

Ruijie Reyee RG-EG Series Router

Implementation Cookbook



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.



and other Ruijie networks logos are trademarks of Ruijie Networks.

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

Disclaimer

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

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

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

Preface

Intended Audience

This document is intended for:

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

Technical Support

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

Conventions

1. GUI Symbols

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

2. Signs

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.

Caution

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

 **Note**

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

 **Specification**

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

3. Note

This manual 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 Product Introduction	1
1.1 Models	1
1.2 LED Indicators	4
1.3 Button.....	5
2 Getting Started	6
2.1 Network Planning.....	6
2.2 Installing the Router.....	7
2.2.1 Safety Suggestions	7
2.2.2 Installation Site Requirement.....	8
2.2.3 Installation Steps.....	10
2.3 Quick Provisioning	10
2.3.1 Quick Provisioning Through Ruijie Cloud App.....	10
2.3.2 Quick Provisioning Through Reyee Eweb	16
3 Device Management	19
3.1 Login	19
3.2 Switching the Work Mode	20
3.3 Configuring the Login Password.....	22
3.4 Configuring the System Time	23
3.5 Configuring Upgrade.....	26
3.5.1 Online Upgrade.....	26
3.5.2 Local Upgrade.....	26
3.6 Backing Up or Restoring the Configuration	27

3.7 Configuring Restart.....	28
3.7.1 Restarting the Current Device	28
3.7.2 Restarting All Devices on the Network	29
3.7.3 Restarting Specified Devices.....	29
3.7.4 Configuring Scheduled Restart.....	29
3.8 Restoring Factory Settings	30
3.9 Configuring Cloud Service.....	30
3.9.1 Overview	30
3.9.2 Configuration Steps	31
3.9.3 Unbinding Cloud Service	32
4 Common Settings.....	33
4.1 Network Access Setting.....	33
4.1.1 PPPoE Configuration Through a WAN Port	33
4.1.2 Static IP Address Configuration Through a WAN Port	34
4.1.3 DHCP Configuration Through a WAN Port.....	35
4.2 AP Management	37
4.2.1 Switching the Working Mode	37
4.2.2 Configuring AP Groups	39
4.2.3 Configuring Wi-Fi	40
4.2.4 Configuring Guest Wi-Fi	43
4.2.5 Healthy Mode.....	44
4.2.6 RF Settings	44
4.2.7 Configuring a Wi-Fi Blocklist or Allowlist	46
4.2.8 Configuring AP Load Balancing.....	48

4.2.9 One-Click Wireless Optimization	52
4.2.10 Scheduled Wireless Optimization	55
4.2.11 Wi-Fi Roaming Optimization (802.11k/v)	56
4.2.12 Enabling Reyee Mesh.....	57
4.2.13 Configuring a LAN Port of a Downlink AP	58
4.3 Switch Settings	59
4.4 Configuring the WAN Ports	60
4.4.1 Configuring the Internet Access Mode.....	60
4.4.2 Modifying the MAC Address	61
4.4.3 Modifying the MTU.....	62
4.4.4 Configuring the Private Line	63
4.4.5 Configuring the VLAN Tag	64
4.4.6 Configuring NAT Mode.....	64
4.4.7 Configuring the Multi-Line Load Balancing Mode	65
4.4.8 Configuring Link Detection.....	69
4.5 Diagnostics	72
4.5.1 Network Check.....	72
4.5.2 Alarms	72
4.5.3 Network Tools	73
4.5.4 Packet Capture	76
4.5.5 Fault Collection	77
4.5.6 Viewing Flow Statistics	77
4.6 Port VLAN	78
4.7 Port Mapping.....	80

4.7.1 Configuring Port Mapping	81
4.7.2 Configuring NAT-DMZ.....	83
4.8 Dynamic DNS	84
4.9 Wi-Fi Authentication.....	86
4.9.1 Overview	86
4.9.2 Getting Started.....	86
4.9.3 Cloud Authentication	87
4.9.4 Configuring Third-Party Authentication.....	89
4.9.5 Local Account Authentication.....	92
4.9.6 Authorized Guest Authentication	94
4.9.7 Guest Authentication Through QR Code Scanning.....	96
4.9.8 Authentication-Free.....	97
4.9.9 Online Authenticated User Management.....	100
4.10 Wireless Authentication	101
4.10.1 Overview	101
4.10.2 Configuring Captive Portal on Ruijie Cloud.....	101
4.10.3 Configuring an Authentication-Free Account on Eweb Management System	115
4.10.4 Checking Authentication User List Eweb Management System	118
4.11 Configuring SNMP	119
4.11.1 Overview	119
4.11.2 Global Configuration	119
4.11.3 View/Group/Community/User Access Control	121
4.11.4 SNMP Service Typical Configuration Examples	129
4.11.5 Configuring Trap Service	134

4.11.6 Trap Service Typical Configuration Examples	138
4.12 Configure IEEE 802.1X authentication	141
4.12.1 Overview	141
4.12.2 Configuring 802.1X Globally	142
4.12.3 Configuring the RADIUS Server	144
4.12.4 Checking Authentication User List	146
4.13 Behavior	147
4.13.1 Application Scenario	147
4.13.2 App Control	148
4.13.3 Website Management	152
4.13.4 Access Control	156
4.13.5 Network Behavior Settings	160
4.14 Flow Control	162
4.14.1 Application Scenario	162
4.14.2 Smart Flow Control	163
4.14.3 Custom Policies	165
4.14.4 Application Priority	172
4.15 Security	175
4.15.1 Application Scenario	175
4.15.2 Configuring the ARP List and ARP Guard	176
4.15.3 Configuring MAC Address Filtering	177
4.16 Configuring Device Security	178
4.16.1 Configuring an Admin IP Address	178
4.16.2 Configuring Security Zones	181

4.16.3	Configuring Session Attack Prevention	183
4.16.4	Checking the Security Log.....	185
4.17	Configuring the PPPoE Server	185
4.17.1	Application Scenario	185
4.17.2	Global Settings.....	186
4.17.3	Configuring a PPPoE User Account	188
4.17.4	Configuring a Flow Control Package	189
4.17.5	Configuring Exceptional IP Addresses	190
4.17.6	Checking Online Users	191
4.18	IPTV	192
4.18.1	Application Scenario	192
4.18.2	Dual-WAN Configuration	192
4.18.3	Single-WAN Configuration	194
4.19	UPnP.....	195
4.19.1	Application Scenario	195
4.19.2	Procedure	196
4.20	Configuring Rate Test.....	197
4.21	Configuring IPv6	198
4.21.1	IPv6 Overview	198
4.21.2	IPv6 Basics	198
4.21.3	IPv6 Address Allocation Modes	199
4.21.4	Enabling the IPv6 Function.....	199
4.21.5	Configuring an IPv6 Address for the WAN Port.....	199
4.21.6	Configuring an IPv6 Address for the LAN Port.....	201

4.21.7 Viewing the DHCPv6 Client	203
4.21.8 Configuring the Static DHCPv6 Address	203
4.21.9 Configuring the IPv6 Neighbor List.....	204
4.22 Configuring Routes	205
4.22.1 Configuring Static Routes.....	205
4.22.2 Configuring PBR	208
4.22.3 Configuring RIP.....	215
4.22.4 Configuring RIPng	222
4.22.5 OSPF v2	227
4.22.6 OSPF v3	237
4.22.7 Viewing Routing Tables	245
4.22.8 Set URL Route.....	246
4.23 Feature Configuration	247
4.24 Configuring Domain Proxy.....	248
4.25 Client Association	249
5 Online Client Management	250
5.2 Configuring Client IP Binding.....	251
5.3 Configuring Client Access Control.....	252
5.4 Configuring Client Association.....	252
5.5 Blocking Clients	253
5.6 Configuring Client Rate Limiting	254
6 VPN.....	257
6.1 Configuring IPsec VPN.....	257
6.1.1 Overview	257

6.1.2 Configuring the IPsec Server.....	257
6.1.3 Configuring the IPsec Client.....	264
6.1.4 Viewing the IPsec Connection Status.....	266
6.1.5 Typical Configuration Example.....	267
6.1.6 Solution to IPsec VPN Connection Failure.....	271
6.2 Configuring L2TP VPN.....	272
6.2.1 Overview.....	272
6.2.2 Configuring the L2TP Server.....	272
6.2.3 Configuring the L2TP Client.....	279
6.2.4 Viewing the L2TP Tunnel Information.....	281
6.2.5 Typical Configuration Example.....	282
6.2.6 Solution to L2TP VPN Connection Failure.....	293
6.3 Configuring PPTP VPN.....	294
6.3.1 Overview.....	294
6.3.2 Configuring the PPTP Service.....	294
6.3.3 Configuring the PPTP Client.....	297
6.3.4 Viewing the PPTP Tunnel Information.....	299
6.3.5 Typical Configuration Example.....	300
6.3.6 Solution to PPTP VPN Connection Failure.....	310
6.4 Configuring OpenVPN.....	311
6.4.1 Overview.....	311
6.4.2 Configuring the OpenVPN Server.....	311
6.4.3 Configuring the OpenVPN Client.....	316
6.4.4 Viewing the OpenVPN Tunnel Information.....	321

6.4.5 Typical Configuration Example	321
7 Appendix: Surveillance.....	329
7.1 Device Info.....	329
7.2 Network Topology.....	330
7.3 Real-Time Flow.....	331
7.4 Traffic History.....	332
7.5 URL Logs.....	332

1 Product Introduction

Reyee RG-EG series router is a cloud managed router designed for villas and smart home, restaurants, small offices, and homestay hotels. It is affordable, small, and easy to use, providing 500–600 Mbps bandwidth and supporting up to 200 clients.

RG-EG series routers provide industry-leading auto-discovery and auto-networking for routers, switches, and wireless devices.

RG-EG series routers can perform per-port VLAN configuration to achieve port isolation, and integrate with smart flow control to achieve comprehensive network planning and perform local and remote network diagnosis.

1.1 Models

The RG-EG series routers come in five models.

Model	10/100/1000 Base-T Ethernet Port	Maximum Number of Concurrent Clients	Recommended Bandwidth	Management Capacity
RG-EG105G-P V2	5 (PoE supported)	100	600 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 300 Router mode: 32
RG-EG105G V2	5	100	600 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 300 Router mode: 32
RG-EG105GW	5	100 (recommended number of wireless terminals: 60)	500 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	Router mode: 32

Model	10/100/1000 Base-T Ethernet Port	Maximum Number of Concurrent Clients	Recommended Bandwidth	Management Capacity
RG-EG210G-E	10	200	1000 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 500 Router mode: 150
RG-EG210G-P	10 (PoE supported)	200	600 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 500 Router mode: 150
RG-EG105GW(T)	5	100	600 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	No. of Manageable Devices (AP + NBS Switches, Router Mode, including this device): 32 No. of Manageable Devices (AP + NBS Switches, Wired Repeater Mode, including this device): N/A No. of Manageable Devices (AP + NBS Switches, Wired Repeater Mode, including this device): 32 No. of Manageable Devices (ES Switches): 128

Model	10/100/1000 Base-T Ethernet Port	Maximum Number of Concurrent Clients	Recommended Bandwidth	Management Capacity
RG-EG105GW-X	5	180	1200 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	Router mode: 64
RG-EG305GH-P-E	5	300	1500 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 500 Router mode: 150
RG-EG310GH-E	10	300	1500 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 500 Router mode: 150
RG-RG1510XS	10 (including 4 x 10/100/1000/2500Base-T ports)	1500	4000 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 600 Router mode: 500
RG-EG310GH-P-E	10	300	1500 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 500 Router mode: 150

Model	10/100/1000 Base-T Ethernet Port	Maximum Number of Concurrent Clients	Recommended Bandwidth	Management Capacity
RG-EG105G-V3	5	100	500 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 300 Router mode: 32
RG-EG105G-P-V3	5 (PoE supported)	100	500 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 300 Router mode: 32
RG-EG210G-P-V3	10 (PoE supported)	200	700 Mbps (Turn off flow control if you want to test the speed of your network or test the maximum throughput)	AC mode: 500 Router mode: 150

1.2 LED Indicators

LED Indicator	Status	Description
SYS	Flashing	<p>Fast flashing (at 8 Hz): The router is starting up.</p> <p>Slow flashing (at 0.5 Hz): The network is unreachable.</p> <p>One long flash followed by three short flashes (at 0.8 Hz): The router is faulty.</p> <p>Flashing twice consecutively (at 0.8 Hz):</p> <ul style="list-style-type: none"> ● The router is restoring factory settings. ● The router is upgrading the software. <p>Note: Do not power off the router in this case.</p>

LED Indicator	Status	Description
	Solid on	The router is functioning properly.
	Off	The router is not powered on.
Port	Flashing	The port is connected and is sending/receiving traffic.
	Solid on	The port is connected and is not sending/receiving traffic.
	Off	No link is detected for this port.
Mesh	Off	<ul style="list-style-type: none"> ● Mesh pairing is not implemented. ● Wireless relay is not set up.
	Flashing alternately	Mesh pairing is in progress.
	Three bars on	<ul style="list-style-type: none"> ● The mesh signal strength is high. ● The wireless relay signal strength is high.
	Two bars on	<ul style="list-style-type: none"> ● The mesh signal strength is medium. ● The wireless relay signal strength is medium.
	One bar on	<ul style="list-style-type: none"> ● The mesh signal strength is low. ● The wireless relay signal strength is low.

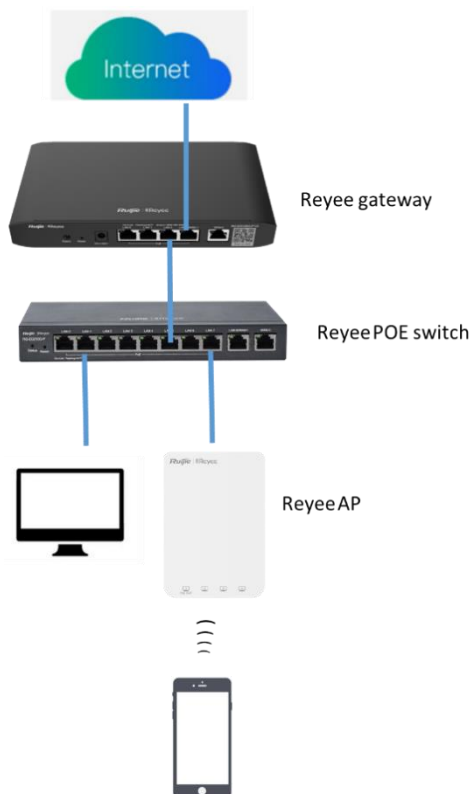
1.3 Button

Button	Description
Reset	<p>Press the Reset button for less than 2 seconds to restart the device.</p> <p>Press the Reset button for over 5 seconds to restore the router to factory settings. (Release the button when the system status LED blinks).</p> <p>The default management IP address is http://192.168.110.1.</p>
Mesh Button	Press the Mesh button for less than 2 seconds to perform mesh pairing.

2 Getting Started

2.1 Network Planning

The following figure shows a typical topology of a Reyee router.



The DHCP server has two address pools on the Reyee router: 192.168.110.0/24 in VLAN 1 for devices of this network and 192.168.10.0/24 in VLAN 10 for clients of this network.

The following ports are used for Ruijie Cloud management. To bring devices to go online on Ruijie Cloud, ensure that these ports are available and data flows are permitted on the network.

Domain name (Cloud-as)	DST.IP	Domain name (Cloud-eu, Cloud-me)	DST.IP	DST.TCP	DST.UDP
Device Online Related:		Device Online Related:			
devicereg.rujiijetworks.com	35.197.150.240	devicereg.rujiijetworks.com	35.190.10.141	80,443	
ryrc.rujiijetworks.com	35.197.150.240	ryrc.rujiijetworks.com	35.234.108.108	80,443	
stunrc.rujiijetworks.com	35.197.150.240	stunrc.rujiijetworks.com	35.234.108.108		34,783,479
stunsvr-as.rujiijetworks.com	34.126.80.150	stunsvr-eu.rujiijetworks.com	35.246.237.78		34,783,479
stunb-as.rujiijetworks.com	34.126.80.150	cwmpsvr-eu.rujiijetworks.com	34.159.112.239		34,783,479
stunc-as.rujiijetworks.com	34.87.169.209	cwmpcp-eu.rujiijetworks.com	34.120.73.71		34,783,479
cwmpsvr-as.rujiijetworks.com	35.197.136.171	cwmpb-eu.rujiijetworks.com	34.159.112.239	80, 443	
cwmpcp-as.rujiijetworks.com	34.160.143.162				
cwmpb-as.rujiijetworks.com	35.197.136.171				
Log Upload:		Log Upload:			
34.87.93.12	34.87.93.12	cloudlog-eu.rujiijetworks.com	35.246.247.49	80,443	
Advanced Service:		Advanced Service:			
firmware.rujiijetworks.com	34.87.32.36	firmware.rujiijetworks.com	34.89.153.55	80,443	
cloudweb.rujiijetworks.com	34.87.32.36	cloudweb.rujiijetworks.com	34.89.153.55	80,443	
fastonline.rujiijetworks.com	34.87.32.36	fastonline.rujiijetworks.com	34.89.153.55	80,443	
cloudapi.rujiijetworks.com	35.197.150.240	cloudapi.rujiijetworks.com	35.234.108.108	80,443	
cdn.rujiijetworks.com	35.201.94.110	cdn.rujiijetworks.com	35.190.93.193	80,443	
ES Series Switch		ES Series Switch			
iotrc.rujiijetworks.com	34.87.101.31	iotrc.rujiijetworks.com	34.107.106.56		7683
iotsvr-as.rujiijetworks.com	35.247.161.22	iotsvr-eu.rujiijetworks.com	35.242.228.40		5683
iotlog-as.rujiijetworks.com	35.240.167.168	iotlog-eu.rujiijetworks.com	35.198.144.180		6683
iotdl-as.rujiijetworks.com	34.87.141.45	iotdl-eu.rujiijetworks.com	35.234.118.145		8683
MQTT Devices with P206 version		MQTT Devices with P206 version			
ryrcmq.rujiijetworks.com	34.120.84.165	ryrcmq.rujiijetworks.com	34.149.186.87	25857	
ehrcmq.rujiijetworks.com	34.120.84.165	ehrcmq.rujiijetworks.com	34.149.186.87	25857	
mqcIt001-as.rj.link	34.160.191.165	mqcIt001-eu.rj.link	34.120.138.185	25857	

2.2 Installing the Router

2.2.1 Safety Suggestions

To avoid personal injury and equipment damage, read safety suggestions carefully before you install each device. The following safety suggestions do not cover all possible dangers

1. Installation

- Keep the chassis clean and free from any dust.
- Do not place devices in a walking area.
- Do not wear loose clothes or accessories that may be hooked or caught by devices during installation and maintenance.

2. Movement

- Do not frequently move devices.
- When moving devices, keep the balance and avoid hurting legs and feet or straining the back.
- Before moving devices, turn off all power supplies and dismantle all power modules.

3. Electricity

- Observe local regulations and specifications when performing electric operations. The operators must be qualified.
- Before installing the device, carefully check any potential danger in the surroundings, such as ungrounded power supply, and damp or wet ground or floor.
- Before installing the device, find out the location of the emergency power supply switch in the room. First cut off the power supply in the case of an accident.
- Try to avoid maintaining the switch that is powered on alone.

- Make a careful check before you cut off the power supply.
- Do not place the equipment in a damp location. Do not let any liquid enter the chassis.

4. Static Discharge Damage Prevention

To prevent damage from static electricity, pay attention to the following points:

- Proper ground grounding screws on the back panel of the device; use a three-wire single-phase socket with the protective earth wire (PE) as the AC power socket.
- Prevent indoor dusts.
- Ensure proper humidity conditions.

5. Laser

Some devices support varying models of optical modules that are Class I laser products sold on the market. Improper use of optical modules may cause damage. Therefore, pay attention to the following points when you use them:

- When a fiber transceiver is working, ensure that the port has been connected to an optical fiber or is covered with a dust cap, to keep out dust and avoid burns.
- When the optical module is working, do not pull out the fiber cable or look directly into a transceiver. The transceiver emit laser light that can damage your eyes.

2.2.2 Installation Site Requirement

The installation site must meet the following requirement to ensure normal working and a prolonged durable life Reyee EG series routers.

1. Ventilation

For installing devices, reserve at least 10 cm distances from both sides and the back plane of the cabinet at ventilation openings to ensure good ventilation. After cables have been connected, bundle or place the cables on the cabling rack to prevent them from blocking the air inlets. It is recommended that the device be cleaned at regular intervals. In particular, avoid dusts from blocking the screen mesh on the back of the cabinet.

2. Temperature and Humidity

To ensure normal operation and prolong the service life of the router, keep proper temperature and humidity in the equipment room.

If the temperature and humidity in the equipment room do not meet the requirements for a long time, the router may be damaged.

In an environment with a high humidity, insulating materials may have bad insulation or even leaking electricity. Sometimes the materials may suffer from mechanical performance change and metallic parts may get rusted.

In an environment with a low humidity, insulating strips may dry and shrink. Static electricity may occur easily and endanger circuits on the device.

In an environment with a high temperature, the router is subject to more serious harm. Its performance may degrade significantly and various hardware faults may occur.

3. Cleanness

Dust poses a severe threat to the running of the router. The indoor dust falling on the equipment may be absorbed by the static electricity, causing bad contact of the metallic joint. Such electrostatic absorption may occur more easily when the relative humidity is low. This affects the lifecycle of the AP and causes communication faults.

4. Grounding

A good grounding system is the basis for stable and reliable operation of the device, preventing lightning strokes and resisting interference. Carefully check the grounding conditions at the installation site according to the grounding requirements, and perform grounding operations properly as required.

- Lightning Grounding

The lightning protection system of a facility is an independent system that consists of the lightning rod, down conductor, and connector to the grounding system, which usually shares the power reference ground and ground cable. The lightning discharge ground is targeted for the facility.

- EMC Grounding

The grounding required for EMC design includes the shielding ground, filter ground, noise and interference suppression, and level reference. All the above constitute the comprehensive grounding requirements. The resistance of earth wires should be less than 1 Ω .

5. EMI

Electro-Magnetic Interference (EMI), from either outside or inside the device or application system, affects the system in the conductive ways such as capacitive coupling, inductive coupling, and electromagnetic radiation.

There are two types of electromagnetic interference: radiated interference and conducted interference, depending on the type of the transmission path.

When the energy, often RF energy, from a component arrives at a sensitive component through the space, the energy is known as radiated interference. The interference source can be either a part of the interfered system or a completely electrically isolated unit. Conducted interference results from an electromagnetic wire or signal cable connection between the source and the sensitive component, along which cable the interference conducts from one unit to another. Conducted interference often affects the power supply of the device, but can be controlled by a filter. Radiated interference may affect any signal path in the device and is difficult to shield.

- For the TN AC power supply system, the single-phase three-core power socket with protective earthing conductors (PE) should be adopted to effectively filter out interference from the power grid through filtering circuits.

- Do not use the grounding device for an electrical device or anti-lightning grounding device. In addition, the grounding device of the device must be deployed far away from the grounding device of the electrical device and anti-lightning grounding device.

- Keep the device away from the high-power radio transmitter, radar transmitting station, and high-frequency large-current device.

- Take measures to shield static electricity.

- Lay interface cables inside the equipment room. Outdoor cabling is prohibited, avoiding damages to device

signal interfaces caused by over-voltage or over-current of lightning.

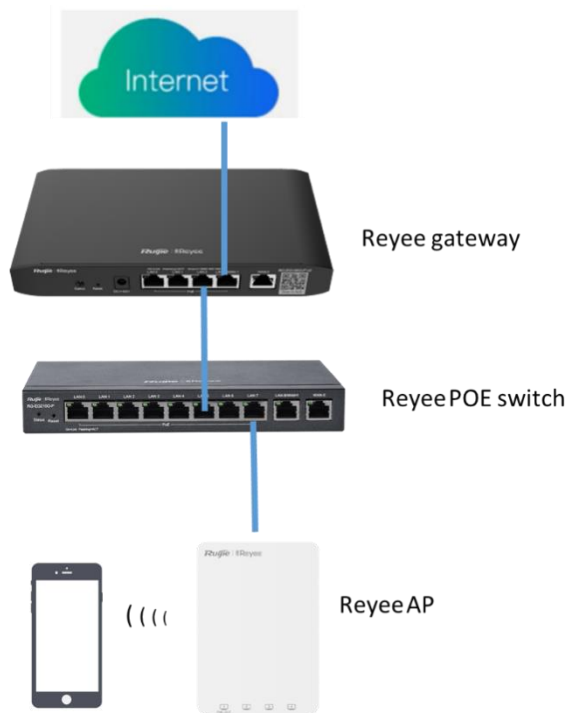
2.2.3 Installation Steps

For details about installation steps, see *Hardware Installation and Reference Guide*.

2.3 Quick Provisioning

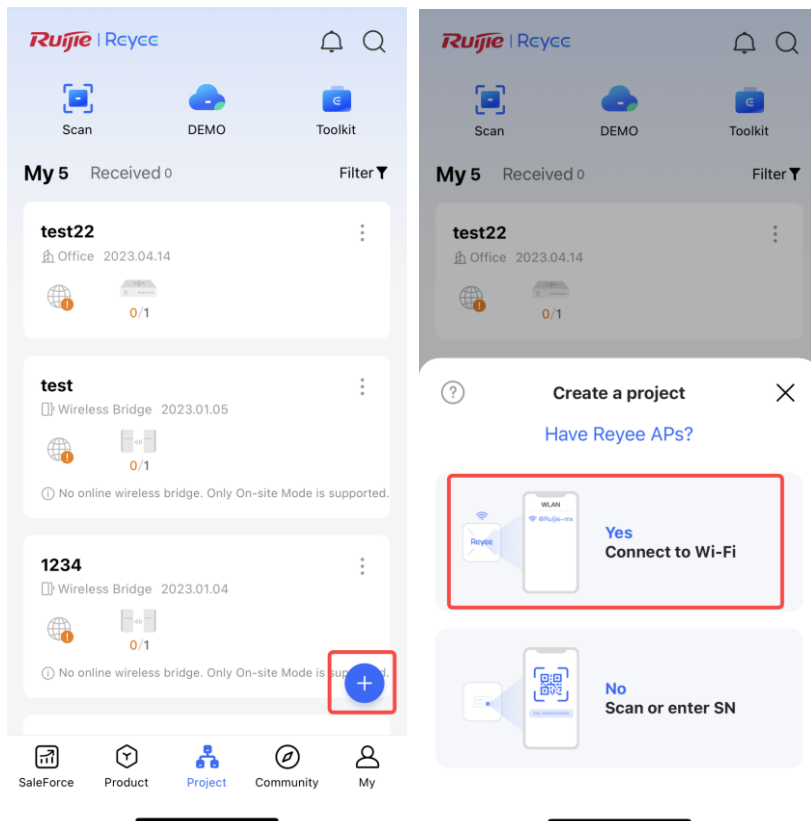
2.3.1 Quick Provisioning Through Ruijie Cloud App

The Reyye router is often used with a Reyye PoE switch and a Reyye RAP.

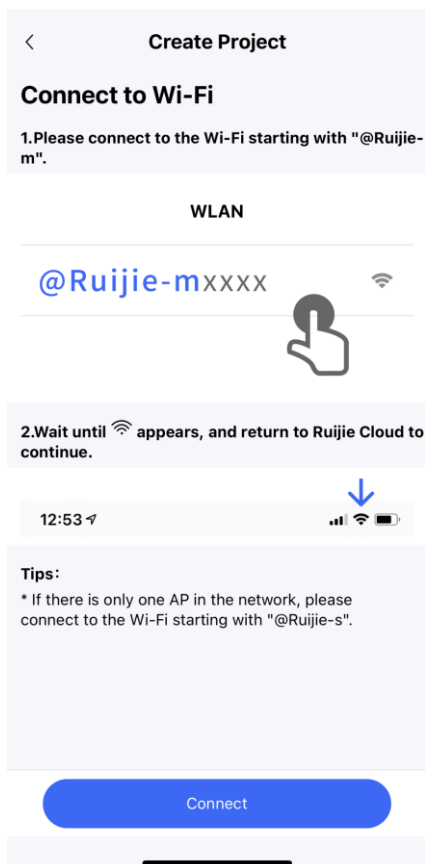


Connect the devices through Ruijie Cloud App for configuration and remote maintenance.

(1) Open Ruijie Cloud App, click **Create a Project**, and select **Connect to Wi-Fi**.



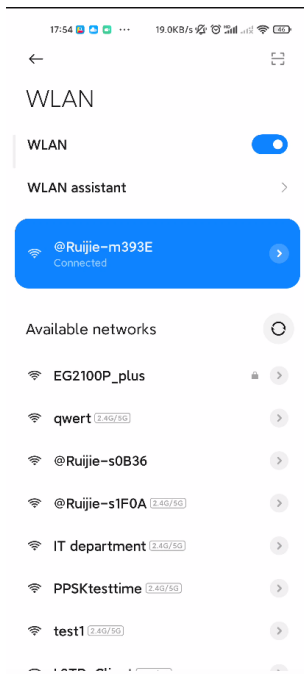
(2) After you click **Yes**, Ruijie Cloud App will ask you to connect SSID **@Ruijie-mxxxx**.



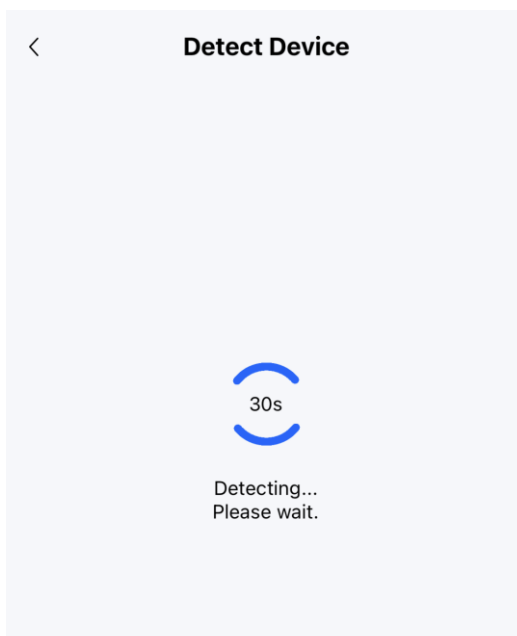
i Note

@Ruijie-mxxxx is generated after network self-organization established successfully, while @Ruijie-sxxxx is generated on a standalone device. xxxx is the last four digits of the MAC address of a device.

- (3) Click **Connect** and access SSID @Ruijie-mxxxx.



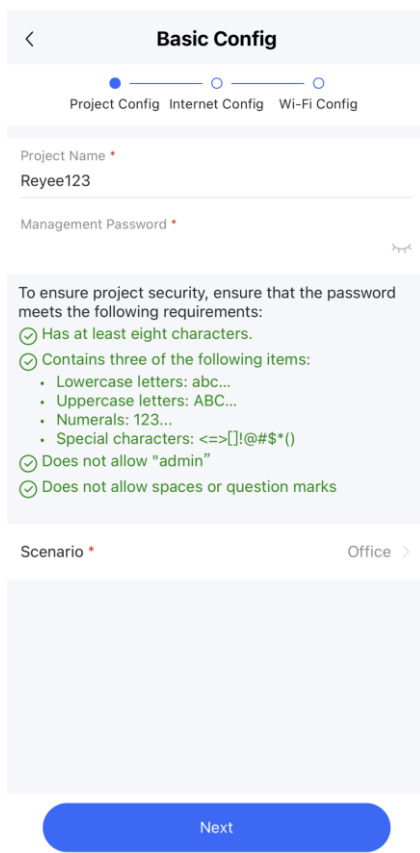
- (4) After you access SSID @Ruijie-mxxxx SSID, Ruijie Cloud App will generate the topology and detect all devices on the SON.



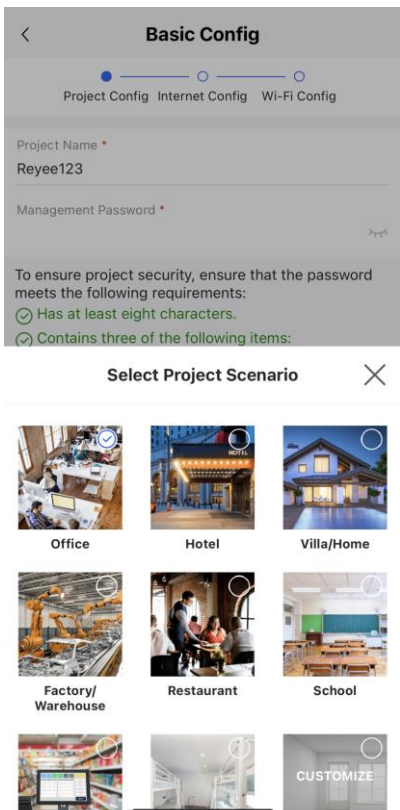
- (5) After all devices are detected, Cloud App will display them and show the topology.



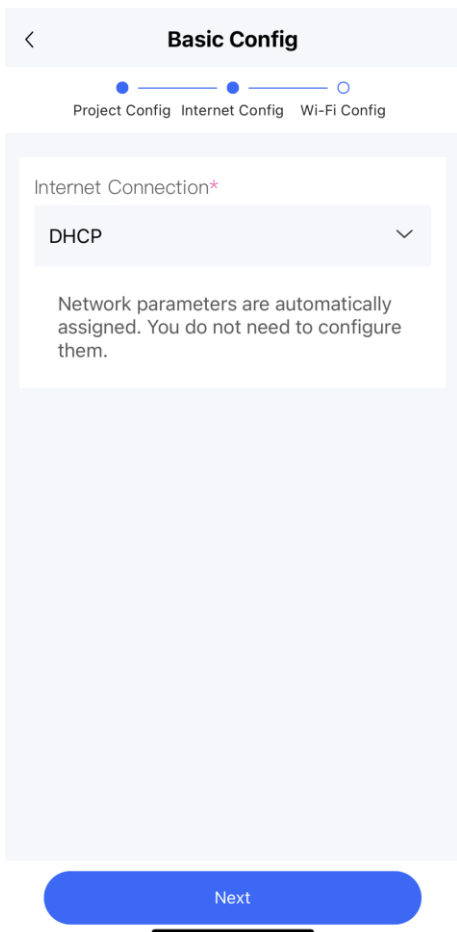
- (6) Click Start Config to perform basic configuration of this project. Set Project Name and Management Password.



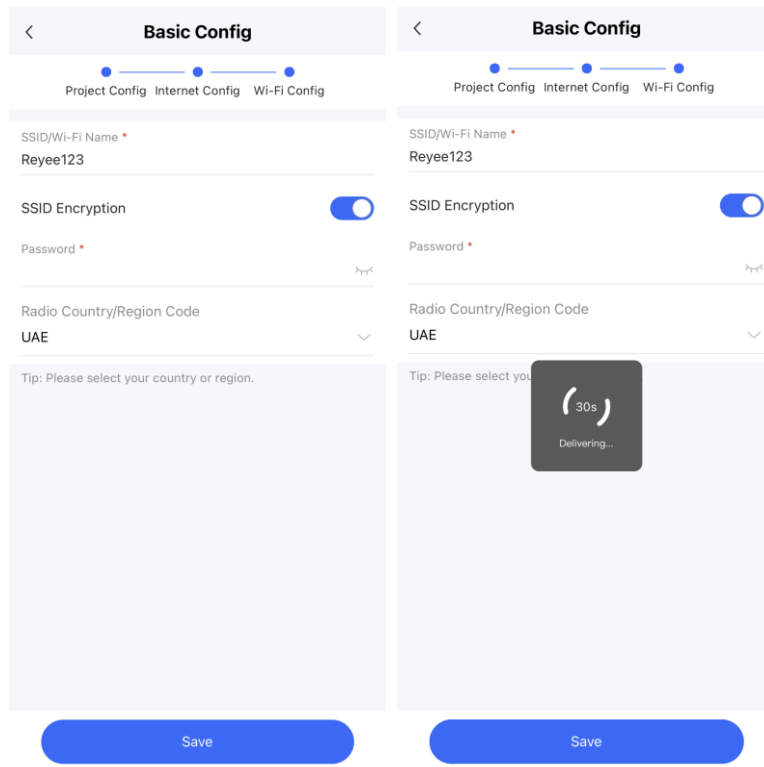
- (7) Select the scenario of this project based on your requirement.



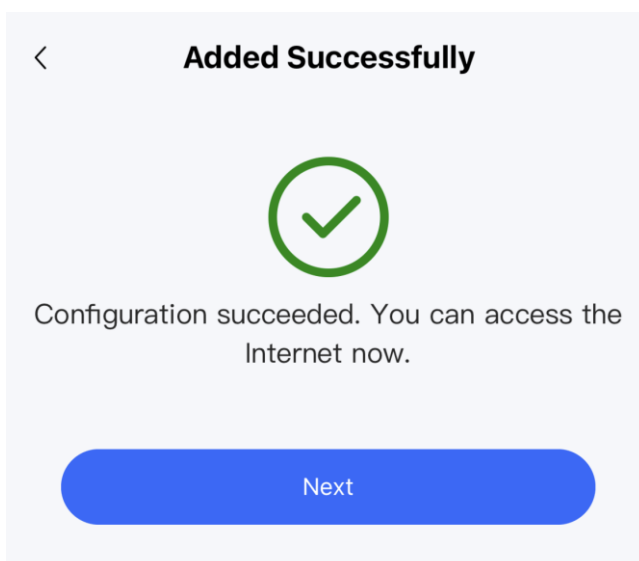
(8) Configure the Internet. For WAN configuration, you can choose **PPPoE**, **DHCP**, or **Static IP**.



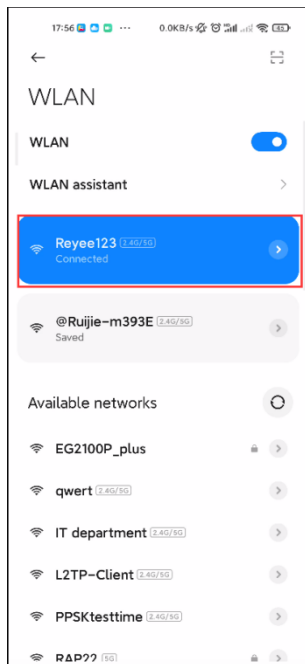
- (9) Configure the SSID.
 - a Enter the name of the SSID.
 - b Configure it as open to allow clients to access this SSID.
 - c Configure the password for this SSID.
 - d Select the region code.
 - e The configuration will be synchronized to the network.



- (10) After about 3s, Ruijie Cloud App will prompt that the configuration is delivery succeed.

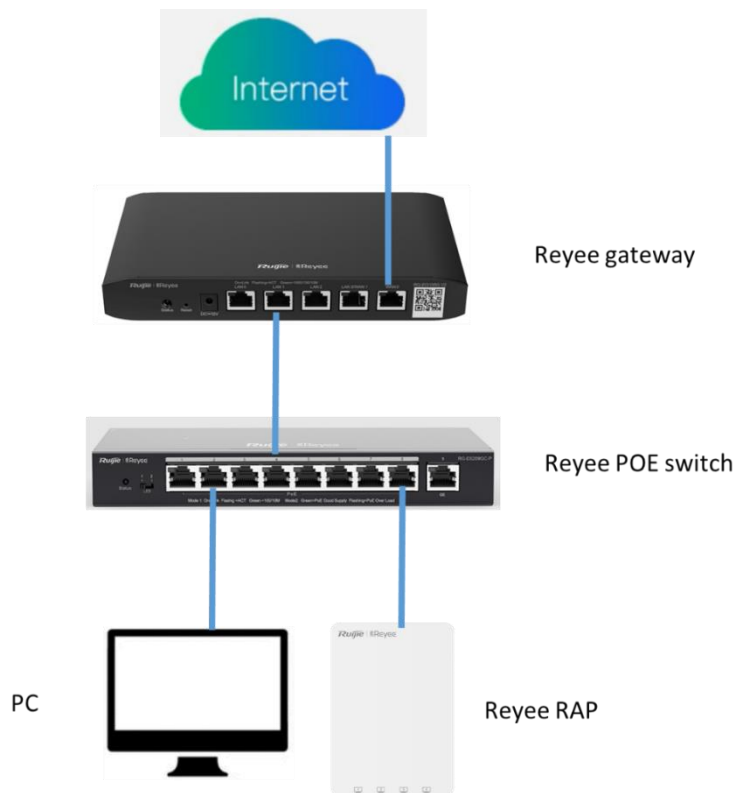


- (11) Connect to the SSID created just now to manage the whole network on Cloud App.



2.3.2 Quick Provisioning Through Reyee Eweb

The Reyee router is often used with a Reyee PoE switch and a Reyee RAP.



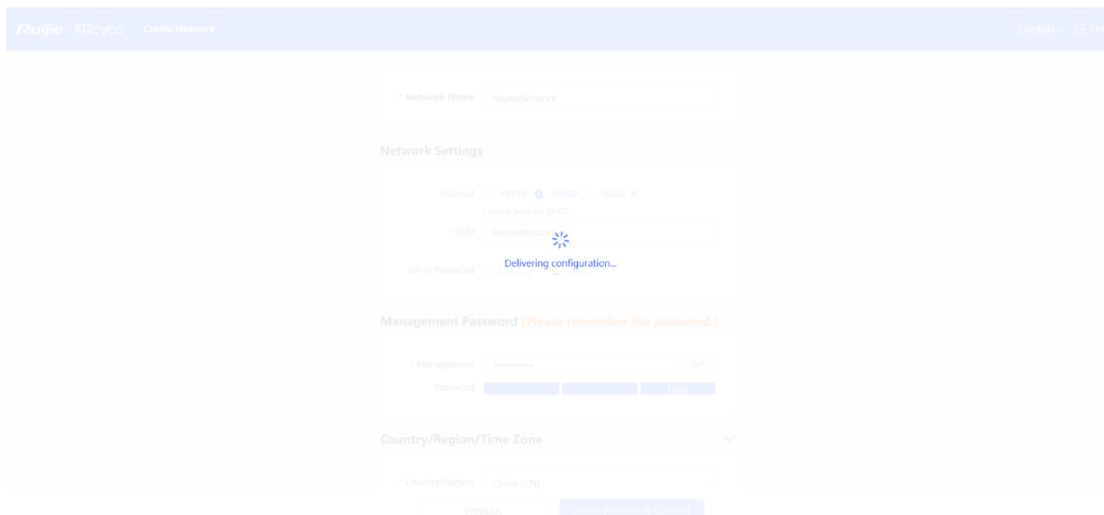
You can use a web management system to configure and maintain the Reyee router.

- (1) Connect a PC to a PoE switch, set the IP address of PC to the static IP address 192.168.110.x.
- (2) Enter 192.168.110.1 in the address bar of the browser to log in to the Eweb of the EG.

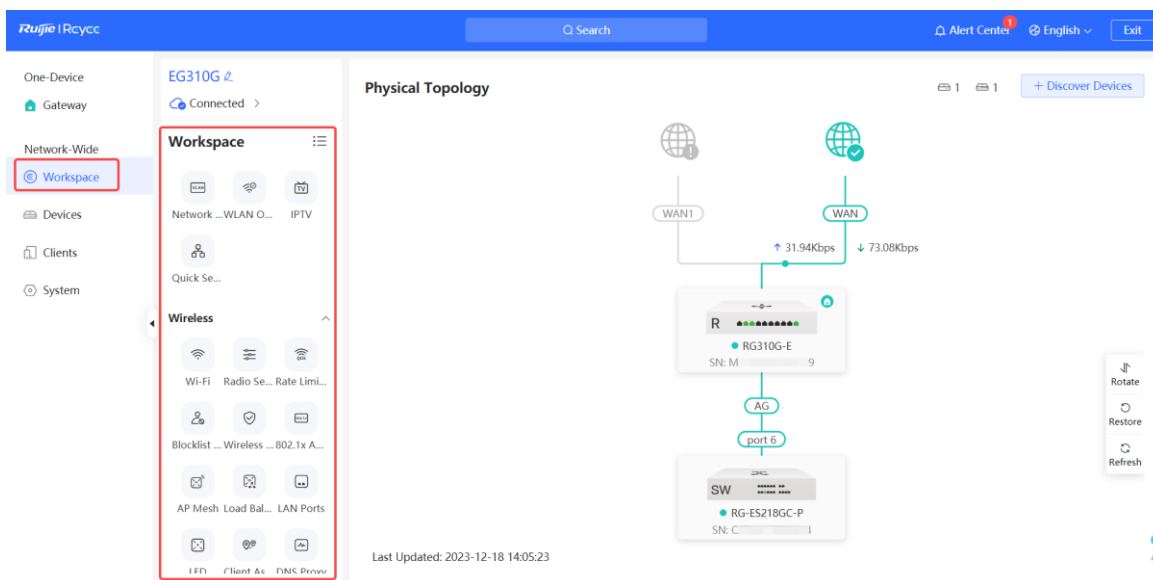
All devices on the network will be displayed in Eweb.

- (3) Click **Start Setup** to perform quick start of the network.

- a Enter the network name, and configure the Internet access mode of this network.
 - b Enter the password of the SSID or configure the SSID as open.
 - c Select the country/region.
- (4) Click **Create Network & Connect**. The configuration will be delivered and activated.



After the configuration has been delivered and activated, you can access the **Overview** page to manage the SON of Reyee devices.



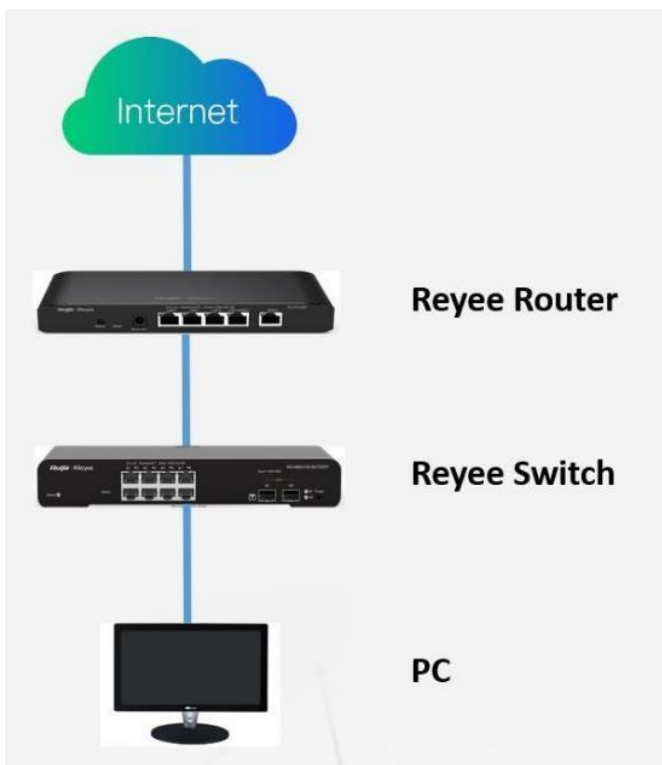
3 Device Management

3.1 Login

Eweb is a web-based network management system used to manage or configure devices. You can access Eweb through a browser such as Google Chrome. Web-based management involves a web server and a web client. The web server, which is integrated in a device, is used to receive and process requests from the client, and to return processing results to the web client. The web client usually refers to a browser, such as Google Chrome, IE, or Firefox.

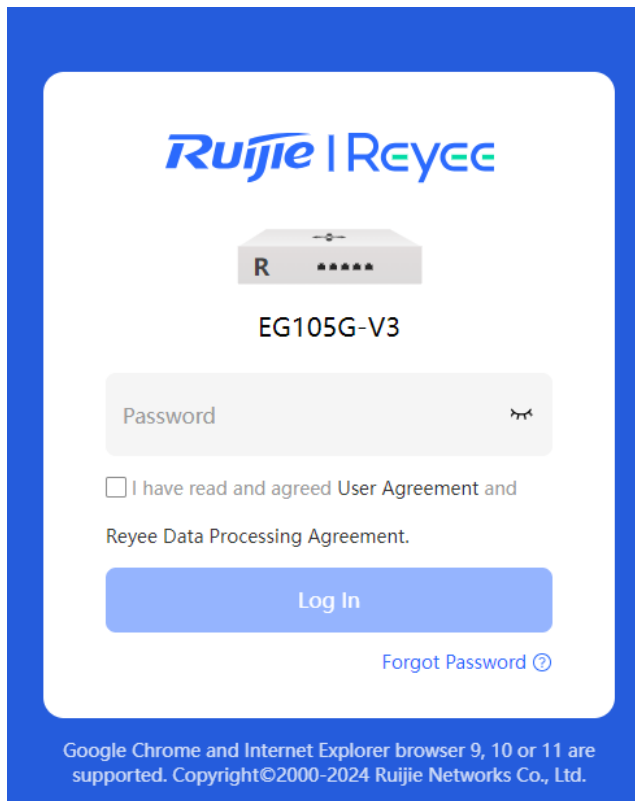
Reyee routers support both web interface management and remote management through life-time-free Ruijie Cloud App and Ruijie Cloud platform. You can view the network status, modify the configuration, and troubleshoot faults easily.

You can access the Eweb management system of an access or aggregation switch through a PC browser to manage and configure the device.



1. Set PC's IP assignment mode to obtain IP addresses automatically.
2. Visit <http://192.168.110.1> through Microsoft Chrome.
3. Enter the password on the login page and click **Login**.

The default password is **admin**.



For the Reyee EG device, you may use either 192.168.110.1 or 10.44.77.254 to access the device.

The default login password for all Reyee devices is **admin**.

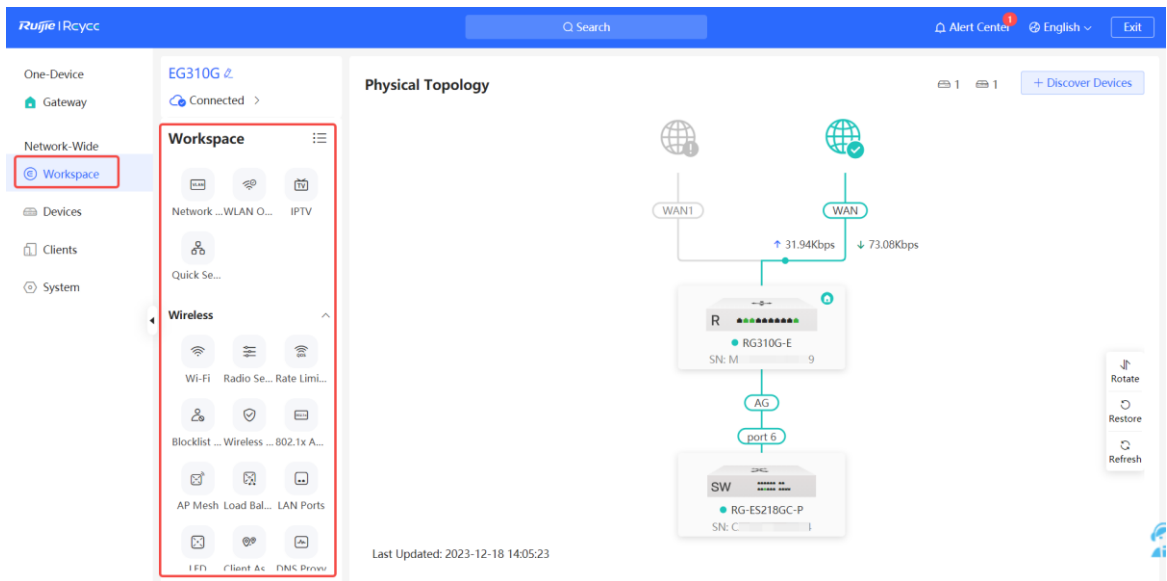
You may visit <https://10.44.77.253> to log in to the master device of the Reyee network.

3.2 Switching the Work Mode

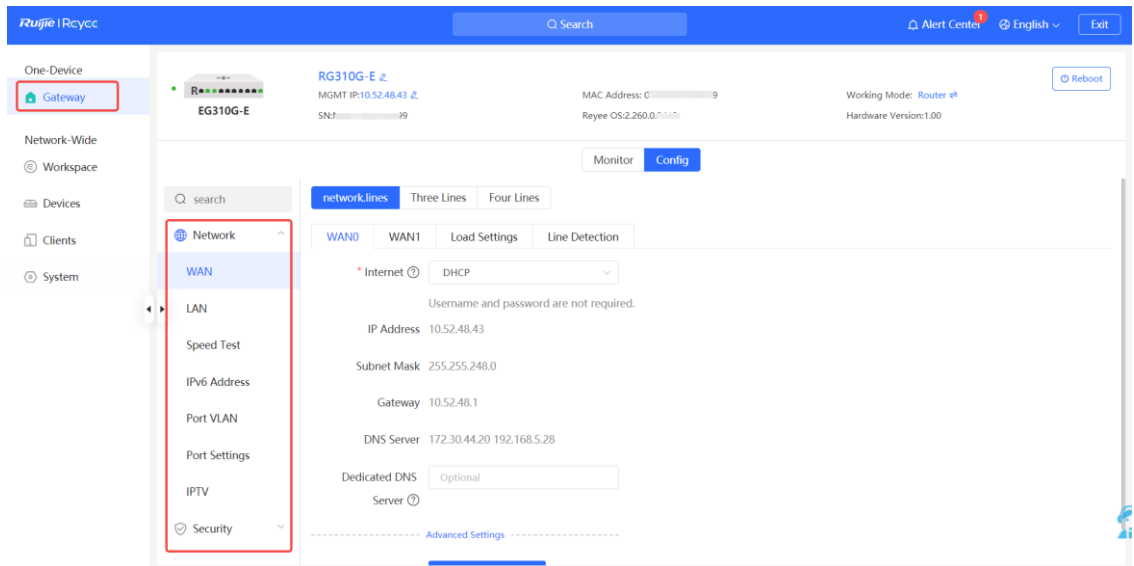
When the self-organizing network discovery function is disabled, which is enabled by default, the web interface will switch to the local device mode.

