: 1111111 You are advised to save the screenshots. Finish			Admin URL: 10.44.77.253	
Finich			Admin Password:11111111	
Finish			tou are advised to save the screenshots,	
			Finish	

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

5.31 Diagnosing Network Problems

Mobile phone view: Choose More > Network Check.

PC view: Choose More > Diagnostics > Network Check.

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

← Network Check	S
Network Check	0
In Progress	
46%	
WAN/LAN Cable	ø
Auto-Negotiated Speed	0
WAN Port	Ø
DHCP-Assigned IP Address	Ø
LAN & WAN Address Conflict	0
Loop	0
DHCP Server Conflict	0

6 Reyee System Settings

6.1 Switching to the 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 a mobile phone.

You can click in the upper left corner to return to the mobile phone view or drag the page to the narrowest position on the PC to enter the mobile phone view.



6.2 Configuring the Login Password

Mobile phone view: Choose **More** > **System** > **Password**.

PC view: Choose More > System > Login > Login Password.

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

\leftarrow	Password	G
I	Change the login password. Please log in again with the new password later.	?
* Old Pa	issword	
* New P	assword	
* Confir	m Password	
	Save	

6.3 Remote Access

Smartphone View: Choose	More > Switching to PC View > More >	
PC View: Choose More >		
Click Enable to enable the	remote access.	

🛕 Caution

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

This function cannot be enabled if the device management password has a weak security strength, such as being purely numerical or alphabetical. See <u>6.2</u> Configuring the Login Password to configure a strong and secure device management password.

Implementation Cookbook

T	Ruíjí	ē ≋Reyee	1 Home	Clients	(Internet	(îr Wi-Fi	-a- -a- More	English ~	0-0 6 X	8
🗇 WLAN	~	Login Password Session Timeout	Remote Acces							
🕼 Work Mode		Barrada Asses								
Security	×	Allow others to log in to the device	through URL link							
S VPN	×	Enable								
🗄 Advanced	~	Login URL http://10.52.16.1	22							
② Diagnostics	~	Save								
System	^									
System Time										
Login										
Management										
Upgrade										
LED										
Reboot										Ai
« Collapse										

6.4 Restoring Factory Settings

Mobile phone view: Choose More > System > Restore.

PC view: Choose More > System > Management > Reset.

Click Reset to restore factory settings.

🛕 Note

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

\leftarrow	Restore	1
i	Resetting the device will clear the current settings. If you want to keep the setup, please Backup Profile first.	
	Reset	

6.5 Configuring the System Time

Mobile phone 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 the 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.

\leftarrow	Time	S
<i>i</i> Configure and view	system time	0
Current Time 2022-01-12 04:24:54	Edit	
* Time Zone	laur Vark	
* NTP Server	iew_tork	~
0.cn.pool.ntp.org		Add
1.cn.pool.ntp.org		Delete

6.6 Configuring Scheduled Reboot

6.6.1 Getting Started

Confirm that the system time is accurate to avoid network interruption caused by device reboot at the incorrect time point. For details, see <u>6.5</u> Configuring the System Time.

6.6.2 Configuration Steps

Mobile phone view: Choose More > System > Scheduled Reboot.

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

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

\leftarrow	Scheduled Reboot	S
Enable		
Day		
🗸 Mon	🗸 Tue 🗸 Wed 🖌 Thu	
🖌 Fri	Sat Sun	
Time		
03	✓ : 00 ✓	
	Save	

6.7 Performing Online Upgrade and Displaying the System Version

Mobile phone view: Choose More > System > Online Upgrade.

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

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

A Note

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 Internet access from being affected.

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



Auto Upgrade

Auto upgrade the device when a new version appears.

6.8 Enabling or Disabling the LED

Mobile phone view: Choose More > System >Healthy Mode.

```
PC view: Choose More > System > LED.
```



6.9 Switching the System Language

Mobile phone view: Choose **More** > **Language**.



PC view: Click

in the upper right corner of the page.

Click a required language to switch the system language.

\leftarrow	Language G
	中文
0	English
	繁體
0	Indonesia

6.10 Network Diagnosis Tools

6.10.1 Network Test Tool

Mobile phone view: Choose More > System > Network Tools.

PC view: Choose More > Diagnostics > Network Check.

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

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.

i Network Tools			
Tool	• Ping		cup
* IP Address/Domain	www.google.com		
* Ping Count	4		
* Packet Size	64	Ву	/tes
	Start	Stop	
Result			

6.10.2 Packet Obtaining Tool

Mobile phone view: Choose More > Switch to PC view > More > Diagnostics > Packet Capture.

PC view: Choose More > Diagnostics > Packet Capture.

Configure the interface, protocol, IP address whose packets need to be obtained, file size limit, and packet count limit to limit the volume of packets obtained. 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.

🛕 Note

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

<i>i</i> Packet Capture			
Interface	ALL	~	
Protocol	ALL	~	
IP Address			
File Size Limit	2M	~	Available Memory 26.61 M
Packet Count Limit	500	~	
	Start	Stop	

6.11 Configuring Backup and Import

Mobile phone view: Choose More > Switch to PC view > More > System > Management.

PC view: Choose More > System > Management > Backup&Import.

To configure backup, click **Backup** to download a configuration file locally.

To 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.