When the self-organizing network discovery function is enabled, you can switch the web interface between network-wide mode and local device mode.

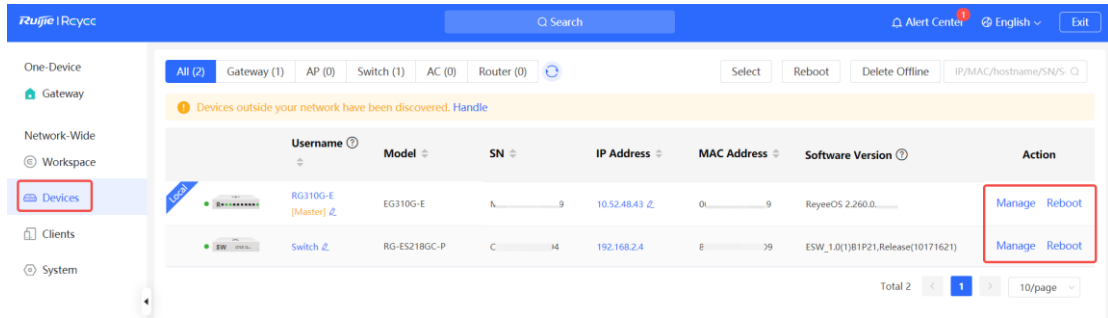
- Network-wide mode: You can view and configure all devices on the network from a network perspective. Click **Workspace** in the left navigation bar to access the corresponding functions for network-wide configuration in the secondary menu.



- Local device mode: You can configure only one device on the network. The configuration and management of an individual device can be accessed as follows:
 - Method 1: Choose **Gateway** > **Config** under the **One-Device** menu. On the displayed page, you can access the corresponding functions for single-device configuration in the secondary menu. This method only supports configuring gateway devices on the network.



- Method 2: Choose **Network-Wide** > **Devices**. In the device list, click the **Manage** button next to the target device. This method supports configuring any type of device on the network.



3.3 Configuring the Login Password

Change your password regularly to ensure account security.

- (1) Log into the web management system by using the default IP address.
- (2) Choose **Network-Wide > Workspace > Network-Wide > Password**.
- (3) Enter the old password and new password.
- (4) Click **Save**.

i Change the login password. Please log in again with the new password later.

* **Old Management Password**

* **New Management Password**

There are four requirements for setting the password:

- The password must contain 8 to 31 characters.
- The password must contain uppercase and lowercase letters, numbers and three types of special characters.
- The password cannot contain admin.
- The password cannot contain question marks, spaces, and Chinese characters.

* **Confirm Password**

Password Hint

Save

After saving the configuration, use the new password to log in.

 Caution


In SON network mode, the login password of all devices on the network will be changed synchronously.

3.4 Configuring the System Time


Choose **Network-Wide > 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 device supports Network Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete the local server as required.

 Configure and view system time (the device has no RTC module, and time settings are not saved upon restart).

Current Time  2023-12-12 14:29:25 Edit

* Time Zone

* NTP Server  Add

Delete

Delete

Delete

Delete

Delete

Delete

Save

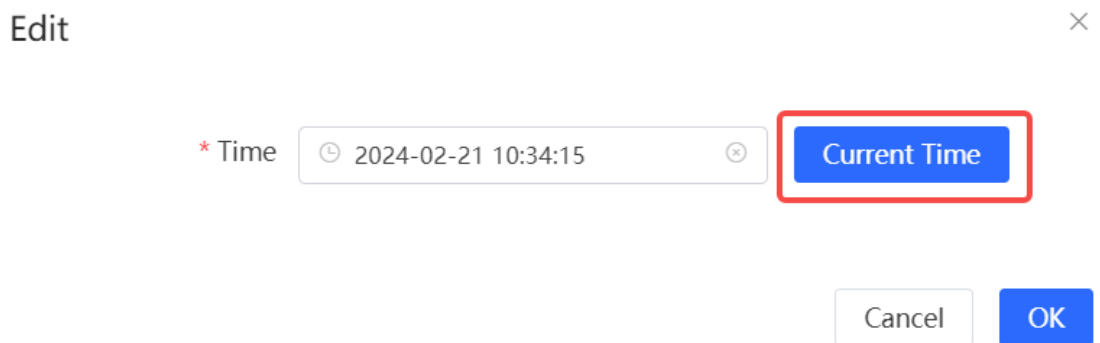
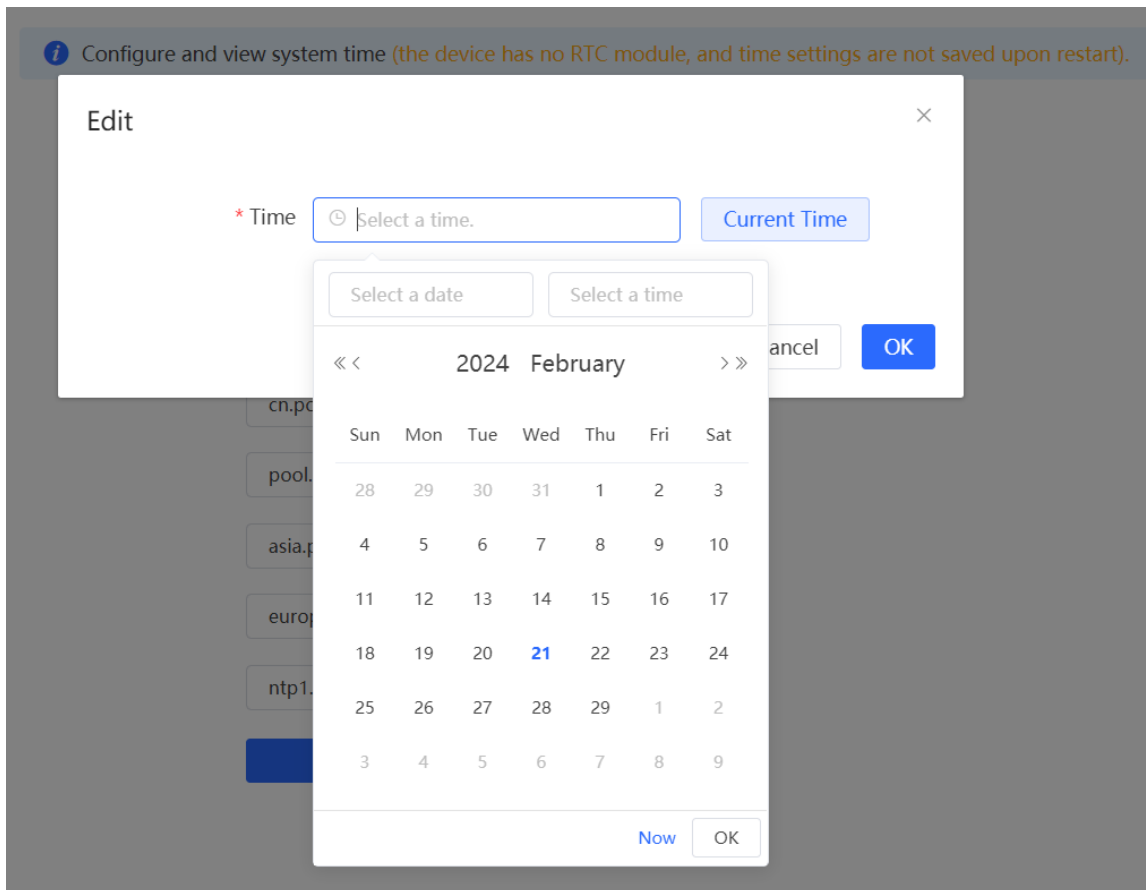
Choose **Current Time > Edit > Current Time**. The current system time will be filled in automatically.

Edit ×

* Time Current Time

Cancel OK

- Manually edit the current time or click **current time** to synchronize the current time automatically.



- Manually select a value from the **Time Zone** drop-down list box.

i Configure and view system time (the device has no RTC module, and time settings are not saved upon restart).

Current Time ⓘ 2024-02-21 10:34:42 Edit

* Time Zone (GMT+8:00)PRC ^

* NTP Server ⓘ

- (GMT+8:00)Asia/Singapore
- (GMT+8:00)Asia/Taipei
- (GMT+8:00)Asia/Ujung_Pandang
- (GMT+8:00)Asia/Ulaanbaatar
- (GMT+8:00)Australia/Eucla
- (GMT+8:00)Australia/Perth
- (GMT+8:00)Australia/West
- (GMT+8:00)PRC**
- europa.pool.ntp.org Delete
- ntp1.aliyun.com Delete

Save

- Add or delete the NTP server.

i Configure and view system time (the device has no RTC module, and time settings are not saved upon restart).

Current Time ⓘ 2024-02-21 10:35:15 Edit

* Time Zone (GMT+8:00)PRC v

* NTP Server ⓘ

- 0.cn.pool.ntp.org Add
- 1.cn.pool.ntp.org Delete
- cn.pool.ntp.org Delete
- pool.ntp.org Delete
- asia.pool.ntp.org Delete
- europa.pool.ntp.org Delete
- ntp1.aliyun.com Delete

Save

3.5 Configuring Upgrade

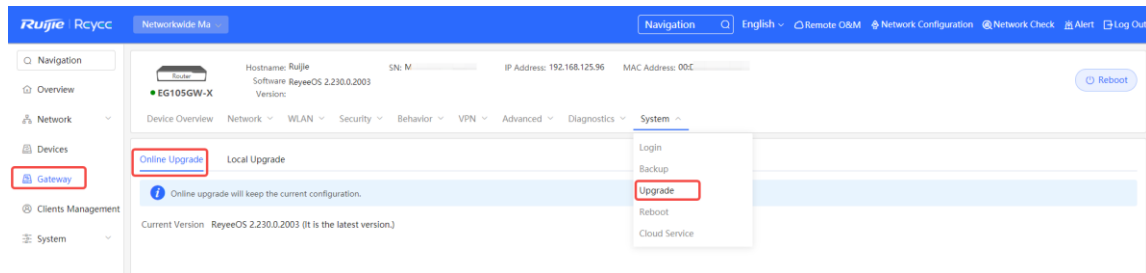
To use new features, upgrade the router to the latest version. There are two methods of upgrading routers: online upgrade and local upgrade.

3.5.1 Online Upgrade

The router that is connected to the Internet can be upgraded online.

Log in to the Eweb of the device.

Choose **One-Device > Gateway > Config > System > Upgrade > Online Upgrade** .



- If a prompt appears indicating the current version is the latest one, you do not need to upgrade the router.
- If a new version is available, you can click **Upgrade Now** to upgrade the router. The upgrade operation does not affect the current configuration, but the router will restart after being upgraded successfully. Do not refresh the page or close the browser during the upgrade. You are redirected to the login page automatically after the upgrade.

[Online Upgrade](#)

[Local Upgrade](#)

i Online upgrade will keep the current configuration.
systool.upgradeWarningTip

Current Version ReyeeOS 2.230.0.2003 (Latest version)

3.5.2 Local Upgrade

Upgrade the router by uploading a local upgrade package.

Confirm the target version and download the upgrade package from the official website.

- (1) Log in to the Eweb of the router.
- (2) Choose **One-Device > Gateway > Config > System > Upgrade > Local Upgrade**.

i systool.upgradeWarningTip

Model E

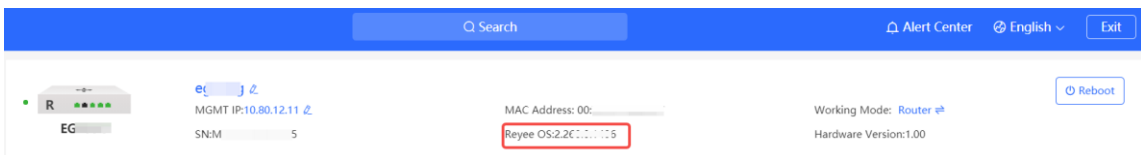
Current Version **?** ReyeeOS 2.0.0.4

Development Mode (It is recommended to be disabled after use.)

Retain Configuration **?** (If the target version is much later than the current version, you are advised not to retain the configuration.)

File Path **?**

- (3) Click **Browse**, select an upgrade package on the local PC, and click **Upload** to upload the file.
- (4) After the file is uploaded successfully, the system displays upgrade package information and asks for the upgrade. Click **OK** to start the upgrade.
- (5) After the upgrade is complete, choose **Gateway > Device Overview** and check whether the current version is consistent with the target version in the **Device Details** pane.
 - o If versions are consistent, the upgrade is successful.
 - o If versions are inconsistent, the upgrade fails. Try again or contact RITA.



3.6 Backing Up or Restoring the Configuration

Back up the configuration to restore the configuration quickly in the case of a failure.

- (1) Log into the Eweb of the router.
- (2) Choose **One-Device > Gateway > Config > System > Backup > Backup & Import**.

[Backup & Import](#) [Reset](#)

i If the target version is much later than the current version, some configuration may be missing.

1. Before importing the configuration file, you are advised to [Reset](#) the device.
2. After the configuration file is imported, the device will reboot automatically.

Backup Config **?**

Backup Config

Import Config **?**

File Path

- (3) Click **Backup** to download a configuration file locally.
- (4) To restore the configuration, click **Browse**, select a backup file on the local PC, and click **Import** to import the configuration file. The router will restart.

If the target version is much later than the current version, some configuration may be missing.

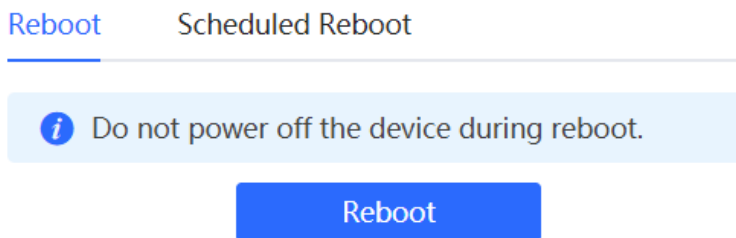
You are advised to restore the settings before importing the configuration. The router will restart automatically if you restore it.

3.7 Configuring Restart

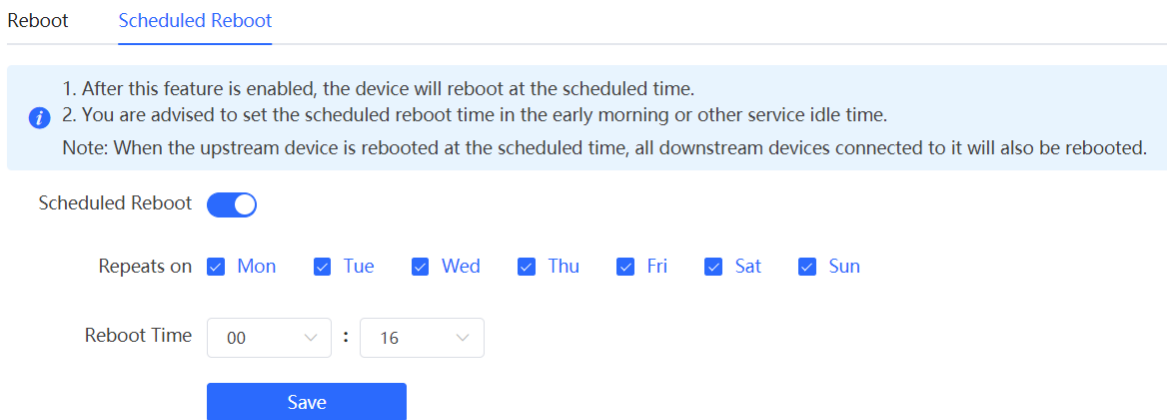
3.7.1 Restarting the Current Device

- Choose **One-Device > Gateway > Config > System > Reboot > Reboot**.

Click **Reboot**. The device will restart immediately. Do not refresh or close the page during restart. After the device restarts, you will be redirected to the login page.

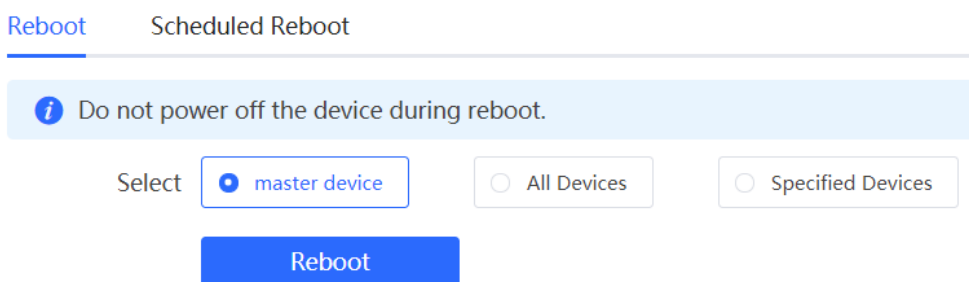


Click **Scheduled Reboot**. Enable this feature and select the scheduled restart time. The device will restart as scheduled.



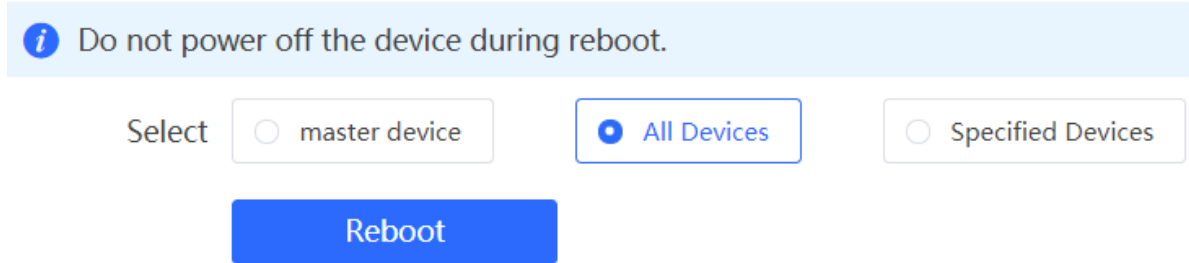
- Choose **Network-wide > System > Reboot > Reboot**.

Select **master device** to restart the current device.



3.7.2 Restarting All Devices on the Network

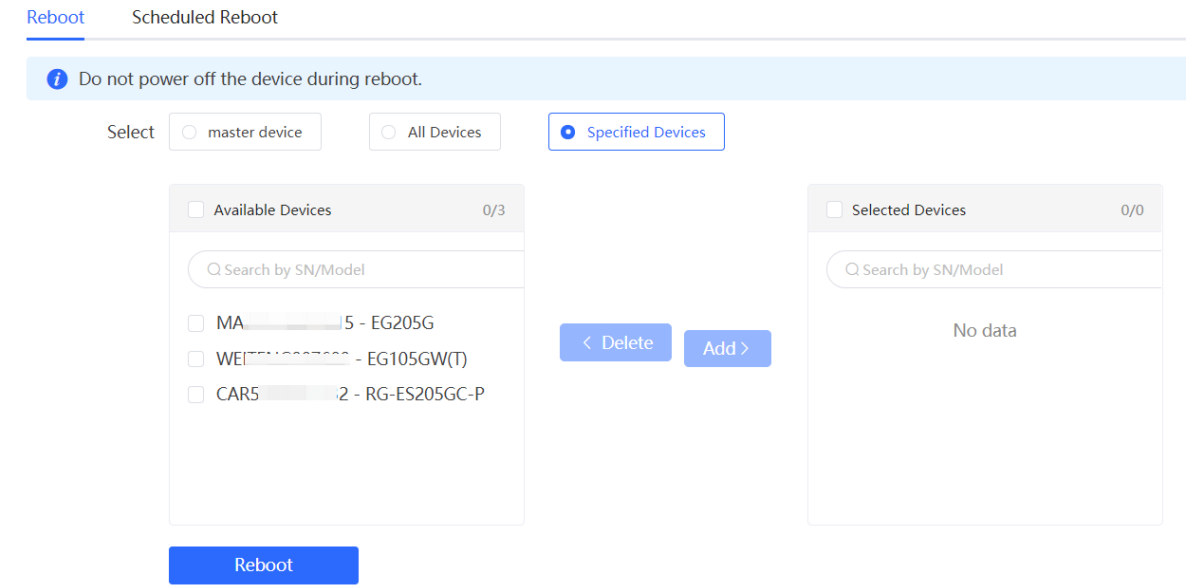
Switch to the **Network** mode. Choose **Network-wide > System > Reboot > Reboot**.
Select **All Devices**, and click **Reboot All Device** to restart all devices on the network.



Caution
The operation takes some time and affects the entire network. Therefore, exercise caution when performing this operation.

3.7.3 Restarting Specified Devices

Switch to the **Network** mode. Choose **Network-wide > System > Reboot > Reboot**.
Click **Specified Devices**, select required devices from the **Available Devices** list, and click **Add** to add devices to the **Selected Devices** list on the right. Click **Reboot**. Specified devices in the **Selected Devices** list will restart.



3.7.4 Configuring Scheduled Restart

Confirm that the system time is accurate to avoid network interruption caused by device restart at an incorrect time point. For details about how to configure the system time, see section [3.4 Configuring the System Time](#).
Choose **Network-Wide > Workspace > Network-Wide > Reboot > Scheduled Reboot**.

Toggle the switch to **Enable**, and select the date and time of scheduled restart every week. Click **Save**. When the system time matches the scheduled restart time, the device will restart. You are advised to set scheduled restart time to off-peak hours.

 **Caution**

The operation affects the entire network. Therefore, exercise caution when performing this operation.

1. After this feature is enabled, the device will reboot at the scheduled time.
 2. You are advised to set the scheduled reboot time in the early morning or other service idle time.
- Note: When the upstream device is rebooted at the scheduled time, all downstream devices connected to it will also be rebooted.

Scheduled Reboot

Repeats on Mon Tue Wed Thu Fri Sat Sun



Reboot Time :

3.8 Restoring Factory Settings

Restore the device to factory settings and the default password.

The operation deletes all current configuration. You are advised to back up the configuration before restoring factory settings.

- (1) Log in to the Eweb of the device.
- (2) Choose **Network-wide > System > Reset**.

 You can reset the device to factory settings by clicking the Factory Reset button below. If you want to retain the current configuration while performing a factory reset, then [back up the profile](#) the configuration file prior to the reset. 

Select master device All Devices

Retain bound account. Selecting this checkbox will allow the cloud account to maintain its project management privileges without requiring you to rebind your account.

- (3) Select the target device.
 - o **Master Device:** Select **Master Device**. Only the local device is restored.
 - o **All Devices:** Select **All Devices**. All devices on the network are restored.
- (4) Click **Reset** to restore the selected devices to factory settings.

3.9 Configuring Cloud Service

3.9.1 Overview

The Cloud Service feature provides powerful remote network management and operation capabilities, making it convenient and efficient to manage geographically dispersed networks with diverse device types. This feature

supports wireless devices, switches, and gateways, enabling unified network management and visualized monitoring and operation. Additionally, it also offers various components such as real-name authentication, dedicated Wi-Fi, and passenger flow analysis, allowing for flexible expansion of network services.

By configuring Cloud Service, you can conveniently manage networks through Ruijie Cloud or the Ruijie Reyee app.

3.9.2 Configuration Steps

Choose **One-Device > Gateway > Config > System > Cloud Service**.

If the device is not currently associated with a cloud account, simply follow the on-screen instructions to add it to the network. Open up the Ruijie Reyee app, click the scan icon at the upper left corner on the **Project** page, and enter the device's management password.



Once the device is associated with a cloud account, it will automatically be bound to a cloud server based on its geographic location.

⚠ Caution

Exercise caution when modifying cloud service configurations as improper modifications may lead to connectivity issues between the device and the cloud service.

Project Name:test

Account: 1

Unbind the account if you no longer wish to manage this project remotely.

Unbind

Cloud Server

China CloudConnected [Configure Cloud Service](#)

To change the Cloud Service configurations, select the cloud server from the **Cloud Server** drop-down list, enter the domain name and IP address, and click **Save**.

This device is connected to Ruijie Cloud. The IP is 118.190.157.52,Exercise caution when modifying the cloud service configuration to ensure uninterrupted device connectivity.

Cloud Server [Reset](#)

* Domain Name [Configure IP](#)

i Note

If the server selected is not **Other Cloud**, the system automatically fills in the domain name and IP address of the cloud server. When **Other Cloud** is selected, you need to manually configure the domain name and IP address and upload the cloud server certificate. .

3.9.3 Unbinding Cloud Service

Choose **One-Device > Gateway > Config > System > Cloud Service**.

You can click **Unbind** to unbind the account if you no longer wish to manage this project remotely.

Account: 1

Unbind the account if you no longer wish to manage this project remotely.

4 Common Settings

4.1 Network Access Setting

Perform network configuration to connect the router to the Internet quickly.

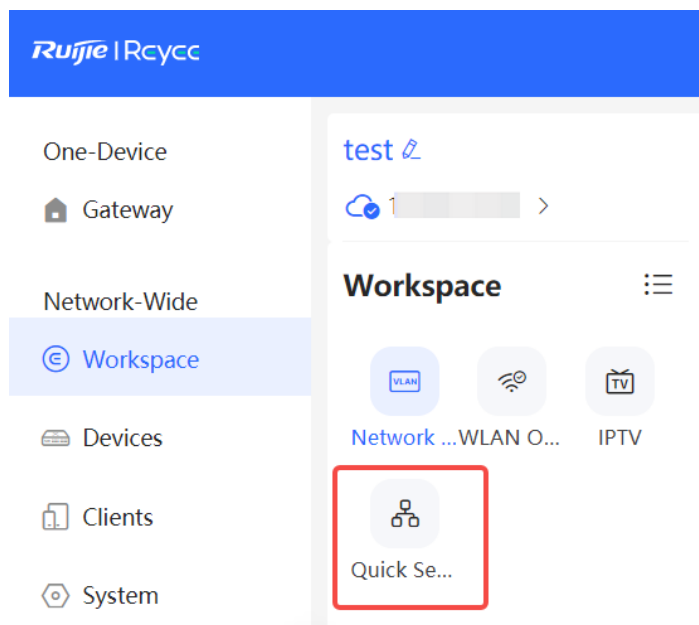


Three Internet access modes are available:

- PPPoE
- DHCP
- Static IP address

4.1.1 PPPoE Configuration Through a WAN Port

(1) Click **Quick Setup** to access the configuration wizard page.



Set **Internet** to **PPPoE** in the **Network Settings** pane.

- (2) Enter your **Username** and **Password** obtained from an ISP. **Service Name** is optional.
- (3) If you forget the password from the ISP, click **Obtain Account from Old Device**.
- (4) Click **Next**, and configure **Network Name** and **Password**.
- (5) Click **Create Network & Connect**. The router initiates a connection with the Internet.
- (6) After connecting the router to the Internet, you can manage the router on Ruijie Cloud or Eweb.

Obtain PPPoE Account from Old Router ×



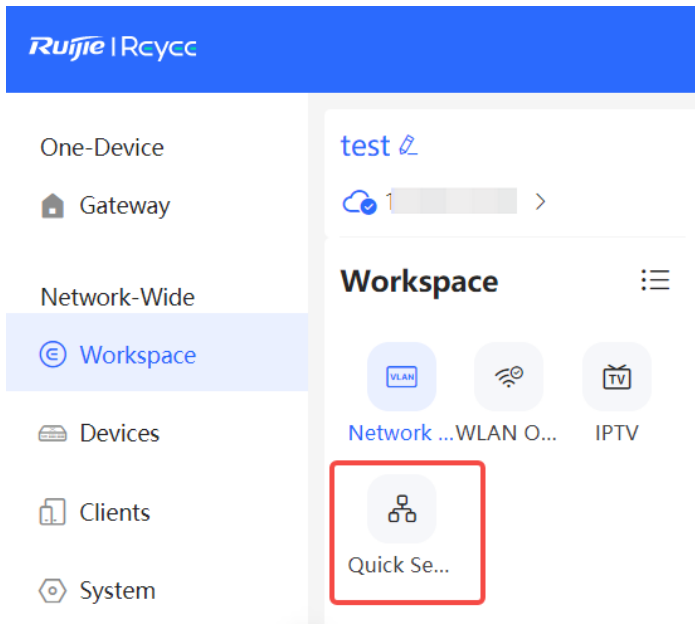
Steps:

1. Transmit Power on the old router and new router.
2. Connect one end of a cable to the WAN port of the old router and connect the other end to the LAN port of the new router.
3. Click "Obtain".

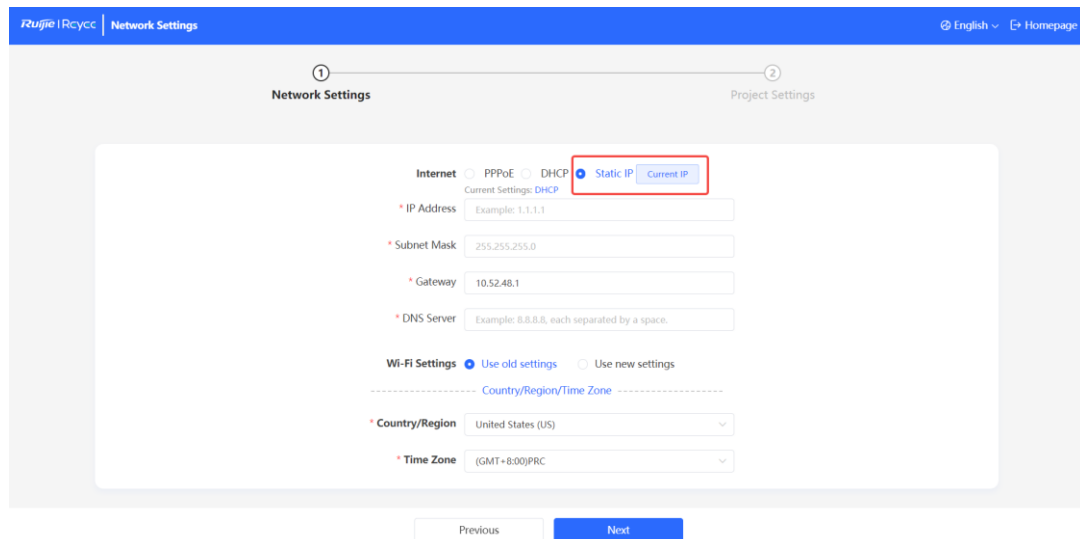
[Obtain](#)

4.1.2 Static IP Address Configuration Through a WAN Port

- (1) Click **Quick Setup** to access the configuration wizard page.



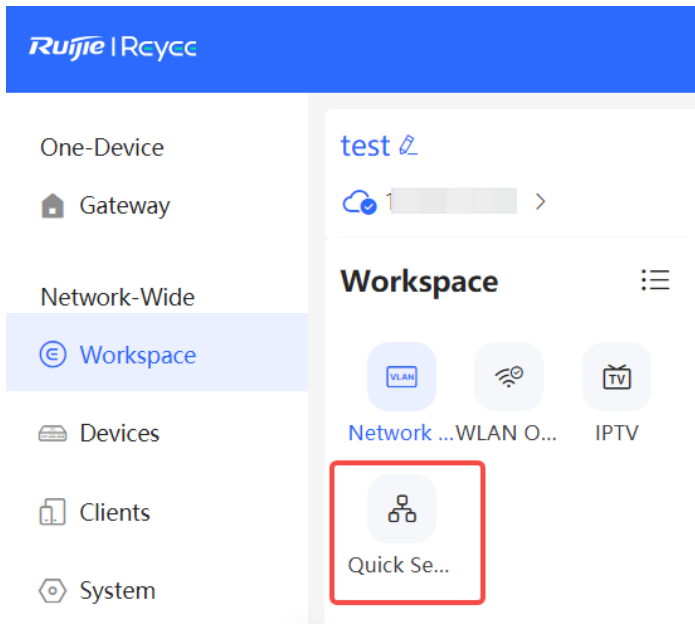
- (2) Set **Internet** to **Static IP** in the **Network Settings** pane.



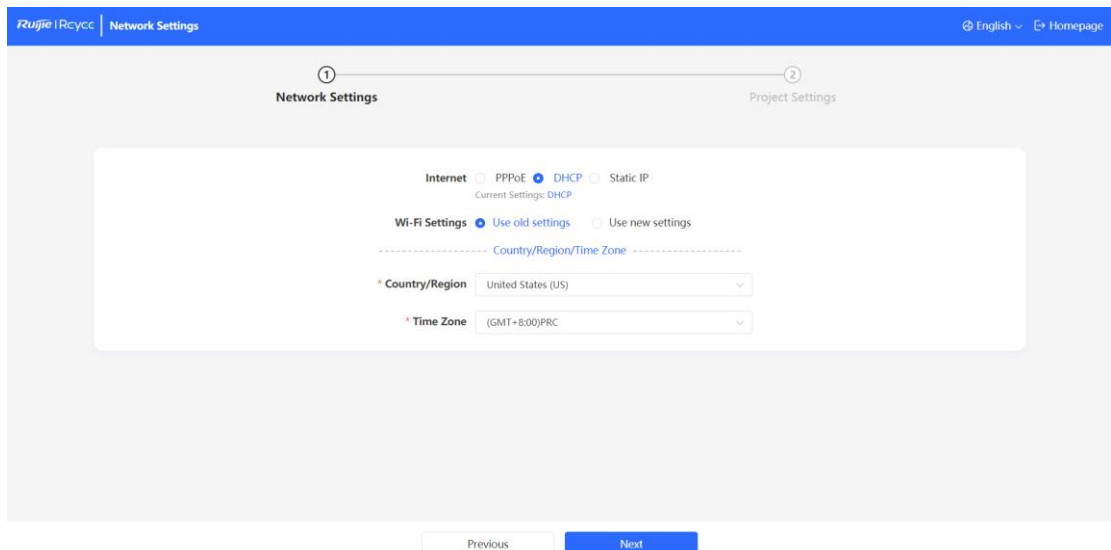
- (3) Configure an IP address, a subnet mask, a gateway IP address, and a DNS server address.
- (4) Click **Next**, and configure **Network Name** and **Password**.
- (5) Click **Create Network & Connect**. The router initiates a connection with the Internet.
- (6) After connecting the router to the Internet, you can manage the router on Ruijie Cloud or Eweb.

4.1.3 DHCP Configuration Through a WAN Port

- (1) Click **Quick Setup** to access the configuration wizard page.



- (2) Set **Internet** to **DHCP** in the **Network Settings** pane.



- (3) Click **Next**, and configure **Network Name** and **Password**.

- (4) Click **Create Network & Connect**. The router initiates a connection with the Internet.

After connecting the router to the Internet, you can manage the router on Ruijie Cloud or Eweb. You can perform WAN configuration through the following page.

Choose **One-Device > Gateway > Config > Network > WAN** .

4.2 AP Management

Note

- To manage the downlink AP, enable self-organizing network (SON) discovery (see section [4.2.1 Switching the Working Mode](#)). The wireless settings are synchronized to all wireless devices on the network by default. You can configure groups to limit the device scope under wireless management. For details, see section [4.2.2 Configuring AP Groups](#).
- Except the RG-EG105GW and RG-105GW(T), other Reyee routers do not send Wi-Fi signals. Wireless settings need to be delivered to make downlink APs take effect.

4.2.1 Switching the Working Mode

1. Working Mode

- Router mode

The device supports routing functions such as route-based forwarding and network address translation (NAT), VPN, and behavior management. It can allocate addresses to downlink devices, forward network data based on routes, and perform NAT operations.

In router mode, the device can access the network through Point-to-Point Protocol over Ethernet (PPPoE) dialing, dynamic IP address, and static IP address. It can also directly connect to a fiber-to-the-home (FTTH) network cable or an uplink device to provide network access and manage downlink devices.

- AC mode

The device supports Layer 2 forwarding only. The device does not provide routing and Dynamic Host Configuration Protocol (DHCP) server functions. By default, a WAN port obtains an IP address through DHCP. The AC mode is applicable to the scenario where the network is working normally. In AC mode, the device serves as the management controller to access the network in bypass mode and manage APs.

2. SON Discovery

When configuring a working mode, you can configure whether to enable the SON discovery function. This function is enabled by default.

After the SON discovery function is enabled, the device can be discovered on a network and discover other devices on the network. Devices interconnect with each other based on the device status and synchronize global configuration. You can log in to the web management page of any device on the network to check information about all devices on the network. After this function is enabled, clients can maintain and manage the current network more efficiently. You are advised to keep this function enabled.

If the SON discovery function is disabled, the device will not be discovered on the network and runs in standalone mode. After logging in to the web page, you can configure and manage only the current login device. If only one device is configured or global configuration does not need to be synchronized to the device, you can disable the SON discovery function.

Note

In AC mode, the SON discovery function is enabled by default.

After the SON discovery function is enabled, you can view the self-organizing role of the device on the **Device Details** page.

The menus on the web page vary depending on whether the SON discovery function is enabled.

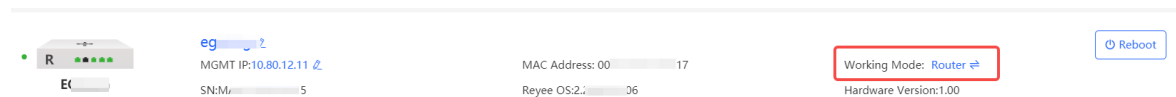
3. Configuration Steps

Choose **One-Device > Gateway**.

Click the current working mode to edit the working mode.

Caution

After you switch the working mode, the device will restore factory settings and restart. Proceed with caution.



AC function: If a device works in router mode and the SON discovery function is enabled, you can enable or disable the AC function. After the AC function is enabled, the device in router mode supports the virtual AC function and can manage downlink devices. If this function is disabled, the device needs to be elected as an AC in SON mode and then manages downlink devices.

Working Mode ×**Description:**

1. The device IP address may change upon mode change.
2. Change the endpoint IP address and ping the device.
3. Enter the new IP address into the address bar of the browser to access Eweb.
4. The system menu varies with different work modes.
5. **The device will be restored and rebooted up on mode change.**

Working Mode ? ▼

Self-Organizing Network ? i Tips

AC ?

4.2.2 Configuring AP Groups

1. Overview

After SON network discovery is enabled, the device can work as the master AP or AC to batch configure and manage its downlink APs by group. Before you configure APs, assign them to different groups.

i Note

If you specify groups when configuring the wireless network, the configuration takes effect on wireless devices in the specified groups.

2. Configuration Steps


Choose **Network-Wide > Devices > AP**.

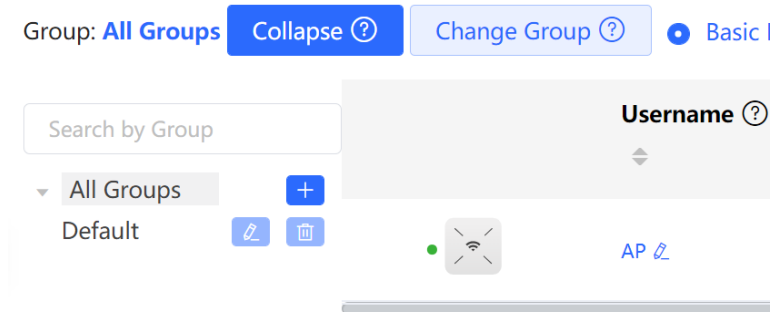
- (1) View the information of all APs on the current network, including basic information, RF information, and model. Click the SN of an AP to configure the AP separately.

Username ?	Model ?	SN ?	IP Address ?	MAC Address ?	Clients ?	Device Group	Relay Information ?	Software Version ?	Action	
AP	EG105GW(T)	W	192.168.110.3	6	D	0	Default	Wired <small>View Details</small>	ReyeeOS 2.248.0.2212	Manage Reboot

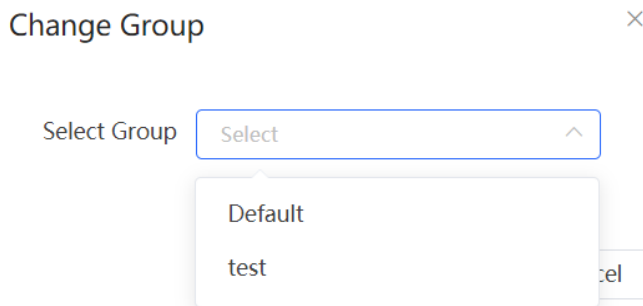
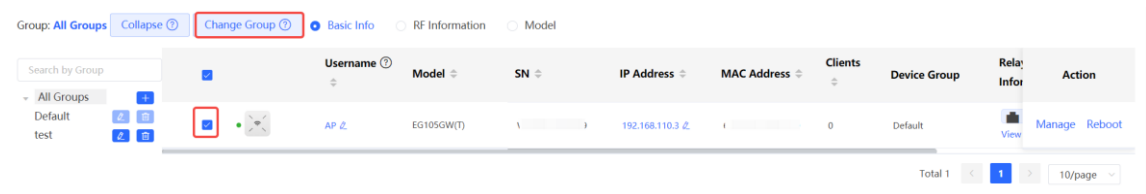
Total 1 1 / 10/page

- (2) Click **Expand**. Information about all the current groups is displayed on the left of the list. Click + to create a group. You can create a maximum of eight groups. Select the target group and click ✎ to modify the

group name or click  to delete the group. You cannot modify the name of the default group or delete the default group.

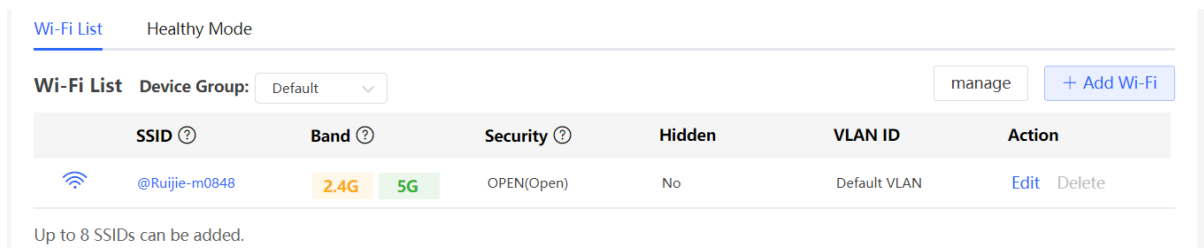


- (3) Click a group name in the left. All devices in the group are displayed. One device can belong to only one group. By default, all devices belong to the default group. Select a device from the device list and click **Change Group** to migrate the selected device to the specified group. After a device is moved to the specified group, the device will use the configuration for the new group. Click **Delete Offline Devices** to remove offline devices from the list.



4.2.3 Configuring Wi-Fi

Choose **Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List**.



Click **Add Wi-Fi**, enter the SSID and Wi-Fi password, select the frequency band used by the Wi-Fi signal, and click **Save**.

Add

✕

* SSID ? Purpose ? **General** | IoT | GuestBand ? 2.4G 5G

No available frequency band? Log in to Ruijie Cloud to add or re-identify the target frequency band. [Re-identify](#) [View Causes](#)

Encryption Open Security 802.1x (Enterprise) !* Security ? * Wi-Fi Password

Click **Advanced Setting** to configure Wi-Fi parameters.

Wi-Fi Standard ? Wireless Schedule ? VLAN Hide SSID (The SSID is hidden and must be manually entered.)Client Isolation ? (Prevent wireless clients of this Wi-Fi from communicating with one another.)Band Steering (The 5G-supported client will access 5G radio preferentially.)XPress (The client will experience faster speed.)Layer 3 Roaming ? (The client will keep the IP address unchanged on the Wi-Fi network.)LimitSpeed

Do you want to edit RF parameters? [Navigate to Radio Frequency for configuration.](#)

⚠ Caution

Configuration modification will cause the wireless configuration to be reset, resulting in logout of connected clients. Exercise caution when performing this operation.

Table 4-1 Wireless Network Configuration

Parameter	Description
SSID	Enter the name displayed when a wireless client searches for a wireless network.
SSID Encoding	The SSID encoding standard is set to "UTF-8" by default when Chinese characters are included in the SSID. If the Chinese characters are garbled, you can choose GB2312 as the SSID encoding standard.
Purpose	Set the Wi-Fi usage scenario. The options include General , IoT , and Guest . The system will recommend different Wi-Fi parameter combinations based on the selected purpose.
Band	Set the band used by the Wi-Fi signal. The options are 2.4 GHz and 5 GHz. The 5 GHz band provides faster network transmission rate and less interference than the 2.4 GHz band, but is inferior to the 2.4 GHz band in terms of signal coverage range and wall penetration performance. Select a proper band based on actual needs. The default value is 2.4G + 5G , indicating that the device provides signals at both 2.4 GHz and 5 GHz bands.
Encryption	The encryption options for a Wi-Fi network include Open , Security , and 802.1x (Enterprise) .
Wi-Fi Password	When the Encryption is set to Security , you need to set the password for connecting to the wireless network. The password is a string of 8 to 16 characters.
Select server group	When the Encryption is set to 802.1x (Enterprise) , you need to configure a remote server set for authentication and authorization.
Wi-Fi Standard	The Wi-Fi standards include 802.11be (Wi-Fi 7) , 802.11ax (Wi-Fi 6) , or Compatibility Mode . The final effective Wi-Fi standard depends on the support of Wi-Fi standards on each device. The latest standard is recommended. If there is a compatibility issue, try use an older standard. However, an old standard setting will affect the bandwidth.
Wireless Schedule	Specify the time periods during which Wi-Fi is enabled. After you set this parameter, users cannot connect to Wi-Fi in other periods.
VLAN	Set the VLAN to which the Wi-Fi signal belongs. You can choose from the available VLANs or click Add New VLAN , and go to the LAN Settings page to add a VLAN.
Hide SSID	Enabling the hide SSID function can prevent unauthorized user access to Wi-Fi, improving security. However, mobile phones or computers cannot find the SSID after this function is enabled. You must manually enter the correct name and password to connect to Wi-Fi. Record the current SSID before you enable this function.

Parameter	Description
Client Isolation	After you enable this parameter, clients associated with the Wi-Fi are isolated from one other, and end users connected to the same AP (in the same network segment) cannot access each other. This improves security.
Band Steering	After this function is enabled, 5G-capable clients select 5G Wi-Fi preferentially. You can enable this function only when Band is set to 2.4G + 5G .
XPress	After this function is enabled, the device sends game packets preferentially, providing more stable wireless network for games.
Layer-3 Roaming	After this function is enabled, clients keep their IP addresses unchanged when associating with the same Wi-Fi. This function improves the roaming experience of users in the cross-VLAN scenario.
802.11r	Enabling the 802.11r function can shorten the roaming handover time. The 802.11r function is supported only when Encryption is set to Security or 802.1x (Enterprise) . Once 802.11r is enabled, the encryption type can only be WPA2-PSK or WPA2-802.1X.
LimitSpeed	After enabling Wi-Fi rate limiting, you can set the uplink and downlink rate limits for users. <ul style="list-style-type: none"> ● Rate Limit Per User: The rate limit applies to all clients connected to the SSID. ● Rate Limit All Users: All clients connected to the SSID share the configured rate limit equally. The rate limit of each client changes dynamically with the number of clients connected to the SSID.

4.2.4 Configuring Guest Wi-Fi

Choose **Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List**.

Guest Wi-Fi is a wireless network provided for guests, and is disabled by default. Client isolation is enabled for guest Wi-Fi by default, and cannot be disabled. In this case, clients associating with guest Wi-Fi are mutually isolated, and they can only access the Internet through Wi-Fi. This improves network access security. You can configure a wireless schedule for the guest network. After the specified schedule expires, the guest network will become unreachable.

Click **Add Wi-Fi**, set the **Purpose** to **Guest**, and configure the Wi-Fi name and password. Click **Advanced Setting** to configure the effective time of the guest Wi-Fi and other Wi-Fi parameters. After the settings are saved, guests can connect to the Internet through the SSID and password. For details, see section [4.2.3 Configuring Wi-Fi](#).

Add

✕

* SSID ⓘ

Purpose ⓘ General | IoT **Guest**

Band ⓘ 2.4G 5G

No available frequency band? Log in to Ruijie Cloud to add or re-identify the target frequency band. [Re-identify](#) [View Causes](#)

Encryption Open Security 802.1x (Enterprise) ⓘ

* Security ⓘ

* Wi-Fi Password

4.2.5 Healthy Mode

Choose **Network-Wide > Workspace > Wireless > Wi-Fi > Healthy Mode**.

Enable the healthy mode and select the effective time for the mode.

After the healthy mode is enabled, the RF transmit power and Wi-Fi coverage range of the device are reduced in the schedule. This may lead to weak signals and network freezing. You are advised to disable the healthy mode or set the wireless schedule to an idle period.

Healthy Mode Device Group:

Enable ⓘ

Effective Time ⓘ

4.2.6 RF Settings

Choose **Network-Wide > Workspace > Wireless > Radio Setting**.

The device can detect the surrounding wireless environment upon power-on and select proper configuration. However, network freezing caused by wireless environment changes cannot be prevented. You can analyze the wireless environment around the APs and routers and manually select proper parameters.

⚠ Caution

Configuration modification will cause the wireless configuration to be reset, resulting in logout of connected clients. Exercise caution when performing this operation.

Radio Setting Device Group: Default

[Not solved yet? Click here to access the Network Optimization page for automatic optimization.](#)

Common Parameter
 No available frequency band? [Log in to Ruijie Cloud](#) to add or re-identify the target frequency band. [Re-identify](#) [View Causes](#)

Country/Region United States (US)

Radio Parameters

2.4G

5G

Global Radio Settings

Channel Width

Multicast Rate (Mbps)

Client Count Limit

Disconnection Threshold Disable -85dBm -65dBm

Table 4-2 RF Configuration

Parameter	Description
Country/Region	Wi-Fi channels stipulated by each country may be different. To ensure that clients can find Wi-Fi signals, select the country or region where the device is located.
2.4G/5G Channel Width	A lower bandwidth indicates a more stable network, and a higher bandwidth indicates less interference. In case of severe interference, select a low bandwidth to prevent network freezing to a certain extent. The 2.4 GHz band supports 20 MHz and 40 MHz bandwidths. The 5 GHz band supports 20 MHz, 40 MHz, and 80 MHz bandwidths. By default, the value is Auto , indicating that the bandwidth is selected automatically based on the environment.
Multicast Rate (Mbps)	Select the data rate of broadcast and multicast packets. <ul style="list-style-type: none"> ● Tip: A higher multicast rate may lead to a higher multicast packet loss rate. A lower multicast rate may cause heavier traffic on the wireless air interface. ● Suggestion: Use a high rate in the case of severe network congestion and a medium rate in the case of mild network lag.

Parameter	Description
Client Count Limit	If a large number of users are connected to an AP or a router, the wireless network performance of the AP or router may be degraded, affecting users' Internet access experience. When this parameter is set and the number of access users reaches the specified value, the AP or router rejects access of new users. If clients require high bandwidth, you can adjust this parameter to a smaller value. You are advised to keep the default value unless otherwise specified.
Disconnection Threshold	When multiple Wi-Fi signals are available, you can set this parameter to optimize the wireless signal quality. When a client is far away from the wireless device and the wireless signal strength of the end user is lower than this value, the Wi-Fi connection is ended. In this case, the client has to select a nearer wireless signal. The client is prone to be disconnected if this value is high. To ensure that the client can normally access the Internet, you are advised to set this parameter to Disable or a value smaller than -75 dBm.



Note

- Available wireless channels depend on the country or region code. Select the country or region code based on the country or region of your device.
- The channel, transmit power, and roaming sensitivity cannot be set globally. You must configure these parameters on devices separately.

4.2.7 Configuring a Wi-Fi Blocklist or Allowlist

1. Overview

You can configure the global or SSID-based blocklist and allowlist. MAC addresses can be exactly matched or based on the OUI.

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

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



Caution

An empty allowlist does not take effect. In this case, all clients are allowed to access the Internet.

2. Configuring a Global Blocklist or Allowlist

Choose **Network-Wide > Workspace > Wireless > Blocklist and Allowlist > Global Blocklist/Allowlist**.

Select the blocklist or allowlist mode and click Add to add a client to the blocklist or allowlist. In the Add dialog box, enter the MAC address and remarks of the target client and click OK. If a client is already associated with the router, its MAC address appears automatically. Click the MAC address for automatic input. All clients in the

blocklist are forced offline and not allowed to access the Wi-Fi network. The global blocklist and allowlist settings take effect on all Wi-Fi networks of the router.

Global Blocklist/Allowlist SSID-Based Blocklist/Allowlist

All STAs except blocklisted STAs are allowed to access Wi-Fi. Only the allowlisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients + Add Delete Selected

<input type="checkbox"/>	Device Name	MAC Address	Action
<input type="checkbox"/>	test ℹ	06:ea:65:38:23:11	Edit Delete

Up to 512 members can be added. Total 1 < 1 > 10/page

Add

Device Name ?

Match Type Full Prefix (OUI)

* MAC Address

Cancel OK

If you delete a client from the blocklist, the client is allowed to connect to the Wi-Fi network. If you delete a client from the allowlist, the client is forced offline and not allowed to access the Wi-Fi network.

Blocked WLAN Clients + Add Delete Selected

<input type="checkbox"/>	Device Name	MAC Address	Action
<input type="checkbox"/>	test ℹ	06:ea:65:38:23:11	Edit Delete

Up to 512 members can be added. Total 1 < 1 > 10/page

3. Configuring an SSID-based Blocklist or Allowlist

Choose **Network-Wide > Workspace > Wireless > Blocklist and Allowlist > SSID-Based Blocklist/ Allowlist**.

Select a target Wi-Fi network from the left column, select the blocklist or allowlist mode, and click Add to add a client to the blocklist or allowlist. The SSID-based blocklist or allowlist restricts the client's access to the specified Wi-Fi network.

Blocklist/Allowlist is used to allow or reject a client's request to connect to the Wi-Fi network.

Note: OUI matching rule and SSID-based blocklist/allowlist are supported by only RAP Net and P32 (and later versions).

Rule:

1. In the Blocklist mode, the clients in the blocklist are not allowed to connect to the Wi-Fi network.
2. In the Allowlist mode, only the clients in the allowlist are allowed to connect to the Wi-Fi network.

Device Group: Default

SSID-Based Blocklist/Allowlist

@Ruijie-m6649

test

All STAs except blocklisted STAs are allowed to access Wi-Fi.

 Only the allowlisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients + Add Delete Selected

Device Name	MAC Address	Action
No Data		

Up to 512 members can be added. Total 0 < 1 > 10/page

4.2.8 Configuring AP Load Balancing

1. Overview

The AP load balancing function is used to balance the load of APs on the wireless network. When APs that are added to a load balancing group are not load balanced, clients will automatically associate with the APs with light load. AP load balancing supports two modes:

- **Client Load Balancing:** The load is balanced according to the number of associated clients. When a large number of clients have been associated with an AP and the count difference of the AP with the lightest load has reached the specified value, the client can only associate with another AP in the group.
- **Traffic Load Balancing:** The load is balanced according to traffic on the APs. When the traffic on an AP is heavy and the traffic difference of the AP with the lightest load has reached the specified value, the client can only associate with another AP in the group.

Example: Add AP1 and AP2 into a group and select client load balancing. Set both the client count threshold and difference to 3. AP1 is associated with five clients and AP2 is associated with two clients, triggering load balancing. New clients' attempt to associate with AP1 will be denied, so they can associate only with AP2.

When a client request is denied by an AP and fails to associate with another AP in the group, the client will keep trying to associate with this AP. If the number of client attempts reaches the specified value, the AP will allow this client, ensuring that the client can normally access the Internet.

2. Configuring Client Load Balancing

Choose **Network-Wide > Workspace > Wireless > Load Balancing**.

Click **Add**. In the dialog box that appears, set **Type** to **Client Load Balancing**, and configure **Group Name**, **Members**, and **Rule**.

Load Balancing

+ Add Delete Selected

By grouping APs in the same area into a load balancing group, they can collaborate to control the access of wireless clients and to achieve optimal traffic distribution. For example, when AP1 and AP2 are added to the same load balancing group, with the load balancing type set to Client Load Balancing and a strategy to trigger load balancing when one AP has 3 clients and the load-balancing threshold is 3, if AP1 has 5 clients and AP2 has 2 clients, any new client trying to connect to AP1 will be denied access and redirected to AP2, achieving load balancing between the two APs.

<input type="checkbox"/>	Group Name	Type	Rule	Members	Action
No Data					

Up to 32 entries can be added.

Add

×

* Group Name

* Type Client Load Balancing ▼

* Rule

Load balancing is triggered when the number of clients connected to an AP in a group reaches i, and the client count difference between the AP and other APs in the group exceeds . Once a client has been denied access to an AP in the group for a total of 10 attempts, it will be allowed to connect to that AP again upon the next attempt.

* Members ▼

Cancel OK

Table 4-3 Client Load Balancing Configuration

Parameter	Description
Group Name	Enter the name of the AP load balancing group.

Parameter	Description
Type	Select Client Load Balancing .
Rule	<p>Configure a detailed load balancing rule, including the maximum number of clients allowed to associate with an AP, difference between the currently associated client count and client count on the AP with the lightest load, and number of attempts to access the AP with a full load.</p> <p>By default, when an AP is associated with three clients and the difference between the currently associated client count and client count on the AP with the lightest load reaches 3, clients can associate only to another AP in the group. After a client's association is denied by an AP for 10 times, the client will be allowed to associate with the AP upon the next attempt.</p>
Members	Specify the APs to be added to the AP load balancing group.

3. Configuring Traffic Load Balancing

Choose **Network-Wide > Workspace > Wireless > Load Balancing**.

Click **Add**. In the dialog box that appears, set **Type** to **Traffic Load Balancing**, and configure **Group Name**, **Members**, and **Rule**.

Add
×

* Group Name

* Type Traffic Load Balancing ▼

* Rule

Load balancing is triggered when the traffic on an AP in a group reaches *100Kbps, and the traffic difference between the AP and other APs in the group exceeds x 100Kbps. Once a client has been denied access to an AP in the group for a total of 10 attempts, it will be allowed to connect to that AP again upon the next attempt.

* Members Enter an AP name or SN. ▼

Cancel
OK

Table 4-4 Traffic Load Balancing Configuration

Parameter	Description
Group Name	Enter the name of the AP load balancing group.
Type	Select Traffic Load Balancing .
Rule	<p>Configure a detailed load balancing rule, including the maximum traffic allowed on an AP, difference between the current traffic and the traffic on the AP with the lightest load, and number of attempts to access the AP with a full load.</p> <p>By default, when the traffic load on an AP reaches 500 kbps and the difference between the current traffic and the traffic on the AP with the lightest load reaches 500 kbps, clients can only associate with another AP in the group. After a client's association is denied by an AP for 10 times, the client will be allowed to associate with the AP upon the next attempt.</p>
Members	Specify the APs to be added to the AP load balancing group.

4.2.9 One-Click Wireless Optimization


Select the optimization mode, the system automatically optimize the wireless network.

Caution

- WIO is supported only in the self-organizing network mode.
- The client may be offline during the optimization process. The configuration cannot be rolled back once optimization starts. Therefore, exercise caution when performing this operation.

Choose **Network-Wide > Workspace > WLAN Optimization > Network Optimization**.

(1) Select the optimization mode. Then, click **OK** to optimize the wireless network.



Wireless Intelligent Optimization

In a networking environment, WIO can help maximize wireless performance by optimizing your network.

Optimization

Optimization Quick optimization Deep optimization mode

Estimated Time

180s Environment scan + 3 minute Optimization

Instructions

- Upgrade all APs to the latest version for optimal network optimization.
- WIO is not supported on APs without an IP address.
- WIO only supports 20 MHz, 40 MHz, and 80 MHz channel bandwidths at the moment.
- Please perform optimization after all APs in the target area are online.

OK

Table 4-5 Description of Tuning Mode

Parameter	Description
Quick tuning	In this mode, external interference and bandwidth are not considered. A quick optimization is performed to optimize channel, power, and management frame power.

Parameter	Description
Deep tuning	<p>In this mode, external interference and bandwidth are considered. A deep optimization is performed to optimize channel, power, and management frame power. Click to expand Advanced Settings to configure the Scan Time, Roaming Sensitivity, Transmit Power, Channel Width and channels.</p> <ul style="list-style-type: none"> ● Scan Time: Indicates the time for scanning channels during the optimization. ● Roaming Sensitivity: You can adjust the roaming sensitivity to balance the roaming performance and connection stability of the device during roaming. ● Transmit Power: You can adjust the transmit power of wireless devices to optimize the performance and coverage of the Wi-Fi network. ● 2.4G <ul style="list-style-type: none"> ○ Channel Width: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. ○ Selected channels: Indicates the channels to be optimized. ● 5G <ul style="list-style-type: none"> ○ Channel Width: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. ○ Selected channels: Indicates the channels to be optimized.

When the **Optimization Mode** is configured as **Deep tuning**, expand the **Advanced Settings** to set the Scan Time, Roaming Sensitivity, Transmit Power, Channel Width and channels.

----- [Advanced Settings](#) -----

Scan time

Roaming

Sensitivity

Transmit Power

2.4G

Channel Width

* Selected channels

1 (2.412GHz)

2 (2.417GHz)

3 (2.422GHz)

4 (2.427GHz)

5 (2.432GHz)

6 (2.437GHz)

7 (2.442GHz)

8 (2.447GHz)

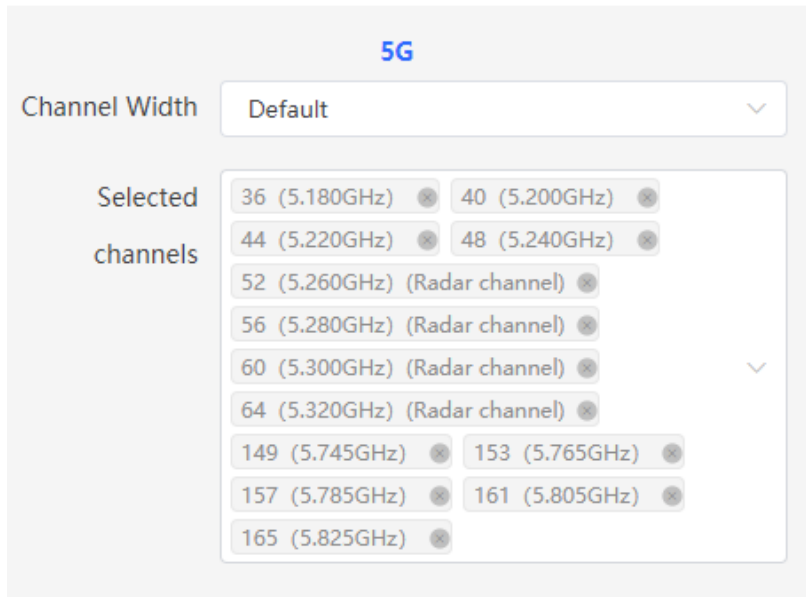
9 (2.452GHz)

10 (2.457GHz)

11 (2.462GHz)

12 (2.467GHz)

13 (2.472GHz)



(2) Confirm the tips, and Click **OK**.

Tips



During optimization, the APs may switch channels and collect data, which may result in temporary disconnection and affect user experience. This situation may last for some time. You are advised to enable scheduled optimization if you require an Internet connection for the time being.

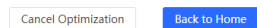


After optimization starts, please wait patiently until optimization is complete. After optimization ends, click **Cancel Optimization** to restore optimized RF parameters to default values.



Finish

Completion time: 2023-12-08 13:32:29
 Optimization mode Quick optimization
 Time consumed: 36 seconds. Optimized 1 APs, resolved severe interference of 0 APs, reduced channel interference by 0.00%, and improved user experience by 0.00%.



Optimization Details

Enter AP name/SN 5G 2.4G

Hostname	Band	SN	Channel Width (Before/After)	Channel (Before/After)	Transmit Power (Before/After)	Sensitivity (Before/After)
Ruijie	5G	G15K9QF069621	80	36	100	0

Total 1 < 1 > 10/page

Click the **Optimization Record** tab to view the latest optimization record details.

Optimization Details

Enter AP name/SN 5G 2.4G

Hostname	Band	SN	Channel Width (Before/After)	Channel (Before/After)	Transmit Power (Before/After)	Sensitivity (Before/After)
Ruijie	5G	G15K9QF069621	80	36	100	0

Total 1 < 1 > 10/page

4.2.10 Scheduled Wireless Optimization

You can configure scheduled optimization to optimize the network at the specified time. You are advised to set the scheduled optimization time to daybreak or the idle periods.

⚠ Caution

Clients may be kicked offline during optimization and the configuration cannot be rolled back after optimization starts. Exercise caution when performing this operation.

Choose **Network-Wide > Workspace > WLAN Optimization > Scheduled Optimization**.

i Optimize the network performance at a scheduled time for a better user experience.

Enable

Day

Time :

Schedule Weekly One time

Optimization mode Quick optimization Deep optimization

----- [Advanced Settings](#) -----

Save

- (1) Configure the scheduled time.
- (2) Select the optimization mode.
- (3) (Optional) When the Tuning Mode is configured as **Deep tuning**, expand the **Advanced Settings** to set the scanning time, roaming sensitivity, transmit power, channel bandwidth and selected channels.

Scan time

Roaming

Sensitivity

Transmit Power

2.4G

Channel Width

* Selected channels

1 (2.412GHz)	2 (2.417GHz)
3 (2.422GHz)	4 (2.427GHz)
5 (2.432GHz)	6 (2.437GHz)
7 (2.442GHz)	8 (2.447GHz)
9 (2.452GHz)	10 (2.457GHz)
11 (2.462GHz)	12 (2.467GHz)
13 (2.472GHz)	

5G

Channel Width

* Selected channels

36 (5.180GHz)	40 (5.200GHz)
44 (5.220GHz)	48 (5.240GHz)
52 (5.260GHz) (Radar channel)	
56 (5.280GHz) (Radar channel)	
60 (5.300GHz) (Radar channel)	
64 (5.320GHz) (Radar channel)	
149 (5.745GHz)	153 (5.765GHz)
157 (5.785GHz)	161 (5.805GHz)
165 (5.825GHz)	

(4) Click **Save**.

4.2.11 Wi-Fi Roaming Optimization (802.11k/v)

Wi-Fi roaming is further optimized through the 802.11k/802.11v protocol. Smart endpoints compliant with IEEE 802.11k/v can switch association to the access points with better signal and faster speed, thereby ensuring high-speed wireless connectivity.

To ensure high quality of smart roaming service, the WLAN environment will be automatically scanned when Wi-Fi roaming optimization is first enabled.

Choose **Network-Wide > Workspace > WLAN Optimization > 802.11k/v Roaming Optimization**.

Start Scanning Optimizing Finish

Description:
The Wi-Fi roaming is further optimized through the 802.11k/v protocol. Smart clients compliant with 802.11k/v can switch to the APs with better signal and faster speed during the roaming process, ensuring high-speed wireless connectivity.
To ensure smart roaming effect, the WLAN environment will be auto scanned when Wi-Fi roaming optimization is first enabled.

Notes:
During the WLAN environment scanning, the APs will switch channels, forcing the clients to go offline. The process will last for 2 minutes.

Optimization Mode ⓘ Performance-prior Roaming-prior

Enable

⚠ Caution
During the optimization, the clients may be forced offline. Please proceed with caution.

Select **Optimization Mode**, and click **Enable** and the optimization starts.

- **Performance-prior:** Maximum negotiation speed is preferentially guaranteed but connection stability may be affected.
- **Roaming-prior:** Connection stability is preferentially guaranteed but maximum negotiation speed may be reduced.

Start Scanning Optimizing Finish

Optimization is enabled.
Optimization finished on 2023-12-08 13:32:29
Time: 36 seconds
To ensure smart roaming effect, please [Click Here](#) to scan the WLAN environment again if the topology changes.

Disable

4.2.12 Enabling Reyeesh Mesh

Choose **Network-Wide > Workspace > Wireless > AP Mesh**.

After Reyeesh Mesh is enabled, the devices that support Reyeesh Mesh can be paired through wireless or wired connection to set up a Mesh network. Auto link optimization is supported in the Mesh network.

i Mesh link optimization algorithm: The algorithm not only covers signal strength, wireless mode, antenna streams and bandwidth parameters, but also considers the attenuation of Mesh hops. The Mesh system will select the optimal uplink automatically for the AP based on the link optimization algorithm.

Enable

Save

After Reyeesh mesh is enabled, you can set up a mesh network through mesh pairing between the devices that support Reyeesh mesh. You can press the **Mesh** button on the device to automatically discover a new device for

mesh pairing or log in to the management page to select a new device for mesh pairing. Reyee mesh is enabled on the device by default with firmware ReyeeOS 1.86 or later.

Perform the following steps to set up a mesh network:

- (1) Connect the first router to the network and configure it as the primary device.
- (2) Place the second router 2 m (6.56 ft) away from the first router. Power on the second router.
- (3) The system status LED of the second router blinks for 2 to 3 minutes. When the system status LED is solid on, the second router is started up.
- (4) Press the **MESH** button on the first router to perform mesh pairing automatically.

The MESH LEDs on both routers are blinking for about 2 minutes. When the MESH LEDs stop blinking and turn solid white, mesh pairing succeeds.

- (5) Place the second router where you want to have Wi-Fi coverage and then power on the router.

Wait for 3 to 5 minutes until the MESH LED turns solid on. Mesh networking succeeds and you can access the Internet by connecting to the new Wi-Fi network.

Note

- Make sure that the new router is around the primary router and there are fewer obstacles between them.
- If three or more routers are added for mesh networking, repeat step 2 to 4. You can add eight devices in a batch at one time.

4.2.13 Configuring a LAN Port of a Downlink AP

Caution

The configuration takes effect only for a downlink AP with a wired LAN port.

Choose **Network-Wide > Workspace > Wireless > LAN Ports**.


This profile takes effect only on APs with wired LAN ports, and is subject to the actual device. For example, the AP wired port profile takes effect on the RG-EAP101 AP.

Note: This profile takes effect on APs on the AP Wired Port Profile List. [The AP Wired Profile Default Profile takes effect on other APs on the network.](#)

Default Settings


VLAN ID [Add VLAN](#)

(Range: 2-232, 234-4090. If this field is left blank, it indicates that the VLAN corresponding to the WAN port is used.)

Apply to APs not on the AP Wired Port Profile List 

[Save](#)

LAN Port Settings [+ Add](#) [Delete Selected](#)

	VLAN ID 	Apply to	Action
<input type="checkbox"/>	20	Ruijie	Edit Delete

Up to 8 VLAN IDs or 32 APs can be added (1 APs have been added).

In the **Default Settings** pane, enter the VLAN ID and click **Save** to configure the VLAN to which the AP's LAN port belongs. If the VLAN ID is empty, the LAN port and WAN port belong to the same VLAN.

Click **Add** to add the AP's wired port. Enter a VLAN ID and select an AP.

Add
×

VLAN ID ?

* Apply to ▼

Cancel
OK

In SON mode, the configuration of AP's wired port applies to all APs that have wired LAN ports on the current network. The configuration applied to APs in **LAN Port Settings** takes effect preferentially.

For APs, if no configuration is applied in **LAN Port Settings**, the default configuration of the AP's wired port will take effect.

4.3 Switch Settings

Choose **Network-Wide > Devices > Switch**.

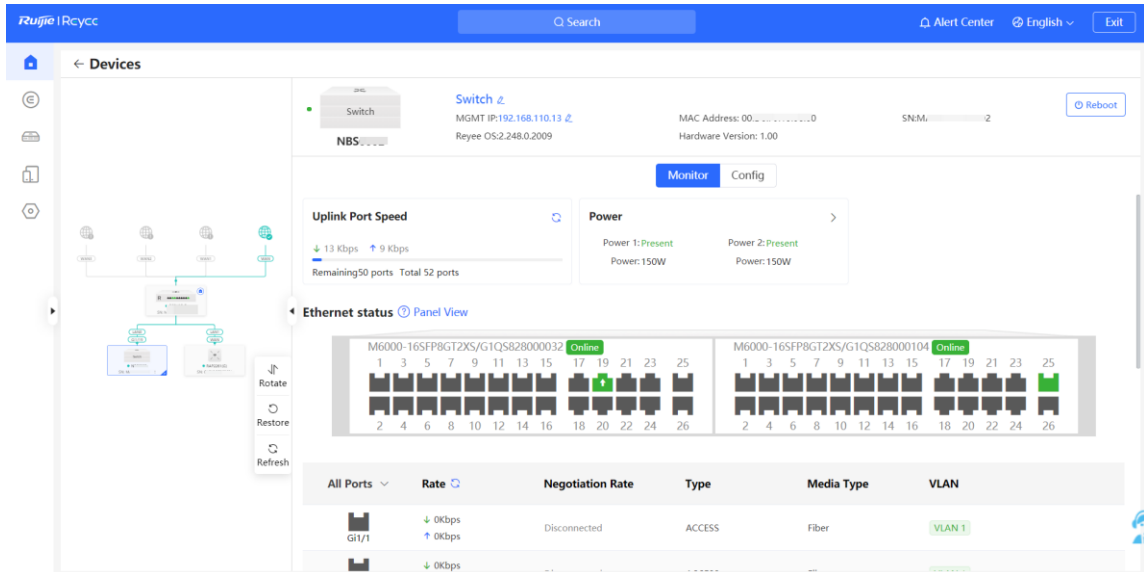
Switch List includes all switches that are managed by the router. The information includes the switch's host name, IP address, MAC address, status, model, software version, and SN. You can check AP categories by clicking ⏷.

The screenshot shows the Ruijie iReycs web interface. The left sidebar has 'Devices' selected. The main content area shows a filter bar with 'Switch (1)' selected. Below the filter bar is a table with the following data:

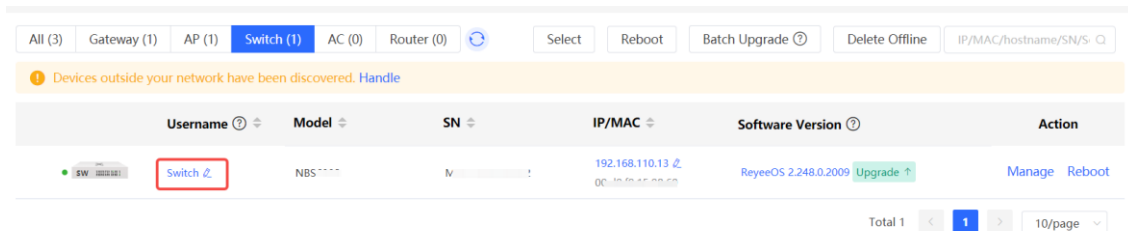
Username	Model	SN	IP/MAC	Software Version	Action
Switch	NBS	M	192.168.110.13 00:00:19:15:08:60	ReyeeOS 2.248.0.2009 Upgrade	Manage Reboot

The 'Manage' button in the Action column is highlighted with a red box. The interface also shows a search bar, alert center, and language settings at the top.

- **Manage:** Go to the detailed configuration page of the switch.



- **Edit Hostname:** Modify the host name of switch.



4.4 Configuring the WAN Ports

Choose **One-Device > Gateway > Config > Network > WAN**.

You can configure multi-line access for the device to allow multiple lines to work simultaneously. After you switch to multi-line access, you need to specify the egress provider of the lines and set the load balancing mode, in addition to setting basic network parameters for the WAN ports.

⚠ Caution

The number of lines supported varies with the product. The actual configuration prevails.

4.4.1 Configuring the Internet Access Mode

Choose **One-Device > Gateway > Config > Network > WAN**.

The device can access the WAN in one of the following three methods: static IP, DHCP, and PPPoE dialing. Select a proper method based on the actual broadband line type. For details, see Section [4.1 Network Access Setting](#).

When the Internet access mode is not **DHCP** or **PPPoE**, you can specify a DNS server to ensure that the device can correctly parse domain names and access Internet resources, thereby improving the access speed and security.

Single Line Dual-Line Three Lines Four Lines

WAN Line Detection

* Internet ? DHCP

Username and password are not required.

IP Address 10.52.48.172

Subnet Mask 255.255.248.0

Gateway 10.52.48.1

DNS Server 172.30.44.20 192.168.5.28

Dedicated DNS Optional

Server ?

----- Advanced Settings -----

Save

4.4.2 Modifying the MAC Address

Choose **One-Device > Gateway > Config > Network > WAN**.

Sometimes, the provider restricts Internet access of devices with unknown MAC addresses out of security considerations. In this case, you can change the MAC addresses of the WAN ports to valid MAC addresses.

Select the target WAN port. Click **Advanced Settings**, enter a MAC address, and click **Save**. You do not need to modify the default MAC address unless otherwise specified.

----- [Advanced Settings](#) -----

* MTU (?) [MTU Detection](#)

* MAC Address (?)

802.1Q Tag

Private Line (?)

NAT Mode (?)

[Save](#)

4.4.3 Modifying the MTU

Choose **One-Device > Gateway > Config > Network > WAN**.

1. Modifying the MTU

MTU specifies the maximum transmission unit allowed to pass a WAN port. By default, the MTU of a WAN port is 1500 bytes. Sometimes, large data packets are limited in transmission speed or prohibited in the ISP network, leading to slow network speed or even network disconnection. If this occurs, you can click **Advanced Settings**, set the MTU to a smaller value.

----- [Advanced Settings](#) -----

* MTU (?) [MTU Detection](#)

* MAC Address (?)

802.1Q Tag

Private Line (?)

NAT Mode (?)

[Save](#)

If the MTU value is unknown, click **MTU Detection** to configure the one-click MTU detection, and adjust the MTU settings based on the results obtained from MTU detection.

2. Detecting the MTU

Click **MTU Detection** to configure the one-click MTU detection to determine the MTU between two communication devices.

Enter the destination IP/domain name, retry count, ICMP echo request timeout, minimum MTU, maximum MTU, and click **Start** to start the detection.

MTU Detection ×

* IP Address/Domain

* Retry Count

* ICMP Echo Request s
Timeout

* Min. MTU

* Max. MTU

Result

4.4.4 Configuring the Private Line

Choose **One-Device > Gateway > Config > Network > WAN**.

Click **Advanced Settings**, turn on **Private Line** and determine whether to set the current WAN line as a private line. Generally, private lines are used for access to specific internal networks but not the Internet. Private lines provide higher network security.

----- Advanced Settings -----

* MTU (?) [MTU Detection](#)

* MAC Address (?)

802.1Q Tag

Private Line (?)

NAT Mode (?)

[Save](#)

4.4.5 Configuring the VLAN Tag

Choose **One-Device > Gateway > Config > Network > WAN**.

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

----- Advanced Settings -----

* MTU (?) [MTU Detection](#)

* MAC Address (?)

802.1Q Tag

*** VLAN ID**

Private Line (?)

NAT Mode (?)

[Save](#)

4.4.6 Configuring NAT Mode

Choose **One-Device > Gateway > Config > Network > WAN**.

When an intranet needs to communicate with an extranet, Network Address Translation (NAT) must be configured to convert the private IP address into a globally unique IP address, so that the private network can access the public network.

Click **Advanced Settings**, toggle on **NAT Mode** to enable the NAT mode. When the NAT mode is disabled, this router operates in router mode to forward data packets, enabling mutual access between hosts connected to the LAN and the WAN ports of this router.

----- Advanced Settings -----

* MTU (?) [MTU Detection](#)

* MAC Address (?)

802.1Q Tag

Private Line (?)

NAT Mode (?)

[Save](#)

⚠ Caution
 Disabling NAT mode may potentially impact the functionality of the self-organizing network (SON) feature.

4.4.7 Configuring the Multi-Line Load Balancing Mode

Choose **One-Device > Gateway > Config > Network > WAN > Load Settings**.

When multiple links are available, some traffic is forwarded along the link selected based on the address library and the remaining traffic is distributed to other links in load balancing mode.

Table 4-6 Load balancing modes

Load Balancing Mode	Description
Loading balancing	<p>The traffic will be distributed across multiple links according to the weight of each WAN port. Larger traffic will be distributed to the WAN port with a higher weight.</p> <p>When you select this mode, you must specify the weight of each WAN port. For example, if the weight of WAN and WAN 1 ports is set to 3 and 2 respectively, then, 60% of the total traffic will be routed over WAN and 40% over WAN 1.</p>
Active/Secondary	<p>All traffic is routed over the primary interface. Once the primary interface fails, traffic will be switched over to the secondary interface.</p> <p>If there are multiple primary or secondary interfaces, the weight of these interfaces must be set. (See balanced mode.)</p>

The system supports IPv4 and IPv6 multi-link load balancing. IPv4 multi-link load balancing is enabled by default, while IPv6 multi-link load balancing needs to be enabled manually.

2. Configuring IPv4 Multi-Link Balancing

Load Balancing Settings v4

Load Mode (?)

Load Balancing Policy

WAN Rate

* Uplink Mbps * Downlink Mbps

WAN1 Rate

* Uplink Mbps * Downlink Mbps

- (1) Select a load balancing mode from the **Load Mode** drop-down list.
- (2) Select a loading balancing policy from the **Load Balancing Policy** drop-down list.

Table 4-7 Description of Load Balancing Policies (IPv4)

Load Balancing Policy	Description
Based on Connections	After you enable this policy, the traffic is routed over multiple links based on the links. Packets with the same source IP address, destination IP address, source port, destination port, and protocol are routed over the same link.
Based on Src IP Address	After you enable this policy, the traffic is routed over multiple links based on the source IP address. The traffic from the same user (same source IP address) will be routed to the same interface. This policy prevents traffic from the same user from being routed to different links, lowering the risks of network access exceptions.
Based on Src and Dest IP Address	After you enable this policy, the traffic is routed over multiple links based on the source IP address and destination. The traffic of the same source IP address and destination IP address will be routed to the same interface.
Smart Load Balancing	After you enable this feature, the traffic is routed over multiple links based on the link bandwidth, the actual loads of the links, application recognition and traffic prediction.

- (3) Set the uplink and downlink bandwidths or the weight for each WAN port.
- o When the load balancing policy is set to **Based on Connections**, **Based on Src IP Address**, or **Based on Src and Dest IP Address**, a weight must be set for each WAN port.

Load Balancing Settings v4

Load Mode (?) Loading balancing

Load Balancing Policy Based on Src IP Addresses

* WAN Weight 1

* WAN1 Weight 1

Note

The higher the value of the weight, the more traffic is directed to the WAN port.

- o When the load balancing policy is set to **Smart Load Balancing**, the uplink and downlink bandwidths must be set for each WAN port.

Load Mode Loading balancing

Load Balancing Policy Smart Load Balancing

WAN0 Rate

* Uplink 1000 Mbps * Downlink 1000 Mbps

WAN1 Rate

* Uplink 1000 Mbps * Downlink 1000 Mbps

- (4) Click **Save**.

2. Configuring IPv6 Multi-Link Balancing

Load Balancing Settings v6

Enable

Load Mode ⓘ Loading balancing

Load Balancing Policy Based on Connections

If you fail to access online bank service, please select Based on Src IP Address.

* WAN Weight 1

* WAN1 Weight 1

Save

- (1) Toggle on **Enable** to enable the IPv6 multi-link load balancing mode.
- (2) Select a load balancing mode from the **Load Mode** drop-down list.
- (3) Select a loading balancing policy from the **Load Balancing Policy** drop-down list.

Table 4-8 Description of Load Balancing Policies (IPv6)

Load Balancing Policy	Description
Based on Connections	After you enable this policy, the traffic is routed over multiple links based on the links. Packets with the same source IP address, destination IP address, source port, destination port, and protocol are routed over the same link.
Based on Src IP Address	After you enable this policy, the traffic is routed over multiple links based on the source IP address. The traffic from the same user (same source IP address) will be routed to the same interface. This policy prevents traffic from the same user from being routed to different links, lowering the risks of network access exceptions.
Based on Src and Dest IP Address	After you enable this policy, the traffic is routed over multiple links based on the source IP address and destination. The traffic of the same source IP address and destination IP address will be routed to the same interface.

- (4) Set a weight for each WAN port.
The valid range of weight is 1 to 100000.

Note

The higher the value of the weight, the more traffic is directed to the WAN port.

- (5) Click **Save**.

4.4.8 Configuring Link Detection

Choose **One-Device > Gateway > Config > Network > WAN > Line Detection**.

After configuring multiple WAN ports, use the link detection function to check whether lines are connected to the external network. If the network is down, the system does not select a route based on the interface, such as load balancing, policy-based routing, and ISP routing.

The system supports IPv4 and IPv6 WAN link detection, which can be enabled separately.

1. Configuring IPv4 WAN Link Detection

- (1) On the **IPv4 WAN Link Detection** page, toggle on **Enable** to enable IPv4 WAN link detection.
- (2) In the WAN port list, select a WAN port for link detection, and click **Edit**.

IPv4 WAN Link Detection

Enable

Interface	Detection Interval	Rounds for Going Online	Rounds for Going Offline	Detected Destination IP	Status	Action
WAN	5s	8	3	114.114.114.114 www.google.com 223.5.5.5	Online	Edit

- (3) Configure the parameters of the link detection function.

WAN Edit

×

* Detection Interval
(unit: s)

* Rounds for Going Online

* Rounds for Going Offline

Detected Destination IP

114.114.114.114	Add
www.google.com	Delete
223.5.5.5	Delete

Cancel

OK

Table 4-9 Description of Line Detection (IPv4)

Parameter	Description
Detection Interval	The time interval of connectivity test.

Parameter	Description
Rounds for Going Online	The system periodically sends a ping message to a detection destination IP address at the specified interval. If the ping succeeds and the number of consecutive successful pings reaches the set number of Rounds for Going Online , the WAN port is set to be online.
Rounds for Going Offline	The system periodically sends a ping message to a detection destination IP address at the specified interval. If the ping fails and the number of consecutive unsuccessful pings reaches the set number of Rounds for Going Offline , the WAN port is set to be offline.
Detected Dest IP	<p>The destination IP address to which the system sends ping messages. You can set up to three destination IP addresses. The system sends ping messages to one of the IP addresses randomly during detection.</p> <hr/> <p>Note</p> <p>For RG-EG105G-V2 and RG-EG210G, the default destination IP address is 114.114.114.114, www.google.com, or 8.8.8.8.</p> <p>For other products, the default destination IP address is 114.114.114.114 or www.google.com.</p>

(4) Click **OK**.

2. Configuring IPv6 WAN Link Detection

- (1) On the **IPv6 WAN Link Detection** page, toggle on **Enable** to enable IPv6 WAN link detection.
- (2) In the WAN port list, select a WAN port for link detection, and click **Edit**.

IPv6 WAN Link Detection

Enable

Interface	Detection Interval	Rounds for Going Online	Rounds for Going Offline	Detected Destination IP	Status	Action
WAN	5s	8	3	240c::6666 240c::6644 2400:3200:1	Offline	Edit

Save

(3) Configure the link detection parameters.

WAN Edit
×

* Detection Interval
(unit: s)

* Rounds for Going Online

* Rounds for Going Offline

Detected Destination IP

Add

Delete

Delete

Cancel OK

Table 4-10 Description of Link Detection (IPv6)

Parameter	Description
Detection Interval	The time interval of connectivity test.
Rounds for Going Online	The system periodically sends a ping message to a detection destination IP address at the specified interval. If the ping succeeds and the number of consecutive successful pings reaches the set number of Rounds for Going Online , the WAN port is set to be online.
Rounds for Going Offline	The system periodically sends a ping message to a detection destination IP address at the specified interval. If the ping fails and the number of consecutive unsuccessful pings reaches the set number of Rounds for Going Offline , the WAN port is set to be offline.
Detected Dest IP	<p style="text-align: right;">The destination IP address (IPv6) to which the system sends ping messages.</p> <p>You can set up to three destination IP addresses. The system sends ping messages to one of the IP addresses randomly during detection.</p>

(4) Click **OK**.

4.5 Diagnostics

4.5.1 Network Check

You can check your network and resolve the problem on this page.

- (1) Switch to the **Local** mode. Choose **One-Device > Gateway > Config > Diagnostics > Diagnose**. Click **Start** and click **OK** in the displayed dialog box to start checking the network status.



- (2) The result is displayed after network check finishes.




4.5.2 Alarms

The **Alerts** page allows you to query and manage alarms.

- (1) Switch to the **Local** mode. Choose **One-Device > Gateway > Config > Diagnostics > Alarms**.
- (2) The **Alert List** page displays possible problems on the network environment and device.

All types of alarms are followed by default. You can click **Unfollow** in the **Action** column to unfollow this type of alarms.

 Caution

After unfollowing a specified alarm type, you will not discover and process all alarms of this type in a timely manner. Therefore, exercise caution when performing this operation.

View and manage alarms.

Alert List View Unfollowed Alert

Expand	Alerts	Suggestion	Action
▼	The IP address of the downlink device is already in use.	Please check the IP address of the downlink device. If it is a static IP address, please change the IP address.	Delete Unfollow

Device Name	SN	Type	Time	Details	Action
RG310G-E	M-99	EG310G-E	2023-12-12 14:32:05	An IP address conflict occurs. IP address: 10.52.48.106. Conflicting MAC address: f0:74:8d:b1:9d:e3 and 00:d0:f8:12:5a:2c	Delete

Total 1 < 1 > 10/page

(3) Click **View Unfollowed Alert** to view the unfollowed alarm. You can follow the alarm again in the pop-up window.

View Unfollowed Alert ×

The IP address of the downlink device is already in use.

[Re-follow](#)

Cancel

4.5.3 Network Tools

Switch to the **Local** mode. Choose **One-Device > Gateway > Config > Diagnostics > Network Tools**.

Tool Ping Traceroute DNS Lookup

Type IPv4 IPv6

* IP Address/Domain

* Ping Count

* Packet Size

Result

Select a diagnostic method, enter an IP address or URL, and click **Start**.

- The ping method is used to test the connectivity between the tested device and the specified IP address or URL. If the ping operation fails, the IP address or URL fails to be pinged from the device.
- The traceroute method is used to trace network paths to the specified IP address or URL.
- The DNS lookup method is used to check the DNS server address for URL parsing.

1. Ping Tool

Set **IP Address/Domain**, **Ping Count**, and **Packet Size** on this page, and click **Start**. The ping result will be displayed.

Tool Ping Traceroute DNS Lookup

Type IPv4 IPv6

* IP Address/Domain

* Ping Count

* Packet Size

Result

2. Traceroute Tool

Set **IP Address/Domain** and **Max TTL** on this page, and click **Start**. The traceroute result will be displayed.

Tool Ping Traceroute DNS Lookup

Type IPv4 IPv6

* IP Address/Domain

* Max TTL

Result

3. DNS Lookup Tool

This tool is used to resolve the domain name to an IP address.

Tool ? Ping Traceroute DNS Lookup

* IP Address/Domain

DNS

```

Server:      8.8.8.8
Address: 8.8.8.8#53

Name:       www.google.com
Address 1:  159.138.20.20
Address 2:  2a03:2880:f11a:83:face:b00c:0:25de
  
```

4.5.4 Packet Capture

Choose **One-Device > Gateway > Config > Diagnostics > Packet Capture**.

If the device fails and troubleshooting is required, the packet obtaining result can be analyzed to locate and rectify the fault.

Configure an interface and a protocol, and specify the host IP address to obtain the content in data packets. Select the file size limit and packet count limit to determine the conditions for automatically stopping packet obtaining. If the file size or number of packets reaches the specified threshold, packet obtaining stops and a diagnostic package download link is generated. Click **Start** to execute the packet obtaining command.

Caution

The packet obtaining operation may occupy many system resources, causing network freezing. Therefore, exercise caution when performing this operation.

Interface ?

Protocol ?

IP Address ?

File Size Limit ? Available Memory **776.54 M**

Packet Count Limit ?

PCAP file [Click to download the PCAP file.](#) i
[Click to delete the file.](#)

Packet obtaining can be stopped at any time. Then a download link is generated. Click this link to save the packet obtaining result in the PCAP format locally. Use analysis software such as Wireshark to view and analyze the result.

Interface ?

Protocol ?

IP Address ?

File Size Limit ? Available Memory **776.54 M**

Packet Count Limit ? File Size: **106.77K**
Captured on: **2023-12-07 19:02:45**

PCAP file [Click to download the PCAP file](#) i
[Click to delete the file.](#)

- **Interface:** Obtain packets passing through this interface.
- **Protocol:** Obtain packets of this protocol.
- **IP Address:** Obtain packets of this IP address
- **File Size Limit:** Limit the size of a packet.
- **Packet Count Limit:** Limit the packet count. When the packet count reaches the limit, packet obtaining will stop and a download link will be generated.

4.5.5 Fault Collection

Switch to the **Local** mode. Choose **One-Device > Gateway > Config > Diagnostics > Fault Collection**.

When the device fails, you need to collect fault information. Click **Start**. Configuration files of the device are packaged into a compressed file. Download the compressed file locally and provide it to R&D personnel for fault locating.

i Compress the configuration file for engineers to identify fault.

Compress the configuration file for engineers to identify faults.

4.5.6 Viewing Flow Statistics

Choose **One-Device > Gateway > Config > Diagnostics > Flow Statistic**.

On the **Flow Table Packet Counters Page**, you can view the details of packets received by the device, including protocol, aging time, state, source IP address, destination IP address, source port, destination port, and so on.

Flow Table Packet Counters Page

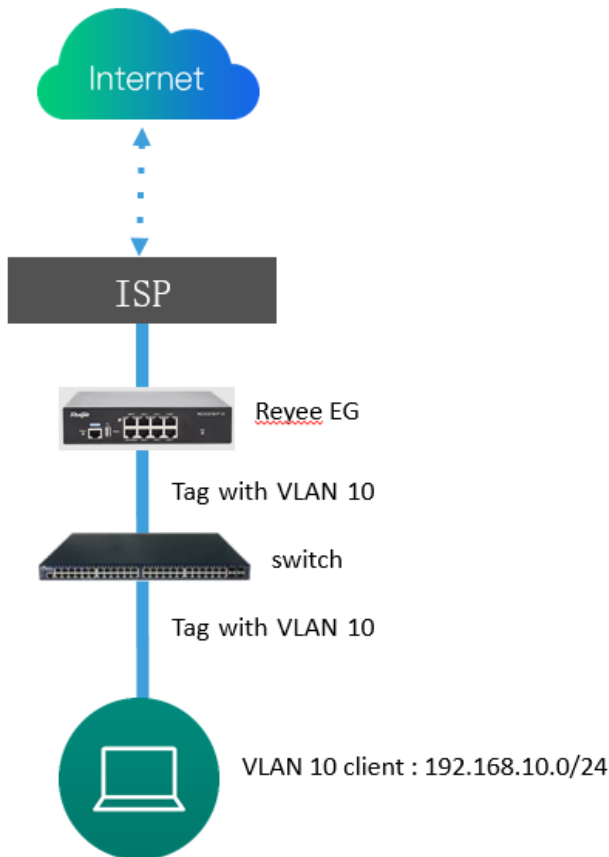
Fuzzy earch by Src IP/Dest IP/Src port/Dest port Q Search

protocol	aging_time	state1	src	dst	sport	dport	packets	bytes	state2	src_down	dst_down	sport_down	dport_down	packets_down	bytes_down	mark	use
udp	3	-	127.0.0.1	127.0.0.1	45982	53	1	71	-	127.0.0.1	127.0.0.1	53	45982	1	71	0	2
udp	1	-	192.168.2.5	192.168.2.1	39498	53	1	59	-	192.168.2.1	192.168.2.5	53	39498	1	169	1	2
udp	5	-	10.52.48.4.3	192.168.5.28	49271	53	1	58	-	192.168.5.28	10.52.48.4.3	53	49271	1	166	1	2
icmp	2	-	10.52.48.4.3	223.5.5.5	type=8 code=0	id=16145	1	84	-	223.5.5.5	10.52.48.4.3	type=0 code=0	id=16145	1	84	1	2
udp	4	-	192.168.2.2	192.168.2.1	59258	53	1	63	-	192.168.2.1	192.168.2.2	53	59258	1	430	1	2
udp	4	-	10.52.48.4.3	172.30.44.20	40322	53	1	63	-	172.30.44.20	10.52.48.4.3	53	40322	1	430	1	2
udp	2	-	127.0.0.1	127.0.0.1	36339	53	2	118	-	127.0.0.1	127.0.0.1	53	36339	2	260	0	2

Note

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

4.6 Port VLAN



- (1) Switch to the **Local** mode. Choose **One-Device > Gateway > Config > Network > LAN > LAN Settings** to create a VLAN first.

LAN Settings + Add Delete Selected

<input type="checkbox"/>	IP Address [?]	Subnet Ma... [?]	VLAN ID [?]	Remarks	DHCP Serv... [?]	Start IP Address [?]	IP Count [?]	Lease Time (Min) [?]	Action
<input checked="" type="checkbox"/>	192.168.2.1	255.255.255.0	Default VLAN	-	Enabled	192.168.2.1	254	8	Edit Delete

Edit ×

* IP Address

* Subnet Mask

Remarks

MAC Address

DHCP Server

* Start IP Address

* IP Count

* Lease Time (Min)

DNS Server 192.168.2.1 [?]

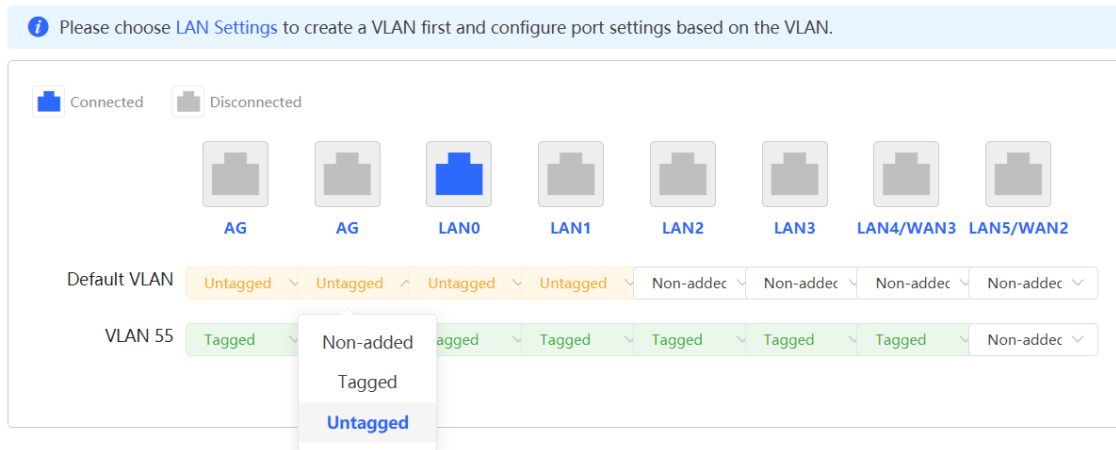
After you configure a LAN successfully, it is displayed in **LAN Settings**.

LAN Settings + Add Delete Selected

<input type="checkbox"/>	IP Address [?]	Subnet Mask [?]	VLAN ID [?]	Remarks	DHCP Server [?]	Start IP Address... [?]	IP Count [?]	Lease Time (Min) [?]	Action
<input checked="" type="checkbox"/>	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	254	30	Edit Delete
<input type="checkbox"/>	192.168.10.1	255.255.255.0	10	test	Enabled	192.168.10.1	254	480	Edit Delete

Up to 8 entries can be added.

- Choose **One-Device > Gateway > Config > Network > Port VLAN**. By default, the tagged mode is used for VLANs.



- **Untagged** : If VLAN 10 is set to **Untagged** on port 2, VLAN 10 will be the native VLAN of port 2. Packets from VLAN 10 are forwarded through port 2 without being tagged with VLAN 10 and all untagged packets on port 2 are considered as the packets from VLAN 10.
- Each port can be configured with only one untagged VLAN.
- The native VLAN of port 1 is the default VLAN and cannot be edited.
- **Tagged** : If both VLAN 10 and VLAN 20 are set to **Tagged** on port 2, packets from VLAN 10 and VLAN 20 are forwarded through port 2.
- **Non-added**: If both VLAN 10 and VLAN 20 are set to **Non-added** on port 2, port 2 will not receive or transmit packets from VLAN 10 or VLAN 20.

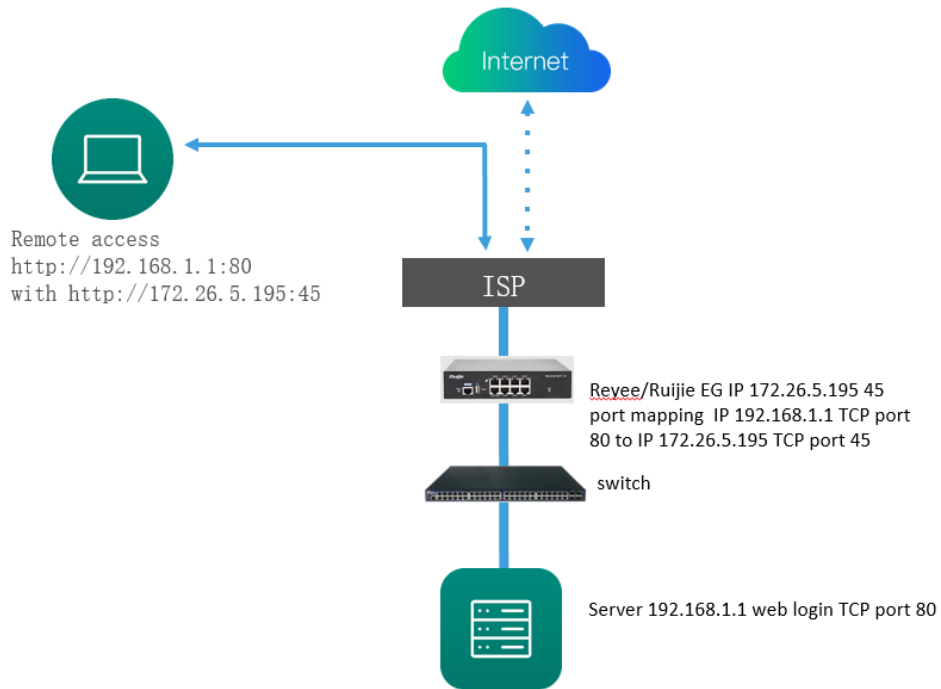
4.7 Port Mapping

Port mapping is used to map the internal server IP address and port number to external IP address so that extranet staffs can access internal servers. The difference between port mapping and DMZ is that port mapping only map one or more ports, but DMZ will map all ports.

- Typical scenario of port mapping

The port mapping function can establish a mapping relationship between the IP address and port number of a WAN port and the IP address and port number of a server on the LAN, so that all access traffic destined for a service port of the WAN port is redirected to the corresponding port of the specified LAN server. This function enables external users to proactively access the service host on the LAN through the IP address and port number of the specified WAN port.

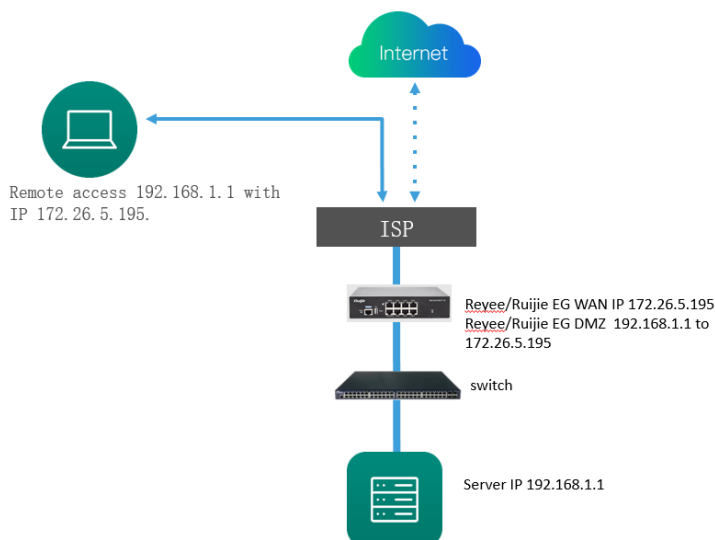
Port mapping enables users to access cameras or computers on their home networks when they are in companies or on a business trip.



- Typical scenario of DMZ

When an incoming data packet does not hit any port mapping entry, the packet is redirected to the LAN server according to the Demilitarized Zone (DMZ) rule. All data packets proactively sent from the Internet to the device are forwarded to the designated DMZ host, realizing LAN server access of external network users. DMZ provides the external network access service while ensuring security of other hosts on the LAN.

Port mapping or DMZ is used when an external network user wants to access the LAN server, for example, access a server deployed on the intranet when the user is in the enterprise or on a business trip.



4.7.1 Configuring Port Mapping

- (1) Switch to the **Local** mode. Choose **One-Device > Gateway > Config > Advanced > Port Mapping > Port Mapping**.

- (2) Click **Add**. In the dialog box that appears, enter the rule name, service type, protocol type, external port/range, internal server IP address, and internal port/range. You can create a maximum of 50 port mapping rules.

Port Mapping List [+ Add](#) [Delete Selected](#)

<input type="checkbox"/>	Name ?	Protocol ?	External IP Address ?	External Port ?	Internal IP Address ?	Internal Port ?	Action
No Data							

Up to 512 entries can be added. Total 0 < 1 > 10/page

Add ×

* Name ?

Preferred Server

Protocol ?

External IP Address ? **Outbound Interface** Enter or select an IP address.

* External Port/Range ?

* Internal IP Address ?

* Internal Port/Range ?