R	Image: Clients Image: Clien
	Backup & Import Reset
(((*	
\bigcirc	 if the target version is much later than the current version, some configuration may be missing. It is recommended to choose Restore before importing the profile. The device will be rebooted automatically later.
Ē	Backup Profile
	Backup Profile Backup
-0-	Import Profile
	File PathPlease select a file.Browse
	Import

6.12 Configuring the Session Timeout

Mobile phone view: Choose More > Switch to PC view > More > System > Login.

PC view: Choose More > System > Login.

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

< .ogin Password	Session Timeout	>
i Session Time	out (?
* Session Timeout		
3600		
	Save	

7 Reyee FAQ

- 7.1 Reyee Password FAQ (Collection)
- 7.2 <u>Reyee Wireless Repeater FAQ (Collection)</u>
- 7.3 Reyee Parental Control FAQ (Collection)
- 7.4 Reyee Mesh FAQ (Collection)
- 7.5 Reyee Self-Organizing Network (SON) FAQ (Collection)
- 7.6 <u>Reyee series Devices Parameters Tables</u>
- 7.7 Reyee Parameter Consultation FAQ (Collection)

8 Appendix: Monitoring of Reyee Mesh Wi-Fi Routers

8.1 Overview

The **Overview** page displays the local connection and information of **Device Details**, **Wi-Fi** and **Interface Details**. The information of the download speed, upload speed, local device, and connected clients is displayed on the top of this page. **Device Details** includes the model, host name, SN, and MAC address. **Interface Details** displays connections of the WAN and LAN.

Rujje	1 Home	Endpoints	Hand Internet		-o- -o- More				8
Internet	<u>↑ 85.37</u> ↓ 1.36N	Kbps /bps	EW1200G-PRO		Wireles	1 • Clients	+ Add		
Device Details Model: EW1200G-FRO MAC: Hardware Ver:		Hostname: Duration: ; Software Ver:	21 days 17 hours 58 minutes	28 seconds	SN: Systime: 2022-03-17 16:) 51:01			
Wi-Fi Primary Wi-Fi: testssid Security: No			Guest Wi-Fi Security	: No					
Interface Details									
		W/ 172.26	AN LAN3 LAN2 1.5.104 192.168.110.1	LAN1					

8.2 Endpoints

This page displays all connected endpoints on this network, including wired and wireless users. The **Clients** page allows you to bind static IP addresses, manage blocked time, and block WLAN clients.

Ruíj	ie I 🕯 F	Reyee	1 Home	Endpoints	Internet	(Wi-Fi	-B- -B- More		English ~		٩	8
	i End	dpoints e client list includes online client	ts and blocked client	s. The client going offli	ne will not disappear imm	ediately. Instead, the	e client will stay in the list	for three more min	utes.			
	Endpo	ints	Search	by IP/MAC/Username	Q C Refresh	© Refresh Blocked Time Management Blocked WLAN Clie		ocked WLAN Clie	nts Management			
		Username/Type		IP/I	MAC	Blocked Time			Action \Leftrightarrow			
	ç	*		192.168.110	147 6 ⁹ 7 Unbinded	09:30- Wednes You ha + Add	11:30 :day ve set 1 blocked time. Blocked Time	×	Block			
I	H ^L Enovo	USER-20191214JF		192.168.11	0.47 6 ⁽²⁾ Unbinded	Not Set + Add	t (No time is blocked.) Blocked Time		Wired Client			
	< 1	> 10/page >							Total 2	2		

Click **Blocked Time Management** to customize the time to block users.

Blocked Time Management					×
Blocked Time List			+ Add	Delete Se	elected
Set a time to prevent clients accessing th	e Internet. Up to 32 entries	can be added.			
Blocked Time	Bl	ocked MAC	Remark	Ad	tion
00:00-23:59 Monday Tuesday Wednesday Thurso	ay Friday	ô	test	Edit	Delete
09:30-11:30 Wednesday			app_Crossra.co F	Edit	Delete
< 1 > 10/page >					Total 2
Add Rule					\times
Blocked Time	Custom		\\	/	
* Date	Please Select [Day	~		
* Time	© 18:54	- 🕓	19:54		
Remark	USER-2019121	4JF			
			Cancel	C	Ж

Click **Blocked WLAN Clients Management** and add the MAC address to prevent WLAN users from connecting the SSID.

Blocked WLAN Clients Manager	×	
Blocked WLAN Clients	+ Add 🗇 Delete Selected	
Up to 30 members can be added.		
MAC	Remark	Action
	No Data	
1 > 10/page		Total 0
Blocked WLAN Clients Manager	ment	×
Blocked WLAN Clients		+ Add Delete Selected
Up to 30 members can be added.		
MAC	Remark	Action
	No Data	
< 1 > 10/page >		Total 0

8.3 Internet

This page displays the mode where the device access the Internet, including **PPPoE**, **DHCP**, and **Static IP**.

Ruíjie MReyee	1 Home	Endpoints	Internet	∲ Wi-Fi	-B- -B- More	English ~	٩	8	
	Internet:				Online (DHCP)				
	PPPoE		DHCP		Static IP				
			ally Assigned IP A	Address					
	172.26.5.104								
	Subnet Mask 255.255.252.0 Gateway 172.26.4.1								
	DNS Server 192.168.58.110 192.168.58.94								
	Save								

DHCP: The router detects whether the IP address can be obtained through DHCP by default. If the router connects to the Internet successfully, you can click **Next** without entering an account.

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

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