Table 4-11 Port Mapping Configuration

Parameter	Description
Name	Enter the description of a port mapping rule, which is used to identify the rule.
Preferred Server	Select the type of a service to be mapped, such as HTTP or FTP. The internal port number commonly used by the service is automatically entered. If the service type is unknown, select Custom .
Protocol	Select the transmission layer protocol type used by a service, such as TCP or UDP. The value ALL indicates that the rule applies to both protocols. The value must comply with the client configuration of the service.

Parameter	Description
External IP Address	Specify the host address used for accessing the external network. <ul style="list-style-type: none"> ● Outbound Interface: You can select All WAN Ports or specify a WAN port. ● Enter or select an IP address: Select or enter the IP address of a WAN port.
External Port/Range	Specify the port number used for Internet access. You need to confirm the port number in the client software, such as the camera monitoring software. You can enter a port number or a port range, such as 1050-1060. If you enter a port range, the value of Internal Port/Range must also be a port range.
Internal IP Address	Specify the IP address of the internal server to be mapped to the WAN port, that is, the IP address of the LAN device that provides Internet access, such as the IP address of a network camera.
Internal Port/Range	Specify the service port number of the internal server to be mapped to the WAN port, that is, the port number of the application that provides Internet access, such as port 8080 of the web service. You can enter a port number or a port range, such as 1050-1060. If you enter a port range, the number of ports must be the same as that specified in External Port/Range .

- (3) Check whether the external network device can access services on the destination host using the external IP address and external port number.

4.7.2 Configuring NAT-DMZ

- (1) Switch to the **Local** mode. Choose **One-Device > Gateway > Config > Advanced > Port Mapping > NAT-DMZ**.
- (2) Click **Add**. Enter the rule name and internal server IP address, select the interface to which the rule applies, specify the rule status, and click **OK**. You can configure only one DMZ rule for an outbound interface.

i You can view NAT-DMZ settings and edit or delete the rule.

NAT-DMZ Rule List + Add Delete Selected

	Name ?	Outbound Interface ?	Dest IP Address ?	Status ?	Action
No Data					

There are 2 outbound interfaces. Up to 2 rules can be added.

Add Rule
×

* Name

* Dest IP Address

Outbound Interface WAN ▼

Status

Cancel
OK

Table 4-12 DMZ Rule Configuration

Parameter	Description
Name	Enter the description of a mapping rule, which is identify the rule.
Dest IP Address	Specify the IP address of the DMZ host to which packets are redirected, that is, the IP address of the internal server that can be accessed from the Internet.
Outbound Interface	Specify the WAN port in the DMZ rule. You can configure only one rule for a WAN port.
Status	Specify whether the rule is effective. The rule is effective when Status is enabled.

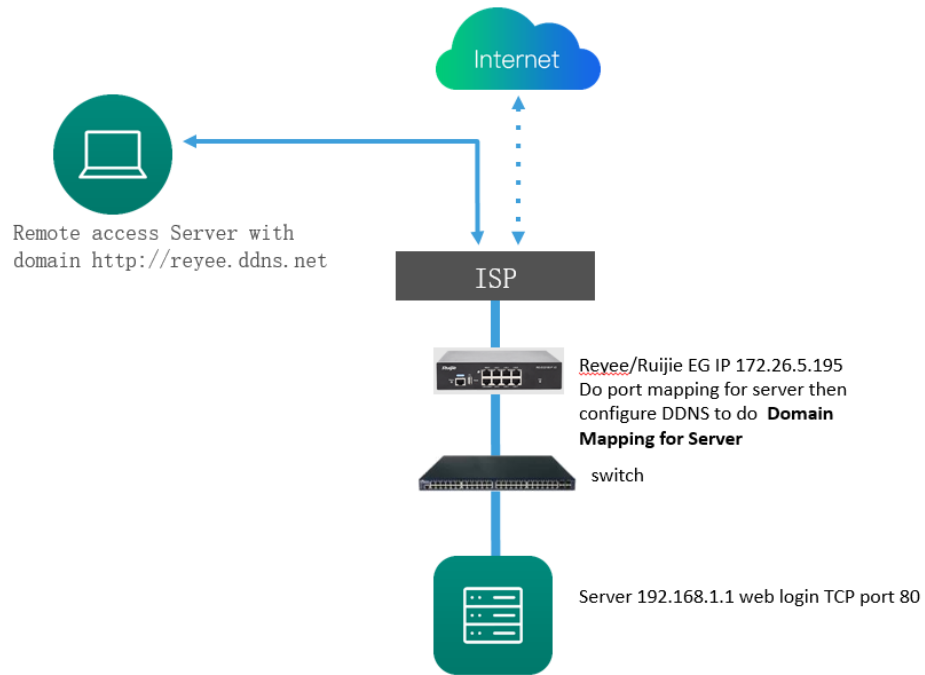
Caution

When both DMZ and port mapping are configured, port mapping takes precedence.

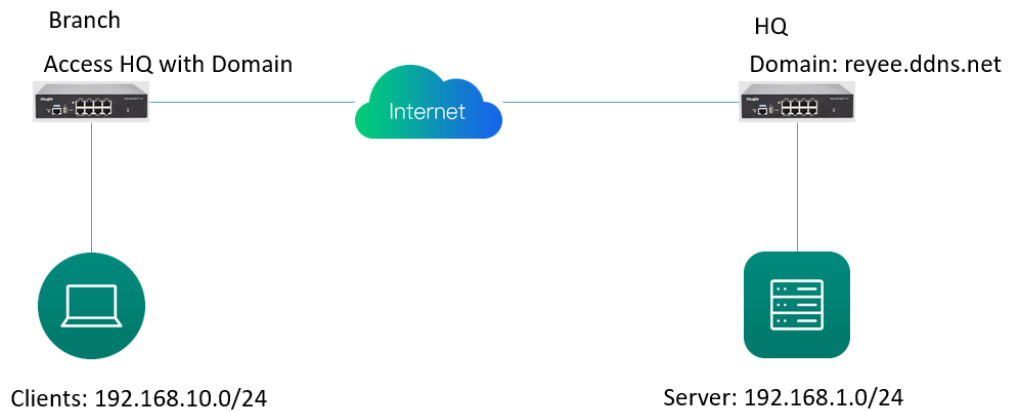
4.8 Dynamic DNS

Dynamic Domain Name Server (DDNS) is to map a user's dynamic IP address to a fixed domain name. Each time a user connects to the network, the client program will transfer the dynamic IP address of the user host to the server program located on a host of a service provider. Then the server program is responsible for providing DNS services and implementing dynamic domain name resolution.

- Server access with the domain name



- VPN connection with the domain name



- (1) Switch to the **One-Device > Gateway > Config > Advanced > Dynamic DNS > No-IP DNS** .

There are two DDNS servers you can choose to connect: NO-IP DNS, and Other DNS.

No-IP DNS
Other DNS

* Service Interface

* Username [Register](#)

* Password

Domain (?)

IPv6 Disable Enable

Log In
Delete

Link Status -

Domain -

(2) You can use the value of **Domain** to access the intranet server or headquarters device.

4.9 Wi-Fi Authentication

4.9.1 Overview

With the popularity of wireless networks, Wi-Fi has become one of the marketing means for merchants. Customers can connect to the Wi-Fi provided by the merchants to surf the Internet after watching advertisements. In addition, to defend against security vulnerabilities, the wireless office network usually allows only employees to associate with Wi-Fi, so the identity of the clients needs to be verified.

The Wi-Fi authentication function of the device uses the Portal authentication technology to implement information display and user management. After users connect to Wi-Fi, the traffic will not be directly routed to the Internet. Wi-Fi users must pass authentication on the Portal authentication website, and only authenticated users are allowed to use network resources. Merchants or enterprises can customize Portal pages for identity authentication and advertisement display.

4.9.2 Getting Started

- (1) Before you enable Wi-Fi authentication, ensure that the wireless signal is stable and users can connect to Wi-Fi and surf the Internet normally. The wireless SSID used for authentication in the network should be set to the open state.
- (2) If the IP address of an AP in the network is within the authentication scope, add the AP as the authentication-free user. For details, see Section [4.9.8 Authentication-Free](#).
 - o In a Layer 2 network, add the MAC address of the AP to the authentication-free MAC address allowlist.
 - o In a Layer 3 network, add the IP address of the AP to the authentication-free IP address allowlist.

4.9.3 Cloud Authentication

1. Overview

The EG device is connected to the MACC authentication server on the cloud. After Wi-Fi users connect to Wi-Fi, a Portal page pops up. The users need to enter the account and password to pass authentication before they can access the Internet. According to the authentication configuration on the MACC server, you can set the authentication mode to SMS authentication, fixed account authentication, or account-free one-click login.

2. Getting Started

- (1) WiFiDog is a Layer 2 protocol. Ensure that the authentication device can obtain the MAC addresses of the wireless users.
 - o The gateway address of the wireless users to be authenticated is deployed on the authentication device.
 - o If the gateway address is not deployed on the authentication device, the device functions as a DHCP server to allocate IP addresses to the wireless users and obtain MAC addresses of the wireless users. In this scenario, you need to set Network Type to Layer-3 Network.
- (2) Complete the corresponding configuration on the NOC MACC platform before you enable the authentication function on the device. If SMS authentication is used, you also need to configure the SMS gateway.

3. Configuration Steps

Choose **One-Device > Gateway > Config > Advanced > Authentication > Cloud Auth**.

- (1) Turn on **Authentication**.
- (2) Set **Server Type** to **Cloud Integration**, configure **Network Type**, **Auth Server URL**, **Client Escape**, and **IP/IP Range**, and click **Save**.

Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication and one-click authentication. Please log into Ruijie Cloud to enable authentication. [View](#)

i In a layer-2 network, if the IP address of the EAP device is in the authentication IP range, please add its MAC address to the MAC address allowlist of [Allowlist](#).
 In a layer-3 network, if the IP address of the EAP device is in the authentication IP range, please add its IP address to the IP address allowlist of [Allowlist](#).

Authentication

* Network Type

* Server Type

* Auth Server URL

Client Escape [Enable](#)

- (3) In the **Net List** area, click **Add**. In the displayed dialog box, enter the Wi-Fi network name and the IP address/range to be authenticated and click **OK**.

Add
×

* VLAN

* Auth IP / IP Range

?

Table 4-13 Description of WiFiDog Authentication Configuration

Parameter	Description
Network Type	The default value is Layer-2 Network . Set the parameter based on the actual network environment.
Server Type	Select Cloud Integration from the drop-down list.
Auth Server URL	After completing the configuration at the MACC server end, the MACC server returns a URL. The device sends authentication requests to the URL during authentication.
Client Escape	After the client escape function is enabled, if an exception occurs on the authentication server, the device disables authentication to allow all clients to directly access the Internet. After the server recovers, the device automatically enables authentication.
VLAN	Specify the name of a Wi-Fi network, to which clients connect. A maximum of eight Wi-Fi network names can be configured.
Auth IP/IP Range	Specify the IP address range to be authenticated. You can enter a single IP address (such as 192.168.112.2) or an IP address range (such as 192.168.112.2–192.168.112.254). A maximum of five IP address ranges can be configured.

4. Verifying Configuration

After a mobile phone connects to a specific Wi-Fi, the Portal authentication page pops up automatically.

If the authentication mode configured on the MACC server is SMS authentication, the user needs to enter the mobile number to obtain an Internet access password and enter the password to complete authentication.

If the authentication mode configured on the MACC server is account-free one-click authentication, the user can directly access the Internet after clicking the corresponding button on the page.

If the authentication mode configured on the MACC server is fixed account login, the user can access the Internet after entering the account and password configured on the cloud.

After successful connection, you can choose **One-Device > Gateway > Config > Advanced > Authentication > Online Clients** to view information about this authenticated user. For details, see Section [4.9.9 Online Authenticated User Management](#).

4.9.4 Configuring Third-Party Authentication

Note

This feature is supported on RG-EG105G-V3, RG-EG105G-P-V3, RG-EG210G-P-V3, RG-EG1510XS, RG-EG310GH-E, RG-EG305GH-P-E and EG310GH-P-E running ReyeeOS 2.237 or later.

1. Overview


Reyee EG series gateway devices can interwork with WISPr-compliant external authentication servers. After a wireless client is connected to the Wi-Fi network, a Portal page pops up. The wireless client needs to be authenticated before it can access the Internet. Based on the services provided by different authentication servers, you can choose RADIUS authentication, local account authentication, or no authentication for third-party authentication.

2. Getting Started

- Ensure that the authentication server can obtain the MAC address of the wireless client:
 - The gateway address of the wireless client to be authenticated is deployed on the authentication server.
 - If the gateway address of the wireless client to be authenticated is not deployed on the authentication server, then the device must act as a DHCP server to assign an IP address to the wireless client in order to obtain its MAC address. In this scenario, the **Network Type** must be set to **Layer 3 Network**.
- Complete relevant configurations on the third-party authentication platform, and then enable the Wi-Fi authentication feature on the device. For specific configurations, see the configuration manual of relevant third-party authentication platforms.

3. Configuration Steps

Choose **One-Device > Gateway > Config > Advanced > Authentication > Cloud Auth**.


 Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication and one-click authentication. Please log into Ruijie Cloud to enable authentication. [View](#)

In a layer-2 network, if the IP address of the EAP device is in the authentication IP range, please add its MAC address to the MAC address allowlist of Allowlist.

In a layer-3 network, if the IP address of the EAP device is in the authentication IP range, please add its IP address to the IP address allowlist of Allowlist.

Authentication

* Network Type

* Server Type [Customized Parameter](#) 

* Auth Server URL

Client Escape Enable

Authentication type RADIUS Local account None

Authentication server [Edit](#)

group

Accounting server [Edit](#)

group

(1) Toggle on **Authentication**.

(2) Set **Server Type** to **Third-party Authentication**, configure **Auth Server URL**, **Client Escape** and **Authentication Type**, and click **Save**.

Table 4-14 Description of Third-Party Authentication Configuration Parameters

Parameter	Description
Network Type	The default value is Layer-2 Network . Set the parameter based on the actual network environment.
Server Type	Select Third-party authentication from the drop-down list.
Auth Server URL	After completing the configuration on the third-party authentication server, the third-party authentication server returns a URL. The device sends authentication requests to the URL during authentication.
Client Escape	After the client escape function is enabled, if an exception occurs on the authentication server or the RADIUS server, the device disables authentication to allow all clients to directly access the Internet. After the server recovers, the device automatically enables authentication.
Authentication Type	Types of third-party authentication, which include: <ul style="list-style-type: none"> ● RADIUS: The wireless client is authenticated by the RADIUS server. ● Local account: The wireless client is authenticated based on local username and password. ● None: No authentication is required for the wireless client.
Auth Server Group	Name of the authentication server group. This parameter is mandatory when the Authentication Type is set to RADIUS . You can configure the authentication server group in the global management mode by going to Network-wide > 802.1X Authentication > RADIUS Server Management .
Accounting Server Group	Name of the accounting server group. This parameter is mandatory when the Authentication Type is set to RADIUS . You can configure the accounting server group in the global management mode by going to Network-wide > 802.1X Authentication > RADIUS Server Management .

- (3) (Optional) Considering the different HTTP parameters and request methods required by different third-party authentication platforms, you can customize third-party authentication parameters.

Customized Parameter
×

Parameter template Ruijie DrayTek Custom

Request Parameters

Request method get post

Parameter	Type	Key	Val
	other	res	notyet
	client_mac	mac	NULL
	other	user	NULL
	other	uamport	NULL
	identity	nasid	NULL
	login_host	uamip	NULL
	other	error	NULL
	chap_id	chap-id	NULL
	chap_challen	chap-challei	NULL

Login Parameters

Name

Login Password

Post Url

Table 4-15 Description of Custom Third-Party Authentication Parameters

Parameter	Description
Parameter template	The built-in parameter template. Default parameters are used when the Parameter Template is set to Ruijie or DrayTek . When the Parameter Template is set to Custom , the parameters can be customized.
Request method	The HTTP request methods used for requesting the portal page.

Parameter	Description
Parameter	<p>Parameters in the parameter template for requesting the portal page:</p> <ul style="list-style-type: none"> ● When the parameter type is not other, the Val field is invalid, and the default value NULL can be used. The Reyee EG gateway device will automatically populate the value of this parameter. ● When the parameter type is other, you need to enter a value in the Val field. <p>Parameters include:</p> <ul style="list-style-type: none"> ● nas_ip: IP address of the Reyee EG series gateway device. Example: 10.52.48.7. ● nas_mac: MAC address of the Reyee EG series gateway device. Example: 11:22:33:44:55:66. ● client_ip: IP address of the wireless client to be authenticated. Example: 192.168.110.5. ● client_mac: MAC address of the wireless client to be authenticated. Example: 11:22:33:44:55:66. ● orig_url: Original URL accessed by the wireless client to be authenticated. Example: https://www.baidu.com. ● login_url: Login interface received by the Reyee EG series gateway device from the third-party authentication platform. Example: http://192.168.110.1:2060/ext_login. ● logout_url: Logout interface received by the Reyee EG series gateway device from the third-party authentication platform. Example: http://192.168.110.1:2060/ext_logout. ● ssid: SSID or VLAN name associated with the wireless client to be authenticated. Example: VLAN233. ● login_host: IP address of the login interface on the Reyee EG series gateway device. Example: 192.168.110.1:2060. ● other: other custom field. Multiple custom fields are supported.
Login Parameters	<p>Custom fields of the login interface received by the Reyee EG series gateway devices from the third-party authentication platform, including:</p> <ul style="list-style-type: none"> ● Username: username. ● Login Password: password. ● Post Url: URL to which the wireless client is redirected after successful authentication.

4. Verifying Configuration

Connect your smartphone to the specific Wi-Fi network to verify that the portal page pops up automatically.

Connect to different authentication platforms to view services provided by these authentication platforms.

After the connection is successful, view the details of the wireless client by going to **Advanced > Authentication > Online Clients**. For details, see [4.9.9 Online Authenticated User Management](#).

4.9.5 Local Account Authentication

1. Overview

The device is connected to the local authentication server, and user identity is verified based on the account and password. Local account authentication is applicable to the wireless office network environment.

2. Getting Started

Ensure that the device with the authentication function enabled has been connected to the Internet. Otherwise, the authentication page does not pop up when a client associates with Wi-Fi.

3. Configuration Steps

Choose **One-Device > Gateway > Config > Advanced > Authentication > Local Account Auth**.

(1) Enable account authentication.

Turn on **Local Account Auth**, enter the IP address range of clients to be authenticated, and click **Save**. After account authentication is enabled, clients in the specified IP address range can access the Internet only after passing authentication.

1. Enable account authentication and create an account.
2. A user logs in with the account created in step 1 and will be allowed to access the Internet.

1 Make sure that the device can access the Internet. Otherwise, the Portal page may not pop up on the terminal.

In a layer-2 network, if the IP address of the EAP device is in the authentication IP range, please add its MAC address to the MAC address allowlist of Allowlist.
In a layer-3 network, if the IP address of the EAP device is in the authentication IP range, please add its IP address to the IP address allowlist of Allowlist.

Local Account Auth

Accounts 1

* Network Type

* Auth IP / IP Range

MAB validity period

* Custom Time days

Note

You can select the default portal page or a customized portal page for local account authentication. See [4.10.2 Configuring Captive Portal on Ruijie Cloud](#) for customizing a portal page.

(2) Configure an authentication account.

Click **Add** to configure an authentication account for Internet access. Multiple clients can access the Internet using the same account and password. The **Concurrent Users** parameter specifies the maximum number of users allowed to access the Internet using the same account.

After a **Wi-Fi user** passes authentication using an account, the IP address of the authenticated user is displayed in the **IP** column next to the account. The account list records a maximum of five latest device IP addresses using the same account.

Account Settings

<input type="checkbox"/>	Username	Password	At most of Concurrent Users	MAC Address <input type="text"/>	Action
<input type="checkbox"/>	test	*****	5		Edit Delete

Up to 200 accounts can be added. Total 1

Add Account×

* Username

* Password

At most of
Concurrent Users

4. Verifying Configuration

After a client connects to the specific Wi-Fi, the authentication page pops up automatically. The user can normally access the Internet only after entering the account and password configured on the local server on the authentication page. You can choose **One-Device > Gateway > Config > Advanced > Authentication > Online Clients** to view information about the successfully connected user. For details, see Section [4.9.9 Online Authenticated User Management](#).

4.9.6 Authorized Guest Authentication

1. Overview

The device is connected to the local authentication server. After a guest connects to Wi-Fi, the guest can access the Internet after the specified authorization IP user or account and password authentication user scans the QR code that pops up for guest authentication. For example, in the wireless office network, users in the employee network segment are authorized to scan the guest authentication QR code for users in the guest network segment.

2. Getting Started

Ensure that the device with the authentication function enabled has been connected to the Internet. Otherwise, the authentication page does not pop up when a client associates with Wi-Fi.

3. Configuration Steps

Choose **One-Device > Gateway > Config > Advanced > Authentication > Authorized Auth**.

Turn on **Authorized Auth**, configure **Popup Message**, **Auth IP / IP Range**, **Authorization IP/IP Range**, and **Limit Online Duration**, and click **Save**.

An authenticated user can authorize guests by scanning his QR code.

i Make sure that the device can access the Internet. Otherwise, the Portal page may not pop up on the terminal.

In a layer-2 network, if the IP address of the EAP device is in the authentication IP range, please add its MAC address to the MAC address allowlist of **Allowlist**.
 In a layer-3 network, if the IP address of the EAP device is in the authentication IP range, please add its IP address to the IP address allowlist of **Allowlist**.

Authorized Auth

Popup Message

* Auth IP / IP Range

Limit Online Duration

* Authorization IP/IP
 Range

Table 4-16 Authorized guest authentication configuration

Parameter	Description
Popup Message	Specify the text to be displayed on the pop-up QR code page.
Auth IP / IP Range	Specify the IP address range for users to be authenticated. The value can be a single IP address (such as 192.168.110.2) or an IP address range (such as 192.168.110.2-192.168.110.254). Users in the specified IP address range can access the Internet only after passing authentication.
Limit Online Duration	Specify whether to limit the online duration of guests. After you enable this function, you need to configure Duration Limit . If the online duration of a guest exceeds the specified value, the guest can continue Internet access only after re-authorization. By default, this function is disabled, indicating that guests can use Wi-Fi without limit on the online duration.
Duration Limit	Specify the maximum online duration of authorized guests. If the online duration of an authorized guest exceeds the specified value, the guest goes offline automatically and needs to be re-authorized for login again.
Authorization IP/IP Range	Specify the IP address range of authorization users. Users in this range can scan the QR code to authorize guests.

4. Verifying Configuration

After a guest connects to Wi-Fi, the QR code authentication page pops up. The guest can access the Internet after the specified authorization user scans this QR code. You can choose **One-Device > Gateway > Config > Advanced > Authentication > Online Clients** to view information about the successfully connected user. For details, see Section [4.9.9 Online Authenticated User Management](#).

4.9.7 Guest Authentication Through QR Code Scanning

1. Overview

Guests scan the specified QR code to access the Internet. For example, in the wireless office network, guests scan the pasted QR code to access the Internet after they connect to Wi-Fi.

2. Getting Started

Ensure that the device with the authentication function enabled has been connected to the Internet. Otherwise, the authentication page does not pop up when a client associates with Wi-Fi.

3. Configuration Steps

Choose **One-Device > Gateway > Config > Advanced > Authentication > QR Code Auth**.

Turn on **QR Code Auth**, configure **Auth IP / IP Range**, **Limit Online Duration**, and **QR Code Generator**, and click **Save**.

QR Code Auth


* Auth IP / IP Range

Limit Online Duration

QR Code Generator

* Dynamic QR Code

Popup Message



Please print and paste the QR code for guests to scan.

Table 4-17 Guest authentication through QR code scanning configuration

Parameter	Description
Auth IP / IP Range	Specify the IP address range for users to be authenticated. The value can be a single IP address (such as 192.168.110.2) or an IP address range (such as 192.168.110.2-192.168.110.254). Users in the specified IP address range can access the Internet only after passing authentication.

Parameter	Description
Limit Online Duration	Specify whether to limit the online duration of guests. After you enable this function, you need to configure Duration Limit . If the online duration of a guest exceeds the specified value, the guest needs to scan the QR code again before continuing Internet access. By default, this function is disabled, indicating that guests can use Wi-Fi without limit on the online duration.
Duration Limit	Specify the maximum online duration of authorized guests. If the online duration of an authorized guest exceeds the specified value, the guest goes offline automatically and needs to be re-authenticated.
Dynamic QR Code	The dynamic QR code is used to generate a QR code image. After the dynamic QR code is updated, the QR code image changes and the previous image becomes invalid. You can print and paste the generated QR code image, which can be scanned by guests to access the Internet.
Popup Message	Specify the QR code prompt message displayed on the page after a guest scans the QR code.

4. Verifying Configuration

After a client connects to Wi-Fi, the guest can scan the QR code to pass authentication and access the Internet. You can choose **One-Device > Gateway > Config > Advanced > Authentication > Online Clients** to view information about the successfully connected user. For details, see Section [4.9.9 Online Authenticated User Management](#).

4.9.8 Authentication-Free

1. Overview

After IP addresses or MAC addresses are configured for authentication-free users, they can directly access the Internet without passing authentication. Traffic from all the users in the blacklist is blocked.

2. Configuring an Authentication-Free User

Choose **One-Device > Gateway > Config > Advanced > Authentication > Allowlist > User Allowlist**.

Authentication-free user: Users in the specified IP address range can directly access the Internet without passing authentication.

Click **Add** to configure the IP address range for authentication-free users. The value can be a single IP address (such as 192.168.110.2) or an IP address range (such as 192.168.110.2-192.168.110.254). A maximum of 50 entries are supported.

User Allowlist

[+ Add](#) [Delete Selected](#)

<input type="checkbox"/>	IP / IP Range	Action
<input type="checkbox"/>	192.168.2.3	Edit Delete

Up to 50 entries can be added.

Total 1 < **1** > 10/page ▾

Add ×

* IP / IP Range

[Cancel](#) [OK](#)

3. Configuring Extranet IP Addresses for Authentication-Free

Choose **One-Device > Gateway > Config > Advanced > Authentication > Allowlist > IP Allowlist**.

Extranet IP address for authentication-free: Specify the IP addresses that can be assessed by all users including unauthenticated users.

Click **Add** to configure extranet IP addresses that can be assessed by users without authentication. A maximum of 50 entries are supported.

IP Allowlist

[+ Add](#) [Delete Selected](#)

<input type="checkbox"/>	IP / IP Range	Action
<input type="checkbox"/>	172.32.10.1	Edit Delete

Up to 50 entries can be added.

Total 1 < **1** > 10/page ▾

Add ×

* IP / IP Range

[Cancel](#) [OK](#)

4. Configuring a Domain Allowlist

Choose **One-Device > Gateway > Config > Advanced > Authentication > Allowlist > Domain Allowlist**.

Domain Allowlist: Specify the URLs that can be accessed without authentication.

Click **Add**. In the dialog box that appears, enter the authentication-free URLs, and then click OK. When the destination URL of the user is in the **Domain Allowlist**, traffic from the user will be permitted directly, regardless of whether the user passes authentication. A maximum of 100 entries are supported.

Domain Allowlist + Add Delete Selected

	URL	Action
<input type="checkbox"/>	rujienetworks.com	Edit Delete

Up to 100 entries can be added. Total 1 1 10/page

Add ×

* URL

Cancel
OK

5. Configuring a MAC Allowlist

Choose **One-Device > Gateway > Config > Advanced > Authentication > Allowlist > MAC Allowlist**.

MAC Allowlist: Clients whose MAC addresses are in the allowlist can access the Internet through Wi-Fi without the need for authentication.

Click **Add**. In the dialog box that appears, enter the MAC addresses of authentication-free users, and then click **OK**. A maximum of 250 entries are supported.

MAC Allowlist + Add Delete Selected

	MAC Address	Action
<input type="checkbox"/>	00:11:22:33:44:55	Edit Delete

Up to 250 entries can be added. Total 1 1 10/page

Add ×

* MAC Address

Cancel
OK

6. Configuring a User MAC Blocklist

Choose **One-Device > Gateway > Config > Advanced > Authentication > Allowlist > MAC Blocklist**.

MAC Blocklist: Clients whose MAC addresses are in the blocklist are prohibited from accessing the Internet.

Click **Add**. In the dialog box that appears, enter the MAC addresses of users in the blocklist, and then click **OK**.

A maximum of 250 entries are supported.

MAC Blocklist + Add Delete Selected

<input type="checkbox"/>	MAC Address	Action
<input type="checkbox"/>	0A:2B:3C:4D:5F:6E	Edit Delete

Up to 250 entries can be added. Total 1 1 10/page

Add ×

* MAC Address

Cancel OK

4.9.9 Online Authenticated User Management

1. Configuring the Idle Client Timeout Period

Choose **One-Device > Gateway > Config > Advanced > Authentication > Online Clients**.

You can configure the idle client timeout period. The default value is 15 minutes. If no traffic from an online user passes through the device within the specified period, the device will force the user offline. The user can continue Internet access only after re-authentication.

Auth Settings

Idle Client Timeout Min (Range: 5-65535)

Save

Online Clients

Search by IP Address Refresh Delete Selected

<input type="checkbox"/>	Username	IP	Device Name	MAC Address	Online Time	Duration(Se c)	Auth Type	Status	Action
--------------------------	----------	----	-------------	-------------	-------------	-------------------	-----------	--------	--------

No Data

Total 0 1 10/page

2. Kicking a User Offline

The online client list displays information about all the current online clients, including the client IP address, client MAC address, login time, and authentication mode. You can find the client information based on the IP address,

MAC address, or username. Find the target client in the online client list and click **Delete** in the **Action** column to kick the client off and disconnect the Wi-Fi connection of the client.

Online Clients

<input type="checkbox"/>	Username	IP	Device Name	MAC Address	Online Time	Duration(Se c)	Auth Type	Status	Action
No Data									

Total 0 < **1** > 10/page

4.10 Wireless Authentication

Note

The function is supported by EG310G-E, EG305GH-E, and EG310GH-E.

4.10.1 Overview

Use the wireless authentication function to perform authentication configuration for the AP connected to the gateway. After users connect to the Wi-Fi signals released by the AP, the traffic will not be directly routed to the Internet. Wi-Fi users must pass authentication before accessing network resources.

Note

- The EG series router supports egress authentication. When an EG router is used independently, you are advised to use the authentication function of the router. Log in to the Eweb of the EG router. Choose **Local Device > Advanced > Authentication**. For details, see [4.9 Wi-Fi Authentication](#).
- When the EG router connects to the AP, the **Wireless Auth** action entry point appears on the **Network** page but not on the **Local Device** page.

4.10.2 Configuring Captive Portal on Ruijie Cloud

1. Prerequisites


If you want to configure **SMS Authentication** on Ruijie Cloud, please add a Twilio account first.

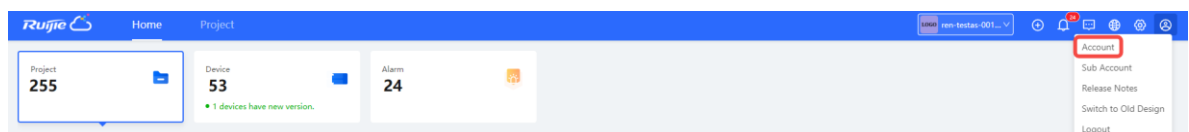
A Twilio account has been applied for from the Twilio official website (<https://www.twilio.com/login>).

Note

A Twilio account is used to send the SMS verification code.

Configuration Steps

- (1) Log in to Ruijie Cloud and choose  > **Account**



- (2) Add Twilio account information and click **Save**

User Info

Modify Password

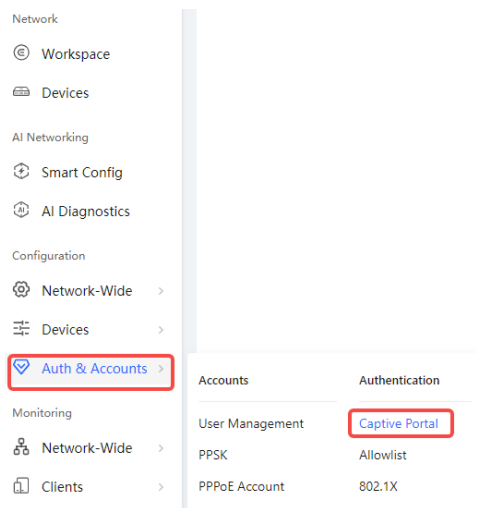
Modify Twilio Account [How to apply twilio account?](#)

Twilio Account SID	<input type="text" value="Account SID of Twilio"/>
Auth Token	<input type="text" value="Auth Token of Twilio"/>
Auth Phone	<input type="text" value="Active Number (Country Code + Phone Number) of Twilio"/>
<input type="button" value="Save"/>	

Delete Account

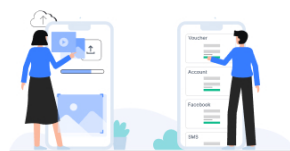
2. Configuring a Portal Page

- (1) Log in to Ruijie Cloud, choose **Project > Configuration > Auth&Account > Authentication > Captive Portal**, and select a network that needs to configure wireless authentication.



- (2) Click **Add Captive Portal** to open the portal template configuration page.

Captive Portal ☺



New Authentication Function

- New version upgrade, support AP/Gateway unified configuration
- Support multiple login methods, one-click login, Voucher, Account, SMS verification, registered account
- Support multi-language and flexible customization of Portal pages.

- (3) Click **Add Page** to customize a portal page.

Portal Page ?

(4) Configure basic information of the portal template.

Portal Basic Settings

Portal Name:

Login Options: One-click Login

Access Duration (Min): Unlimited 15 30 60 Custom

Voucher

Account

SMS

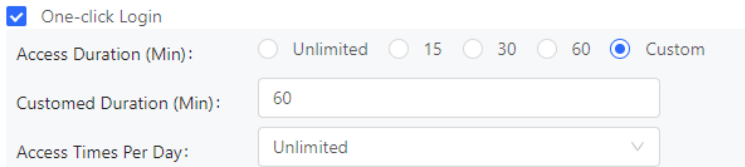
Registration

Facebook Account

Show Balance Page:

Post-login URL:

Table 4-18 Basic Information of the Portal Settings

Parameter	Description
Portal Name	Indicates the name of a captive portal template.
Login Options	<p>Indicates the option to perform the desired action.</p> <ul style="list-style-type: none"> ● One-click Login: indicates login without the username and password. You can set Access Duration and Access Times Per Day.  <ul style="list-style-type: none"> ● Voucher: indicates login with a random eight-digit password. ● Account: indicates login with the account and password. ● SMS: indicates login with the phone number and code. ● Registration: Facebook Account: indicates login with the Facebook account.
Show Balance Page	Indicates the available duration, time, or data after portal authentication.
Post-login URL	Indicates the URL that is displayed after portal authentication.

(5) Configure visual settings of the portal template.

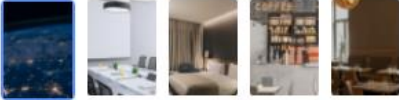
Portal Visual Settings

Logo:

Logo Image:

Logo Position:

Background: Picture Solid Color

Background Image: 

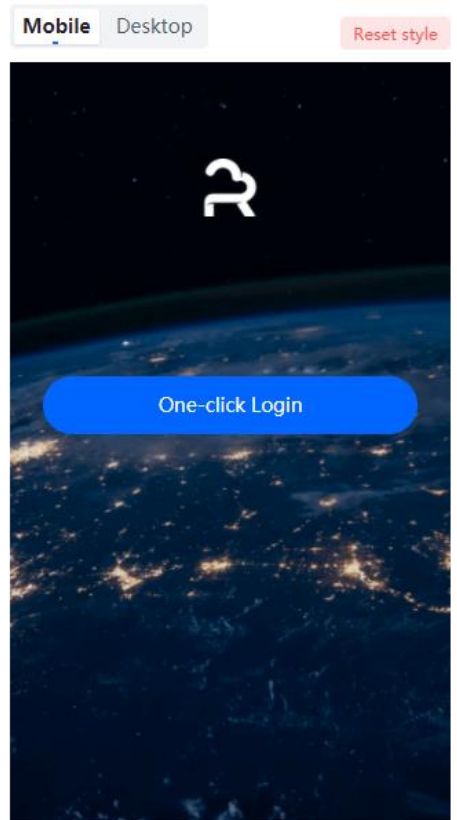
Background Mask Color: #999999

Welcome Message: Text Picture

English

Welcome Text:

Marketing Message:



English +

Welcome Text:

Marketing Message:

Terms & Conditions:

Copyright:

One-click Login

Login Button:

Advertisement: ?

Welcome Text Color:

Welcome Text Size:

Button Color:

Button Text Color:

Link Color:

Text Color in Box:

Table 4-19 Visual Settings of the Portal Page

Parameter	Description
Logo	Select whether to display the logo image.
Logo Image	When Logo is set to Image , upload the logo picture or select the default logo.
Logo Position	Select the logo position (Upper, Middle, or Lower).
Background	Select the background with the image or the solid color.
Background Image	When Background is set to Image , upload the background image or select the default image.
Background Mask Color	When Background is set to Solid Color , configure the background color. The default value is #ffffff .
Welcome Message	Select the welcome message with the image or text.

<p>Language</p>	<p>Select the language of the portal page and configure the content displayed on the portal page as required. You can click <input type="button" value="+"/> to add portal pages in other languages.</p> <ul style="list-style-type: none"> ● Welcome Text: Select the welcome message with the image or text. ● Marketing message: Enter the marketing message. ● Terms & Conditions: Enter terms and conditions. ● Copyright: Enter the copyright. ● One-click Login: After One-click Login is enabled, you can customize the button name displayed on the portal page, which is set to One-click Login by default. <p style="margin-left: 20px;">One-click Login</p> <p>Login Button: <input type="text" value="One-click Login"/></p> <ul style="list-style-type: none"> ● Voucher Login: After Voucher Login is enabled, you can customize the names of controls related to voucher authentication. <p style="margin-left: 20px;">Voucher</p> <p>Title: <input type="text" value="Voucher Login"/></p> <p>Code Placeholder: <input type="text" value="Access Code"/></p> <p>Login Button: <input type="text" value="Login"/></p> <p>Switching Button: <input type="text" value="Voucher Login"/></p> <ul style="list-style-type: none"> ● Account Login: After Account Login is enabled, you can customize the names of the controls related to account authentication. <p style="margin-left: 20px;">Account</p> <p>Title: <input type="text" value="Account Login"/></p> <p>Account Placeholder: <input type="text" value="Account"/></p> <p>Password Placeholder: <input type="text" value="Password"/></p> <p>Login Button: <input type="text" value="Login"/></p> <p>Switching Button: <input type="text" value="Account Login"/></p> <ul style="list-style-type: none"> ● SMS Login: After SMS Login is enabled, you can customize the names of the controls related to SMS authentication.
-----------------	---

Parameter	Description
	<p>SMS</p> <p>Title: <input type="text" value="SMS Login"/></p> <p>Phone Placeholder: <input type="text" value="Phone"/></p> <p>Code Placeholder: <input type="text" value="Verification Code"/></p> <p>Code Button: <input type="text" value="Get Code"/></p> <p>Login Button: <input type="text" value="Login"/></p> <p>Switching Button: <input type="text" value="SMS Login"/></p> <ul style="list-style-type: none"> Registration: After Registration is enabled, you can customize the names of the controls related to register new account. <p>Registration</p> <p>Title: <input type="text" value="Login"/></p> <p>Email: <input type="text" value="Email"/></p> <p>Phone number: <input type="text" value="Phone"/></p> <p>User: <input type="text" value="Your Name"/></p> <p>Registration Button: <input type="text" value="Login"/></p> <p>Switching Button: <input type="text" value="Register New Account"/></p>
Advertisement	Select whether to display the advertisement.
Welcome Text Color	Select the welcome message text color. The default value is #ffffff.
Welcome Text Size	Select the welcome text size.
Button Color	Select the button color. The default value is #0066ff.
Button Text Color	Select the button text color. The default value is #ffffff.
Link Color	Select the link color. The default value is #ffffff.
Text Color in Box	Select the text color in the box. The default value is #ffffff.

(6) After the configuration, click **OK** to save the portal template configurations.

3. Configuring Policy Info

Configure basic information of the policy info to add captive portal. After the configuration, click **OK** for the configurations to take effect.


 Note


When Encryption Mode is set to a value other than WPA2-Enterprise(802.1x), Auth is available and you can select whether to perform wireless authentication.

Add Captive Portal

Policy Info

* Policy Name:

Policy Mode : Inner External

Authentication Device : Router AP

* SSID:

Seamless Online:

Seamless Online Period:

Portal Escape:

Table 4-20 Basic Information of the Captive Portal

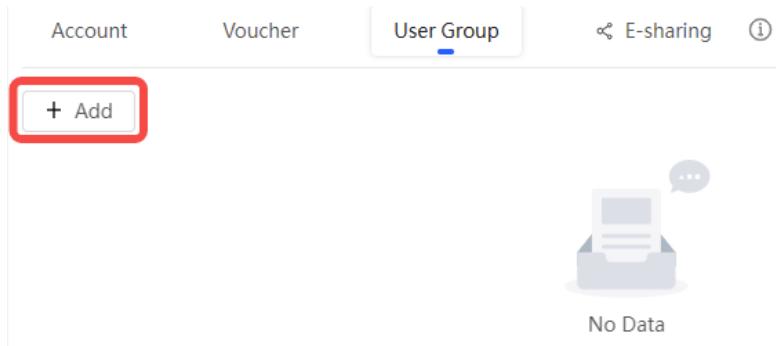
Parameter	Description
Policy Name	Indicates the name of a captive portal template.
Policy Mode	Indicates the authentication mode to which the captive portal applies: Inner: Cloud-based authentication. The built-in authentication server in the public cloud is used for authentication. Local: Device-based local authentication and acceleration. Portal pages and accounts in the cloud are synchronized with the device for local authentication and acceleration. External: Third-party authentication, facilitating integration between the device and a third-party authentication server for authentication.

Parameter	Description
Authentication Device	<p>Indicates the device that performs the authentication.</p> <p>When there is a router on the network, you are advised to enable authentication on the router. You can perform authentication on either an access point (AP) or a router.</p> <p>AP: An AP acts as the NAS.</p> <p>Router: A router or gateway acts as the NAS responsible for performing authentication at the gateway exit.</p> <p>Reyee AP Authentication: RAP/EWR, ReyeeOS 1.219 or later version.</p> <p>Reyee EG WiFiDog Authentication: EG/EGW, ReyeeOS 1.202 or later version.</p> <p>Reyee EG Local Authentication: EG210G-E, EG210G-P-E, EG310GH-E, EG310GH-P-E, EG305GH-E, EG305GH-P-E, ReyeeOS 1.230 or later version.</p> <p>This parameter is not required if the policy mode is Local.</p>
Network	<p>Indicates the wired network that requires authentication. Enter the network segment in this field.</p> <p>Users connecting to the wired network corresponding to this network segment must be authenticated.</p> <p>This parameter is required if the Authentication Device is Router.</p>
SSID	<p>Indicates the network name of the Wi-Fi network that requires authentication.</p> <p>Users connecting to this wireless network must be authenticated.</p> <p>This parameter is required if the Authentication Device is AP.</p>
Seamless Online	<p>After this function is enabled, if the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within a certain period of time.</p>
Seamless Online Period	<p>Indicates the time period for seamless online. If the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within this period of time.</p>
Portal Page	<p>Indicates the portal page that is displayed after portal authentication.</p> <p>Click Current Project to select the portal page for an existing project.</p> <p>Click Shared Portals to select an existing portal page.</p> <p>Click Add Page to customize a portal page.</p>

4. (Optional) Adding a Voucher

If the **Login Options** is **Voucher**, you should configure a voucher as the following steps.

- (1) Log in to Ruijie Cloud, choose **Project > Authentication > User Management**, and select a network in this account.
- (2) Configure a user group.
 - a On the **User Group** tab, click **Add**.



- b Configure user group parameters. After the configuration, click **OK**.

Add user group
✕

* User group name

User Group Policy

Price

Concurrent devices

Period

Quota ⓘ

Maximum upload rate

Maximum download rate

Bind MAC on first use

User Group Name: indicates the user group name.

Price: indicates the price of the user group. Mark user groups by numeral. The current version has no impact on network usage.

Concurrent Devices: indicates the number of concurrent devices for one account.

Period: indicates the maximum validity time of an account. The maximum value is counted after the client passes authentication and successfully accesses the Internet.

Quota: indicates the maximum amount of data transfer.

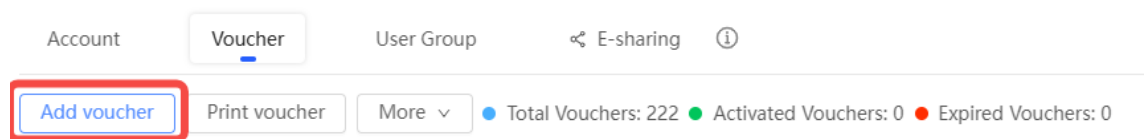
Maximum upload rate: indicates the maximum upload rate.

Maximum download rate: indicates the maximum download rate.

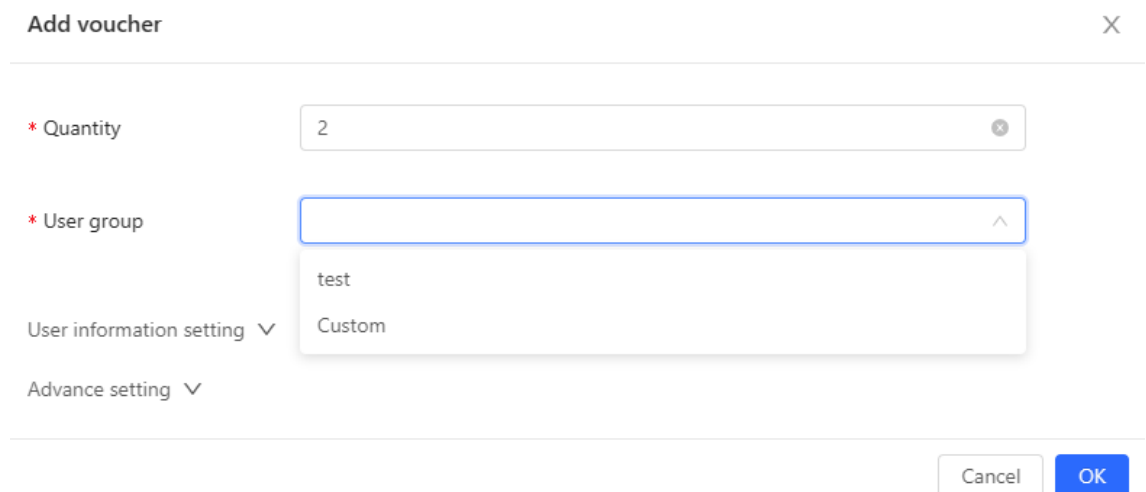
Bind MAC on first use: indicates that the MAC address of the first device used will be bound and other devices used by the same user will be prohibited from accessing the Internet.

(3) Configure a voucher.

a On the **Voucher** tab, click **Add voucher**.



b Configure voucher parameters. After the configuration, click **OK**.



Quantity: Enter the quantity of the voucher to print. When the value is set to 1, you can add a voucher and configure the name and the email address. When the value is greater than 1, you can add vouchers in batches. In this case, you can only configure the name and email address separately after the vouchers are added.

User group: Select a created user group from the drop-down list. If the created user group does not meet the requirements, click **Custom** to create a user group.

User information setting: Configure user information, which is optional.

Advance setting:

o **Voucher code type:** Set the value to Alphanumeric 0-9, a-z, Alphabetic a-z, or Numeric 0-9.

Advance Setting ^

Voucher code type

Alphanumeric 0-9, a-z

Voucher length

Alphanumeric 0-9, a-z

Alphabetic a-z

Numeric 0-9

Cancel

OK

- o **Voucher length:** Select the voucher length. The value ranges from 6 to 9.

Voucher length

6

6

7

8

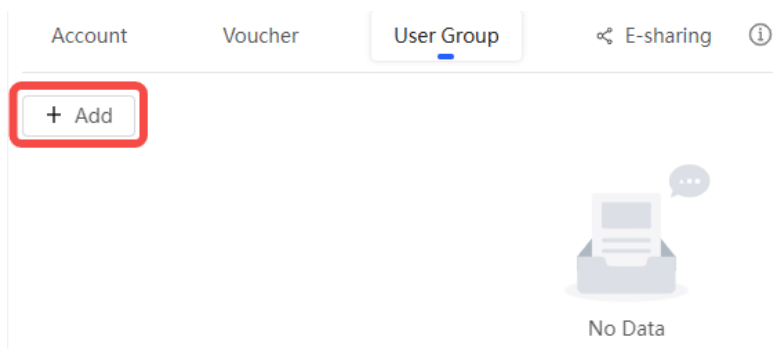
9

- (4) Obtain the voucher code from the voucher list.

5. (Optional) Adding an Account

If the Login Options is **Account**, you should add accounts as the following steps.

- (1) Log in to Ruijie Cloud, choose **Project > Authentication > User Management**, and select a network in this account.
- (2) Configure a user group.
 - a On the **User Group** tab, click **Add**.



- b Configure user group parameters. After the configuration, click **OK**.

Add user group
✕

* User group name

User Group Policy

Price

Concurrent devices ▼

Period ▼

Quota ⓘ ▼

Maximum upload rate ▼

Maximum download rate ▼

Bind MAC on first use

User Group Name: indicates the user group name.

Price: indicates the price of the user group. Mark user groups by numeral. The current version has no impact on network usage.

Concurrent Devices: indicates the number of concurrent devices for one account.

Period: indicates the maximum validity time of an account. The maximum value is counted after the client passes authentication and successfully accesses the Internet.

Quota: indicates the maximum amount of data transfer.

Maximum upload rate: indicates the maximum upload rate.

Maximum download rate: indicates the maximum download rate.

Bind MAC on first use: indicates that the MAC address of the first device used will be bound and other devices used by the same user will be prohibited from accessing the Internet.

(3) On the **Account** tab, add an account. Accounts can be added manually or through batch import.

- Adding an account manually

Click **Add an Account**, set parameters about the account, and click **OK**.

Add account X

* User name

* Password

* User group

Allow VPN connection

Tips: By enabling this option, the user can use this account to log in remotely using a VPN.

User information setting ▼

User name: The value is a string of less than 32 characters, consisting of letters, numerals, and underscores.

Password: The value is a string of less than 32 characters, consisting of letters, numerals, and underscores.

User group: Select a created user group from the drop-down list. If the created user group does not meet the requirements, click Custom to create a user group.

Allow VPN connection: By enabling this option, the user can use this account to log in remotely using a VPN.


User information setting: You can expand it to have more user information displayed, including the first name, last name, email, phone number, and alias.

- Adding accounts through batch import
 - a Click **Bulk import**.

Bulk import accounts X

Step1: Download and fill in the device information in the template. Up to 500 records can be imported each time.

Account and Password fields are required. Please enter less than 32 characters, consisting of letters, numbers or underscores.



- b Click **Download Template** to download the template.
 - c Edit the template and save it.

Note

- **Account, Password, and User Group** are mandatory.
- Check that the user group already exists and the added accounts are not duplicate with existing accounts.

Account	Password	First name	Last name	Alias	User group	Email
test2	test2				test	
test3	test3				test	
test4	test4				test	

d Click **Please select an .xls or .xlsx file** to upload the file. After uploading, users are automatically created.

The screenshot shows a user management interface with a table of accounts. The table has columns for Account, Password, User group, Status, Period, First name, Alias, Created at, Activated at, and Operation. Three accounts are listed: test3, test4, and test2, all with a status of 'Not used' and a period of '30Minutes'. The 'First name' and 'Alias' fields are empty. The 'Created at' and 'Activated at' fields show dates and times. The 'Operation' column contains icons for edit, delete, and refresh. At the bottom right, it says '3 in total' and '10 / page'.

4.10.3 Configuring an Authentication-Free Account on Eweb Management System

1. Configuring an Authentication-Free Account

The authentication-free user can access the Internet without authentication.

Choose **Network-Wide > Workspace > Wireless > Wireless Auth > Allowlist**.

- (1) Click **User Allowlist**.
- (2) Click **Add**.

The screenshot shows the 'User Allowlist' configuration page. At the top, there is a note: 'A user configured with allowlisted IP or MAC address can access the Internet without authentication.' Below this, there are four tabs: 'User Allowlist', 'IP Allowlist', 'Domain Allowlist', and 'MAC Blocklist/Allowlist'. The 'User Allowlist' tab is selected. On the right side, there are two buttons: '+ Add' (highlighted with a red box) and 'Delete Selected'. Below the buttons, it says 'Up to 50 entries can be added.' There is a table with columns 'IP / IP Range' and 'Action'. The table is currently empty, showing 'No Data'. At the bottom right, it says 'Total 0' and '10/page'.

- (3) Configure the IP address or IP address range for authentication-free users.

Add ×

* IP / IP Range

(4) Click **OK**.

2. Configuring Authentication-Free External IP Addresses

After configuration, the user can access the authentication-free external IP address without authentication.

Choose **Network-Wide > Workspace > Wireless > Wireless Auth > Allowlist**.

(1) Click **IP Allowlist**.

(2) Click **Add**.

i A user configured with allowlisted IP or MAC address can access the Internet without authentication.

IP Allowlist

Up to 50 entries can be added.

<input type="checkbox"/>	IP / IP Range	Action
No Data		

Total 0

(3) Configure authentication-free external IP address or IP address range.

Add ×

* IP / IP Range

(4) Click **OK**.

3. Configuring a Domain Allowlist

The user can access the URL in the domain allowlist without authentication.

(1) Choose **Network-Wide > Workspace > Wireless > Wireless Auth > Allowlist**.

(2) Click **Domain Allowlist**.

(3) Click **Add**.

Cloud Integration **Allowlist** Client List

i A user configured with whitelisted IP or MAC address can access the Internet without authentication.

User Allowlist IP Allowlist **Domain Allowlist** MAC Blocklist/Allowlist

Domain Allowlist + Add Delete Selected

Up to **100** entries can be added.

<input type="checkbox"/>	URL	Action
No Data		

< **1** > 10/page Total 0

(4) Configure authentication-free domains.

Add ×

* URL

Cancel OK

(5) Click **OK**.

4. Configuring a MAC Address Blocklist and Allowlist

After configuration, the STA with an Allowlist MAC address can access the Internet without authentication while the STA with a blocklist MAC address is forbidden to access the Internet.

- (1) Choose **Network-Wide > Workspace > Wireless > Wireless Auth > Allowlist**.
- (2) Click **MAC Blocklist/Allowlist**.
- (3) Configure a MAC address allowlist.
 - a Click **Add** on the **MAC Allowlist** page.

i A user configured with allowlisted IP or MAC address can access the Internet without authentication.

User Allowlist IP Allowlist Domain Allowlist **MAC Blocklist/Allowlist**

MAC Allowlist + Add Delete Selected

Up to **250** entries can be added.

<input type="checkbox"/>	MAC Address	Action
No Data		

Total 0 < **1** > 10/page

- b Add the MAC address to the allowlist.

Add
×

* MAC Address

- c Click **OK**.
- (4) Configure a MAC address blacklist.
 - a Click **Add** on the **MAC Blacklist** page.

MAC Blacklist

Up to **250** entries can be added.

	MAC Address	Action
<input type="checkbox"/>		

No Data

Total 0 < 1 > 10/page ▾

- b Add the MAC address to the blacklist.

Add
×

* MAC Address

- c Click **OK**.

4.10.4 Checking Authentication User List Eweb Management System

Check authentication users in the list view.

Choose **Network-Wide > Workspace > Wireless > Wireless Auth > Client List**.

Client List

i The client going offline will not disappear immediately. Instead, the client will stay in the list for 5 more minutes.

	Username	IP	MAC Address	Online Time	Auth Type	Connect the SSID	Access Name	Action
<input type="checkbox"/>								

No Data

Total 0 < 1 > 10/page ▾

Click **Offline** in the **Action** column to disconnect users to release network resources.

4.11 Configuring SNMP

Note

This feature is only supported on RG-EG105G-V3, RG-EG105G-P-V3, RG-EG210G-P-V3, RG-EG1510XS, RG-EG3XX series devices (such as RG-EG310GH-E), RG-EG105GW-X and RG-EG205GW.

4.11.1 Overview

The Simple Network Management Protocol (SNMP) is a protocol for managing network devices. Based on the client/server model, it can achieve remote monitoring and control of network devices.

SNMP uses a manager and agent architecture. The manager communicates with agents through the SNMP protocol to retrieve information such as device status, configuration details, and performance data. It can also be used to configure and manage devices.

SNMP can be used to manage various network devices, including routers, switches, servers, firewalls, etc. You can achieve user management through the SNMP configuration interface and monitor and control devices through the third-party software.

4.11.2 Global Configuration

1. Overview

The purpose of global configuration is to enable the SNMP service and make the SNMP protocol version (v1/v2c/v3) take effect, so as to achieve basic configuration of local port, device location, and contact information.

SNMP v1: As the earliest version of SNMP, SNMP v1 has poor security, and only supports simple community string authentication. SNMP v1 has certain flaws, such as plaintext transmission of community strings and vulnerability to attacks. Therefore, SNMP v1 is not recommended for modern networks.

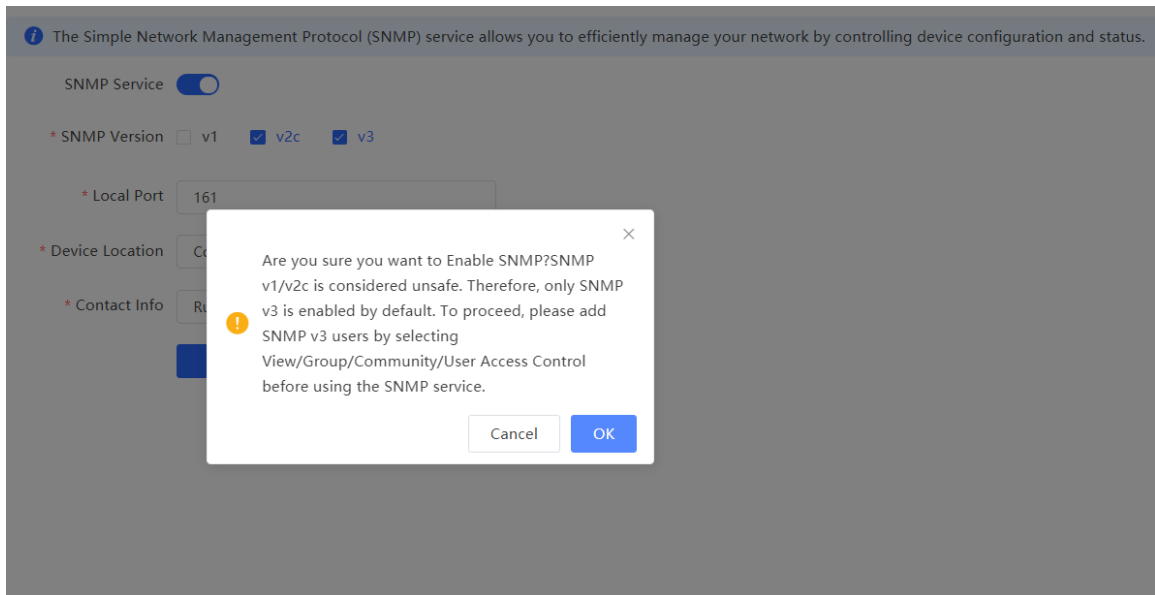
SNMP v2c: As an improved version of SNMP v1, SNMP v2c supports richer functions and more complex data types, with enhanced security. SNMP v2c performs better than SNMP v1 in terms of security and functionality, and is more flexible. It can be configured according to different needs.

SNMP v3: As the newest version, SNMP v3 supports security mechanisms such as message authentication and encryption compared to SNMP v1 and SNMP v2c. SNMP v3 has achieved significant improvements in security and access control.

2. Configuration Steps

Choose **Network-Wide > Workspace > Network-Wide > SNMP > Global Config**

(1) Enable the SNMP service.



When it is enabled for the first time, SNMP v3 is enabled by default. Click **OK**.

(2) Set SNMP service global configuration parameters.

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

Table 4-21 Global Configuration Parameters

Parameter	Description
SNMP Server	Indicates whether SNMP service is enabled.
SNMP Version	Indicates the SNMP protocol version, including v1, v2c, and v3 versions.
Local Port	The port range is 1 to 65535.
Device Location	1-64 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.
Contact Info	1-64 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.

(3) Click **Save**.

After the SNMP service is enabled, click **Save** to make basic configurations such as the SNMP protocol version number take effect.

4.11.3 View/Group/Community/User Access Control

1. Configuring Views

- Overview

Management Information Base (MIB) can be regarded as a database storing the status information and performance data of network devices. It contains a large number of object identifiers (OIDs) to identify the status information and performance data of these network devices.

Views in SNMP can limit the range of MIB nodes that the management system can access, thereby improving the security and reliability of network management. Views are an indispensable part of SNMP and need to be configured or customized according to specific management requirements.

A view can have multiple subtrees. The management system can only access MIB nodes in these subtrees, and cannot access other unauthorized MIB nodes. This can prevent unauthorized system administrators from accessing sensitive MIB nodes, thereby protecting the security of network devices. Moreover, views can also improve the efficiency of network management and speed up the response from the management system.

- Configuration Steps

Choose **Network-Wide > Workspace > Network-Wide > SNMP > View/Group/Community/Client Access Control**.

(1) Click **Add** under the **View List** to add a view.

View List

+ Add
Delete Selected

	View Name	Action
<input type="checkbox"/>	all	
<input type="checkbox"/>	none	
<input type="checkbox"/>	public_view	Edit Delete
<input type="checkbox"/>	system	Edit Delete

Up to 20 entries can be added.
Total 4 1 > 10/page

(2) Configure basic information of a view.

Add
×

* View Name

OID

Add Included Rule
Add Excluded Rule

Rule/OID List
Delete Selected

Up to **100** entries are allowed.

	Rule	OID	Action
<input type="checkbox"/>			
No Data			

Total 0
<
1
>
Go to page

Cancel
OK

Table 4-22 View Configuration Parameters

Parameter	Description
View Name	Indicates the name of the view. 1-32 characters. Chinese or full width characters are not allowed.
OID	Indicates the range of OIDs included in the view, which can be a single OID or a subtree of OIDs.
Type	There are two types of rules: included and excluded rules. <ul style="list-style-type: none"> ● The included rule only allows access to OIDs within the OID range. Click Add Included Rule to set this type of view. ● Excluded rules allow access to all OIDs except those in the OID range. Click Add Excluded Rule to configure this type of view.

Note

A least one OID rule must be configured for a view. Otherwise, an alarm message will appear.

(3) Click **OK**.

2. Configuring v1/v2c Users

- Overview

When the SNMP version is set to v1/v2c, user configuration is required.

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

- Configuration Steps

Choose **Network-Wide > Workspace > Network-Wide > SNMP > View/Group/Community/Client Access Control**.

(1) Click **Add** in the **SNMP v1/v2c Community Name List** pane.

SNMP v1/v2c Community Name List

<input type="checkbox"/>	Community Name	Access Mode	MIB View	Action
<input type="checkbox"/>	snmp_v2c_group	Read-Only	all	Edit Delete

Up to 20 entries can be added.

Total 1 10/page

(2) Add a v1/v2c user.

Add
×

* Community Name

* Access Mode Read-Only ▼

* MIB View all ▼ Add View +

Cancel
OK

Table 4-23 v1/v2c User Configuration Parameters

Parameter	Description
Community Name	<ul style="list-style-type: none"> ● At least 8 characters. ● It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. ● Admin, public or private community names are not allowed. ● Question marks, spaces, and Chinese characters are not allowed.
Access Mode	Indicates the access permission (read-only or read & write) for the community name.
MIB View	The options under the drop-down box are configured views (default: all, none).

Note

- Community names cannot be the same among v1/v2c users.
- Click **Add View** to add a view.

3. Configuring v3 Groups

- Overview

SNMP v3 introduces the concept of grouping to achieve better security and access control. A group is a group of SNMP users with the same security policies and access control settings. With SNMP v3, multiple groups can be configured, each with its own security policies and access control settings. Each group can have one or more users.

- Prerequisites

When the SNMP version is set to v3, the v3 group configuration is required.

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

[Save](#)

 Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

● Configuration Steps

Choose **Network-Wide > Workspace > Network-Wide > SNMP > View/Group/Community/Client Access Control**.

(1) Click **Add** in the **SNMP v3 Group List** pane to create a group.

SNMP v3 Group List ▼

[+ Add](#) [Delete Selected](#)

<input type="checkbox"/>	Group Name	Security Level	Read-Only View	Read & Write View	Notification View	Action
<input type="checkbox"/>	default_group	Auth & Security	all	none	none	Edit Delete

Up to 20 entries can be added.

Total 1 < **1** > 10/page ▼

(2) Configure v3 group parameters.

Add
×

* Group Name

* Security Level Allowlist & Security

* Read-Only View all Add View +

* Read & Write View all Add View +

* Notification View none Add View +

Cancel
OK

Table 4-24 v3 Group Configuration Parameters

Parameter	Description
Group Name	Indicates the name of the group. <ul style="list-style-type: none"> ● 1-32 characters. ● Chinese characters, full-width characters, question marks, and spaces are not allowed.
Security Level	Indicates the minimum security level (authentication and encryption, authentication but no encryption, no authentication and encryption) of the group.
Read-Only View	The options under the drop-down box are configured views (default: all, none).
Read & Write View	The options under the drop-down box are configured views (default: all, none).
Notify View	The options under the drop-down box are configured views (default: all, none).

Note

- A group defines the minimum security level, read and write permissions, and scope for users within the group.
- The group name must be unique. To add a view, click **Add View**.

(3) Click **OK**.

4. Configuring v3 Users

- Prerequisites

When the SNMP version is set to v3, the v3 group configuration is required.

SNMP Service * SNMP Version v1 v2c v3* Local Port * Device Location * Contact Info **Note**

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

● Configuration Steps

Choose **Network-Wide > Workspace > Network-Wide > SNMP > View/Group/Community/Client Access Control**.

(1) Click **Add** in the **SNMP v3 Client List** pane to add a v3 user.

SNMP v3 Client List

<input type="checkbox"/>	Username	Group Name	Security Level	Auth Protocol	Auth Password	Encryption Protocol	Encrypted Password	Action
No Data								

Up to 50 entries can be added. Total 0 < **1** > 10/page

(2) Configure v3 user parameters.

Add
×

* Username

* Group Name

* Security Level

* Auth Protocol * Auth Password

* Encryption Protocol * Encrypted Password

Table 4-25 v3 User Configuration Parameters

Parameter	Description
Username	<ul style="list-style-type: none"> ● At least 8 characters. ● It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. ● Admin, public or private community names are not allowed. ● Question marks, spaces, and Chinese characters are not allowed.
Group Name	Indicates the group to which the user belongs.
Security Level	Indicates the security level (authentication and encryption, authentication but no encryption, and no authentication and encryption) of the user.
Auth Protocol, Auth Password	<p>Authentication protocols supported: MD5/SHA/SHA224/SHA256/SHA384/SHA512.</p> <p>Authentication password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.</p> <p>Note: This parameter is mandatory when the security level is authentication and encryption, or authentication but no encryption.</p>

Parameter	Description
Encryption Protocol, Encryption Password	<p>Encryption protocols supported: DES/AES/AES192/AES256.</p> <p>Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.</p> <p>It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.</p> <p>Note: This parameter is mandatory when the security level is authentication and encryption.</p>

 Note

- The security level of v3 users must be greater than or equal to that of the group.
- There are three security levels, among which authentication and encryption requires the configuration of authentication protocol, authentication password, encryption protocol, and encryption password. Authentication but no encryption only requires the configuration of authentication protocol and encryption protocol, while no authentication and encryption does not require any configuration.

4.11.4 SNMP Service Typical Configuration Examples

1. Configuring SNMP v2c

- Application Scenario

You only need to monitor the device information, but do not need to set and deliver it. A third-party software can be used to monitor the data of nodes like 1.3.6.1.2.1.1 if v2c version is configured.

- Configuration Specification

According to the user's application scenario, the requirements are shown in the following table:

Table 4-26 User Requirement Specification

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1.1, and the custom view name is "system".
Version	For SNMP v2c, the custom community name is "snmp_v2c_group", and the default port number is 161.
Read & write permission	Read-only permission.

- Configuration Steps

(1) In the global configuration interface, select v2c and set other settings as default. Then, click **Save**.

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

Save

(2) Add a view on the **View/Group/Community/Client Access Control** interface.

- a Click **Add** in the **View List** pane to add a view.
- b Enter the view name and OID in the pop-up window, and click **Add Included Rule**.

Add ×

* View Name

OID

Rule/OID List

Up to **100** entries are allowed.

<input type="checkbox"/>	Rule	OID	Action
<input type="checkbox"/>	Included	.1.3.6.1.2.1.1	Delete

Total 1 Go to page

c Click **OK**.

(3) On the View/Group/Community/Client Access Control interface, enter the SNMP v1/v2c community name.

- a Click **Add** in the **SNMP v1/v2c Community Name List** pane.
- b Enter the group name, access mode, and view in the pop-up window.

Add



* Community Name

* Access Mode

* MIB View [Add View +](#)

Cancel

OK

c Click **OK**.

2. Configuring SNMP v3

- Application Scenario

You need to monitor and control devices, and use the third-party software to monitor and deliver device information to public nodes (1.3.6.1.2.1). The security level of v3 is authentication and encryption.

- Configuration Specification

According to the user's application scenario, the requirements are shown in the following table:

Table 4-27 User Requirement Specification

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1, and the custom view name is "public_view".
Group configuration	Group name: group Security level: authentication and encryption Select public_view for a read-only view. Select public_view for a read & write view. Select none for a notify view.
Configuring v3 Users	User name: snmp_v3_user Group name: default_group Security level: authentication and encryption Authentication protocol/password: MD5/Ruijie123 Encryption protocol/password: AES/Ruijie123
Version	For SNMP v3, the default port number is 161.

- Configuration Steps

- (1) On the global configuration interface, select v3, and change the port number to 161. Set other settings to defaults. Then, click **Save**.

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

Save

- (2) Add a view on the **View/Group/Community/Client Access Control** interface.

- a Click **Add** in the **View List** pane.
- b Enter the view name and OID in the pop-up window, and click **Add Included Rule**.

Add ×

* View Name

OID

Add Included Rule **Add Excluded Rule**

Rule/OID List Delete Selected

Up to **100** entries are allowed.

<input type="checkbox"/>	Rule	OID	Action
<input type="checkbox"/>	Included	.1.3.2.6.1.2.1	Delete

Total 1

Cancel **OK**

- c Click **OK**.

- (3) On the View/Group/Community/Client Access Control interface, add an SNMP v3 group.
- Click **Add** in the **SNMP v3 Group List** pane.
 - Enter the group name and security level on the pop-up window. As this user has read and write permissions, select `public_view` for read-only and read & write views, and select none for notify views.

Add ×

* Group Name

* Security Level ▾

* Read-Only View ▾ [Add View +](#)

* Read & Write View ▾ [Add View +](#)

* Notification View ▾ [Add View +](#)

- Click **OK**.
- (4) On the View/Group/Community/Client Access Control interface, add an SNMP v3 user.
- Click Add in the SNMP v3 Client List pane.
 - Enter the user name and group name in the pop-up window. As the user's security level is authentication and encryption, enter the authentication protocol, authentication password, encryption protocol, and encryption password.

Add
✕

* Username

* Group Name

* Security Level

* Auth Protocol * Auth Password

* Encryption Protocol * Encrypted Password

c Click **OK**.

4.11.5 Configuring Trap Service

Trap is a notification mechanism of the Simple Network Management Protocol (SNMP) protocol. It is used to report the status and events of network devices to administrators, including device status, faults, performance, configuration, and security management. Trap provides real-time network monitoring and fault diagnosis services, helping administrators discover and solve network problems in a timely manner.

1. Enabling Trap Service

Enable the trap service and select the effective trap version, including v1, v2c, and v3 versions.

Choose **Network-Wide > Workspace > Network-Wide > SNMP > Trap Setting**

(1) Enable the trap service.

When the trap service is enabled for the first time, the system will pop up a prompt message. Click **OK**.

Trap Service

* Trap Version v1 v2c v3

[Save](#)

(2) Set the trap version.

The trap versions include v1, v2c, and v3.

(3) Click **OK**.

After the trap service is enabled, click **Save** for the configuration to take effect.

2. Configuring Trap v1/v2c Users

● Overview

Trap is a notification mechanism that is used to send alerts to administrators when important events or failures occur on devices or services. Trap v1/v2c are two versions in the SNMP protocol for network management and monitoring.

Trap v1 is the first version that supports basic alert notification functionality. Trap v2c is the second version, which supports more alert notification options and advanced security features.

By using trap v1/v2c, administrators can promptly understand problems on the network and take corresponding measures.

● Prerequisites

Once trap v1 and v2c versions are selected, it is necessary to add trap v1/v2c users.

● Procedure

Choose **Network-Wide > Workspace > Network-Wide > SNMP > Trap Setting**

(1) Click **Add** in the **Trap v1/v2c Client List** pane to add a trap v1/v2c user.

Trap v1/v2c Client List [+ Add](#) [Delete Selected](#)

Up to **20** entries are allowed.

<input type="checkbox"/>	Dest Host IP	Version Number	Port ID	Community Name	Action
No Data					

Total 0

(2) Configure trap v1/v2c user parameters.

Add
×

* Dest Host IP

* Version Number

* Port ID

* Community

Name/Username

Table 4-28 Trap v1/v2c User Configuration Parameters

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.
Version Number	Trap version, including v1 and v2c.
Port ID	The port range of the trap peer device is 1 to 65535.
Community name/User name	<p>Community name of the trap user.</p> <p>At least 8 characters.</p> <p>It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.</p> <p>Admin, public or private community names are not allowed.</p> <p>Question marks, spaces, and Chinese characters are not allowed.</p>

 Note

- The destination host IP address of trap v1/ v1/v2c users cannot be the same.
- Community names of trap v1/ v1/v2c users cannot be the same.

(3) Click **OK**.

1. Configuring Trap v3 Users

- Overview

Trap v3 is a network management mechanism based on the SNMP protocol. It is used to send alert notifications to administrators. Unlike previous versions, trap v3 provides more secure and flexible configuration options, including authentication and encryption features.

Trap v3 offers custom conditions and methods for sending alerts, as well as the recipients and notification methods for receiving alerts. This enables administrators to have a more accurate understanding of the status of network devices and to take timely measures to ensure the security and reliability of the network.

- Prerequisites

When the v3 version is selected for the trap service, it is necessary to add a trap v3 user.

- Configuration Steps

Choose **Network-Wide > Workspace > Network-Wide > SNMP > Trap Setting**

(1) Click **Add** in the **Trap v3 User** pane to add a trap v3 user.

(2) Configure trap v3 user parameters.

Table 4-29 Trap v3 User Configuration Parameters

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.

Parameter	Description
Port ID	The port range of the trap peer device is 1 to 65535.
Username	Name of the trap v3 user. <ul style="list-style-type: none"> ● At least 8 characters. ● It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. ● Admin, public or private community names are not allowed. ● Question marks, spaces, and Chinese characters are not allowed.
Security Level	Indicates the security level of the trap v3 user. The security levels include authentication and encryption, authentication but no encryption, and no authentication and encryption.
Auth Protocol, Auth Password	Authentication protocols supported: MD5/SHA/SHA224/SHA256/SHA384/SHA512. Authentication password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption, or authentication but no encryption.
Encryption Protocol, Encryption Password	Encryption protocols supported: DES/AES/AES192/AES256. Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption.

 Note

The destination host IP address of trap v1/ v1/v2c users cannot be the same.

4.11.6 Trap Service Typical Configuration Examples

1. Configuring Trap v2c

- Application Scenarios

During device monitoring, if the device is suddenly disconnected or encounters an abnormality, and the third-party monitoring software cannot detect and handle the abnormal situation in a timely manner, you can configure the device with a destination IP address of 192.168.110.85 and a port number of 166 to enable the device to send a v2c trap in case of an abnormality.

- Configuration Specification

According to the user's application scenario, the requirements are shown in the following table:

Table 4-30 User Requirement Specification

Item	Description
IP address and port number	The destination host IP is 192.168.110.85, and the port number is 166.
Version	Select the v2 version.
Community name/User name	Trap_user

● Configuration Steps

(1) Select the v2c version in the **Trap Setting** interface and click **Save**.

Trap Service

* Trap Version v1 v2c v3

Save

Trap v1/v2c Client List **+ Add**

Up to 20 entries are allowed.

<input type="checkbox"/>	Dest Host IP	Version Number	Port ID	Community Name	Action
No Data					

Total 0

(2) Click **Add** in the Trap v1/v2c Client List to add a trap v2c user.

(3) Enter the destination host IP address, version, port number, user name, and other information. Then, click **OK**.

Add ×

* Dest Host IP

* Version Number

* Port ID

* Community Name/Username

2. Configuring Trap v3

- Application Scenarios

During device monitoring, if the device is suddenly disconnected or encounters an abnormality, and the third-party monitoring software cannot detect and handle the abnormal situation in a timely manner, you can configure the device with a destination IP address of 192.168.110.87 and a port number of 167 to enable the device to send a v3 trap, which is a safer trap compared with v1/v2c traps.

- Configuration Specification

According to the user's application scenario, the requirements are shown in the following table:

Table 4-31 User Requirement Specification

Item	Description
IP address and port number	The destination host IP is 192.168.110.87, and the port number is 167.
Version and user name	Select the v3 version and trapv3_user for the user name.
Authentication protocol/authentication password	Authentication protocol/password: MD5/Ruijie123
Encryption protocol/encryption password	Encryption protocol/password: AES/Ruijie123

- Configuration Steps

(1) Select the v3 version in the **Trap Setting** interface and click **Save**.

The screenshot shows the 'Trap Setting' interface. At the top, there is a 'Trap Service' toggle switch which is turned on. Below it, the '* Trap Version' section has three radio button options: 'v1', 'v2c', and 'v3'. The 'v3' option is selected and highlighted with a red box. A blue 'Save' button is located below the radio buttons.

Below the 'Save' button is the 'Trap v3 Client List' section. It features a '+ Add' button (highlighted with a red box) and a 'Delete Selected' button. A light blue banner indicates 'Up to 20 entries are allowed.' Below this is a table with the following columns: Dest Host IP, Port ID, Username, Security Level, Auth Password, Encrypted Password, and Action. The table is currently empty, with 'No Data' displayed below it. At the bottom of the interface, there is a pagination control showing 'Total 0', a dropdown for '10/page', a page number '1' in a blue box, and a 'Go to page' field with '1' entered.

(2) Click **Add** in the Trap v3 Client List to add a trap v3 user.

(3) Enter the destination host IP address, port number, user name, and other information. Then, click **OK**.

Add
×

* Dest Host IP <input style="width: 90%;" type="text" value="192.168.110.87"/>	* Port ID <input style="width: 90%;" type="text" value="167"/>
* Username <input style="width: 90%;" type="text" value="trap_v3_user"/>	* Security Level <input style="width: 90%;" type="text" value="Auth & Security"/>
* Auth Protocol <input style="width: 90%;" type="text" value="MD5"/>	* Auth Password <input style="width: 90%;" type="text" value="Ruijie123"/>
* Encryption Protocol <input style="width: 90%;" type="text" value="AES"/>	* Encrypted Password <input style="width: 90%;" type="text" value="Ruijie123"/>

4.12 Configure IEEE 802.1X authentication

i Note

This feature is only supported on RG-EG310G-E, RG-EG305GH-E, RG-EG310GH-E, RG-EG105GW-X and RG-EG205GW.

4.12.1 Overview

IEEE 802.1X is a port-based network access control standard that provides secure access services for LANs.

On an IEEE 802 LAN, a user can directly access network resources without authentication and authorization as long as it can connect to a network device. This uncontrolled behavior can bring security risks to the network. The IEEE 802.1X protocol was proposed to address the security issues on an IEEE 802 LAN.

The IEEE 802.1X protocol supports three security applications: Authentication, Authorization, and Accounting, abbreviated as AAA.

- Authentication: Determines whether a user can obtain access, and restricts unauthorized users.
- Authorization: Authorizes services available for authorized users, and controls the permissions of unauthorized users.
- Accounting: Records the usage of network resources by users, and provides a basis for traffic billing.

The 802.1X feature can be deployed on networks to control user authentication, authorization, and more.

An 802.1X network uses a typical client/server architecture, consisting of three entities: client, access device, and authentication server. A typical architecture is shown here.

Figure 4-1 Typical Architecture of 802.1X Network



- The client is usually an endpoint device which can initiate 802.1X authentication through the client software. The client must support the Extensible Authentication Protocol over LANs (EAPoL) on the local area network.
- The access device is usually a network device (AP or switching device) that supports the IEEE 802.1X protocol. It provides an interface for clients to access the local area network, which can be a physical or a

logical interface.

Note

- The RG-EG gateway device itself does not support the IEEE 802.1X authentication, and can only serve as the primary device to support 802.1X global configuration and deliver the configuration to APs and switching devices on the entire network.
- To achieve IEEE 802.1X authentication, ensure that the network includes an AP or switching device.
- The authentication server can realize user authentication, authorization, and accounting. Usually a RADIUS server is used as the authentication server.

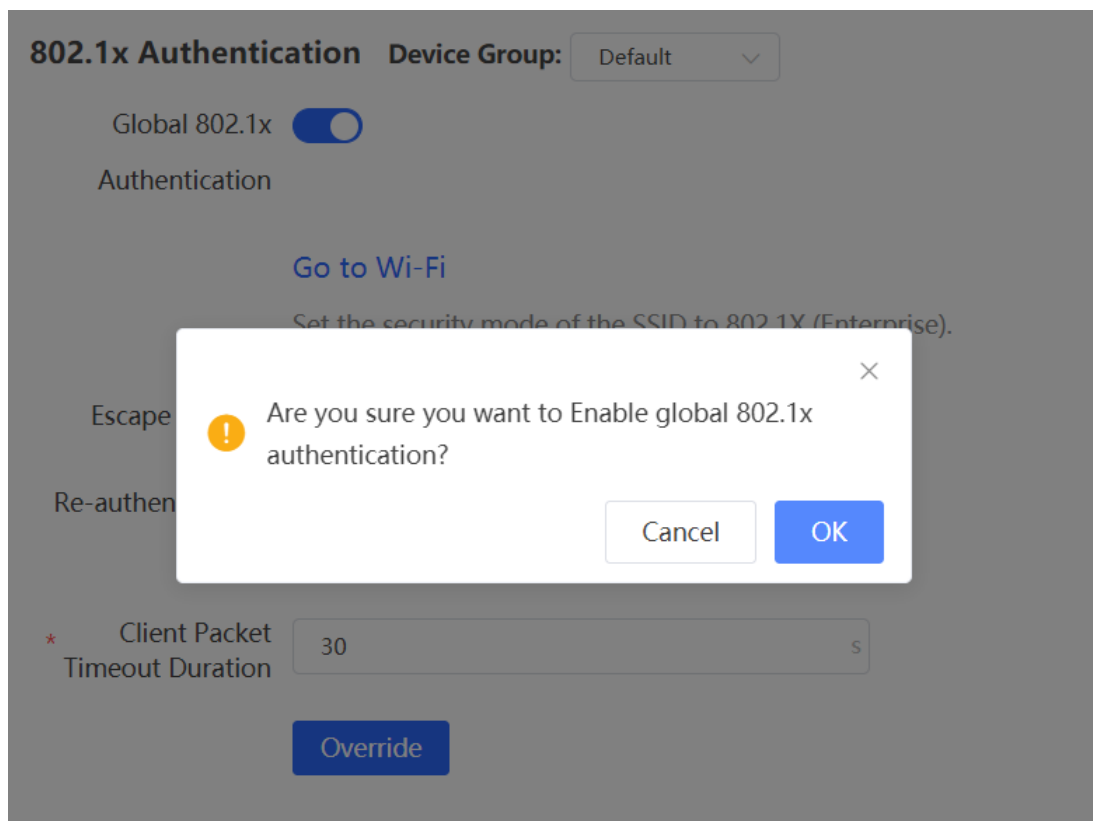
4.12.2 Configuring 802.1X Globally

The gateway device supports the 802.1X global configuration, and can synchronously deliver the configuration to APs and switching devices on the network.

Choose **Network-Wide > Workspace > Wireless > 802.1x Authentication**.

- (1) Click the **802.1x Authentication** tab to configure global configuration for 802.1x wireless authentication.
- (2) Select the authentication device group, and enable the global 802.1x authentication.

You will be prompted to enable this feature or not. Click **Yes**.



- (3) Click **Go to Wi-Fi**, and set the encryption method of SSID to **802.1x (Enterprise)**.

802.1x Authentication Device Group: Default

Global 802.1x

Authentication

[Go to Wi-Fi](#)
Set the security mode of the SSID to 802.1X (Enterprise).

Escape SSID

Re-authentication

* Client Packet Timeout Duration

Edit

×

* SSID

Purpose | |

Band 2.4G 5G

No available frequency band? Log in to Ruijie Cloud to add or re-identify the target frequency band. [Re-identify](#) [View Causes](#)

Encryption Open Security 802.1x (Enterprise)

* Security

Server Group [Edit](#)

----- advanced Setting -----

(4) Configure global parameters.

802.1x Authentication Device Group:

Global 802.1x

Authentication

[Go to Wi-Fi](#)

Set the security mode of the SSID to 802.1X (Enterprise).

Escape SSID ?

Re-authentication

?

* Client Packet Timeout Duration s

Override

Parameter	Description
Escape SSID	Once this feature is enabled, when the authentication server is unavailable, the system will create a temporary Wi-Fi network for users. If this function is enabled, it is necessary to set the Escape SSID, encryption type, and Wi-Fi password.
Re-authentication	Once this feature is enabled, the system regularly re-authenticates users. Users who do not match the information on the server will be automatically disconnected. If this function is enabled, it is necessary to set the re-authentication cycle, which is 3600 seconds by default.
Client Packet Timeout Duration	The timeout period for the switching device to wait for the authentication server to send an EAP response message. The default value is 30 seconds.

(5) Click **Override**.

4.12.3 Configuring the RADIUS Server

1. Prerequisites

Before configuration, ensure that the RADIUS server is ready, and that the IP address and shared key of the RADIUS server are configured.

2. Configuration Steps

Choose **Network-Wide > Workspace > Wireless > 802.1x Authentication**

- (1) Click the **RADIUS Server Management** tab.
- (2) Click **Add Server** to configure related server parameters.

RADIUS Server Management Add Server Group

Server Group Name	Server IP	Auth Port	Accounting Port	Shared Password	Action
No Data					

Up to 20 entries can be added.

Add ×

* Server Group Name

🗑 Server 1

* Server IP

* Server Name

* Auth Port

* Accounting Port

* Shared Password

* Match Order

⊕ Add Server

Table 4-32 Description of RADIUS Server Management Configuration

Parameter	Description
Server IP	IP address of the RADIUS server.
Auth Port	The port number for the RADIUS server to perform user authentication.
Accounting Port	The port number for the RADIUS server to perform user accounting.
Shared Password	Shared key of the RADIUS server.
Match Order	The system supports up to five RADIUS servers. A larger value indicates a higher priority.

- (3) Enter the server global configuration parameters, and click **Save**.

Server global configuration

Proxy Server

* Packet Retransmission Interval s

* Packet Retransmission Count time

Server Detection

MAC Address Format

Save

Table 4-33 Description of Server Global Configuration

Parameter	Description
Proxy Server	After this function is enabled, local device will act as a proxy for the RADIUS server to send RADIUS messages.
Packet Retransmission Interval	Configure the interval during which the device sends a request to a RADIUS server before confirming that the RADIUS server is unreachable.
Packet Retransmission Count	Configure the number of times that the device sends requests to a RADIUS server before confirming that the RADIUS server is unreachable.
Server Detection	If this function is enabled, it is necessary to set the server detection cycle, server detection times, and server detection username. Determines the server status and whether to enable functions such as the escape function.
MAC Address Format	Configure the format of the MAC address used in attribute 31 (Calling-Station-ID) of a RADIUS message. The following formats are supported: <ul style="list-style-type: none"> ● Dotted hexadecimal format. For example, 00d0.f8aa.bbcc. ● IETF format. For example: 00-D0-F8-AA-BB-CC. ● Unformatted (default). For example: 00d0f8aabbcc

4.12.4 Checking Authentication User List

When the 802.1x feature is configured on the entire network, and a terminal is authenticated and connected to the network, you can view the list of authenticated users.

Choose **Network-Wide > Workspace > Wireless > 802.1x Authentication**

Click **Wireless User List** or **Wired User List** to view specific user information.

i The client going offline will not disappear immediately. Instead, the client will stay in the list for a more minutes.

Wireless User List **Refresh** **Batch Logout**

<input type="checkbox"/>	Name	IP	MAC Address	Online Time	Connect SSID	Access Name	Action
No Data							

Total 0 < **1** > 10/page

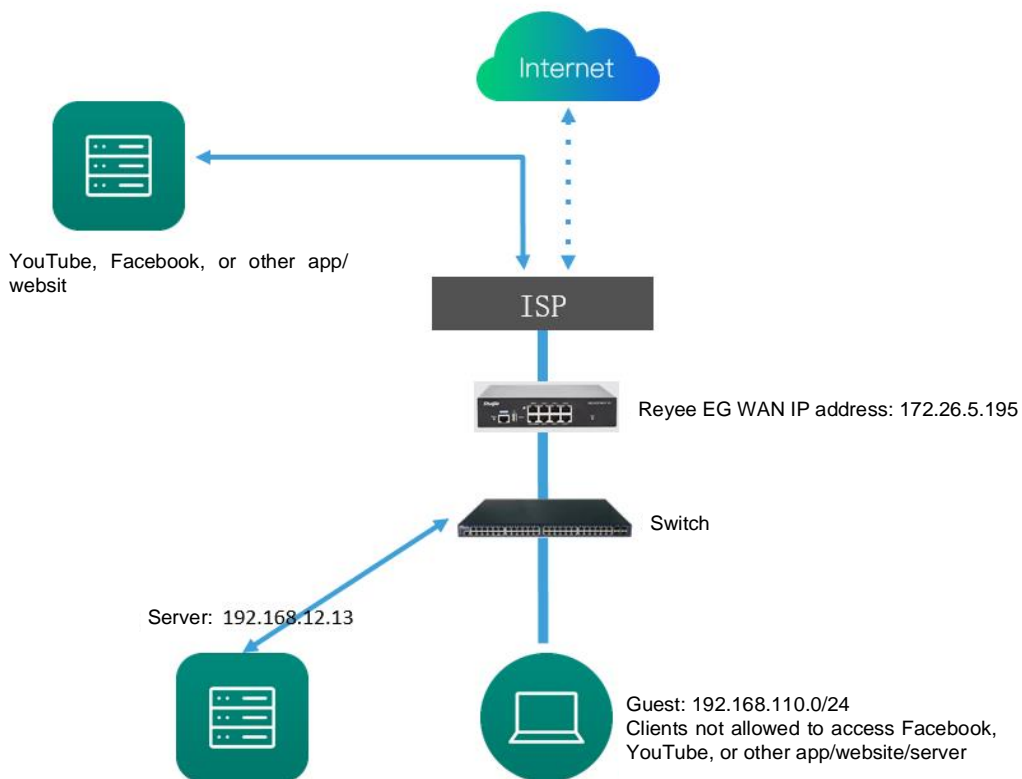
Click **Refresh** to view the latest user list.

If you want to disconnect a user from the network, select the user and click **Logout** under the **Action** column. You can also select multiple users and click **Batch Logout** to disconnect selected users.

4.13 Behavior

4.13.1 Application Scenario

Online behavior management aims to block or prohibit specific Internet access behaviors of LAN users. Online behavior management is classified into five categories: app control, website filtering, QQ management, flow control, and access control. The effective range of each behavior management policy is flexibly controlled by the specified client IP address and effective time.



4.13.2 App Control

App control aims at controlling the range of specific apps that can be accessed by users. By default, users can access any app. After an app control policy is configured, users on the current network cannot access prohibited apps. App access can be prohibited based on the specified user group and time range. For example, employees on the office network are prohibited from accessing entertainment and game software during work periods to improve network security.

1. Configuring App Control

(1) Switch to the **Local** mode. Choose **One-Device > Gateway > Config > Behavior > App Control**.

(2) Switch the application library.

The application lists vary depending on regions. Chinese and International versions of the application library are available. Select the version based on the regions.

Click to select **Application Library Version** and click **OK**. The version is switched after a few minutes.

Caution

- It takes about 1 minute to switch the application library version. Please wait.
- If you switch the application library, the old application control policy may take ineffective. Proceed with caution.

② Application Library Version: International + Add Delete Selected

(3) Configure App Control.

Click **Add** to create an App control policy.

App Control + Add Delete Selected

<input type="checkbox"/>	User Group	Time ?	Blocked applications ?	Status ?	Remarks ?	Action
<input type="checkbox"/>	User Group	All Time		Enable		Edit Delete
<input type="checkbox"/>	User Group/3dbbuser Unknown	All Time	... More	Enable	BLOCK_7708EBC4CF4490C 55D68	Edit Delete

Up to 50 entries can be added.

Add
×

Type User Group Custom

* User Group ?

Time ?

Application Blocked applications Blocked Application Group

* Application List ?

Remarks ?

Status ?

Parameter	Description
Type	<ul style="list-style-type: none"> ● User Group: The policy is applicable to users in the specified user group. Select the target user group. ● Custom: The policy is applicable to users in the specified IP address range. Enter the managed IP address range manually.
User Group	Select the users managed by the policy from the list of user groups. If all members in the user group are selected, the policy takes effect for the user group and is also valid for new members added to this group.
IP Address Group	If the IP address range is restricted by the app control policy and the type of the policy is set to Custom , enter the IP address range manually.
Time	Specify the time range under app control. In the specified time range, managed clients cannot access the selected apps in the list of prohibited apps. You can select a time range from the drop-down list box, or select Custom and manually enter the specific time range.
Application	Specify the applications or application groups to block.
Application List	When Blocked applications is selected, you can select the applications that need to be blocked.
App Group	When Blocked Application Group is selected, you can select the application groups that need to be blocked.

Parameter	Description
Remark	Enter the policy description.
Status	Specify whether to enable the app control policy.

2. Upgrading the Application Library

The app control function relies on the application library, and the application library is updated with the app version. You can upgrade the application library to the latest version on the **Application Library Update** page.

- (1) Switch to the **Local** mode. Choose **One-Device > Gateway > Config > Behavior > Application Library Update > Local Application Library Update**.

Caution

- Upgrading the application library version takes about 1 minute to take effect. Do not cut off power during the upgrade. You can view the current application library version on the page.
- Perform subsequent operations based on memory information displayed on the page. If the memory is insufficient, you are advised to restart the device and then upgrade the application library.
- After the application library is upgraded, the original app control policy may become invalid. Therefore, exercise caution when performing this operation.

- (2) Click **Browse**. Select an application library upgrade file.
- (3) Click **Upload** to upload the upgrade file.
- (4) Click **OK**. Wait for the system to automatically complete the upgrade.

Current Version 2023.12.01.23.12.01(V2.0)

File Path

Please select a file.

Browse

Upload

3. Configuring Custom Apps

Based on traffic packets of certain websites or apps that are obtained by the device, users can analyze and extract 5-tuple information (protocol, source IP address, source port, destination IP address, and destination port) of the packets. You can define apps that are not in the default application list.

After custom apps are configured successfully, you can configure control policies for custom apps on the app control page to block users from accessing the custom apps on the current network.

- (1) Switch to the **Local** mode. Choose **One-Device > Gateway > Config > Behavior > App Control > Custom**.
- (2) (Optional) Switch the application library.

Note

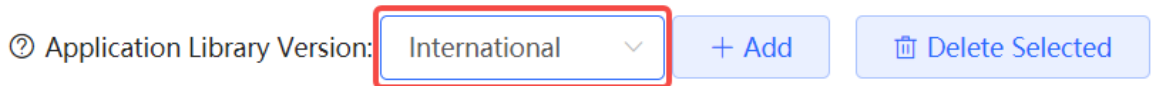
Switching the Application Library is only supported on RG-EG105G-V2 and RG-EG210G.

The supported app list varies depending on regions. Chinese and international versions of the application library are available. Select an application library version based on the actual region.

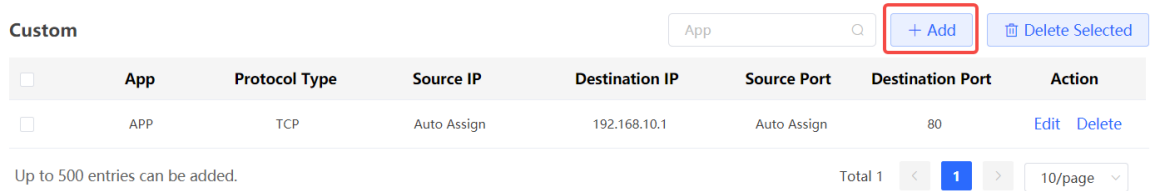
Click **Application Library Version** and select a version. In the displayed dialog box, click **OK**. Wait for a period of time for the system to complete switching.

 **Caution**

- Switching the application library version takes about 1 minute to take effect.
- After the application library version is switched, the original app control policy may become invalid. Therefore, exercise caution when performing this operation.



(3) Click **Add**. Enter information about a custom app.



Add ×

* App

Protocol Type

Control Type

* Destination IP Enter Manually Auto Assign
 ?

* Destination Port Enter Manually Auto Assign

Parameter	Description
App	Configure the app name (the name must be unique in the app list).

Parameter	Description
Protocol Type	Select a protocol type based on the protocol used by obtained packets. It can be set to TCP, UDP, or IP.
Control Type	Select a rule type based on 5-tuple information of extracted packets. It can be set to the following: <ul style="list-style-type: none"> ● Src IP + Src Port ● Dest IP + Dest Port ● Src IP + Dest IP
Source/Destination IP	Enter the source or destination IP address.
Source/Destination Port	Enter the source or destination port number.

 Note

- If **Control Type** is set to **Src IP + Src Port**, you need to set the source IP address and source port.
- If **Control Type** is set to **Dest IP + Dest Port**, you need to set the destination IP address and destination port.
- If **Control Type** is set to **Src IP + Dest IP**, you need to set the source and destination IP addresses. The source IP address can be also to **Auto Assign**.

(4) Click **OK**.

4. Verifying the Configuration

Add a policy for rejecting access to Facebook and YouTube according to [1. Configuring App Control](#).

Try to access Facebook on the guest PC. Then you will find the access failure.



This site can't be reached

www.facebook.com took too long to respond.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)
- [Running Windows Network Diagnostics](#)

ERR_CONNECTION_TIMED_OUT

Reload

Details

4.13.3 Website Management

Website management consists of website grouping and filtering. Website grouping refers to the classification of website URLs. You can modify existing website groups or create website groups. Website filtering refers to access control for existing website groups to prohibit users' access to websites in specific groups. Website filtering can be applied based on the specified user group and time range. For example, employees on the office network are prohibited from accessing game websites during work periods to improve network security.

- (1) Switch to the **Local** mode. Choose **One-Device > Gateway > Config > Behavior > Website Management** .
- (2) Configure website groups.
 - a Click the **Website Group** tab. On the page that appears, all the created website groups are displayed in the list. Find the target group and click **More** in the **Member** column to view all the website URLs in the group. Find the target group and click **Edit** in the **Action** column to modify the member website URLs in the group. Find the target group and click **Delete** in the **Action** column to delete the group.
 - b Click **Add** to create a website group.

 **Caution**

If a website filtering rule in a website group is being referenced, the group cannot be deleted from the website group list. To delete this group, modify the website filtering configuration to remove the reference relationship first.

Website Group			
<input type="checkbox"/>	Group Name	Member	Action
<input type="checkbox"/>	Games	duowan.com... More	Edit Delete
<input type="checkbox"/>	Finance	*.10jqka.com.cn... More	Edit Delete
<input type="checkbox"/>	Social	*.baihe.com... More	Edit Delete
<input type="checkbox"/>	Shopping	*.taobao.com... More	Edit Delete
<input type="checkbox"/>	Life	*.55bbs.com... More	Edit Delete
<input type="checkbox"/>	Music	*.1ting.com... More	Edit Delete

Add Group



* Group Name

Please enter a group name 1-64 characters

* Member

Set group members. The group member can be a complete URL (example: www.baidu.com) or a domain (example: *.56.com). If you want to add a domain, please make sure that the domain starts with *.

Cancel

OK

Table 4-34 Website group configuration

Parameter	Description
Group Name	Configure a unique name for a website group. The name can be a string of 1 to 64 characters.
Member	Specify members in the website group. You can enter multiple websites in a batch. The group member can be a complete URL (such as www.baidu.com) or keyword in the URL (domain name with a wildcard in front, such as *.baidu.com). The wildcard can only appear at the beginning of a URL, and cannot be in the middle or end of the domain name.

(3) Configure website filtering.

- a Choose **One-Device > Gateway > Config > Behavior > Website Management > Website Filtering**.
- b Click the **Website Filtering** tab. On the page that appears, all the created website filtering rules are displayed in the list. Click **Edit** to modify rule information and click **Delete** to delete the specific filtering rule.
- c Click **Add** to create a website filtering rule.

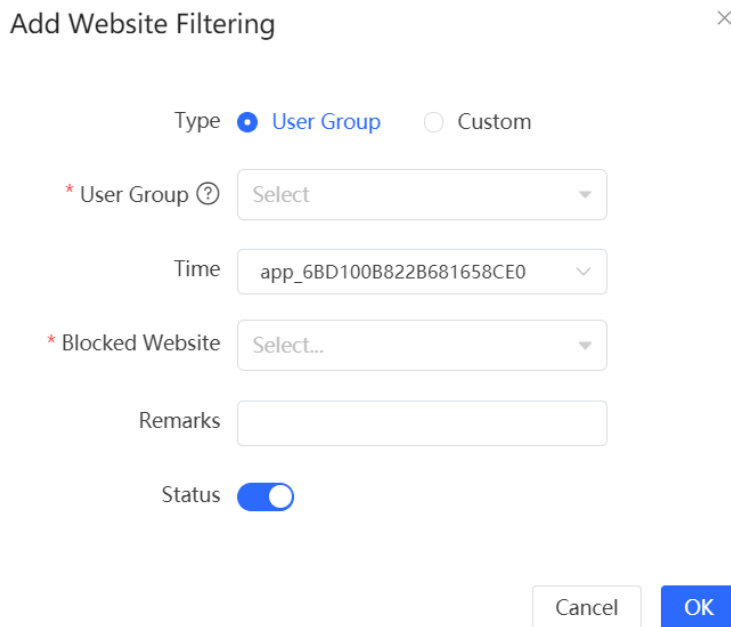
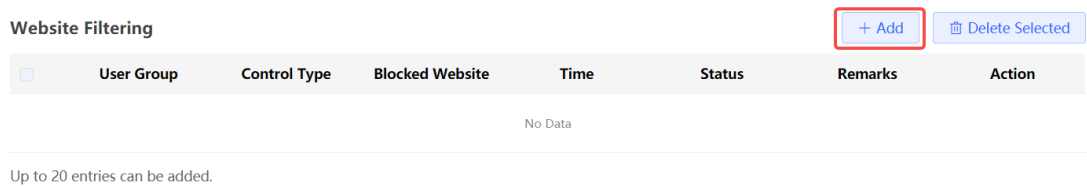


Table 4-35 Website filtering rule configuration

Parameter	Description
Type	<ul style="list-style-type: none"> ● User Group: The policy is applicable to users in the specified user group. Select the target user group. ● Custom: The policy is applicable to users in the specified IP address range. Enter the managed IP address range manually.
User Group	Select the users managed by the policy from the list of user groups. If all members in the user group are selected, the policy takes effect for the user group and is also valid for new members added to this group.
IP Address Group	If the IP address range is restricted by the app control policy and the type of the policy is set to Custom , enter the IP address range manually.
Time	Specify the time range under website filtering control. In the specified time range, managed clients cannot access the prohibited websites. You can select a time range from the drop-down list box, or select Custom and manually enter the specific time range.
Blocked Website	Configure the type of websites to be blocked. You can select an existing website group. After a website group is selected, users are prohibited from accessing all websites in this group.
Remark	Enter the rule description.
Status	Specify whether to enable the website filtering rule.

d Click **OK**.

(4) Try to access Facebook on the guest PC. Then you will find the access fails.



This site can't be reached

www.facebook.com took too long to respond.

Try:

- [Checking the connection](#)
- [Checking the proxy and the firewall](#)
- [Running Windows Network Diagnostics](#)

ERR_CONNECTION_TIMED_OUT

Reload

Details

4.13.4 Access Control

Access control enables the device to match data packets passing through the device based on specific rules and to permit or drop data packets in the specified time range. This function controls whether to permit LAN users' access to the Internet and whether to block a specific data flow. The device matches packets based on the MAC address or IP address.

(1) Switch to the **Local** mode. Choose **One-Device > Gateway > Config > Behavior > Access Control**.

The access control rule list displays the created access control rules. Click **Add** to add an access control rule.

Configure ACL based on IP addresses. **Default reverse flow mismatches**.
 The L2TP/PPTP/OpenVPN VPN only supports the IP-based ACL. The dest networks must be configured in the internal network.
 Example: **Configure a deny ACL entry containing source IP address 192.168.1.0/24 and destination IP address 192.168.2.0/24.** Device configured with IP address 192.168.1.x will fail to access device 192.168.2.x. **But device 192.168.2.x will be allowed to access device 192.168.1.x.**
 Tips: **Configure one more deny ACL entry containing source IP address 192.168.2.0/24 and destination IP address 192.168.1.0/24.** The two devices will be mutually unreachable.




ACL List + Add Delete Selected

<input type="checkbox"/>	Username ?	Rule ?	Control Type ?	Effective Time ?	Src Networks	Dest Networks	Status	Effective Sta... ?
No Data								

Up to 50 entries can be added. Total 0 1 10/page

Table 4-36 Access Control Rule Information

Parameter	Description
Username	Identify the purpose of the rule.
Rule	Display a summary of the control information. MAC-based: Display the MAC address matching the rule. IP-based: Display the connection type, source IP address, destination IP address, and protocol type of packets matching the rule.
Control Type	Indicate how packets that match the rule are processed. <ul style="list-style-type: none"> Allow: Permit the packets that match the rule. Block: Discard the packets that match the rule.
Effective Time	Indicate the time period during which the rule takes effect.
Src Networks	Indicate the source interface that matches the rule. If the rule is based on the MAC address, then this field is set to "All Intranets" by default. If the rule is based on IP addresses, then this field can be set to "All Networks", "All Extranets", "All Intranets", or a specific network.
Dest Networks	Indicate the destination interface that matches the rule. If the rule is based on the MAC address, then this field is set to "All Extranets" by default. If the rule is based on IP addresses, then this field can be set to "All Networks", "All Extranets", "All Intranets", or a specific network.

Parameter	Description
Status	Indicate whether the rule is enabled. You can click to switch the status. When this toggle switch is off, the rule will not take effect.
Effective State	Indicate whether the rule is effective. If Ineffective is displayed, it might be because the current system time is not within the designated effective period. You can hover the mouse over  to view more details on the cause.
Match Order	All the created rules are displayed in the ACL list, with the latest rule listed on the top. The device matches the rules according to their sorting in the list. You can manually adjust the rule matching sequence by clicking  or  in the list.
Action	You can modify or delete a rule.

(2) Configure a MAC address-based ACL rule.

MAC address-based ACL rules enable the device to match data packets based on the source MAC address, and are typically used to control Internet access from online users or specific clients.

Set **Based on MAC**, enter the MAC address of a client, select a rule type, set the effective time range, and click **OK**.

 Note

MAC address-based ACL rules are valid on WAN ports by default.

Add Rule




Status

Name

Based on **MAC Address** IP Address

* MAC Address

Control Type 

Effective Time 

Cancel

OK

Table 4-37 MAC Address-based ACL Configuration

Parameter	Description
Status	Indicate whether the rule is enabled. You can click to switch the status. When this toggle switch is off, the rule will not take effect.
Name	Enter the rule description, which is used to uniquely identify a rule.
MAC Address	Enter the client's MAC address to be controlled by the ACL rule. After you click the input field, the current client information is displayed. You can click to automatically enter the corresponding MAC address.
Control Type	Specify the method for processing data packets matching conditions. <ul style="list-style-type: none"> ● Allow: Permit the data packets matching the conditions. ● Block: Drop the data packets matching the conditions.
Effective Time	You can select a time range from the drop-down list box, or select Custom and manually enter the specific time range.

(3) Configure an IP address-based ACL rule.

IP address-based ACL rules enable the device to match data flows based on the source IP address, destination IP address, and protocol number.

Set **Based on IP**, enter the source IP address and port of a data flow, set the destination IP address and port of the data flow, select the protocol type, rule type, effective time range, and effective port, and click **OK**.

 Caution

- IP address-based ACL rules take effect in only one direction. For example, in a rule that defines Block, the source IP address segment is 192.168.1.0/24 and the destination IP address segment is 192.168.2.0/24. Based on this rule, the device at 192.168.1.x cannot access the device at 192.168.2.x, but the device at 192.168.2.x can access the device at 192.168.1.x. To block bidirectional access on this network segment, you need to configure another blocking rule with the source IP address segment 192.168.2.0/24 and destination IP address segment 192.168.1.0/24.
- L2TP and PPTP VPN support only IP address-based access control, and effective ports must be on the LAN.

Add Rule
×

Status

Name

Based on MAC Address IP Address

Internet IPv4 IPv6

Enable User Groups

Src IP Address

Dest IP Address

Protocol Type

Control Type

Effective Time

Src Networks

Dest Networks

----- Advanced Settings -----

Table 4-38 IP Address-based ACL Configuration

Parameter	Description
Status	Indicate whether the rule is enabled. You can click to switch the status. When this toggle switch is off, the rule will not take effect.
Name	Enter the rule description, which is used to uniquely identify a rule.
Internet	Format of the IP address. Both IPv4 and IPv6 address formats are supported.
Src IP Address	Enter the source IP address for data packet matching. If this parameter is not specified, the device matches all the IP addresses and port numbers. The source IP address can be a single IP address (such as 192.168.1.1) or an IP address range (such as 192.168.1.1/24).

Parameter	Description
Dest IP Address	Enter the destination IP address for data packet matching. If this parameter is not specified, the device matches all the IP addresses and port numbers. The destination IP address can be a single IP address (such as 192.168.1.1) or an IP address range (such as 192.168.1.1/24).
Protocol Type	Specify the protocol type for data packet matching. The options are All Protocols , TCP , UDP , ICMP , and TCP&UDP .
Control Type	Specify the method for processing data packets matching conditions. <ul style="list-style-type: none"> ● Allow: Permit the data packets matching the conditions. ● Block: Drop the data packets matching the conditions. This rule is valid only in one direction, and does not block reverse flows.
Effective Time	You can select a time range from the drop-down list box, or select Custom and manually enter the specific time range.
Src Networks	Indicate the source interface that matches the rule. If the rule is based on the MAC address, then this field is set to "All Intranets" by default. If the rule is based on IP addresses, then this field can be set to "All Networks", "All Extranets", "All Intranets", or a specific network.
Dest Networks	Indicate the destination interface that matches the rule. If the rule is based on the MAC address, then this field is set to "All Extranets" by default. If the rule is based on IP addresses, then this field can be set to "All Networks", "All Extranets", "All Intranets", or a specific network.

4.13.5 Network Behavior Settings

1. Internet Alert

Choose **One-Device > Gateway > Config > Behavior > Network Settings > Internet Alert**.

Click **Add** to create a network access notification policy and notify users of their online behaviors or application usage.

Notification List + Add Delete Selected

<input type="checkbox"/>	User Group	Notification Type	Status	Action
<input type="checkbox"/>	Authentication Group	Network Activity Notification; App Use Notification: Game	Enable	Edit Delete
<input type="checkbox"/>	VPN Group	App Use Notification: Video	Enable	Edit Delete
<input type="checkbox"/>	User Group/3dbbuser Unknown	Network Activity Notification;	Enable	Edit Delete
<input type="checkbox"/>	User Group/c3f4user Unknown	Network Activity Notification;	Enable	Edit Delete

Up to 20 entries can be added.

Add ×

* User Group Select

App Alert Select All

Game Video Payment

Data Usage Alert

Status

Cancel
OK

Table 4-39 Internet Access Notification Configuration Parameters

Parameter	Description
User group	Select a user group managed by the policy from the user group list. If you select all members of a user group, the policy takes effect on the entire user group (and members added to the user group later).
App Alert	To enable the App Alert function, enable Traffic Audit first. Choose One-Device > Gateway > Monitor . Click More to the right of Traffic Trend to access the gateway's monitoring details page. On the page that is displayed, click the App Real-Time Traffic tab and enable Traffic Audit .
App category	When App Alert is enabled, you need to select the application category for the policy. When a user uses an application in the corresponding application category, a notification will be received.
Data Usage	After the Data Usage Alert function is enabled, you will receive a notification when a

Parameter	Description
Alert	specified user accesses the Internet.
Status	Enable/disable the Data Usage Alert function. If it is disabled, the policy does not take effect.

2. Online Time Control

Note

The **Online Time Control** feature can only be configured on the app, and the web interface only displays the synchronization status.

Choose **One-Device > Gateway > Config > Behavior > Network Settings > Online Time Control**.

The **Online Time Control** list displays the type, schedule, accounting status, status, and operation information.

Online Time Control

Type	Schedule	Accounting Status	Status	Action
No Data				

3. Internet Block Policy



Note

The Internet block policy can be configured only on the app, and the web interface only displays the synchronization status.

Choose **One-Device > Gateway > Config > Behavior > Network Settings > Internet Block Policy**.

The **Policy List** displays the user group, start time of network disconnection, end time of network disconnection, start time of temporary access, and end time of temporary access.

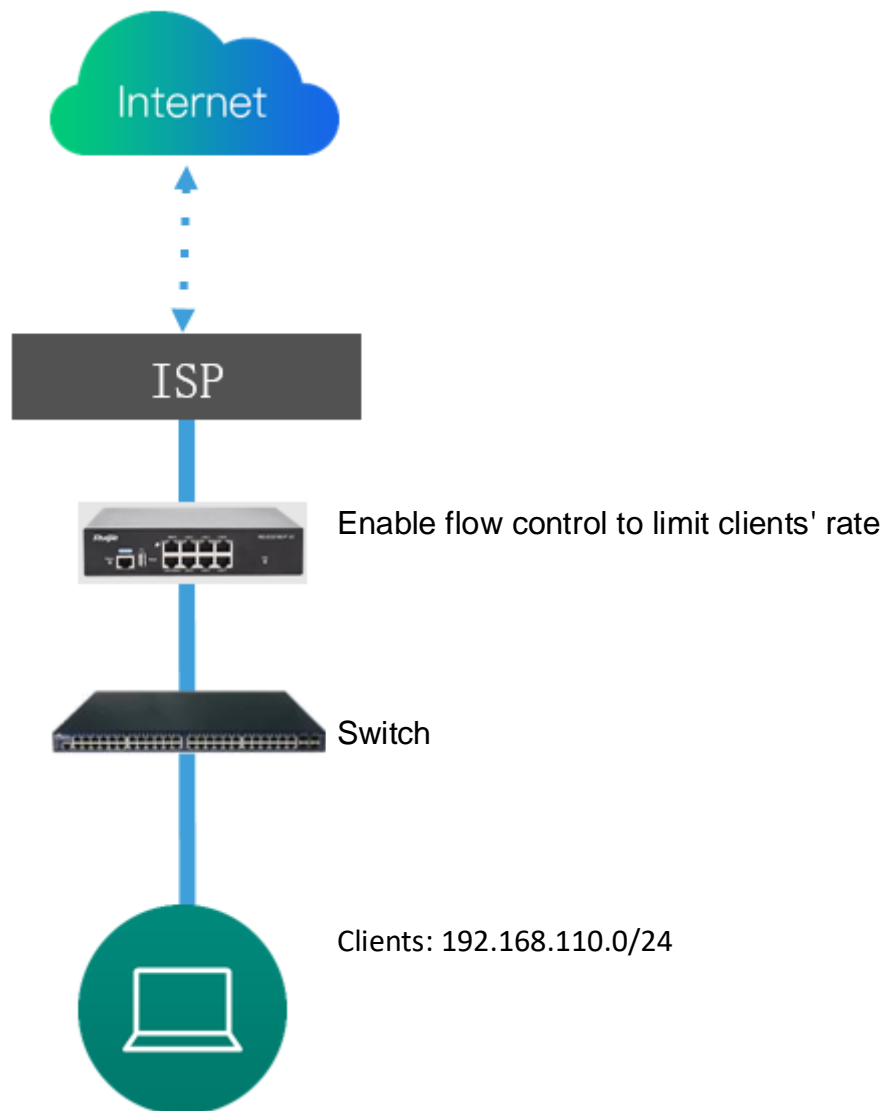
Policy List

User Group	Start Time	End Time 	Temporary Access Start Time	Temporary Access End Time 
No Data				

4.14 Flow Control

4.14.1 Application Scenario

Flow control enables the device to classify flows based on rules and process flows using different policies based on their categories. Flow control can be used to guarantee key flows and suppress malicious flows. It can be also used when the bandwidth is insufficient or flows need to be distributed properly.



4.14.2 Smart Flow Control

1. Overview

To limit uplink and downlink traffic bandwidth of device ports (such as WAN and WAN 1), you can enable smart flow control. After the line bandwidth is configured for a port, the uplink and downlink traffic of the port will be limited within the specified range. In addition, per-user bandwidth must be intelligently adjusted according to the number of users so that users can fairly share the bandwidth.

2. Configuration Steps

- (1) Switch to the **Local** mode. Choose **One-Device > Gateway > Config > Behavior > Flow Control > Smart Flow Control**.
- (2) Toggle the switch to **Enable** on the **Smart Flow Control** tab and set the line bandwidth based on the bandwidth actually allocated by an ISP. If the device has multiple lines, you can set the bandwidth for these WAN ports separately.

Enable **If you want to test the WAN rate, please disable smart flow control first.**

WAN0 Bandwidth Mbps * Uplink Mbps * Downlink

WAN1 Bandwidth Mbps * Uplink Mbps * Downlink

Save

Table 4-40 Smart Flow Control Configuration

Parameter	Description
Enable	Specify whether to enable the smart flow control function. By default, smart flow control is disabled.
WAN Bandwidth	Set the uplink and downlink bandwidth limits for WAN ports, in Mbps.

(3) Click **Save** to make the configuration take effect.

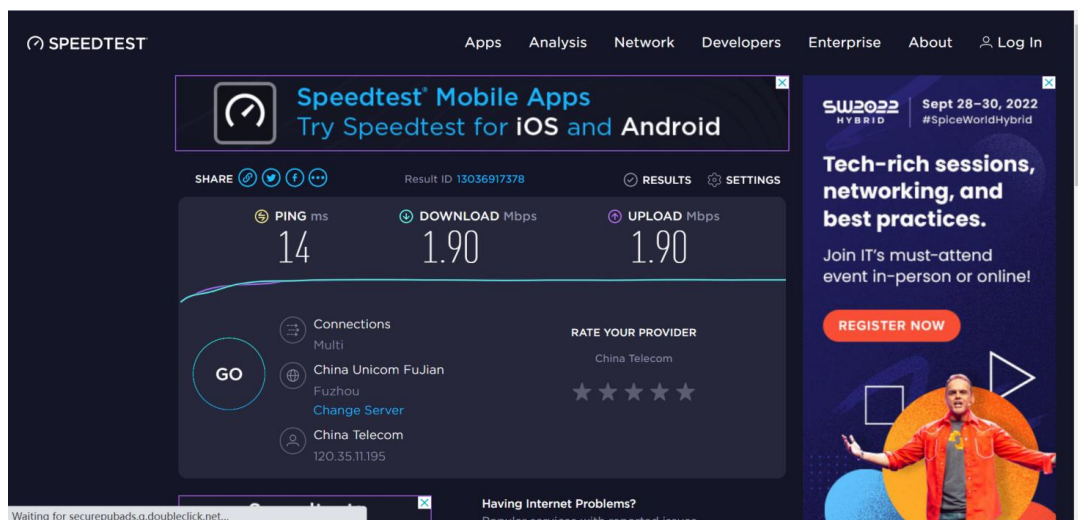
Note

Enabling flow control will affect network speed testing. To test the network speed, disable flow control first.

Note

Smart flow control can be used to control the line traffic in different networking modes, including bandwidth-based, static IP address, and dynamic IP address.

(4) Perform the speed test. The following figure shows that the guest's upload or download speed falls below 2 Mbps.



4.14.3 Custom Policies

1. Overview

Custom policies are used to restrict the traffic with specific IP addresses based on smart flow control, thereby meeting bandwidth requirements of specific users or servers. When creating a custom flow control policy, you can flexibly configure the limited user range, bandwidth limit, limited application traffic, and rate limit mode. A custom policy takes precedence over the smart flow control configuration.

Custom policies are classified into normal policies, MACC policies, and VPN policies based on their application scope:

- Normal policies are used to control common traffic.
- VPN policies are used to control VPN traffic.
- MACC policies are flow control policies configured on the cloud. The web management page only displays the policies. MACC policies cannot be modified on the web management page. To modify an MACC policy, log in to the MACC.

2. Getting Started

Before you configure a custom policy, enable smart flow control. For details, see section [4.14.2 Smart Flow Control](#).

3. Configuration Steps

Choose **One-Device > Gateway > Config > Behavior > Flow Control > Custom Policy**.

(1) Set **Policy Type**.

Policy Type Normal Policy VPN Policy

 Note

The **Cloud Policy** option is displayed in **Policy Type** only after a MACC policy is configured on the MACC.

(2) (Optional) Switch the application library.

 Note

This feature is only supported on RG-EG105G-V2 and RG-EG210G.

The application lists vary depending on regions. Chinese and International versions of the application library are available. Select the version based on the regions.

Click to select **Application Library Version** and click **OK**. The version is switched after a few minutes.

 Caution

- It takes about 1 minute to switch the application library version. Please wait.
-

- If you switch the application library, the template of the application priority will be reset (see section [4.14.4 Application Priority](#)), and the old application control policy may take ineffective (see section [4.13.2 App Control](#)). Proceed with caution.

Application Library Version: International

- (3) Set a custom policy.
- Set a custom normal policy.
 - Set **Policy Type** to **Normal Policy** and click **Add** to create a custom normal flow control policy. A maximum of 30 custom normal policies can be configured.

Add ×

* Policy Name

Type User Group Custom

* User Group

Bandwidth Type Shared Independent

Application All Applications App Group Custom

Channel Priority

Bandwidth Limit Limit No Limit

Uplink Bandwidth Mbps Mbps

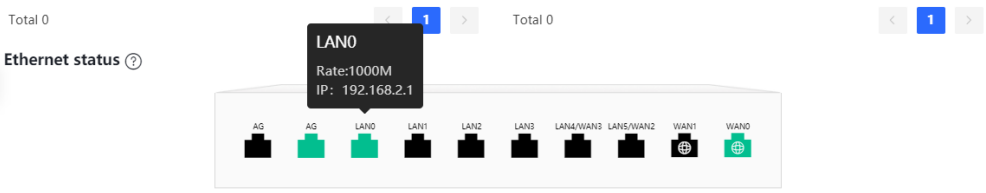
Downlink Bandwidth Mbps Mbps

* Interface

Enabled

- Configure items related to a normal policy.

Parameter	Description
Policy Name	A policy name uniquely identifies a custom flow control policy. It cannot be modified.

Parameter	Description
Type	<p>Type of a flow control policy:</p> <ul style="list-style-type: none"> ● User Group: The policy is applied to users in a specified user group. You need to select a user group to be managed. ● Custom: The policy is applied to users in a specified IP address segment. You need to manually enter the IP address range to be managed.
User Group	<p>Select a user to be managed by the policy from the user group list. .</p> <p>If you select all members of a user group, the policy takes effect on the entire user group (it also takes effect on members added to the user group later).</p>
IP/IP Range	<p>Specify the IP address range for the flow control policy to take effect. When Type is set to Custom, enter the IP address manually. You can enter a single IP address or an IP address segment.</p> <p>The IP address range must be within a LAN segment. You can choose One-Device > Gateway > Monitor > Ethernet status to check the network segment of the current LAN port. For example, the network segment of the LAN port shown in the figure below is 192.168.110.0/24.</p>  <p>The screenshot shows a network interface status window titled 'Ethernet status'. It displays a row of network ports: AG, AG, LAN0, LAN1, LAN2, LAN3, LAN4/WAN3, LAN5/WAN2, WAN1, and WAN0. The LAN0 port is highlighted with a tooltip that reads 'LAN0', 'Rate:1000M', and 'IP: 192.168.2.1'. Navigation arrows and a page number '1' are visible at the top of the window.</p>
Bandwidth Type	<ul style="list-style-type: none"> ● Shared: All users in a user group (all IP addresses in an address range) share the configured uplink and downlink bandwidths, and the bandwidth of a single user is not limited. ● Independent: All users in a user group (all IP addresses in an address range) share the configured uplink and downlink bandwidths, and the maximum bandwidth of a single user can be limited.
Application	<p>When Bandwidth Type is set to Shared, the flow control policy can be configured to take effect only on specified applications.</p> <ul style="list-style-type: none"> ● All Applications: The flow control policy takes effect on all applications in the current application library. ● Custom: The flow control policy takes effect only on specified applications in the application list. <p>When Bandwidth Type is set to Independent, some models do not support application selection and the flow control policy takes effect on all applications in the current application library by default.</p> <p>For the models, contact technical support engineers.</p>
Application List	<p>When Application is set to Custom, it specifies the applications on which the policy takes effect. Traffic of the selected applications is limited by the policy.</p>
Application Group	<p>When Application is set to Application Group, it specifies the application groups, on which the policy takes effect. The traffic of the selected application group is subject to the policy.</p>

Parameter	Description
Channel Priority	Specify the traffic guarantee level. The value ranges from 0 to 7. A smaller value indicates a higher priority and the value 0 indicates the highest priority. Different traffic priority values correspond to different application groups in an application template. The value 2 indicates the key group, value 4 indicates the normal group, and value 6 indicates the suppression group. For the description of application groups in a priority template, see 4.14.4 Application Priority .
Bandwidth Limit	Configure whether to limit the bandwidth. <ul style="list-style-type: none"> ● Limit Kbps: You can set the uplink and downlink bandwidth limits as required. ● No Limit: When the bandwidth is sufficient, the used maximum bandwidth is not limited. When the bandwidth is insufficient, the minimum bandwidth cannot be guaranteed.
Uplink Bandwidth/ Downlink Rate	Configure the data transmission rate in uploading, in Kbps. It includes Limit-at, Max-Limit, and Max-Limit per User. <ul style="list-style-type: none"> ● Limit-at: Specifies the minimum bandwidth that can be shared by all users when the bandwidth is insufficient. ● Max-Limit: Specifies the total maximum bandwidth that can be occupied by all users when the bandwidth is sufficient. ● Max-Limit per User: Specifies the maximum bandwidth that can be occupied by each user when multiple users share the bandwidth. It is optional and can be configured only when Bandwidth Type is set to Independent. The rate is not limited by default.
Interface	Specify the WAN port on which the policy takes effect. When it is set to All WAN Ports , the policy will be applied to all WAN ports.
Enabled	Set whether to enable the flow control policy. If it is disabled, the policy does not take effect.

 **Caution**

After switching the application library version, you may need to reconfigure the application list.

- c Click **OK**.
- Set a custom VPN policy.
 - a Set **Policy Type** to **VPN Policy** and click **Add** to create a custom VPN flow control policy. A maximum of 10 VPN policies can be configured.

Add



* Policy Name

Type User Group Custom

* User Group (?)

Effective User (?) Internal IP/User External IP/External User

Application (?) All Applications App Group Custom

Bandwidth Limit Limit No Limit

Uplink Bandwidth (?) * Max-Limit Mbps (?)

Max-Limit Mbps
per User

Downlink Bandwidth (?) * Max-Limit Mbps (?)

Max-Limit Mbps
per User

* Interface (?)

Enabled

Cancel

b Configure items related to a VPN policy.

Parameter	Description
Policy Name	A policy name uniquely identifies a custom flow control policy. It cannot be modified.
Type	Type of a flow control policy: <ul style="list-style-type: none"> ● User Group: The policy is applied to users in a specified user group. You need to select a user group to be managed. ● Custom: The policy is applied to users in a specified IP address segment. You need to manually enter the IP address range to be managed.
User Group	Select a user to be managed by the policy from the user group list. If you select all members of a user group, the policy takes effect on the entire user group (it also takes effect on members added to the user group later).

Parameter	Description
IP/IP Range	<p>Enter an IP address or IP range manually.</p> <p>This parameter is required when Type is set to Client.</p>
Effective User	<p>Specify the type of effective users:</p> <ul style="list-style-type: none"> ● Internal IP/User: For a gateway, IP addresses of clients connected to the gateway are internal IP addresses. ● External IP/External User: For a gateway, non-gateway internal IP addresses are external IP addresses, such as the internal IP address of the VPN server. <p>Configuration suggestions are as follows:</p> <ul style="list-style-type: none"> ● When clients are configured to control VPN traffic, select Internal IP/ User to control traffic of internal network users. When the VPN server is configured to control VPN traffic, select External IP/External User to control traffic of external network users. ● For the VPN of the NAT model, the external IP address of the server must be in the IP address segment of the VPN address pool. ● For the VPN in router mode, the IP address segment must be set to IP addresses of restricted users. For the VPN in router mode, to configure flow control on internal IP addresses of clients, set internal IP addresses to the IP addresses of the flow control objects. <p>Note: The external IP address configured by the Open VPN server is the IP address of the address pool. The internal IP address configured by the client is the actual IP address of the client.</p>
Application	<p>When Bandwidth Type is set to Shared, the flow control policy can be configured to take effect only on specified applications.</p> <ul style="list-style-type: none"> ● All Applications: Indicates that the flow control policy takes effect on all applications in the current application library. ● Custom: Indicates that the flow control policy takes effect only on specified applications in the application list. ● Application Group: Indicates that the flow control policy takes effect only on specified application groups. The traffic of applications involved in the application group is subject to the policy. <p>When Bandwidth Type is set to Independent, some models do not support application selection and the flow control policy takes effect on all applications in the current application library by default.</p> <p>For the models, contact technical support engineers.</p>
Application List	<p>When Application is set to Custom, it specifies the applications on which the policy takes effect. The traffic of the selected applications is limited by the policy.</p>
Application Group	<p>When Application is set to Application Group, it specifies the application group, on which the policy takes effect. The traffic of the selected application group is subject to the policy.</p>
Bandwidth Limit	<p>Configure whether to limit the bandwidth.</p> <ul style="list-style-type: none"> ● Limit: You can set uplink and downlink bandwidth limits as needed. ● No Limit: When the bandwidth is sufficient, the maximum bandwidth is not limited. When the bandwidth is insufficient, the minimum bandwidth is not guaranteed.

Parameter	Description
Max Uplink Rate per User/ Max Downlink Rate per User	Configure the maximum uplink or downlink data transmission rate when multiple users share the bandwidth, in kbps. It is optional and can be configured only when Bandwidth Type is set to Independent . The rate is not limited by default.
Interface	Specify the VPN port on which the policy takes effect. When it is set to All VPN Ports , the policy is applied to all traffic of the VPN type.
Enabled	Set whether to enable the flow control policy. If it is disabled, the policy does not take effect.

c Click OK.

(4) View Custom Policies

The current custom policies are displayed in the **Policy List** section. You can modify and delete a custom policy. To delete multiple custom policies in a batch, select the desired policies and click **Delete Selected**.

o Normal policy list

Policy Type Normal Policy VPN Policy

Policy List ? + Add Delete Selected

<input type="checkbox"/>	Policy Name ?	User Group	Bandwidth Type ?	Channel Priority	Application List ?	Uplink Bandwidth ?
<input type="checkbox"/>	test	User Group	Shared	4	All Applications	Limit-at 2Mbps Max-Limit 1000Mbps

Up to 30 entries can be added. 1 entries are already added.

o VPN policy list

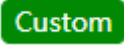
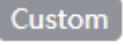


Policy Type Normal Policy VPN Policy

Policy List ? + Add Delete Selected

<input type="checkbox"/>	Policy Name ?	User Group	Application List ?	Uplink Bandwidth ?	Downlink Bandwidth ?
<input type="checkbox"/>	L2TP	VPN Group	All Applications	Max-Limit 1000Mbps Max-Limit per User 100Mbps	Max-Limit 1000Mbps Max-Limit per User 100Mbps
<input type="checkbox"/>	IPSec	VPN Group	All Applications	Max-Limit 1000Mbps Max-Limit per User 100Mbps	Max-Limit 1000Mbps Max-Limit per User 100Mbps

Up to 10 entries can be added. The Ruijie Cloud policy cannot be edited. 2 entries are already added.

Table 4-41 Policy List Information

Parameter	Description
Application List	Application List contains the applications for which the policy is valid. If Application Library matches Application that is set to Custom and supported by the policy,  is displayed in Application List . If not,  is displayed.
Status	Whether the current policy is enabled. You can click to edit the status. If Application Library does not match Application that is set to Custom and supported by the policy, you cannot edit Status directly. Click Edit in the action bar to edit the policy or switch the application library.
Effective State	Whether the policy is effective in the current system. If Inactive is displayed, check whether the policy is enabled, whether the policy-enabled port exists, and whether Application Library matches Application for which the policy is valid.
Match Order	All the created custom policies are displayed in the policy list, with the latest policy listed on the top. The device matches policies according to their sorting in the list. You can manually adjust the policy matching sequence by clicking  or  in the list.
Action	You can modify and delete a custom policy.

4.14.4 Application Priority

1. Overview

After smart flow control is enabled, you can set the application priority to provide guaranteed bandwidth for applications with a high priority and suppress the bandwidth for applications with a low priority. You can predefine a list of applications whose bandwidth needs to be guaranteed preferentially and a list of applications whose bandwidth needs to be suppressed as needed.

Caution

If one application exists in both the custom policy list and application priority list, the custom policy takes effect.

2. Getting Started

- Before you configure an application priority, enable smart flow control. For details, see section [4.14.2 Smart Flow Control](#).
- Confirm that the appropriate application library is selected on the **Custom Policy** page (see section [4.14.3 Custom Policies](#)).

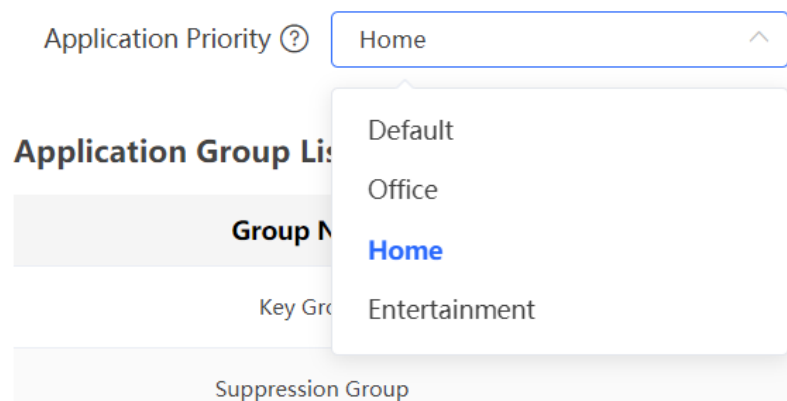
3. Configuration Steps

Choose **One-Device > Gateway > Config > Behavior > Flow Control > Application Priority**.

(1) Create an application priority template.

Select a template from the **Application Priority** drop-down list box.

Four application priority templates are predefined to meet needs in different scenarios. You can switch among the templates as needed.



The application priority templates are as follows:

- **Default:** This template is used during device initialization. The traffic bandwidth is not guaranteed or suppressed for any application.
- **Office:** This template is designed for the office scenario, where application traffic from the office network is guaranteed preferentially.
- **Home:** This template is designed for the home scenario, where application traffic from the home network is guaranteed preferentially.
- **Entertainment:** This template is designed for the entertainment scenario, where application traffic from the entertainment network is guaranteed preferentially.

(2) Create an application group list.

Each default template has three application groups: key group, block group, and normal group. The application priorities of the key group, normal group, and block group are in descending order:

- **Key Group:** Traffic from applications in the application list for this group is guaranteed preferentially.
- **Block Group:** Traffic from applications in the application list for this group is suppressed to preferentially guarantee the traffic from applications with a higher priority.
- **Normal Group:** All the applications in the application library beyond **Key Group** and **Block Group** are included in this group. Traffic from applications in this group are guaranteed after traffic from applications of **Key Group** is guaranteed.

After you select a template, **Key Group**, **Block Group**, **Normal Group**, and the application list for each group in the current template are displayed. You can click **More** to view details of each application list.

You can click **Edit** in the **Action** column next to the key group and block group to edit the application list, allowing traffic from these applications to be guaranteed or suppressed.

Application Group List

Group Name	Application List	Action
Key Group	Video... More	Edit
Suppression Group	Databank... More	Edit
Normal Group	Other	Edit

Application List(2)

[Databank](#) [P2PSoftware](#)

Edit ×

Group Name

Application List

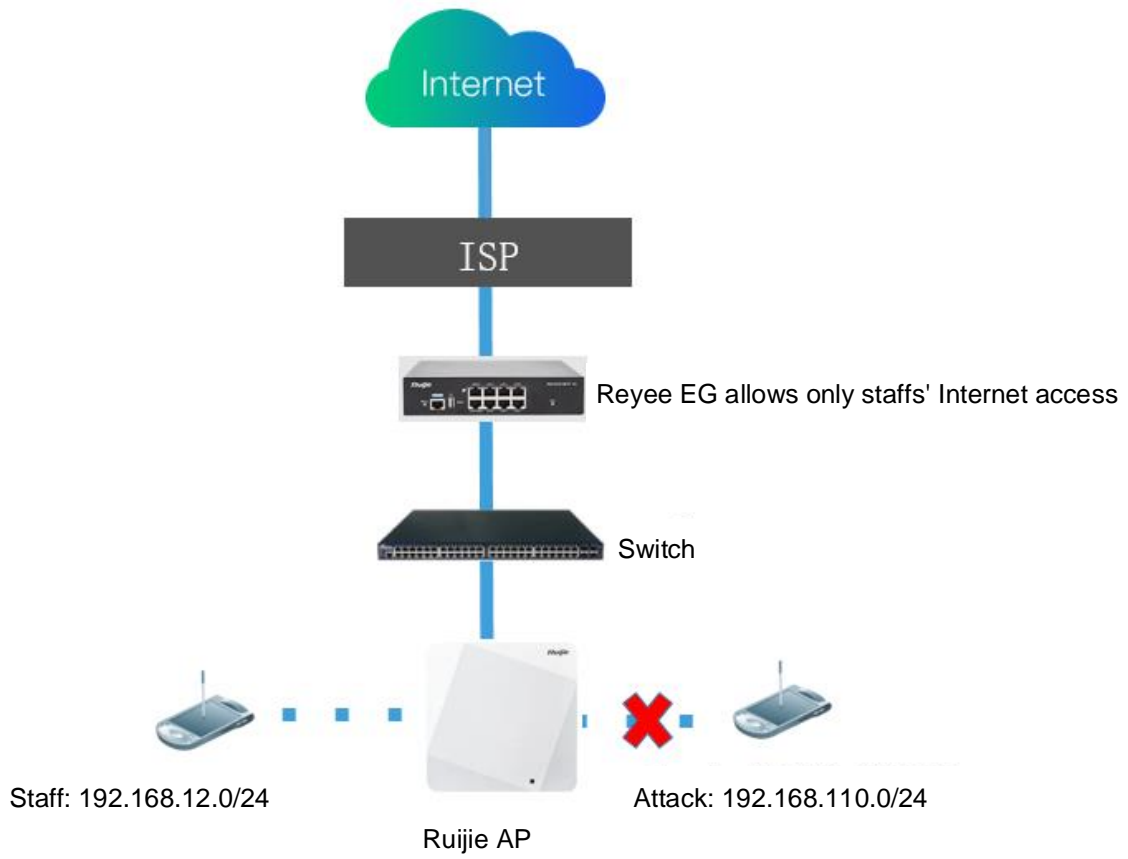
- ▶ Communication
- ▶ Shopping
 - Play
- ▶ Databank
- ▶ P2PSoftware
- ▶ Payment
- ▶ NetworkService

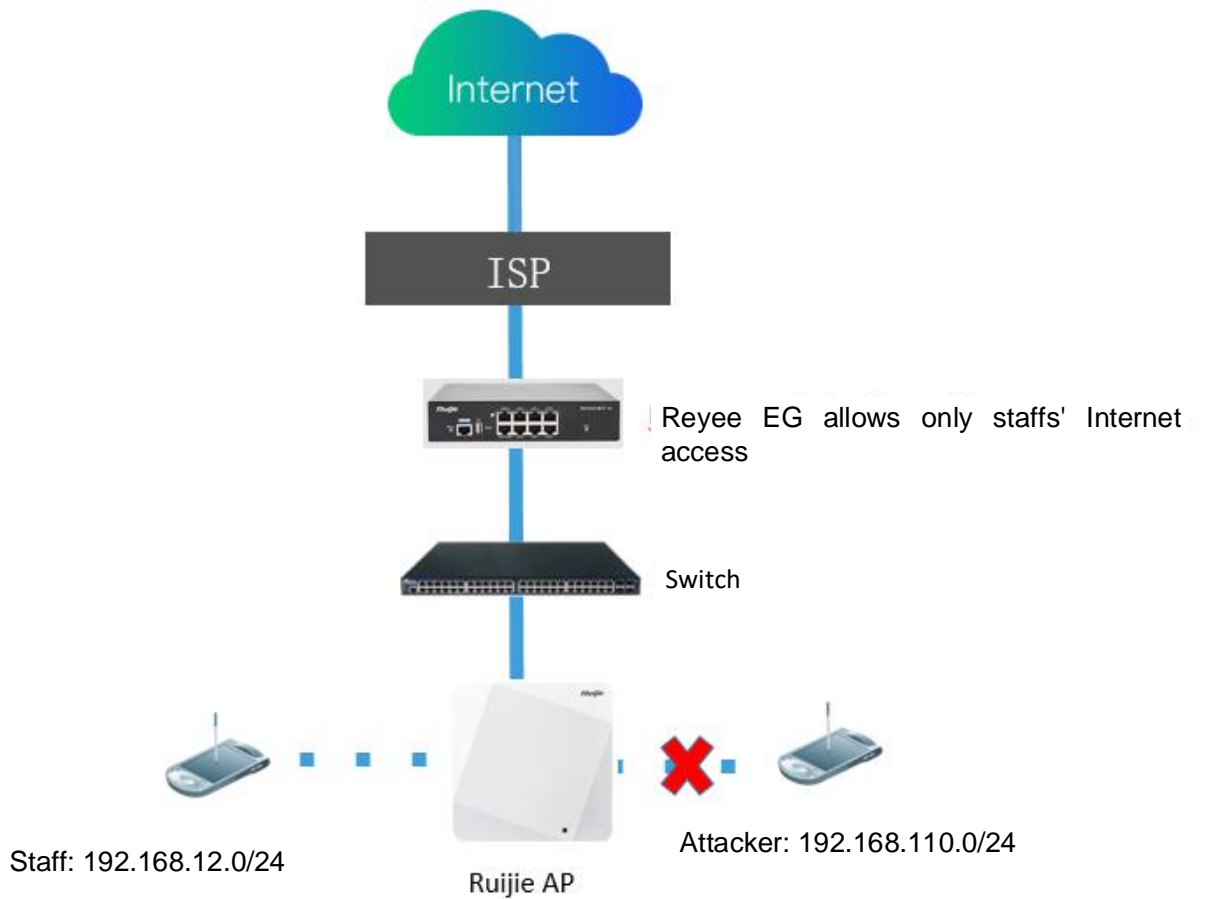
⚠ Caution

- If you switch the application library, the application list will change.
- The application list will be reset after you switch the application priority template.

4.15 Security

4.15.1 Application Scenario





4.15.2 Configuring the ARP List and ARP Guard

The device learns IP addresses and MAC addresses of network devices connected to its interfaces and generates ARP entries. You can enable ARP guard and configure IP-MAC binding to restrict Internet access of LAN hosts and improve network security.

- (1) Switch to the **Local** mode. Choose **One-Device > Gateway > Config > Security > ARP List**.
- (2) Before enabling ARP guard, you must configure the binding between IP addresses and MAC addresses in either of the following ways:
 - Select a dynamic ARP entry in the ARP list and click **Bind**. You can select multiple entries to be bound at one time and click **Bind Selected** to bind them.

ARP List 🔄 Q + Add Bind Selected Delete Selected

<input checked="" type="checkbox"/>	No.	Device Name	MAC Address	IP Address	Type	Action
<input checked="" type="checkbox"/>	1	Click to edit	ec...98	10.52.48.1	Dynamic	Bind
<input checked="" type="checkbox"/>	2	Click to edit	cc...5	10.52.49.26	Dynamic	Bind
<input type="checkbox"/>	3	Click to edit	00...79	10.52.48.53	Dynamic	Bind
<input type="checkbox"/>	4	Click to edit	00...3c	10.52.48.110	Dynamic	Bind
<input type="checkbox"/>	5	Click to edit	00...36	10.52.50.239	Dynamic	Bind

- Click **Add**, enter the IP address and MAC address to be bound, and click **OK**. The text box can display

existing address mappings in the ARP list. You can click a mapping to automatically enter the address mapping.

×

Add

Device Name (?)

* IP Address

* MAC Address

- (3) Click **Enable** to enable ARP guard.

After ARP guard is enabled, only LAN hosts with IP-MAC binding can access the external network.

ARP Guard

Enable (?) **Only the devices configured with IP-MAC binding are allowed to access the Internet.**

Interface Select All

Default VLAN
 VLAN 55
 VLAN 555

Set the range for the function to take effect.

If you check **Select All**, the ARP guard function will take effect on all clients on the LAN. If you select a specified port, the ARP guard function will take effect only on clients connected to the port.

4.15.3 Configuring MAC Address Filtering

You can enable MAC address filtering and configure an allowlist or blocklist to effectively control Internet access from LAN hosts.

- Allowlist: Allow only hosts whose MAC addresses are in the filter rule list to access the Internet.
- Blocklist: Prevent hosts whose MAC addresses are in the filter rule list from accessing the Internet.

- (1) Switch to the **Local** mode. Choose **One-Device > Gateway > Config > Security > MAC Filtering**.
- (2) Click **Add**. In the dialog box that appears, enter the MAC address and remarks. The text box can display existing address mappings in the ARP list. You can click a mapping to automatically enter the MAC address. Click **OK**. A filter rule is created.

Filtering Rule List Search by mac + Add Delete Selected

	Device Name	MAC Address	Action
No Data			

Up to 512 entries can be added. Total 0 < 1 > 10/page v

Add ×

Device Name ?

* MAC Address

Cancel
OK

(3) Enable MAC address filtering, set **Filtering Type**, and click **Save**.

MAC Filtering

MAC Filtering

The following hosts are not allowed to access the Internet.

Filtering Type

Save

4.16 Configuring Device Security

4.16.1 Configuring an Admin IP Address

Admin IP addresses are exempt from the ping prohibition function. Packets sent from admin IP addresses can pass through and will not be discarded.

Choose **One-Device > Gateway > Config > Security > Local Security > Security Zone**.

Click **Add**. Then, you can configure admin IP address information.

Up to 8 entries can be added.

Admin IP Address + Add Delete Selected

	Username	IP Range/Interface	Action
<input type="checkbox"/>	admin	WAN0	Edit Delete

Up to 32 entries can be added. Total 1 < 1 > 10/page v

1. Configuring an Admin IP Address (Based on an IP Address)

Add ×

* Username

Specified Mode IP Range Interface

- (1) Configure a name for the admin IP address.
The name is a string of 1–32 characters.
- (2) Set **Specific Mode** to **IP Range**.
- (3) Configure an IP address.
You can specify a single IP address or an IP address range.

2. Configuring an Admin IP Address (Based on a Port)

Add ×

* Username

Specified Mode IP Range Interface

▾

- (1) Configure a name for the admin IP address.
The name is a string of 1–32 characters.
- (2) Set **Specific Mode** to **Interface**.
- (3) Specify the port.
You can select a LAN port or WAN port as the interface.

3. Deleting an Admin IP Address

- Select an entry and click **Delete** to delete information about the admin IP address.
- Select multiple entries and click **Delete Selected** to bulk delete selected entries.

Admin IP Address + Add Delete Selected

<input type="checkbox"/>	Username	IP Range/Interface	Action
<input type="checkbox"/>	admin	WAN0	Edit Delete
<input type="checkbox"/>	test	WAN1	Edit Delete

Up to 32 entries can be added. Total 2 < 1 > 10/page ▾

4. Editing Information About an Admin IP Address

You cannot modify the name and specified mode of an admin IP address but modify the IP address range or port in the specified mode.

Edit



* Username

Specified Mode

 IP Range

 Interface

Edit



* Username

Specified Mode

 IP Range

 Interface

4.16.2 Configuring Security Zones

Note

- This feature is not supported on RG-EG105G-P-L.
- For devices that do not support SNMP, the SNMP service cannot be disabled in a LAN zone.

A security zone is a logical zone consisting of a group of systems that trust each other and share the same security protection requirements. Generally, a security zone consists of a group of interfaces. Networks formed by interfaces in the same security zone share the same security attributes. Each interface can only belong to one security zone.

- Up to eight security zones can be added.
- Pre-defined security zones include:
 - Pre-defined LAN zone: By default, all VLANs are mapped to the pre-defined LAN zone.
 - Pre-defined WAN zone: By default, all WAN interfaces are mapped to the pre-defined WAN zone.

Choose One-Device > Gateway > Config > Security > Local Security > Security Zone.

Security Zone

[+ Add](#)
[Delete Selected](#)

<input type="checkbox"/>	Name	Network Interface	Accessible Security Zones	Authorized Security Zones	Disabled Service	Action
<input type="checkbox"/>	Default LAN Zone	LAN Default VLAN VLAN 555 VLAN 55	Default WAN Zone Default Route Zone			Edit Delete
<input type="checkbox"/>	Default WAN Zone	WAN WAN1 WAN0		Default LAN Zone		Edit Delete
<input type="checkbox"/>	Default Route Zone	WAN	Default LAN Zone	Default LAN Zone		Edit Delete

Up to 8 entries can be added.

- (1) Click **Add**.
- (2) Configure parameters for the security zone.

Add
×

* Name

* Network Interface LAN WAN

Accessible Security Zones

Authorized Security Zones

Disabled Service ? WEB PING DNS
 DHCP SNMP

Table 4-42 Description of Security Zone Configuration Parameters

Parameter	Description
Name	Name of the security zone.
Network Interface	Interfaces mapped to the security zone, including LAN and WAN. LAN refers to VLAN, and WAN refers to WAN interfaces. Note: After a new security zone is created and VLANs or WAN interfaces are mapped to this new security zone, the VLANs or WAN interfaces will be removed from the pre-defined LAN zone or pre-defined WAN zone.
Accessible Security Zones	Other security zones to which this security zone can access.
Authorized Security Zones	Other security zones that can access this security zone.

Parameter	Description
Disabled Service	<p>Services disabled for the security zone.</p> <ul style="list-style-type: none"> ● If PING is selected, clients in the security zone cannot ping the local device. ● If Web is selected: clients in the security zone cannot access the local web page. ● If DNS is selected, the address of the DNS server used by clients in the security zone is the local IP address, and web pages cannot be accessed normally. ● If DHCP is selected, clients in the security zone cannot obtain IP addresses. ● If SNMP is selected, clients in the security zone cannot use the SNMP service of the device.

(3) Click **OK**.

4.16.3 Configuring Session Attack Prevention

1. Overview

- Session Attack Prevention

In a session attack, an attacker sends heavy traffic to the device. In this case, the device has to consume many resources when creating connections. To reduce the impact of the attack, you can limit the rate of creating sessions.

- Flood Attack Prevention

In a flood attack, an attacker sends tremendous abnormal packets to a device. As a result, the device uses a large amount of resources to handle the packets. This causes the device performance to deteriorate or the system to break down.

If the value of TCP SYN and other TCP Flood parameters is too small, the authentication function and access to local web pages will be affected.

If the value of UDP Flood parameter is too small, the DHCP address allocation, DNS domain name resolution, and VPN functionalities will be affected.

You are advised to set the value to be greater than the load capacity of the local device.

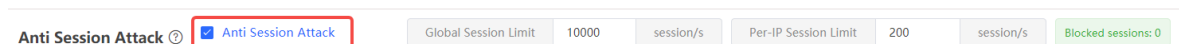
- Suspicious Packet Attack Prevention

In a suspicious packet attack, an attacker sends tremendous error packets to the device. When the host or server handles the error packets, its system will crash.

2. Configuring Session Attack Prevention

Choose **One-Device > Gateway > Config > Security > Local Security > Attack Defense**.

(1) Enable **Anti Session Attack**.



(2) Configure the session creation rate limit, including global and per-IP values.

(3) Click **Save**.

3. Configuring DDoS Attack Prevention

Choose **One-Device > Gateway > Config > Security > Local Security > Attack Defense**.

(1) Select required attack prevention types and enable this feature.

Refresh Every 10s ▾

Anti TCP SYN Flood Attack Rate Limit 3500 Pkt/s 0 packets blocked

Anti UDP Flood Attack Rate Limit 3500 Pkt/s

Anti ICMP Flood Attack Rate Limit 1400 Pkt/s

Anti ARP Flood Attack Rate Limit 1400 Pkt/s

Anti Other TCP Flood Attack Rate Limit 2000 Pkt/s

Anti Other Packet Flood Attack Rate Limit 3500 Pkt/s

Anti DDoS Attack ⓘ

(2) Configure rate limiting.

(3) Click **Save**.

4. Configuring Suspicious Packet Attack Prevention

Choose **One-Device > Gateway > Config > Security > Local Security > Attack Defense**.

(1) Select required attack prevention types and validity check types to enable this feature.

Anti Malformed Packet Attack
medium ⓘ

Anti Large Ping Attack Packet Length 4000 0 packets blocked

Anti Fraggle Attack

ICMP Validity Check ⓘ

IP Protocol Validity Check ⓘ

(2) To enable large ping attack prevention, enter the packet length.

(3) Click **Save**.

5. Configuring Packet Receiving and Sending Control

Choose **One-Device > Gateway > Config > Security > Local Security > Attack Defense**.

(1) Select the packet types that are prohibited from being sent by the device. Select at least one packet type.

ICMP Packet Management ⓘ

Disable ICMP Error Messages ICMP Timeout (type:11) × ▾ 0 packets blocked Details

Disable ICMPv6 Error Messages Time Exceeded × ▾ 0 packets blocked Details

- o Enable **Disable ICMP Error Messages**. You can select **ICMP Timeout**, **Destination Unreachable**, **Redirection**, and **Parameter**.

Anti Malformed Packet Attack
medium ⓘ

Anti Large Ping Attack Packet Length 4000

Anti Fraggle Attack

ICMP Validity Check ⓘ 0 packets blocked

IP Protocol Validity Check ⓘ

Disable ICMP Error Messages ICMP Timeout (type:11) × ▾ 0 packets blocked Details

ICMP Packet Management ⓘ

Disable ICMPv6 Error Messages Time Exceeded × ▾ 0 packets blocked Details

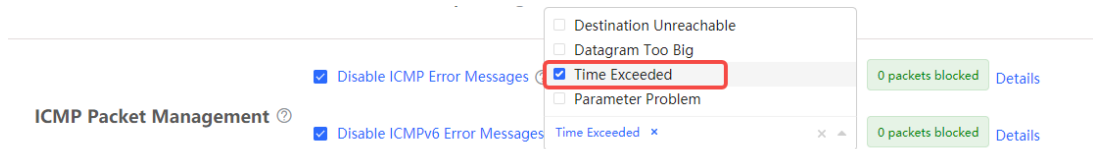
▸ Destination Unreachable (type:3)

▸ Redirection (type:5)

ICMP Timeout (type:11)

▸ Parameter (type:12)

- o Enable **Disable ICMPv6 Error Message**. You can select **Destination Unreachable**, **Datagram too Big**, **Time Exceeded**, and **Parameter Problem**.



(2) Click **Save**.

4.16.4 Checking the Security Log

Choose **One-Device > Gateway > Config > Security > Local Security > Security Log**.

Check defense results of the device against various attacks on the **Security Log** page.

Refresh Every 10s

Security Log

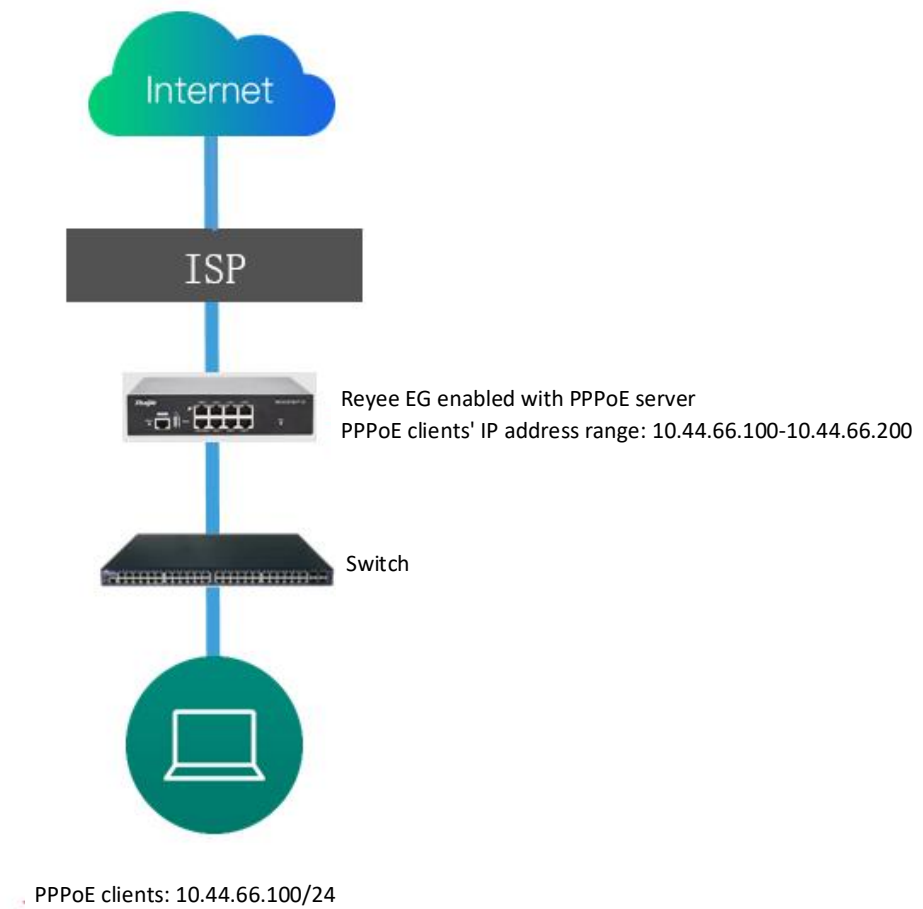
Timestamp <input type="button" value="v"/>	Attack Type <input type="button" value="v"/>	Severity <input type="button" value="v"/>	Description
The device has been running safely for 3 days			

Total 0

4.17 Configuring the PPPoE Server

4.17.1 Application Scenario

Point-to-Point Protocol over Ethernet (PPPoE) is a network tunneling protocol that encapsulates PPP frames into Ethernet frames. When the router functions as a PPPoE server, it provides the access service to LAN users and supports bandwidth management.



4.17.2 Global Settings

Choose **One-Device > Gateway > Config > Advanced > PPPoE Server > Global Settings**.

Set **PPPoE Server** to **Enable** and configure PPPoE server parameters.

Disabled
 Enable

Mandatory PPPoE Dialup Enable **Disable**

* Local Tunnel IP

* IP Range

VLAN

Primary DNS Server

Secondary DNS Server

* Unanswered LCP Packet Limit Range: 1-60

Auth Mode PAP CHAP
 MSCHAP
 MSCHAP2

Table 4-43 PPPoE Server Configuration

Parameter	Description
PPPoE Server	Specify whether to enable the PPPoE server function.
Mandatory PPPoE Dialup	Specify whether LAN users must access the Internet through dialing.
Local Tunnel IP	Set the P2P address of the PPPoE server.
IP Range	Specify the IP address range that can be allocated by the PPPoE server to authenticated users.
VLAN	Set the VLAN ID of the PPPoE server.
Primary/Secondary DNS Server	Specify the DNS server address delivered to authenticated users.
Unanswered LCP Packet Limit	When the number of LCP packets with no response in one link exceeds the specified value, the PPPoE server automatically disconnects the link.
Auth Mode	Select at least one authentication mode among PAP, CHAP, MSCHAP, and MSCHAP2.

4.17.3 Configuring a PPPoE User Account

Choose **One-Device > Gateway > Config > Advanced > PPPoE Server > Account Settings**.

Click **Add** to create a PPPoE authentication user account. Created PPPoE authentication user accounts are displayed in the **Account List** section. Find the target account and click **Edit** to modify account information. Find the target account and click **Delete** to delete the account.

i If you want to use the Batch Config or Backup Config feature, Office 2019 or a later version is required. Otherwise, invalid format and garbled text may occur.

Account List Search by Username
Batch Config
Backup Config
+ Add
Delete Selected

<input type="checkbox"/>	Username	Password <small>🔒</small>	Expire Date <small>?</small>	Status	Account Management	Remarks <small>?</small>	Action
<input type="checkbox"/>	test	***		Enable	-		Edit Delete
<input type="checkbox"/>	1	*		Enable	-		Edit Delete
<input type="checkbox"/>	9	*		Enable	-		Edit Delete

Add
✕

*** Username**

*** Password**

Expire Date

Remarks

Status

Rate Limiting

*** Account Management**

Cancel
OK

Table 4-44 PPPoE User Account Configuration

Parameter	Description
Username/Password	Set the username and password of the authentication account for Internet access through PPPoE dialing.

Parameter	Description
Expire Date	Set the expiration date of the authentication account. After the account expires, it can no longer be used for Internet access through PPPoE authentication.
Remark	Enter the account description.
Status	Specify whether to enable this user account. If the account is disabled, the account is invalid and cannot be used for Internet access through PPPoE authentication.
Rate Limiting	Specify whether to apply flow control on the account. If flow control is enabled, you need to configure flow control policies for the PPPoE authentication user. If smart flow control is disabled, Rate Limiting must be turned off. To turn on Rate Limiting, enable smart flow control first.
Account Management	After flow control is enabled, you need to configure a flow control package for the current account to restrict user bandwidth accordingly. For details on how to configure and view flow control packages, see section 4.17.4 Configuring a Flow Control Package .

4.17.4 Configuring a Flow Control Package

Choose **One-Device > Gateway > Config > Advanced > PPPoE Server > Account Management**.

If smart flow control is disabled, the flow control package for the account does not take effect. Before you configure a flow control package, enable smart flow control. For details on how to configure smart flow control, see section [4.14.2 Smart Flow Control](#).

Click **Add** to create a flow control package. Created flow control packages are displayed in the **Account Management List**. You can modify or delete the packages.

Account Management List					+ Add	Delete Selected
<input type="checkbox"/>	Account Name	Uplink Bandwidth	Downlink Bandwidth	Interface	Action	
<input type="checkbox"/>	test1	Limit-at 2Mbps Max-Limit 10Mbps Max-Limit per User No Limit	Limit-at 2Mbps Max-Limit 10Mbps Max-Limit per User No Limit	All WAN Ports	Edit	Delete

Up to 10 entries can be added.

Add
×

* Account Name

Uplink Bandwidth * Limit-at Mbps * Max-Limit Mbps ?

Max-Limit Mbps
per User

Downlink Bandwidth * Limit-at Mbps * Max-Limit Mbps ?

Max-Limit Mbps
per User

* Interface

Table 4-45 PPPoE User Flow Control Package Configuration

Parameter	Description
Account Name	Set the name of the flow control package. When configuring an authentication account, you can select a flow control package based on the name.
Uplink Bandwidth/ Downlink Bandwidth	<p>The following uplink/downlink bandwidth options can be configured, all measured in Mbps.</p> <ul style="list-style-type: none"> ● Limit-at: Guaranteed available uplink/downlink bandwidth for authenticated users when bandwidth resources are limited. ● Max-Limit: Maximum available uplink/downlink bandwidth for authenticated users when bandwidth resources are sufficient. ● Max-Limit per User: Maximum available uplink/downlink bandwidth for each user. This parameter is optional and the default value is no limit.
Interface	Specify the interface to which the flow control package applies.

4.17.5 Configuring Exceptional IP Addresses

Choose **One-Device > Gateway > Config > Advanced > PPPoE Server > Exceptional IP Address**.

To configure clients with some IP addresses in a specific VLAN to access the Internet without passing account and password authentication, you can configure these IP addresses as exceptional IP addresses on the device enabled with the PPPoE server.

The created exceptional IP addresses are displayed in **Exceptional IP Address List**. Click **Edit** to modify the exceptional IP address and click **Delete** to delete the exceptional IP address.

Start IP Address/End IP Address: indicates the start or end exceptional IP address.

Remark: indicates the description of an exceptional IP address.

Status: indicates whether an exceptional IP address is valid.

Exceptional IP Address List + Add Delete Selected

<input type="checkbox"/>	Start IP Address ?	End IP Address ?	Remarks ?	Status ?	Action
<input type="checkbox"/>	192.168.2.3	192.168.2.4		Enable	Edit Delete

Up to 5 entries can be added.

Add



* Start IP Address ?

* End IP Address ?

Remarks ?

Status ?

Cancel OK

4.17.6 Checking Online Users

Choose **One-Device > Gateway > Config > Advanced > PPPoE Server > Online Clients**.

Check information about end users that access the Internet through PPPoE dialing. Click **Disconnect** to disconnect a user from the PPPoE server.

Online User List Disconnect Refresh

<input type="checkbox"/>	Username ?	IP Address ?	MAC Address ?	Online Time ?	Action
No Data					

Online Clients0

Table 4-46 PPPoE Online User Information

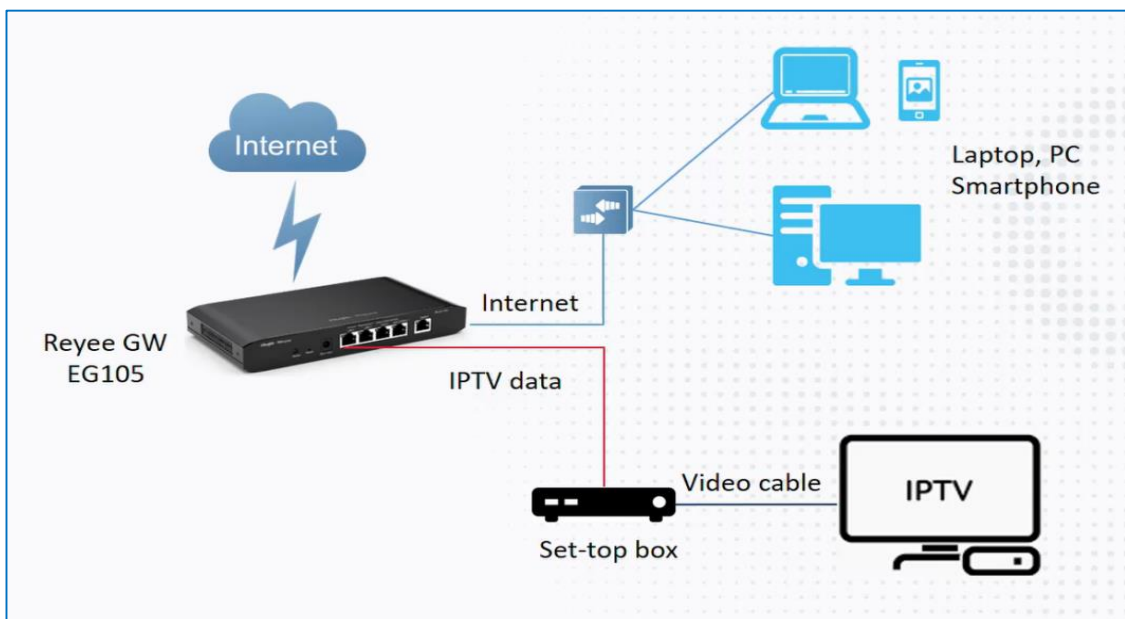
Parameter	Description
Username	Total number of online users that access the Internet through PPPoE dialing.
IP Address	IP address of the client.

Parameter	Description
MAC Address	MAC address of the client.
Online Time	Time when the user accesses the Internet.

4.18 IPTV

4.18.1 Application Scenario

- Scenario 1: Dual-WAN Scenario



- Scenario 2: Single-WAN Scenario



4.18.2 Dual-WAN Configuration

- (1) Connect the ISP cable with a WAN port, and connect your PC with a LAN port. Use the default IP address of 192.168.110.1 to log in to the Reyee EG and configure your EG to access the Internet successfully according to the wizard.
- (2) Choose **One-Device > Gateway > Config > Network > IPTV > IPTV/VLAN**.
- (3) Configure **IPTV VLAN ID** or **IP-Phone VLAN ID**.
 - If you are in following regions listed in the red box, you can choose the mode directly.

IPTV/VLAN IPTV/IGMP

* Mode

* AG

* AG

* LAN0

* LAN1

* LAN2

* LAN2

* LAN2

* LAN3

Internet VLAN (WAN) 802.1Q Tag

- o If you are not in these regions, you can choose **Custom**. Then contact with an ISP for IPTV settings and connect the IPTV and IP phone with LAN ports. For example, the VLAN IDs for IPTV, IP phone, and Internet services are 100, 200, and 300, respectively.

[IPTV/VLAN](#) [IPTV/IGMP](#)

i IPTV/VLAN settings.

IPTV/VLAN

* Mode

* LAN0

* LAN1/WAN3

* LAN2/WAN2

* LAN3/WAN1

* IPTV VLAN ID

* IP-Phone VLAN ID

Internet VLAN (WAN) 802.1Q Tag

* Internet VLAN ID

Save

4.18.3 Single-WAN Configuration

After performing IPTV configuration on the Reyee EG that has only one WAN port, you need to configure the IPTV VLAN 100 on the LAN port of the wall AP. If the router has two WAN ports, ignore this step.

- (1) Log in to the web management system. Choose **One-Device > Gateway > Config > Network > IPTV > IPTV/IGMP** and enable **IPTV/IGMP**.

[IPTV/VLAN](#) [IPTV/IGMP](#)

Enable

Save

- (2) Log in to the web management system of a wall AP. Choose **Network > LAN Ports > Add**.

The screenshot shows the Ruijie Rcycc Network Configuration interface. The left sidebar has 'LAN Ports' highlighted. The main content area is titled 'LAN Port Settings'. Under 'Default Settings', there is a 'VLAN ID' input field and a 'Save' button. Below that, the 'LAN Port Settings' table is empty, and a '+ Add' button is highlighted with a red box.

Set the VLAN ID to 100, which is applied to the wall AP.

The screenshot shows the 'Add' dialog box in the Ruijie Rcycc Network Configuration interface. The 'VLAN ID' field is set to 100, and the 'Applied to' dropdown is set to 'G1/1'. The 'OK' button is highlighted.

⚠ Caution

IPTV is supported by only Reye OS 1.55 and later versions.

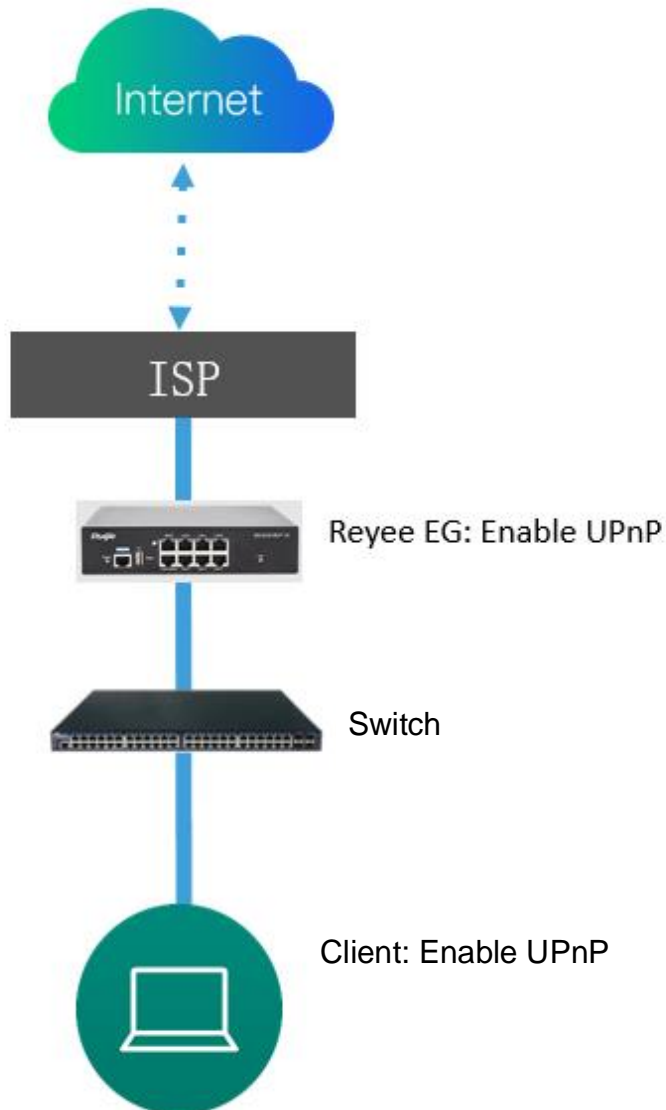
4.19 UPnP

4.19.1 Application Scenario

With the Universal Plug and Play (UPnP) function enabled, the device can switch the port used by the terminal's Internet service according to the terminal's request, achieving NAT conversion. When a terminal on the Internet wants to access resources of the device's intranet, the device can automatically add port mapping entries to realize service transmission across internal and external networks. Common applications that support the UPnP protocol include MSN Messenger, Thunder, BT, and PPLive.

There are three requirements for applying UPnP:

- The device must be enabled with UPnP.
- The operating system of internal hosts must support UPnP.
- Applications must support UPnP.



4.19.2 Procedure

- (1) Switch to the **Local** mode. **One-Device > Gateway > Config > Advanced > UPnP**, turn on **Enable** to enable the UPnP function on your phone or PC.

UPnP (Universal Plug and Play) is a new Internet protocol aimed at improving communication between devices.

Enable

Default Interface: WAN0

Save

UPnP List

Protocol	App	Client IP Address	Internal Port	External Port
No UPnP Device				

(2) The router will automatically detect your device and enable port mapping for the device. Finally you can use the external IP address and port to access your phone or PC service.

4.20 Configuring Rate Test

Note

Only RG-EG3XX series devices (such as RG-EG310G-E) and RG-EG1510XS support this function.

You can use the rate test function to easily monitor the transmission rate of individual ports. In the case of ports with low transmission rates, you can identify and address potential issues to ensure that service quality remains high.


Choose **One-Device > Gateway > Config > Network > Rate Test**.

Available Select All WAN0 WAN1

Start Test

WAN0 | WAN1 | Multi-WAN bandwidth aggregation test

Latency/ms	Jitter/ms	Packet loss/%
0	0	0



- (1) Select the WAN port to be tested. You can click **Select All** to select all WAN ports for the rate test.
- (2) Click **Start Test**.

After the rate test is complete, the system will display the test results, including latency, jitter, and packet loss.

4.21 Configuring IPv6

4.21.1 IPv6 Overview

Internet Protocol Version 6 (IPv6) is the next-generation IP protocol designed by Internet Engineering Task Force (IETF) to substitute IPv4. It is used to compensate insufficient IPv4 network addresses.

4.21.2 IPv6 Basics

1. IPv6 Address Format

IPv6 extends 32-bit IPv4 address into 128 bits, providing wider address space than IPv4.

The basic format of an IPv6 address is X:X:X:X:X:X:X. It is represented as eight groups of four hexadecimal digits (0-9, A-F), each group representing 16 bits. The groups are separated by colons (:). In this format, each X represents a group of four hexadecimal digits.

Samples of IPv6 addresses are 2001:ABCD:1234:5678:AAAA:BBBB:1200:2100, 800:0:0:0:0:0:1, and 1080:0:0:0:8:800:200C:417A.

The digit 0 in an IPv6 address can be suppressed as follows:

- Leading zeros in each 16-bit field are suppressed. For example, 2001:00CD:0034:0078:000A:000B:1200:2100 can be suppressed to 2001:CD:34:78:A:B:1200:2100.
- The long sequence of consecutive all-zero fields in some IPv6 addresses can be replaced with two colons (::). For example, 800:0:0:0:0:0:1 can be represented as 800::1. The two colons (::) can be used only when all the 16 bits in a group are 0s, and it can appear only once in an IPv6 address.

2. IPv6 Prefix

IPv6 addresses are typically composed of two logical parts:

- Network prefix: n bits, corresponding to the network ID in IPv4 addresses
- interface ID: $(128 - n)$ bits, corresponding to the host ID in IPv4 addresses

A slash (/) is used to separate the length of network prefix from an IPv6 address. For example, 12AB::CD30:0:0:0/60 indicates that the 60-bit network prefix in the address is used for route selection. IPv6 prefixes can be obtained from the IPv6 DHCP server, along with IPv6 addresses. A downlink DHCP server can also automatically obtain IPv6 prefixes from its uplink DHCP server.

3. Special IPv6 Addresses

There are some special IPv6 addresses:

fe80::/8: loopback address, similar to the IPv4 address 169.254.0.0/16

fc00::/7: local address, similar to IPv4 addresses 10.0.0.0/8, 172.16.0.0/16, and 192.168.0.0/16

ff00::/12: multicast address, similar to the IPv4 address 224.0.0.0/8

4. NAT66

IPv6-to-IPv6 Network Address Translation (NAT66) is a process of converting the IPv6 address in the IPv6 data packet header into another IPv6 address. NAT66 can be implemented by converting the prefix in an IPv6 address in an IPv6 data packet header into another IPv6 address prefix. NAT66 enables mutual access between an internal network and an external public network.

4.21.3 IPv6 Address Allocation Modes

- Manual configuration: IPv6 addresses, prefixes, and other network parameters are configured manually.
- Stateless Address Autoconfiguration (SLAAC): The link-local address is generated based on the interface ID, and the IPv6 address is automatically allocated based on the prefix information in the Router Advertisement (RA) packet.
- Stateful address allocation (DHCPv6): Two DHCPv6 allocation methods are as follows:
 - Automatic DHCPv6 allocation: The DHCPv6 server automatically allocates IPv6 addresses, prefixes, and other network parameters.
 - Automatic allocation of DHCPv6 Prefix Delegations (PDs): The lower-layer network device submits a prefix allocation application to the upper-layer network device. The upper-layer network device allocates an appropriate address prefix to the lower-layer device. The lower-layer device further divides the obtained prefix (usually less than 64 bits) into 64-bit prefixed subnet segments and advertises the address prefixes to the user link directly connected to the IPv6 host through the RA packet, implementing automatic address configuration for hosts.

4.21.4 Enabling the IPv6 Function

Choose **One-Device > Gateway > Config > Network > IPv6 Address**.

Turn on **Enable** to enable the IPv6 function.

Enable 

4.21.5 Configuring an IPv6 Address for the WAN Port

Choose **One-Device > Gateway > Config > Network > IPv6 Address > WAN Settings**.

After you enable the IPv6 function, you can set related parameters on the **WAN Settings** tab. The number of **WAN_V6** tabs indicates the number of WAN ports on the current device.

[WAN Settings](#) [LAN Settings](#) [DHCPv6 Clients](#) [Static DHCPv6](#)

[WAN0](#) [WAN1](#)

* Internet DHCP/PPPoE

IPv6 Address

IPv6 Prefix

Gateway

DNS Server

NAT66 ⓘ

----- [Advanced Settings](#) -----

[Save](#)

Table 4-47 IPv6 address configuration for WAN port

Parameter	Description
Internet	Configure a method for the WAN port to obtain an IPv6 address. <ul style="list-style-type: none"> ● DHCP: The current device functions as the DHCPv6 client, and it applies for an IPv6 address and prefix from the uplink network device. ● Static IP: You need to manually configure a static IPv6 address, gateway address, and DNS server. ● Null: The IPv6 function is disabled on the WAN port.
IPv6 Address	When Internet is set to DHCP , the automatically obtained IPv6 address is displayed. When Internet is set to Static IP , you need to configure this parameter manually.
IPv6 Prefix	When Internet is set to DHCP , the IPv6 address prefix automatically obtained by the current device is displayed.
Gateway	When Internet is set to DHCP , the automatically obtained gateway address is displayed. When Internet is set to Static IP , you need to configure this parameter manually.
DNS Server	When Internet is set to DHCP , the automatically obtained DNS server address is displayed. When Internet is set to Static IP , you need to configure this parameter manually.

Parameter	Description
NAT66	If the current device cannot access the Internet through DHCP or cannot obtain the IPv6 prefix, you need to enable the NAT66 function to allocate IPv6 addresses to clients on the internal network.
Default Preference	Set the default route preference for the current line. A smaller value indicates a higher preference. For the same destination address, the route with the highest preference is selected as the optimal route.

 Caution

The RG-EG105G and RG-EG105G-P does not support the NAT66 function.

4.21.6 Configuring an IPv6 Address for the LAN Port

Choose **One-Device > Gateway > Config > Network > IPv6 Address > LAN Settings**.

When the device accesses the Internet through DHCP, it can obtain LAN port IPv6 addresses from the uplink device and allocate IPv6 addresses to the clients in the LAN based on the IPv6 address prefix. If the uplink device cannot allocate an IPv6 address prefix to the device, you need to manually configure an IPv6 address prefix for the LAN port and enable the NAT66 function to allocate IPv6 addresses to the clients in the LAN. For details, see Section [4.21.5 Configuring an IPv6 Address for the WAN Port](#).

LAN Settings ⓘ							+ Add	🗑 Delete Selected
<input type="checkbox"/>	VLAN ID	IPv6 Assignment	Subnet Prefix Name	Subnet ID	Subnet Prefix Length	IPv6 Address/Prefix Length	Action	
<input type="checkbox"/>	Default	Auto		0	64		<div style="border: 1px solid red; padding: 2px;">Edit</div> Delete	

Up to 8 entries can be added.

Click **Edit** next to the default VLAN, and set **IPv6 Address/Prefix Length** to a local address with no more than 64 bits. This address is also used as the IPv6 address prefix.

You can use either of the following methods to allocate IPv6 addresses to clients:

- **Auto**: Allocate IPv6 addresses to clients in DHCPv6 or SLAAC mode.
- **DHCPv6**: Allocate IPv6 addresses to clients through DHCPv6.
- **SLAAC**: Allocate IPv6 addresses to clients through SLAAC.
- **Null**: Do not allocate addresses to clients.

You should select an allocation method based on the protocol supported by clients on the internal network. If you are not sure about the supported protocol, select **Auto**.

Edit
×

IPv6 Assignment ?

IPv6 Address/Prefix

Length ?

Click **Advanced Settings** to configure more address attributes.

Edit
×

IPv6 Assignment ?

IPv6 Address/Prefix

Length ?

[Advanced Settings](#)

Subnet Prefix Name ?

Subnet Prefix Length ?

Subnet ID ?

* Lease Time (Min) ?

DNS Server

Table 4-48 IPv6 address configuration for LAN port


Parameter	Description
Subnet Prefix Name	Specify the interface from which the prefix is obtained, such as WAN_V6 or WAN1_V6 . By default, the device obtains prefixes from all interfaces.
Subnet Prefix Length	Specify the length of the subnet prefix. The value is in the range of 48 to 64.

Parameter	Description
Subnet ID	Configure the subnet ID in the hexadecimal format. The value 0 indicates auto increment.
Lease Time(Min)	Set the lease of the IPv6 address, in minutes.
DNS Server	Configure the IPv6 DNS server address.

4.21.7 Viewing the DHCPv6 Client

Choose **One-Device > Gateway > Config > Network > IPv6 Address > DHCPv6 Clients**.

When the device functions as a DHCPv6 server to allocate IPv6 addresses to clients, you can view the information about the client that obtains an IPv6 address from the device on the current page. The client information includes the host name, IPv6 address, remaining lease time, and DHCPv6 Unique Identifier (DUID).

Enter the DUID in the search bar and click  to quickly find relative information of the specified DHCPv6 client.

IPv6 Address

1. When IPv6 is enabled, The MTU of IPv4 WAN port need higher than 1280.
2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.

Enable

WAN Settings LAN Settings **DHCPv6 Clients** Static DHCPv6

DHCPv6 Clients
You can view the DHCPv6 clients information on this page.

DHCPv6 Clients Search by IPv6 Address/DUID

No.	Hostname	IPv6 Address	Remaining Lease Time(min)	DUID	Status
<input type="checkbox"/> 1	DESKTOP-3K15PA7	2000::1000	30	000100012a6eb9268cec4b83d7d6	Convert to Static IP

Total 1

- Click **Convert to Static IP** to convert the IP binding of a client with an IP address to static binding. Then the DHCP server assigns a static IP address to the client.
- Click **Bind Selected** to convert the IP binding of multiple clients with IP addresses to static binding. Then the DHCP server assigns static IP addresses to the clients.

4.21.8 Configuring the Static DHCPv6 Address

Configure the IPv6 address statically bound to the DUID of a client so that the client can obtain the specified address each time.

Choose **One-Device > Gateway > Config > Network > IPv6 Address > Static DHCPv6**.

Static IP Address List Search by IPv6 Address/DUID

No.	IPv6 Address	DUID	Action
No Data			

Up to 200 entries can be added. Total 0

- (1) Click **Add**.

Add
×

* Interface

* IPv6 Address

* MAC Address

- (2) Select the MAC address and IP address to be bound, and click **Bind** in the **Action** column to bind the IP address to the MAC address to prevent ND attacks.

IPv6 Neighbor List

No.	IPv6 Address	MAC Address	Type	Ethernet status	Action
<input type="checkbox"/> 1	fe80::139:bf7:aa4f:dc1	7c:.....:lc	Dynamic	WAN	Bind
<input type="checkbox"/> 2	fe80::79e8:e7c0:9949:45a2	30:.....:1	Dynamic	WAN	Bind

4.22 Configuring Routes

4.22.1 Configuring Static Routes

Static routes are manually configured by the user. When a data packet matches a static route, the packet will be forwarded according to the specified forwarding mode.

⚠ Caution

Static routes cannot automatically adapt to changes of the network topology. When the network topology changes, you need to reconfigure the static routes.

1. Configuring IPv4 Static Routing

Choose **One-Device > Gateway > Config > Advanced > Routing > Static Routing**.

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

Static Route List ? + Add Delete Selected

<input type="checkbox"/>	Dest IP Address ?	Subnet Mask ?	Outbound Interface ?	Next Hop ?	Reachable ?	Action
<input type="checkbox"/>	10.52.48.0	255.255.255.0	WAN0	10.52.48.43	Yes	Edit Delete

Up to 100 entries can be added. Total 1 < 1 > 10/page ▾

Add ×

* Dest IP Address

* Subnet Mask

* Outbound Interface ▾

* Next Hop

Table 4-49 Static route configuration

Parameter	Description
Dest IP Address	Specify the destination network to which the data packet is to be sent. The device matches the data packet based on the destination address and subnet mask.
Subnet Mask	Specify the subnet mask of the destination network. The device matches the data packet based on the destination address and subnet mask.
Outbound Interface	Specify the interface that forwards the data packet.
Next Hop	Specify the IP address of the next hop in the route for the data packet. If the outbound interface accesses the Internet through PPPoE dialing, you do not need to configure the next-hop address.

After a static route is created, you can find the relevant route configuration and reachability status in the static route list. The **Reachable** parameter specifies whether the next hop is reachable, based on which you can determine whether the route takes effect. If the value is **No**, check whether the outbound interface in the current route can ping the next-hop address.

Static Route List ? + Add Delete Selected

<input type="checkbox"/>	Dest IP Address ?	Subnet Mask ?	Outbound Interface ?	Next Hop ?	Reachable ?	Action
<input type="checkbox"/>	10.52.48.0	255.255.255.0	WAN0			
<input type="checkbox"/>	192.168.110.0	255.255.255.0	WAN0	192.168.10.1	No ?	Edit Delete

The route is unreachable. Please initiate a Ping test from the outbound interface to the next hop.

Up to 100 entries can be added. Total 2 < 1 > 10/page

2. Configuring the IPv6 Static Route

Choose **One-Device > Gateway > Config > Advanced > Routing > IPv6 Static Routing**.

Static Route List ? + Add Delete Selected

<input type="checkbox"/>	IPv6 Address	Prefix Length	Interface ?	Next Hop ?	Action
No Data					

Up to 100 entries can be added. Total 0 < 1 > 10/page

(1) Click **Add**.

Add ×

* IPv6 Address/Prefix Length ?

* Interface ? ▼

* Next Hop ?

(2) Configure an IPv6 static route of the device.

Table 4-50 Description of IPv6 Static Routing Configuration Parameters

Parameter	Description
IPv6 Address/Prefix Length	Destination network of the packet. The destination address of the packet is matched according to the IPv6 address and prefix length.
Outbound Interface	Interface that forwards the packet.

Parameter	Description
Next Hop	IP address of the next routing node to which the packet is sent.

(3) Click **OK**.

4.22.2 Configuring PBR

Policy-based routing (PBR) is a mechanism for routing and forwarding based on user-specified policies. When a router forwards data packets, it filters the packets according to the configured rules, and then forwards the matched packets according to the specified forwarding policy. The PBR feature enables the device to formulate rules according to specific fields (source or destination IP address and protocol type) in the data packets, and forward the data packets from a specific interface.

In a multi-line scenario, if the device is connected to the Internet and the internal network through different lines, the traffic will be evenly routed over the lines if no routing settings are available. In this case, access data to the internal network may be sent to the external network, or access data to the external network may be sent to the internal network, resulting in network exceptions. To prevent these exceptions, you need to configure PBR to control data isolation and forwarding on the internal and external networks.

The device can forward data packets using either of the following three policies: PBR, address-based routing, and static routing. When all the policies exist, PBR, static routing, and address-based routing have descending order in priority. For details on address-based routing, see Section [4.4.7 Configuring the Multi-Line Load Balancing Mode](#).

1. Configuring IPv4 PBR

Choose **One-Device > Gateway > Config > Advanced > Routing > PBR**.

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

Route Priority: PBR > > URL > Static Routing > ISP Routing.


PBR List ? + Add Delete Selected


<input type="checkbox"/>	Name ?	Protocol Type ?	Src IP Address ?	Dest IP Address ?	Src Port Range ?	Dest Port Range ?	Outbound Interface ?	Traffic Assurance	Effective State	Action
No Data										


Up to 30 entries can be added. Total 0 1 10/page


Add PBR





* Name 

Protocol Type 

Src IP/IP Range 

Dest IP/IP Range 

Outbound Interface 

Traffic Assurance 

Effective State

Cancel

OK



Table 4-51 Description of IPv4 PBR Configuration Parameters

Parameter	Description
Name	Specify the name of the PBR rule, which uniquely identifies a PBR rule. The name must be unique for each rule.
Protocol Type	Specify the protocol to which the PBR rule is effective. You can set this parameter to IP , ICMP , UDP , TCP , or Custom .
Protocol Number	When Protocol Type is set to Custom , you need to enter the protocol number.
Src IP/IP Range	Configure the source IP address or IP address range for matching PBR entries. The default value is All IP Addresses. <ul style="list-style-type: none"> ● All IP Addresses: Match all the source IP addresses. ● Custom: Match the source IP addresses in the specified IP range.
Custom Src IP	When Src IP/IP Range is set to Custom , you need to enter a single source IP address or a source IP range.

Parameter	Description
Dest IP/IP Range	Configure the destination IP address or IP address range for matching PBR entries. The default value is All IP Addresses. <ul style="list-style-type: none"> ● All IP Addresses: Match all the destination IP addresses. ● Custom: Match the destination IP addresses in the specified IP range.
Custom Dest IP	When Dest IP/IP Range is set to Custom, you need to enter a destination source IP address or a destination IP range.
Src Port Range	This parameter is available only when Protocol Type is set to TCP or UDP. This parameter specifies the source port range for packet matching using PBR.
Dest Port Range	This parameter is available only when Protocol Type is set to TCP or UDP. This parameter specifies the destination port range for packet matching using PBR.
Outbound Interface	Specify the interface that forwards the data packet based on the hit PBR rule.
Traffic Assurance	When an outbound interface is unreachable, the traffic will be automatically routed to other reachable outbound interfaces.
Effective State	Turn on Effective State to specify whether to enable the PBR rule. If Effective State is turned off, this rule does not take effect.

Note

If you want to restrict the access device to access only the specified internal network, you can set the outbound interface in the corresponding route to the WAN port in the private line network.

All the created PBR policies are displayed in the PBR list, with the latest policy listed on the top. The device matches the policies according to their sorting in the list. You can manually adjust the policy matching sequence by clicking  or  in the **Match Order** column.

PBR List ⓘ + Add Delete Selected

<input type="checkbox"/>	Name ⓘ	Protocol Type ⓘ	Src IP Address ⓘ	Dest IP Address ⓘ	Src Port Range ⓘ	Dest Port Range ⓘ	Outbound Interface ⓘ	Traffic Assurance	Effective State ⓘ	Match Order ⓘ	Action
<input type="checkbox"/>	test2	IP	1.1.1.1	2.2.2.2	-	-	WAN0	Enable	Enable ⓘ	↓	Edit Delete
<input type="checkbox"/>	test1	IP	All IP Addresses	All IP Addresses	-	-	WAN0	Enable	Enable ⓘ	↑	Edit Delete

Up to 30 entries can be added. Total 2 1 10/page

2. Configuring IPv6 PBR

Choose **One-Device > Gateway > Config > Advanced > Routing > IPv6 PBR**.

PBR List ? + Add Delete Selected

<input type="checkbox"/>	Name ?	Protocol Type ?	Src IP Address	Dest IP Address	Src Port Range ?	Dest Port Range ?	Outbound Interface ?	Traffic Assurance	Effective State	Action
No Data										

Up to 30 entries can be added. Total 0 < 1 > 10/page

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

Add PBR ×

* Name ?

Protocol Type ?

Src IP/IP Range ?

Dest IP/IP Range ?

Outbound Interface ?

Traffic Assurance ?

Effective State ?



Table 4-52 Description of IPv6 PBR Configuration Parameters


Parameter	Description
Name	Specify the name of the PBR rule, which uniquely identifies a PBR rule. The name must be unique for each rule.
Protocol Type	Specify the protocol to which the PBR rule is effective. You can set this parameter to IP , ICMPv6 , UDP , TCP , or Custom .
Protocol Number	When Protocol Type is set to Custom , you need to enter the protocol number.
Src IP/IP Range	Configure the source IP address or IP address range for matching PBR entries. The default value is All IP Addresses. <ul style="list-style-type: none"> ● All IP Addresses: Match all the source IP addresses. ● Custom: Match the source IP addresses in the specified IP range.


Parameter	Description
Custom Src IP	When Src IP/IP Range is set to Custom , you need to enter a single source IP address or a source IP range.
Dest IP/IP Range	Configure the destination IP address or IP address range for matching PBR entries. The default value is All IP Addresses. <ul style="list-style-type: none"> ● All IP Addresses: Match all the destination IP addresses. ● Custom: Match the destination IP addresses in the specified IP range.
Custom Dest IP	When Dest IP/IP Range is set to Custom, you need to enter a destination source IP address or a destination IP range.
Src Port Range	This parameter is available only when Protocol Type is set to TCP or UDP. This parameter specifies the source port range for packet matching using PBR.
Dest Port Range	This parameter is available only when Protocol Type is set to TCP or UDP. This parameter specifies the destination port range for packet matching using PBR.
Outbound Interface	Specify the interface that forwards the data packet based on the hit PBR rule.
Traffic Assurance	When an outbound interface is unreachable, the traffic will be automatically routed to other reachable outbound interfaces.
Effective State	Turn on Effective State to specify whether to enable the PBR rule. If Effective State is turned off, this rule does not take effect.








 Note




If you want to restrict the access device to access only the specified internal network, you can set the outbound interface in the corresponding route to the WAN port in the private line network.

All the created PBR policies are displayed in the PBR list, with the latest policy listed on the top. The device matches the policies according to their sorting in the list. You can manually adjust the policy matching sequence by clicking  or  in the **Match Order** column.

PBR List 

+ Add  Delete Selected

<input type="checkbox"/>	Name 	Protocol Type 	Src IP Address	Dest IP Address	Src Port Range 	Dest Port Range 	Outbound Interface 	Traffic Assurance	Effective State	Match Order	Action
<input type="checkbox"/>	test2	IP	2000::1	All IP Addresses	-	-	WAN0	Enable	Enable 	↓	Edit Delete
<input type="checkbox"/>	test1	IP	All IP Addresses	All IP Addresses	-	-	WAN0	Enable	Enable 	↑	Edit Delete

Up to 30 entries can be added. Total 2  **1**  10/page 

3. Typical Configuration Example

- Networking Requirements

Two lines with different bandwidths are deployed for an enterprise. Line A (WAN 1) is used for access to the Internet and Line B (WAN 2) is used for access to the specific internal network (10.1.1.0/24). The enterprise wants to configure PBR to guarantee correct data flows between the internal and external networks, isolate devices in the specified address range (172.26.31.1 to 172.26.31.200) from the external network, and allow these devices to access the specific internal network only.

- Configuration Roadmap
- Configure the private line.
- Add a PBR policy for access to the internal network.
- Add a PBR policy for access to the external network.
- Add a PBR policy to restrict specific devices to access the internal network only.
- Configuration Steps

(1) Configure WAN 2 as the private line for the internal network.

When you configure networking parameters for WAN 2 port, click **Advanced Settings**, turn on **Private Line**, and click **Save**.

----- Advanced Settings -----

* MTU (?) [MTU Detection](#)

* MAC Address (?)

802.1Q Tag

Private Line (?)

NAT Mode (?)

[Save](#)

(2) Add a PBR policy to forward data packets destined to the external network through WAN 1 port.

Choose **One-Device > Gateway > Config > Advanced > Routing > PBR** and click **Add**. In the dialog box that appears, create a PBR policy and set **Outbound Interface** to **WAN1**.

Add PBR ×

* Name ?

Protocol Type ?

Src IP/IP Range ?

Dest IP/IP Range ?

Outbound Interface ?

Traffic Assurance ?

Effective State

- (3) Add a PBR policy to forward data packets destined to the internal network through WAN 2 port.
In this policy, set **Custom Dest IP** to 10.1.1.1-10.1.1.254 and **Outbound Interface** to WAN2.

Add PBR ×

* Name ?

Protocol Type ?

Src IP/IP Range ?

Dest IP/IP Range ?

* Custom Dest IP

Outbound Interface ?

Traffic Assurance ?

Effective State

- (4) Add a PBR policy to restrict devices in the IP range 172.26.31.1 to 172.26.31.200 to access the internal private line only.

In this policy, set **Src IP/IP Range** to **Custom**, **Custom Src IP** to 172.26.31.1-172.26.31.200, and **Outbound Interface** to WAN2.

Add PBR
×

* Name ?

Protocol Type ?

Src IP/IP Range ?

* Custom Src IP

Dest IP/IP Range ?

Outbound Interface ?

Traffic Assurance ?

Effective State

4.22.3 Configuring RIP

i Note

Only RG-EG105G-V3, RG-EG105G-P-V3, RG-EG210G-P-V3, RG-EG1510XS and RG-EG3XX series devices (such as RG-EG310GH-E) support this function.

Routing Information Protocol (RIP) is applicable to small and medium-sized networks and is a dynamic routing protocol that is easy to configure. RIP measures the network distance based on the number of hops and selects a route based on the distance. RIP uses UDP port 520 to exchange the routing information.

1. Configuring RIP Basic Functions

Choose **One-Device > Gateway > Config > Advanced > Routing > RIP Settings**

Click **Add** and configure the network segment and interface.

RIP Settings | Port Settings | Advanced | Neighbor Info

Network Segment/Port List ? + Add Delete Selected

No.	Network Segment/Port	Auth Mode	Action
No Data			

Add ×

Type Network Segment Port

* Network Segment

Cancel OK

Add ×

Type Network Segment Port

* Port

Auth Mode

* Auth Key

Cancel OK

Table 4-53 RIP Configuration Parameters

Parameter	Description
Type	<ul style="list-style-type: none"> ● Network Segment: Enable RIP in the specified network segment. The IP addresses of this network segment are added to the RIP routing table. The device and its RIP-enabled neighbor devices learn the routing table from each other. ● Port: Enable RIP on the specified port. All the IP addresses of this port are added to the RIP routing table. The device and its RIP-enabled neighbor devices learn the routing table from each other.

Network Segment	Enter the network segment, for example, 10.1.0.0/24 , when Type is set to Network Segment . RIP will be enabled on all interfaces of the device covered by this network segment.
Port	Select a VLAN interface or physical port when Type is set to Port .
Auth Mode	<ul style="list-style-type: none"> ● No Authentication: The protocol packets are not authenticated. ● Plain Text: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text.
Auth Key	Enter the authentication key to authenticate protocol packets when Auth Mode is set to Plain Text .

2. Configuring the RIP Port

Choose **One-Device > Gateway > Config > Advanced > Routing > RIP Settings > Port Settings**

RIP Settings	Port Settings	Advanced	Neighbor Info					
Port Name	Rx Status	Tx Status	Poison Reverse	v2 Broadcast Packet	Auth Mode	Auth Key	Action	
WAN	v2	v2	Off	Off	Encrypted Text	ruijie123	Edit	

Table 4-54 Configuration Parameters in the Port List

Parameter	Description
Port Name	Name of the port where RIP is enabled.
Rx Status	RIP version of packets currently received.
Tx Status	RIP version of packets currently transmitted.
Poison Reverse	After the port learns the route, the route overhead is set to 16 (indicating that the route is unreachable), and the route is sent back to the neighbor from the original port to avoid a loop.
v2 Broadcast Packet	When a neighbor does not support multicast, broadcast packets can be sent. You are advised to disable RIPv2 broadcast packets to improve network performance.
Auth Mode	<ul style="list-style-type: none"> ● No Authentication: The protocol packets are not authenticated. ● Plain Text: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text.
Auth Key	Enter the authentication key to authenticate protocol packets when Auth Mode is set to Plain Text .

Action	Click Edit to modify RIP settings of the port.
--------	---

3. Configuring the RIP Global Configuration

Choose **One-Device > Gateway > Config > Advanced > Routing > RIP Settings > Advanced**, click **Edit Config**, and configure RIP global configuration parameters.

RIP Settings Port Settings **Advanced** Neighbor Info

RIP Global Config ⓘ Edit Config

RIP Version	Equal-cost Load Balancing	Route Advertisement	Administrative Distance	Update Timer	Invalid Timer	Flush Timer
Default	Off	Off	1 (Default)	30 s	180 s	120 s

Edit Config



RIP Version ⓘ

Equal-cost Load Balancing

Route Advertisement

Administrative Distance

* Update Timer s (5-2147483647)

* Invalid Timer s (5-2147483647)

* Flush Timer s (5-2147483647)

Table 4-55 RIP Global Configuration Parameters

Parameter	Description
RIP Version	<ul style="list-style-type: none"> ● Default: Select RIPv2 for sending packets and RIPv1/v2 for receiving packets. ● V1: Select RIPv1 for sending and receiving packets. ● V2: Select RIPv2 for sending and receiving packets.
Route Advertisement	After route advertisement is enabled, the current device generates a default route and sends it to the neighbor.
Administrative Distance	Redistribute routes of other protocols to the RIP domain so that RIP can interwork with other routing domains.
Update Timer	RIP update cycle. The routing information is updated every 30 seconds by default.
Invalid Timer	If no update is received before a route becomes invalid, the route is considered unreachable. The default value is 180 seconds.
Flush Timer	If no update is received before the flush timer of an invalid route expires, the route is completely deleted from the RIP routing table. The default value is 120 seconds.

4. Configuring the RIP Route Redistribution List

Redistribute routes of other protocols to the RIP domain so that RIP can interwork with other routing domains.

Choose **One-Device > Gateway > Config > Advanced > Routing > RIP Settings > Advanced**, click **Add** in **Route Redistribution List**, and select the type and administrative distance.

Route Redistribution List ⓘ

+ Add

Delete Selected

<input type="checkbox"/>	Type	Administrative Distance	Instance ID	Action
No Data				

Add
×

* Type ▼

* Administrative Distance ▼

* Instance ID ▼

Table 4-56 RIP Route Redistribution Parameters

Parameter	Description
Type	Configure the type of routes that are learned by a routing protocol and then redistributed to RIP. The types include direct routes, OSPF routes, and static routes.
Administrative Distance	The device converts the metric of the routes learned from other routing protocols into the metric used by the target protocol so that the target protocol can select the optimal route. A smaller administrative distance indicates a higher priority. The default value is 0. The value ranges from 0 to 16.
Instance ID	Select the instance ID of OSPF that needs to be redistributed. OSPFv2 needs to be enabled on the local device.

5. Configuring the Passive Interface

If an interface is configured as a passive interface, it will suppress RIP update packets. If the connected peer device does not run RIP, you are advised to enable the passive interface.

Choose **One-Device > Gateway > Config > Advanced > Routing > RIP Settings > Advanced**, click **Add** in **Passive Interface** and select a passive interface.

Passive Interface ⓘ

	Port Name	Action
<input type="checkbox"/>		
No Data		

Add
×

* Passive Interface

Cancel
OK

6. Configuring the Neighbor Route

When the router cannot process broadcast packets, another router can be designated as the neighbor to establish a RIP direct link.

Choose **One-Device > Gateway > Config > Advanced > Routing > RIP Settings > Advanced**, click **Add** in **Neighbor Route**, and enter the IP address of the neighbor router.

Neighbor Route ⓘ

+ Add
Delete Selected

	Address	Action
<input type="checkbox"/>		
No Data		

Add
×

* Neighbor Route

Cancel
OK

7. Viewing the Neighbor Information

Choose **One-Device > Gateway > Config > Advanced > Routing > RIP Settings > Neighbor Info**.

The neighbor list displays information about neighbors of the device, including the neighbor address, neighbor protocol version, local address, connected interface, number of received error packets, and number of received error routes.

Neighbor Address	Neighbor Protocol Version	Local Address	Connected Interface	Rx Error Packets	Rx Error Routes
10.52.48.4	0	10.52.48.43	--	28	0

Total 1 < **1** > 10/page ▾

4.22.4 Configuring RIPng

Note

Only RG-EG105G-V3, RG-EG105G-P-V3, RG-EG210G-P-V3, RG-EG1510XS and RG-EG3XX series devices (such as RG-EG310GH-E) support this function.

RIP Next Generation (RIPng) provides the routing function for IPv6 networks.

RIPng uses UDP port 512 to exchange the routing information.

1. Configuring RIPng Basic Functions

Choose **One-Device > Gateway > Config > Advanced > Routing > RIPng Settings**

Click **Add**, set **Type** to **Network Segment** or **Port**, and specify the network segment or port accordingly.

No.	Network Segment/Port	Action
No Data		

Add ×

Type Network Segment Port

* Network Segment ?

Example: 2000::1

Cancel

OK

Add

✕

Type Network Segment Port* Port

Cancel

OK

Table 4-57 RIPng Configuration Parameters

Parameter	Description
Type	<ul style="list-style-type: none"> ● Network Segment: Enable RIP in the specified network segment. The IP addresses of this network segment are added to the RIP routing table, and the device and its RIP-enabled neighbor devices learn the routing table from each other. ● Port: Enable RIP on the specified port. All the IP addresses of this port are added to the RIP routing table, and the device and its RIP-enabled neighbor devices learn the routing table from each other.
Network Segment	Enter the IPv6 address and prefix length when Type is set to Network Segment . RIPng will be enabled on all interfaces of the device covered by this network segment.
Port	Select a VLAN interface or physical port when Type is set to Port .

2. Configuring the RIPng Port

RIPng poison reverse: After the port learns the route, the route overhead is set to **16** (indicating that the route is unreachable), and the route is sent back to the neighbor from the original port to avoid a loop.

Choose **One-Device > Gateway > Config > Advanced > Routing > RIPng Settings > Port Settings**, click **Edit**, and enable IPv6 poison reverse.

Port Name	IPv6 Poison Reverse	Action
VLAN 55	Off	Edit

Edit ×

* Port Name VLAN 55 ▼

IPv6 Poison Reverse

Cancel OK

3. Configuring the RIPng Global Configuration

Choose **One-Device > Gateway > Config > Advanced > Routing > RIPng Settings > Advanced**, click **Edit Config** in **RIPng Global Config**, and configure RIPng global configuration parameters.

RIPng Settings
Port Settings
Advanced
Neighbor Info

RIPng Global Config Edit Config

Equal-cost Load Balancing	Route Advertisement	Administrative Distance	Update Timer	Invalid Timer	Flush Timer
Off	Off	1 (Default)	30 s	180 s	120 s

Edit Config ×

Equal-cost Load
Balancing

Route Advertisement

Administrative 1 (Default) ▼
Distance

* Update Timer 30 s (1-65535)

* Invalid Timer 180 s (1-65535)

* Flush Timer 120 s (1-65535)

Cancel OK

Table 4-58 RIPng Global Configuration Parameters

Parameter	Description
Equal-cost Load Balancing	After this function is enabled, equal-cost routes are automatically balanced and forwarded with a weight of 1:1.
Route Advertisement	After this function is enabled, the current device generates a default route and sends it to the neighbor.
Administrative Distance	Routes of other protocols are redistributed to the RIP domain so that RIP can communicate with other routing domains.
Update Timer	RIP update cycle. The routing information is updated every 30 seconds by default.
Invalid Timer	If no update is received before a route becomes invalid, the route is considered unreachable. The default value is 180 seconds.
Flush Timer	If no update is received before the flush timer of an invalid route expires, the route is completely deleted from the RIP routing table. The default value is 120 seconds.

4. Configuring the RIPng Route Redistribution List

Redistribute routes of other protocols to the RIPng domain to interwork with other routing domains.

Choose **One-Device > Gateway > Config > Advanced > Routing > RIPng Settings > Advanced**, click **Add** in **Route Redistribution List**, and configure RIPng route redistribution.

Route Redistribution List ⓘ + Add Delete Selected

<input type="checkbox"/>	Type	Administrative Distance	Action
No Data			

Add ×

* Type ▼

* Administrative Distance ▼

Table 4-59 RIP Route Redistribution Parameters

Parameter	Description
Type	Configure the type of routes that are learned by a routing protocol and then redistributed to RIP. The types include direct routes, OSPF routes, and static routes.
Administrative Distance	The device converts the metric of the routes learned from other routing protocols into the metric used by the target protocol so that the target protocol can select the optimal route. A smaller administrative distance indicates a higher priority. The default value is 0. The value ranges from 0 to 16.

5. Configuring the RIPng Passive Interface

If an interface is configured as a passive interface, it will suppress RIPng update packets. If the connected peer device does not run RIP, you are advised to enable the passive interface.

Choose **One-Device > Gateway > Config > Advanced > Routing > RIPng Settings > Advanced**, click **Add** in **Passive Interface**, and select a passive interface.

Passive Interface ? + Add Delete Selected

	Port Name	Action
<input type="checkbox"/>		

No Data

Add ×

* Passive Interface Select ▼

Cancel
OK

6. Configuring the IPv6 Aggregate Route

Choose **One-Device > Gateway > Config > Advanced > Routing > RIPng Settings > Advanced**, click **Add** in **RIPng Aggregate Routing**, and enter the IPv6 address or length. The length of IPv6 address prefix ranges from 0 bit to 128 bits.

RIPng Aggregate Routing ? + Add Delete Selected

	Address	Action
<input type="checkbox"/>		

No Data

Add
×

* IPv6 Aggregate

Routing

Cancel
OK

7. Viewing the Neighbor Information

Choose **One-Device > Gateway > Config > Advanced > Routing > RIP Settings > Neighbor Info**.

The neighbor list displays information about neighbors of the device, including the neighbor address, neighbor protocol version, local address, connected interface, number of received error packets, and number of received error routes.

Neighbor Address	Neighbor Protocol Version	Local Address	Connected Interface	Rx Error Packets	Rx Error Routes
No Data					

Total 0 < 1 > 10/page

4.22.5 OSPF v2

i Note

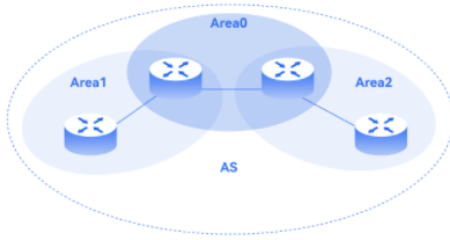
Only RG-EG105G-V3, RG-EG105G-P-V3, RG-EG210G-P-V3, RG-EG1510XS and RG-EG3XX series devices (such as RG-EG310GH-E) support this function.

Open Shortest Path First (OSPF) can be applied to large-scale networks. IPv4 uses OSPFv2, and IPv6 uses OSPFv3.

OSPF is a typical link-state routing protocol, which can solve the problems of slow route update, inaccurate measurement, and poor scalability in large networks. It is suitable for networks of various sizes, and even a network with up to thousands of devices.

1. Configuring OSPFv2 Basic Parameters

Choose **One-Device > Gateway > Config > Advanced > Routing > OSPFV2**, click **Start Setup**, and then configure an instance and an interface respectively.



OSPF

OSPF is a typical link-state routing protocol. To satisfy users' increasing requirements for network reliability and heterogeneity on a large network, OSPF solves the problems such as slow convergence, unscientific metric values, and poor scalability.

Highlights

- Achieves fast convergence.
- Minimizes routing overhead.
- Reduces routing update traffic through area partition.
- Applies to various networks with up to thousands of switches.

[Start Setup](#)

- Configure an instance
 - (1) Configure basic parameters for an instance.

1 ————— 2 ————— 3
 Configure the instance. **Configure the interface.** Operation succeeded.

* Instance ID

* Router ID (?)

Advertise Default Route

- Import External Route
- Static Route Redistribution
 - Direct Route Redistribution
 - RIP Redistribution

----- [Details](#) -----

Table 4-60 Description of Basic OSPF Instance Configuration Parameters

Parameter	Description
Instance ID	Create an OSPF instance based on the service type. The instance only takes effect locally, and does not affect packet exchange with other devices.

Parameter	Description
Router ID	<p>It identifies a router in an OSPF domain.</p> <p>Caution: Router IDs within the same domain must be unique. The same configuration may cause neighbor discovery failures.</p>
Advertise Default Route	<p>Generate a default route and send it to the neighbor.</p> <p>After this function is enabled, you need to enter the metric and select a type. The default metric is 1.</p> <ul style="list-style-type: none">● Type 1: The metrics displayed on different routers vary.● Type 2: The metrics displayed on all routers are the same.
Import External Route	<p>Redistribute routes of other protocols to the OSPF domain to interwork with other routing domains.</p> <ul style="list-style-type: none">● If Static Route Redistribution is selected, enter the metric, which is 20 by default.● If Direct Route Redistribution is selected, enter the metric, which is 20 by default.● If RIP Redistribution is selected, enter the metric, which is 20 by default.

(2) Click **Details** to display detailed configurations.

----- Details -----

Distance

Intra-Area Default:110

Inter-Area Default:110

External Default:110

LSA

Generation Delay Default:5000ms

Received Delay Default:1000ms

SPF Calculation

Waiting Interval Default:0ms

Min Interval Default:50ms

Max Interval Default:5000ms

Graceful Restart Graceful Restart

Helper

LSA Check

* Max Wait Time 1800

Table 4-61 Description of Detailed OSPF Instance Configuration Parameters

Parameter	Description
Distance	It is used for protocol selection. By default, the intra-area, inter-area, and external distances are all 110 .
LSA	Frequent network changes and route flapping may occupy too much network bandwidth and device resources. The LSA generation and reception delays are specified in OSPF by default. The default value is 1000 ms.

Parameter	Description
SPF Calculation	<p>When the link state database (LSDB) changes, OSPF recalculates the shortest path, and sets the interval to prevent frequent network changes from occupying a large number of resources</p> <ul style="list-style-type: none"> ● Waiting Interval: When the state changes, the timer is triggered. The delay is calculated for the first time after the timer expires. The default value is 0 ms. ● Min Interval: As the number of changes increases, the time of each interval will increase according to the algorithm, and the default value is 50 ms. ● Max Interval: When the calculated interval reaches the maximum interval, the subsequent interval is always equal to the maximum interval. If the time from the last calculation exceeds the maximum interval and the LSDB is not updated, the timer is disabled.
Graceful Restart	<p>Graceful Restart (GR) can avoid route flapping caused by traffic interruption and active/standby board switchover, thus ensuring the stability of key services.</p> <ul style="list-style-type: none"> ● Graceful Restart Helper: The Graceful Restart Helper function is enabled when this switch is turned on. ● LSA Check: LSA packets outside the domain are checked when this switch is turned on. ● Max Wait Time: Timing starts after the device receives the GR packet from the peer device. If the peer device does not complete GR within Max Wait Time, the device exits the GR Helper mode. The default value is 1800 seconds.

- Configure an interface
 - (1) Configure basic parameters for an OSPFv2 interface.

① ————— ② ————— ③

Configure the instance. Configure the interface. **Operation succeeded.**

* Interface

* Area

Stub Area

----- Details -----

Table 4-62 Description of Basic OSPFv2 Interface Configuration Parameters

Parameter	Description
Interface	Select the OSPF-enabled L3 interface.
Area	Configure the area ID. Value range: 0-4294967295

Parameter	Description
Stub Area	<p>If Stub Area is enabled, you need to configure the Area Type and Inter-Route Isolation</p> <ul style="list-style-type: none"> ● Area Type <ul style="list-style-type: none"> ○ Stub area: Routers at the edge of the area do not advertise routes outside the area, and the routing table in the area is small. ○ Not-So-Stubby Area (NSSA): A few external routes can be imported. ● Inter-Route Isolation <p>After this function is enabled, inter-area routes will not be imported to this area.</p>

(2) Click **Details** to display detailed configurations.

----- Details -----

Priority

Network Type ▼

Hello Packets

Dead Interval

LSA Transmission

Delay

LSA Retransmission

Interval

Interface Auth ▼

Ignore MTU Check

Table 4-63 Description of Detailed OSPFv2 Interface Configuration Parameters

Parameter	Description
Priority	A higher priority value indicates a greater chance of being elected as the DR or BDR. The default value is 1.
Network Type	OSPFv2 defines different network types, which affect the establishment of OSPF neighbor relationships, route update, and network convergence. The supported network types include broadcast, unicast, multicast, and non-broadcast multi-access (NBMA).
Hello Packets	Interval for periodic transmission, which is used to discover and maintain OSPF neighbor relationship. The default value is 10 seconds.
Dead Interval	Time after which the neighbor becomes invalid. The default value is 40 seconds.
LSA Transmission Delay	LSA transmission delay of the interface. The default value is 1 second.
LSA Retransmission Interval	Time after which LSA is retransmitted after LSA is lost. The default value is 5 seconds.
Interface Auth	<ul style="list-style-type: none"> ● No Auth: The protocol packets are not authenticated. It is the default value. ● Plain Text: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text. ● MD5: The protocol packets are authenticated, and the authentication key is MD5 encrypted and then transmitted with the protocol packets.
Ignore MTU Check	The purpose of ignoring MTU check is to ensure that OSPF-enabled routers can update routing information in time when the network topology changes. This function is enabled by default.

(3) Click **Add** to add an interface to **Interface List**.

Port List

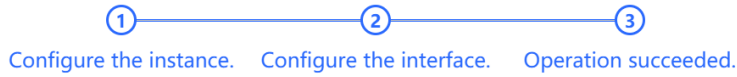
Up to 16 entries can be added.

Interface	Area	Priority	Network Type	Hello Packets	Dead Interval	Interface Auth	LSA Transmission Delay	LSA Retransmission Interval	Action
WAN0	1		Broadcast			No Auth			Delete

Total 1 1 / 10/page

[Previous](#) [Finish](#)

(4) Click **Finish**.



Operation succeeded.

After you create an instance and an interface, choose **One-Device > Gateway > Advanced > Routing > OSPFV2** to check the current **Instance List**.

Instance List + Add

Instance ID	Router ID	Interface	Area	Advertise Default Route	Import External Route	Action
1	1.1.1.1	WAN0	1(Normal Area)	Disable	Static Route Redistribution : Off Direct Route Redistribution : Off RIP Redistribution : Off	More Neighbor Info Edit Delete

Up to 16 entries can be added. Total 1 < 1 > 10/page

2. Adding an OSPFv2 Interface

Choose **One-Device > Gateway > Config > Advanced > Routing > OSPFV2**, select the instance to be configured in **Instance List**, and choose **More > V2 Interface**.

Instance List + Add

Instance ID	Router ID	Interface	Area	Advertise	Import External Route	Action
1	1.1.1.1	WAN0	1(Normal Area)	V2 Interface V2 Instance Route Redistribution V2 Neighbor Management	RIP Redistribution : Off	More Neighbor Info Edit Delete

Up to 16 entries can be added. Total 1 < 1 > 10/page

V2 Interface
✕

* Interface

* Area

Stub Area

[Details](#)

Port List
Add
Reset

Up to 64 entries can be added.

Interface	Area	Priority	Network Type	Hello Packets	Dead Interval	Interface Auth	LSA Transmission Delay	LSA Retransmission Interval	Action
WAN0	1		Broadcast			No Auth			Edit

Total 1

<
1
>

10/page
▾

3. Redistributing OSPFv2 Instance Routes

Choose **One-Device > Gateway > Config > Advanced > Routing > OSPFV2**, select the instance to be configured in **Instance List**, and choose **More > V2 Instance Route Redistribution**.

Caution

The instance ID cannot be selected for route redistribution.

Instance List
+ Add

Instance ID	Router ID	Interface	Area	Advertise	Import External Route	Action
1	1.1.1.1	WAN0	1(Normal Area)	<div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>V2 Interface</p> <p style="border: 2px solid red; padding: 2px;">V2 Instance Route Redistribution</p> <p>V2 Neighbor Management</p> </div>		<div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p style="border: 2px solid red; padding: 2px;">More</p> <p>Neighbor Info</p> <p>Edit Delete</p> </div>

RIP Redistribution : Off

Up to 16 entries can be added.

Total 1

<
1
>

10/page
▾

V2 Instance Route Redistribution
✕

!

* Instance ID

Metric

Add
Reset

Up to 63 entries can be added.

Instance ID	Metric	Action
No Data		

Total 0
<
1
>
10/page

4. Managing OSPFv2 Neighbors

Choose **One-Device > Gateway > Config > Advanced > Routing > OSPFv2**, select the instance to be configured in **Instance List**, and choose **More > V2 Neighbor Management**.

Instance List
+ Add

Instance ID	Router ID	Interface	Area	Advertise	Import External Route	Action
1	1.1.1.1	WAN0	1(Normal Area)	<div style="border: 1px solid #ccc; padding: 2px; width: 150px; margin: 0 auto;"> V2 Interface V2 Instance Route Redistribution V2 Neighbor Management </div>		<div style="border: 1px solid #ccc; padding: 2px; width: 100px; margin: 0 auto;"> More Neighbor Info Edit Delete </div>

RIP Redistribution : Off

Up to 16 entries can be added.
Total 1
<
1
>
10/page

V2 Neighbor Management
✕

* Neighbor IP

Add
Reset

Up to 64 entries can be added.

Neighbor IP	Action
No Data	

Total 0
<
1
>
10/page

5. Viewing OSPFv2 Neighbor Information

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **OSPFV2**, select the instance to be configured in **Instance List**, and click **Neighbor Info**.

Instance List + Add

Instance ID	Router ID	Interface	Area	Advertise Default Route	Import External Route	Action
1	1.1.1.1	WAN0	1(Normal Area)	Disable	Static Route Redistribution : Off Direct Route Redistribution : Off RIP Redistribution : Off	More Neighbor Info Edit Delete

Up to 16 entries can be added. Total 1 < 1 > 10/page

Neighbor Info

Instance ID	Router ID	Status	Neighbor IP	Interface
No Data				

Total 0 < 1 > 10/page

4.22.6 OSPF v3

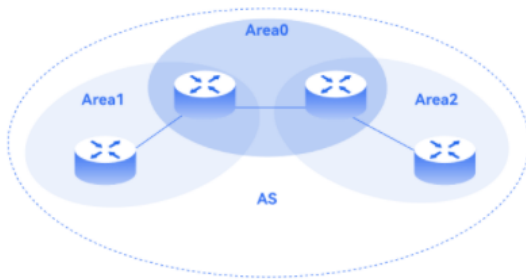
Note

Only RG-EG105G-V3, RG-EG105G-P-V3, RG-EG210G-P-V3, RG-EG1510XS and RG-EG3XX series devices (such as RG-EG310GH-E) support this function.

Open Shortest Path First (OSPF) can be applied to large-scale networks. IPv4 uses OSPFv2, and IPv6 uses OSPFv3.

1. Configuring OSPFv3 Basic Parameters

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **OSPFV3**, click **Start Setup**, and then configure an instance and an interface respectively.



OSPF

OSPF is a typical link-state routing protocol. To satisfy users' increasing requirements for network reliability and heterogeneity on a large network, OSPF solves the problems such as slow convergence, unscientific metric values, and poor scalability.

Highlights

- Achieves fast convergence.
- Minimizes routing overhead.
- Reduces routing update traffic through area partition.
- Applies to various networks with up to thousands of switches.

Start Setup

- Configure an instance
- (1) Configure basic parameters for an instance.

① ————— ② ————— ③
Configure the instance. **Configure the interface.** Operation succeeded.


* Router ID (?)

Advertise Default Route

Import External Route Static Route Redistribution
 Direct Route Redistribution
 RIP Redistribution

----- [Details](#) -----

Table 4-64 Description of Basic OSPF Instance Configuration Parameters

Parameter	Description
Router ID	<p>It identifies a router in an OSPF domain.</p> <hr/> <p> Caution</p> <p>Router IDs within the same domain must be unique. The same configuration may cause neighbor discovery failures.</p> <hr/>
Advertise Default Route	<p>Generate a default route and send it to the neighbor.</p> <p>After this function is enabled, you need to enter the metric and select a type. The default metric is 1.</p> <ul style="list-style-type: none"> ● Type 1: The metrics displayed on different routers vary. ● Type 2: The metrics displayed on all routers are the same.
Import External Route	<p>Redistribute routes of other protocols to the OSPF domain to interwork with other routing domains.</p> <ul style="list-style-type: none"> ● If Static Route Redistribution is selected, enter the metric, which is 20 by default. ● If Direct Route Redistribution is selected, enter the metric, which is 20 by default. ● If RIP Redistribution is selected, enter the metric, which is 20 by default.

(2) Click **Details** to display detailed configurations.

----- Details -----

Distance

LSA

SPF Calculation

Graceful Restart Graceful Restart Helper

LSA Check

* Max Wait Time

[Previous](#) [Next](#)

Table 4-65 Description of Detailed OSPF Instance Configuration Parameters

Parameter	Description
Distance	It is used for protocol selection. By default, the intra-area, inter-area, and external distances are all 110 .
LSA	Frequent network changes and route flapping may occupy too much network bandwidth and device resources. The LSA generation and reception delays are specified in OSPF by default. The default value is 1000 ms.

Parameter	Description
SPF Calculation	<p>When the link state database (LSDB) changes, OSPF recalculates the shortest path, and sets the interval to prevent frequent network changes from occupying a large number of resources</p> <ul style="list-style-type: none"> ● Waiting Interval: When the state changes, the timer is triggered. The delay is calculated for the first time after the timer expires. The default value is 0 ms. ● Min Interval: As the number of changes increases, the time of each interval will increase according to the algorithm, and the default value is 50 ms. ● Max Interval: When the calculated interval reaches the maximum interval, the subsequent interval is always equal to the maximum interval. If the time from the last calculation exceeds the maximum interval and the LSDB is not updated, the timer is disabled.
Graceful Restart	<p>Graceful Restart (GR) can avoid route flapping caused by traffic interruption and active/standby board switchover, thus ensuring the stability of key services.</p> <ul style="list-style-type: none"> ● Graceful Restart Helper: The Graceful Restart Helper function is enabled when this switch is turned on. ● LSA Check: LSA packets outside the domain are checked when this switch is turned on. ● Max Wait Time: Timing starts after the device receives the GR packet from the peer device. If the peer device does not complete GR within Max Wait Time, the device exits the GR Helper mode. The default value is 1800 seconds.

- Configure an interface
 - (1) Configure basic parameters for an interface.

① ————— ② ————— ③

Configure the instance. Configure the interface. **Operation succeeded.**

* Interface

* Area

Stub Area

----- Details -----

Table 4-66 Description of Basic OSPF Interface Configuration Parameters

Parameter	Description
Interface	Select the OSPF-enabled L3 interface.
Area	Configure the area ID. Value range: 0-4294967295

Parameter	Description
Stub Area	<p>If Stub Area is enabled, you need to configure the Area Type and Inter-Route Isolation</p> <ul style="list-style-type: none"> ● Area Type <ul style="list-style-type: none"> ○ Stub area: Routers at the edge of the area do not advertise routes outside the area, and the routing table in the area is small. ○ Not-So-Stubby Area (NSSA): A few external routes can be imported. ● Inter-Route Isolation <p>After this function is enabled, inter-area routes will not be imported to this area.</p>

(2) Click **Details** to display detailed configurations.

----- [Details](#) -----

Priority

Network Type

Hello Packets

Dead Interval

LSA Transmission Delay

LSA Retransmission Interval

Ignore MTU Check

Table 4-67 Description of Detailed OSPF Interface Configuration Parameters

Parameter	Description
Priority	A higher priority value indicates a greater chance of being elected as the DR or BDR. The default value is 1.
Network Type	OSPFv3 defines different network types, which affect the establishment of OSPF neighbor relationships, route update, and network convergence. The supported network types are broadcast and unicast.

Parameter	Description
Hello Packets	Interval for periodic transmission, which is used to discover and maintain OSPF neighbor relationship. The default value is 10 seconds.
Dead Interval	Time after which the neighbor becomes invalid. The default value is 40 seconds.
LSA Transmission Delay	LSA transmission delay of the interface. The default value is 1 second.
LSA Retransmission Interval	Time after which LSA is retransmitted after LSA is lost. The default value is 5 seconds.
Interface Auth	<ul style="list-style-type: none"> ● No Auth: The protocol packets are not authenticated. It is the default value. ● Plain Text: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text. ● MD5: The protocol packets are authenticated, and the authentication key is MD5 encrypted and then transmitted with the protocol packets.
Ignore MTU Check	The purpose of ignoring MTU check is to ensure that OSPF-enabled routers can update routing information in time when the network topology changes. This function is enabled by default.

(3) Click **Add** to add an interface to **Interface List**.

Port List

Up to 16 entries can be added.

Interface	Area	Priority	Network Type	Hello Packets	Dead Interval	LSA Transmission Delay	LSA Retransmission Interval	Action
WANO	1		Broadcast					Delete

Total 1 < 1 > 10/page

Previous Finish

(4) Click **Finish**.

After you complete configuration, choose **One-Device > Gateway > Config > Advanced > Routing > OSPFV3** to check **Instance List**.

OSPFV3

Up to 1 entries can be added.

Router ID	Interface	Area	Advertise Default Route	Import External Route	Distance	SPF Calculation	Graceful Restart Helper	Action
1.1.1.1	WANO	1(stub)	Disable	Static Route Redistribution : Off Direct Route Redistribution : Off RIP Redistribution : Off			Enable	More Neighbor Info Edit Delete

Total 1 < 1 > 10/page

2. Adding an OSPFv3 Interface

Choose **One-Device > Gateway > Config > Advanced > Routing > OSPFV3**, select the instance to be configured in **Instance List**, and choose **More > V3 Interface**.

OSPFv3

Up to 1 entries can be added.

Router ID	Interface	Area	Advertise Default Route	Import External Route	Distance	SPF Calculation	Graceful Restart Helper	Action
1.1.1.1	WAN0	1(stub)	Disable	Static I Redistribu Direct Route Redistribution : Off RIP Redistribution : Off			Enable	More Neighbor Info Edit Delete

Total 1 < 1 > 10/page

V3 Interface ×

* Interface

* Area

Stub Area ?

[Details](#)

Port List

[Add](#) [Reset](#)

Up to 64 entries can be added.

Interface	Area	Priority	Network Type	Hello Packets	Dead Interval	LSA Transmission Delay	LSA Retransmission Interval	Action
WAN0	1		Broadcast					Edit Delete

Total 1 < 1 > 10/page

3. Viewing OSPFv3 Neighbor Information

Choose **One-Device > Gateway > Config > Advanced > Routing > OSPFV3**, select the instance to be configured in **Instance List**, and click **Neighbor Info**.

Router ID	Interface	Area	Advertise Default Route	Import External Route	Distance	SPF Calculation	Graceful Restart Helper	Action
1.1.1.1	WAN0	1(stub)	Disable	Static Route Redistribution : Off Direct Route Redistribution : Off RIP Redistribution : Off			Enable	More Neighbor Info Edit Delete

Total 1 < 1 > 10/page

Neighbor Info

Router ID	Status	Interface
No Data		

Total 0 < 1 > 10/page

4.22.7 Viewing Routing Tables

 Note

Only RG-EG105G-V3, RG-EG105G-P-V3, RG-EG210G-P-V3, RG-EG1510XS and RG-EG3XX series devices (such as RG-EG310GH-E) support this function.

Choose **One-Device > Gateway > Config > Advanced > Routing > Routing Table Info** to view IPv4 and IPv6 routing table details.

[IPv4](#) [IPv6](#)

Route Info

Entry Type [Re-fetch](#)

Dest IP Address	Route Type	Distance/Metric	Interface	Next Hop
0.0.0.0/0	System routing	[0/0]	WAN0	10.52.48.1
4.4.4.0/24	Direct Routing	[0/0]	VLAN 555	*
5.5.5.0/24	Direct Routing	[0/0]	VLAN 55	*
10.52.48.0/21	Direct Routing	[0/0]	WAN0	*
10.80.12.0/24	Direct Routing	[0/0]	--	*
192.168.2.0/24	Direct Routing	[0/0]	Default VLAN	*
10.52.48.0/24	Static Routing	[1/20]	WAN0	10.52.48.43

Total 7 < 1 > 10/page

IPv4 [IPv6](#)

Route Info Entry Type: Global Data

Dest IP Address	Route Type	Distance/Metric	Interface	Next Hop
No Data				

Total 0 < **1** > 10/page

4.22.8 Set URL Route

Choose **One-Device > Gateway > Config > Advanced > Routing Settings > URL Routing**.

Configure the outbound interface for accessing a website URL. When a data packet matches the URL route, the data packet is forwarded in the specified mode.

URL Routing When a packet successfully matches a URL route, the packet is forwarded based on the defined routing rules.

URL Routing Table

<input type="checkbox"/>	User Group	Website Group	Time	Outbound Interface	Traffic Assurance	Effective State	Remarks	Action
No Data								

Up to 30 entries can be added. Total 0 < **1** > 10/page

Click Add. In the dialog box that appears, set the type, website group, outbound interface, and managed time range, and then click Add to create a URL route.

×

Add

Type User Group Custom

* User Group

* Website Group

Time

Outbound Interface

Remarks

Traffic Assurance

Effective State

Table 4-68 URL Routing Configuration Parameters

Parameter	Description
Type	URL route type, which can be: <ul style="list-style-type: none"> ● User group: select the user group to which the route-policy applies. ● Custom: apply the route to users with IP addresses in the specified IP address range. You need to manually enter the IP address range.
User group	This parameter is required when type is set to user group. Select users to which the URL route applies from the user group list. The user group list is available in One-Device > Gateway > Config > Behavior > User Management . If all members in a user group are selected, the configuration takes effect for the entire user group (including members added to the user group later).
IP Address Group	Configure this information when type is set to custom. Enter the IP address range managed by URL routing.
Website group	Set the website type for which URL routes need to be configured. Select a website group from the created website groups. For details on how to create or modify a website group, see 4.13.3 Website Management .
Managed time period	During the controlled period, when the managed client accesses the application in the website group, the packets are forwarded through the outbound interface. Select from the drop-down list. Time range defined in One-Device > Gateway > Config > Behavior > Time Management , or select custom and manually configure a time range.
Outgoing interface	Specify the interface that forwards the data packet based on the hit PBR rule.
Remarks	Configuring the description of a URL route
Network disconnection protection	After this function is enabled, if the outbound interface is unreachable, traffic is automatically switched to another reachable outbound interface.
Effective status	Turn on status to specify whether to enable the PBR rule. If status is turned off, this rule does not take effect.

4.23 Feature Configuration

Note

Only RG-EG105G-V3, RG-EG105G-P-V3 and RG-EG210G-P-V3 support this function.

Choose **One-Device > Gateway > Config > System > Feature Configuration**.

On the page, you can view the current configuration status of some device functions and the amount of memory space they occupy. This allows users to make informed decisions about which functions to enable or disable

based on their device's memory consumption. This can help prevent device lagging and ensure a smoother internet browsing experience.

Monitor **Config**

Total: 122.40MB, Available: 50.91MB (Free: 19.86MB, Cache: 31.05MB)

Authentication	Enable/Disable	Memory Consumed
Authentication Framework	--	--
Cloud Auth	<input type="checkbox"/>	--
Local Account Auth	<input type="checkbox"/>	--
Authorized Auth	<input type="checkbox"/>	--
QR Code Auth	<input type="checkbox"/>	--
RADIUS Server Management	<input type="checkbox"/>	--
802.1x Authentication	--	--

Behavior	Enable/Disable	Memory Consumed
Clients Management	<input checked="" type="checkbox"/>	2.61MB

4.24 Configuring Domain Proxy

Choose **Network-Wide > Workspace > Wireless > DNS Proxy**.

When a client accesses a Wi-Fi network, the message "No Internet connection" or "The Wi-Fi is not connected to the Internet" may be displayed. The possible cause is that the client's operating system introduces an Internet detection mechanism. Generally, the detection mechanism sends a probe packet to a specified domain name and evaluates whether the wireless network can access the Internet based on the detection result. If the DNS server takes a long time to parse a domain name or returns a probe node with a long delay, the probe may be deemed unreachable, causing a false network unavailability.

After the **Smart DNS Proxy** function is enabled, the device returns the preset domain name node to the client, reducing the misjudgment of network unavailability of the client.



Click **+Add**, enter the preset domain name and IP address, and click **OK**.

User Configuration List **+ Add** Delete Selected

<input type="checkbox"/>	Domain Name	IP	Action
No Data			

Up to 32 entries can be added. Total 0 < **1** > 10/page

4.25 Client Association

Choose **Network-Wide > Workspace > Wireless > Client Association**.

Client Association ↻

Enter MAC 🔍

Delete Selected

+ Add Association

<input type="checkbox"/> Client	IP/MAC	Associated Device 🔍	Signal Strength ⌵	Action
<input type="checkbox"/> -	9c:.....ie	AP @Ruijie-m6649 5G	-42dBm Channel: 36	Edit Delete

Up to 128 entries can be added.
Total 1 1 ⏪ ⏩ 10/page

Click **Add Association**. Select the client and the associated device. You can associate the client with a specified AP on the network to reduce remote association and improve the wireless experience.

Add Association ✕

* Client Enter the MAC address ⌵

* Associated Device 🔍 Select ⌵

[Advanced Settings](#)

Click **Advanced Settings** to configure the SSID for client association and to enable **Forced Association**.

[Advanced Settings](#)

SSID Select ⌵

Forced Association

Enabling this feature will forcefully associate the client with a specific AP. However, since the client cannot initiate automatic association, this may cause disconnection and unsuccessful association attempts.

⚠ Caution

The **Forced Association** feature may cause the client to go offline or fail to associate with the AP. Therefore, exercise caution when performing this configuration.

5 Online Client Management

Choose **Network-Wide > Clients**.

The client list displays wired, wireless, and users not connected on the current network, including the username, connection mode, associated device, IP/MAC address, IP address binding status, rate, and related operations.

The screenshot shows a web interface for managing online clients. At the top, there are filters for 'All (5)', 'Wired (2)', 'Wireless (3)', and 'User not connected (0)'. There are also buttons for 'Select', 'Block', and 'Bind IP', and a search bar. A notification states: 'The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.' The main table has the following columns: Username, SSID and Band, Connected To, IP/MAC, Rate, and Action. The table contains five rows of client data. The 'Action' column for each row contains buttons for 'Access Control', 'Associate', and 'Block'.

Username	SSID and Band	Connected To	IP/MAC	Rate	Action
Click to edit	5G @@@@zzzzzzzzzz	AP W 9	192.168.110.6 1 a	Not bound ↑ 0.00bps ↓ 0.00bps	Access Control Associate Block
M2102J25C	5G @@@@zzzzzzzzzz	AP V 9	192.168.110.7 E	Not bound ↑ 571.00bps ↓ 1.35Kbps	Access Control Associate Block
DESKTOP-DTTUM8V	Wired LAN3/WAN1	eg205g M 5	192.168.110.9 7 5	Not bound ↑ 0.00bps ↓ 475.00bps	Access Control
DESKTOP-IPV6G6R	Wired LAN1/WAN3	eg205g M 5	192.168.110.14 c 4	Not bound ↑ 295.54Kbps ↓ 79.64Kbps	Access Control
zhuyihan	2.4G @@@@zzzzzzzzzz	AP V 9	192.168.110.16 0	Not bound ↑ 132.00bps ↓ 43.00bps	Access Control Associate Block

Total 5 < 1 > 10/page

- Click **Not Bound** in the **IP/MAC** column to bind the client to a static IP address.
- Click a button in the **Action** column to perform the corresponding operation on the online client.
 - Wired: Only access control can be configured.
 - Wireless: Access control, associate, and block can be configured.

Table 5-1 Online Client Management Configuration Parameters

Parameter	Description
Username	Name of the connected client.
SSID and Band	Indicates the access mode of the client, which can be wireless or wired. The SSID and frequency band is displayed when a client is connected wirelessly.
Connected To	Indicates wired or wireless connection, the associated device and SN.
IP/MAC	Indicates the IP address and MAC address of the client.
Rate	Indicates the uplink and downlink rates of the client.
Action	You can click the corresponding button to perform access control, association, and block operations on online clients.

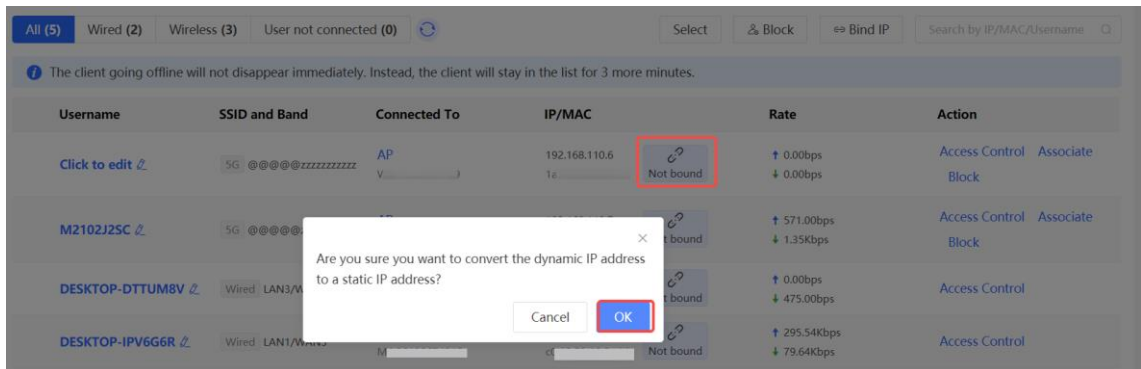
5.2 Configuring Client IP Binding

Choose **Network-Wide > Clients**.

IP address binding is a security and access control policy that associates a specific IP address with a specific device or user to achieve identity authentication, access control, monitoring, and accounting.

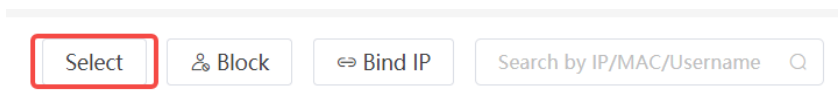
- Single client IP address binding

Select the client to be bound with an IP address in the list, click Not bound, and click OK in the pop-up box to bind the client to a static IP address.

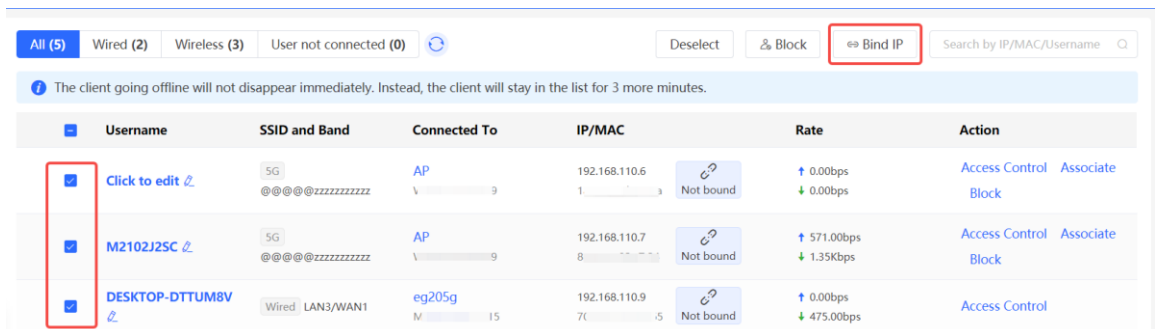


- Batch IP binding

Click Select.

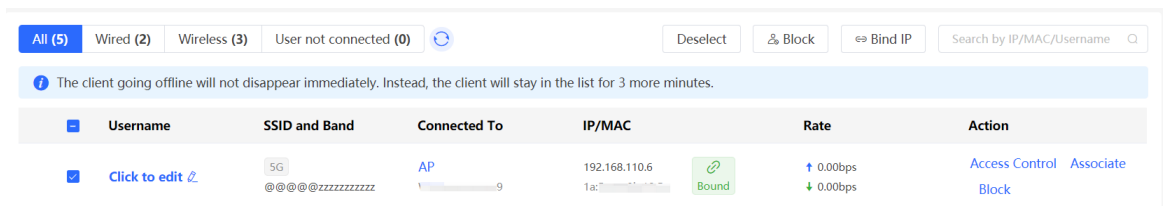


Select the clients to be bound, click Bind IP, and click OK in the pop-up box to bind the selected clients to a static IP address.



- Unbind IP address

Select the client to be unbound from the list, click **Bound**, and click **OK** in the pop-up box.



Edit Association
×

* Client

* Associated Device

Advanced Settings

SSID

Forced Association

Enabling this feature will forcefully associate the client with a specific AP. However, since the client cannot initiate automatic association, this may cause disconnection and unsuccessful association attempts.

5.5 Blocking Clients

Choose **Network-Wide > Clients**.

An unauthorized client may occupy network bandwidth and pose security risks. You can block specified clients to solve the unauthorized access problem.

i Note

Client Block is available only for wireless clients.

- Block a single client

Select a client to block in the list, click **Block** in the **Action** column, and click **OK** in the pop-up box to block the selected client.

All (4) | Wired (1) | Wireless (3) | User not connected (0) ↻
Select
⚙️ Block
⇄ Bind IP

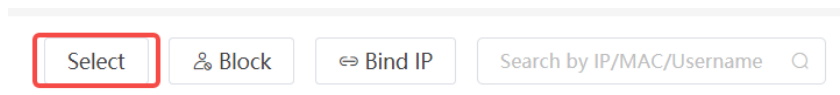
i The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

Username	SSID and Band	Connected To	IP/MAC	Rate	Action
* 🔗	5G @@@@zxxxxxxxx	AP W 9	192.168.110.6 1: a	↑ 0.00bps ↓ 0.00bps	Access Control Associate Block
M2102J2SC 🔗	5G @@@@zxxxxxxxx	AP V j	192.168.110.7 8: 4	↑ 2.95Kbps ↓ 5.79Kbps	Access Control Associate Block

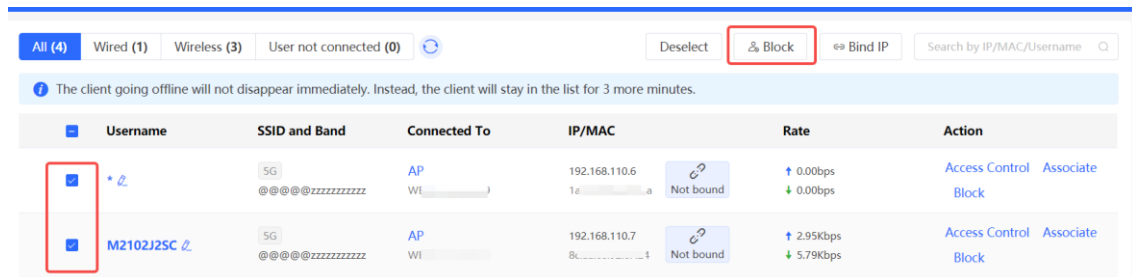


- Batch block clients

Click **Select**.



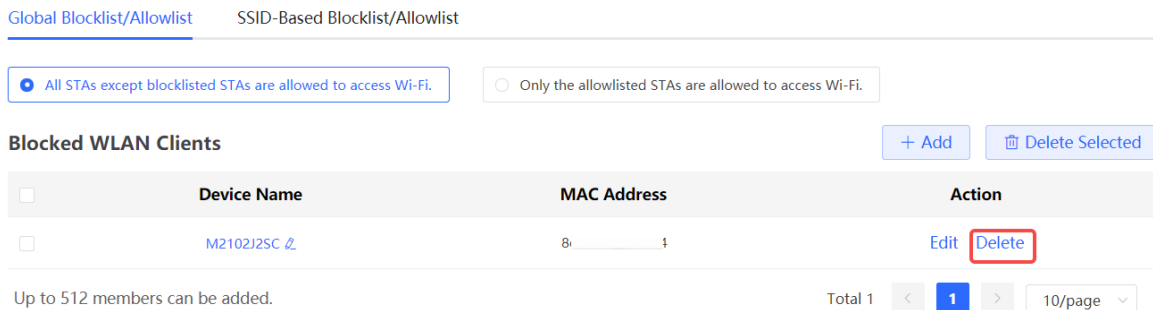
Select the target clients, click **Block**, and click **OK** in the pop-up box to block the selected clients.



- Cancel Block

Choose **Network-Wide > Workspace > Wireless > Blocklist/Allowlist > Global Blocklist/Allowlist**.

Select the client to be removed from the blacklist in the wireless blocklist and click **Delete**.



5.6 Configuring Client Rate Limiting

Choose **Network-Wide > Clients > Wireless**.

To ensure fair resource allocation, the network administrator can implement wireless rate limiting to prevent some users or devices from occupying a large amount of bandwidth and affecting the network experience of other users.

Note

Rate limiting applies only to wireless clients.

- Configure rate limits for clients

LimitSpeed



Uplink Rate Mbps ▼

Limit Current: **102400** Kbps. Range: 1-1700000 Kbps

Downlink Rate Mbps ▼

Limit Current: **102400** Kbps. Range: 1-1700000 Kbps

6 VPN

6.1 Configuring IPsec VPN

6.1.1 Overview

1. IPsec Overview

IP Security (IPsec) is a Layer 3 tunnel encryption protocol defined by the IETF. IPsec is used to provide end-to-end encryption and verification services in the network to provide high quality and interoperability for data transmission over the network and ensure transmission security by using cryptographic algorithms. The communicating parties obtain the following security services at the IP layer through encryption and data source authentication:

- Confidentiality: The IPsec sender encrypts packets before transmitting the packets over the network.
- Data integrity: The IPsec receiver authenticates packets received from the sender to ensure that data is not tampered with during the transmission.
- Data authentication: The IPsec receiver authenticates whether the sender of IPsec packets is valid.
- Anti-replay: The IPsec receiver detects and denies expired or repeated packets.
- The IPsec protocol is widely used for communication between the HQ and branches of an organization. Currently, the device can be deployed as the IPsec server or client. A secure tunnel is established between the HQ and each branch based on the IPsec protocol to ensure the confidentiality of data transmission and improve network security.

2. IKE Overview

IPsec provides secure communication between two endpoints, which are called IPsec peers. Security Association (SA) is the establishment of shared security attributes between the peers to support secure communication. An SA may include attributes such as: security protocol used by the peers, characteristics of data flows to be protected, encapsulation mode of data transmitted between the peers, encryption and authentication algorithms, keys for secure data conversion and transmission, and the SA lifetime. When you configure IPsec, you can use the Internet Key Exchange (IKE) protocol to establish an SA. IKE provides automatically negotiated keys for establishing and maintaining SAs, simplifying IPsec usage and management.

3. IPsec Security Policy

IPsec security policies define security proposals (equivalent to SA) for data flows. You can configure matching security policies on both parties engaged in the communication to establish IPsec tunnels between the IPsec client and the IPsec server, protecting the communication data. An IPsec security policy consists of two parts: basic settings and advanced settings. Advanced settings are optional and include the specific IKE policy and connection policy. You can keep the default settings unless otherwise specified. For details, see the Configuration Steps below.

6.1.2 Configuring the IPsec Server

Choose **One-Device > Gateway > Config > VPN > IPsec > IPsec Security Policy**.

1. Basic Settings

Click **Add**. In the dialog box that appears, set **Policy Type** to **Server**, enter the policy name and local subnet range, set the pre-shared key, and click **OK**.

Note: Example: IP address/number of subnet mask bits.
Tips: If it is set to 192.168.110.x/24, the address range is from 192.168.110.1 to 192.168.110.254.
 Up to **3** entries with the policy type of client can be configured.
 Up to **1** entry with the policy type of server can be configured.
 The server and client cannot be configured at the same time.

Policy List + Add

Policy Type ?	Policy Name ?	Peer Gateway ?	Key Exchange Version	Local Subnet ?	Peer Subnet ?	Status	Action
Client	test	10.52.50.239	IKEv1	192.168.2.0/24	192.168.68.0/24	Enable ☑	Edit Delete

Total 1 < 1 > 10/page ▾

Add ×

i If clients want to access from different WAN ports, please set Local ID Type to Name. Otherwise, all clients will access from the same one WAN port.

Policy Type ? Client Server

Internet ? IPv4 IPv6

* Policy Name ?

Interface ?

Key Exchange Version IKEv1 IKEv2

* Subnets

+ Local Subnets

* Pre-shared Key ?

Status

- 1. Set IKE Policy -----
- 2. Connection Policy -----

Table 6-1 IPsec server basic settings

Parameter	Description
Policy Name	Specify the name of the IPsec security policy. The name must be a string of 1 to 28 characters.
Internet	Format of the IP address. Both IPv4 and IPv6 address formats are supported.
Interface	Select a local WAN port from the drop-down list box. The Peer Gateway parameter set for the communication peer (IPsec client) must use the IP address of the WAN port specified here. In the multi-line scenario, you are advised to set this parameter to Auto .
Key Exchange Version	Select the IKE version for SA negotiation. There are two options available: <ul style="list-style-type: none"> ● IKEv1: The negotiation of SA in IKEv1 primarily consists of two phases. <ul style="list-style-type: none"> ○ Phase 1: The purpose is to establish an IKE SA using one of two negotiation modes: Main Mode and Aggressive Mode. Main Mode requires six ISAKMP (Internet Security Association and Key Management Protocol) messages to complete the negotiation, while Aggressive Mode only requires three ISAKMP messages. Aggressive Mode offers faster IKE SA establishment. However, it combines key exchange and identity authentication, which means it does not provide identity protection. ○ Phase 2: The purpose is to establish an IPsec SA for data transmission, utilizing a fast exchange mode that requires only three ISAKMP messages to complete the negotiation. ● IKEv2: In IKEv2, the negotiation process for SA is simplified. The establishment of one IKE SA and one pair of IPsec SAs can be accomplished using two exchanges with four messages. If there is a need to establish more than one pair of IPsec SAs, only one additional exchange is needed for each pair. This enables the negotiation to be completed with just two messages per pair.
Subnet	Specify the local subnet address range for the data flows to be protected, that is, the LAN port network segment of the server. The value is the combination of IP address and subnet mask.
Pre-shared Key	Specify the same pre-shared key as the credential for authentication between communicating parties. For higher security, different peers must be configured with different pre-shared keys. That is, a pair of interface bound to the IPsec server and peer gateway of the IPsec client must be configured with the same unique pre-shared key.
Status	Specify whether to enable the security policy.

2. Advanced Settings (Phase 1)

- The key exchange version in the basic setting is IKEv1:

Click **1. Set IKE Policy** to expand the configuration items. Keep the default settings unless otherwise specified.

----- 1. Set IKE Policy -----

Authentication-Encryption-DH Group

IKE Policy 1	<input type="text" value="sha1-3des-dh1"/>
IKE Policy 2	<input type="text" value="sha1-des-dh1"/>
IKE Policy 3	<input type="text" value="sha1-3des-dh2"/>
IKE Policy 4	<input type="text" value="md5-des-dh1"/>
IKE Policy 5	<input type="text" value="md5-3des-dh2"/>

Negotiation Mode Main Mode Aggressive Mode

Local ID Type IP Name

Peer ID Type (?) IP Name

* Lifetime

DPD Enable Disable

* DPD Interval
seconds

- The key exchange version in the basic setting is IKEv2:

Click **IKE Policy** to expand the configuration items. Keep the default settings unless otherwise specified.

----- IKE Policy -----

Authentication-Encryption-DH Group

IKE Policy 1

IKE Policy 2

IKE Policy 3

IKE Policy 4

IKE Policy 5

Local ID Type IP Name

Peer ID Type IP Name

* Lifetime

DPD Enable Disable

* DPD Interval

seconds

Table 6-2 IPsec server IKE policy configuration

Parameter	Description
IKE Policy	<p>Select the hash algorithm, encryption algorithm, and Diffie-Hellman (DH) group ID used by the IKE protocol. An IKE policy is composed of the three parameters. You can set five sets of IKE policies. To ensure successful IKE negotiation, the two parties engaged in IKE negotiation must have at least one set of consistent IKE policy.</p> <ul style="list-style-type: none"> ● Hash algorithm: <ul style="list-style-type: none"> ○ sha1: SHA-1 algorithm ○ md5: MD5 algorithm ● Encryption algorithm: <ul style="list-style-type: none"> ○ des: DES algorithm using 56-bit keys ○ 3des: 3DES algorithm using 168-bit keys ○ aes-128: AES algorithm using 128-bit keys ○ aes-192: AES algorithm using 192-bit keys ○ aes-256: AES algorithm using 256-bit keys ● DH group ID: <ul style="list-style-type: none"> ○ dh1: 768-bit DH group ○ dh2: 1024-bit DH group ○ dh5: 1536-bit DH group
Negotiation Mode	<p>Select Main Mode or Aggressive Mode. The negotiation mode on the IPsec server and IPsec client must be the same.</p> <ul style="list-style-type: none"> ● Main Mode: Generally, this mode is applicable to communication between fixed public network IP addresses and point-to-point communication between devices. In this mode, the peer identity is authenticated to provide high security. ● Aggressive Mode: The public network IP addresses obtained by ADSL dial-up users are not fixed and a NAT device may exist. Therefore, the aggressive mode is used to implement NAT traversal. In this mode, you need to set the local and peer ID type to NAME as the IP address is not fixed. The aggressive mode does not authenticate the peer identity, so it has low security.
Local/Peer ID Type	<p>Specify the ID type of the local or peer device. The local ID type of the peer device must be the same as the peer ID type of the local device.</p> <ul style="list-style-type: none"> ● IP: The IP address is used as the identity ID. The IDs of the local and peer devices are generated automatically. ● NAME: The host character string is used as the identity ID. The IDs of the local and peer devices are generated automatically. When the IP address is not fixed, you need to set Local ID Type to NAME and modify the peer device settings accordingly. In this case, you also need to configure the host character string that is used as the identity ID.
Local/Peer ID	<p>When the local or peer ID type is set to NAME, you also need to host character string that is used as the identity ID. The local ID of the peer device must be the same as peer ID of the local device.</p>

Parameter	Description
Lifetime	Specify the lifetime of the IKE SA. (The negotiated IKE SA lifetime prevails.) You are advised to use the default value.
DPD	Specify whether to enable Dead Peer Detection (DPD) to detect the IPsec neighbor status. After DPD is enabled, if the receiver does not receive IPsec encrypted packets from the peer within the DPD detection interval, DPD query will be triggered and the receiver actively sends a request packet to detect whether the IKE peer exists. You are advised to configure DPD when links are unstable.
DPD Interval	Specify the DPD detection interval. That is, the interval for triggering DPD query. You are advised to keep the default setting.

3. Advanced Settings (Phase 2)

Click **Connection Policy** to expand the configuration items. Keep the default settings unless otherwise specified.

----- [Connection Policy](#) -----

Protocol Type-Authentication-Encryption

Transform 1

Transform 2

Perfect Forward Secrecy

* Lifetime

Table 6-3 IPsec server connection policy configuration

Parameter	Description
Transform Set	<p>Specify the set of security protocol and algorithms. During IPsec SA negotiation, the two parties use the same transform set to protect specific data flow. The transform set on the IPsec server and IPsec client must be the same.</p> <ul style="list-style-type: none"> ● Security protocol: The Encapsulating Security Payload (ESP) protocol provides data source authentication, data integrity check, and anti-replay functions for IPsec connections and guarantees data confidentiality. ● Verification algorithm: <ul style="list-style-type: none"> ○ sha1: SHA-1 HMAC ○ md5: MD5 HMAC ● Encryption algorithm: <ul style="list-style-type: none"> ○ des: DES algorithm using 56-bit keys ○ 3des: 3DES algorithm using 168-bit keys ○ aes-128: AES algorithm using 128-bit keys ○ aes-192: AES algorithm using 192-bit keys ○ aes-256: AES algorithm using 256-bit keys
Perfect Forward Secrecy	<p>Perfect Forward Secrecy (PFS) is a security feature that can guarantee the security of other keys when one key is cracked, because there is no derivative relationship among the keys. After PFS is enabled, temporary private key exchange is performed when an IKE negotiation is initiated using a security policy. If PFS is configured on the local device, it must also be configured on the peer device that initiates negotiation and the DH group specified on the local and peer devices must be the same. Otherwise, negotiation will fail.</p> <ul style="list-style-type: none"> ● none: Disable PFS. ● d1: 768-bit DH group ● d2: 1024-bit DH group ● d5: 1536-bit DH group <p>By default, PFS is disabled.</p>
Lifetime	<p>Indicates the duration of an IPsec tunnel, which defines the time for data transmission over the IPsec tunnel.</p>

6.1.3 Configuring the IPsec Client

Choose **One-Device > Gateway > Config > VPN > IPsec > IPsec Security Policy**.

Click **Add**. In the dialog box that appears, set **Policy Type** to **Client**, enter the policy name, peer gateway, local subnet range, and peer subnet range, set the pre-shared key, and click **OK**.

Note: Example: IP address/number of subnet mask bits.
Tips: If it is set to 192.168.110.x/24, the address range is from 192.168.110.1 to 192.168.110.254.
 Up to 3 entries with the policy type of client can be configured.
 Up to 1 entry with the policy type of server can be configured.
 The server and client cannot be configured at the same time.

Policy List + Add

Policy Type ?	Policy Name ?	Peer Gateway ?	Key Exchange Version	Local Subnet ?	Peer Subnet ?	Status	Action
No Data							

Total 0 < 1 > 10/page

Add ×

Policy Type ? Client Server

Internet ? IPv4 IPv6

* Policy Name ?

* Peer Gateway ? +

Interface ? ▼

Key Exchange Version IKEv1 IKEv2
 ?

* Subnets

Local Subnets + Peer Subnets

* Pre-shared Key ?

Status

Table 6-4 IPsec client basic settings

Parameter	Description
Policy Name	Specify the name of the IPsec security policy. The name must be a string of 1 to 28 characters.
Internet	Format of the IP address. Both IPv4 and IPv6 address formats are supported.

Parameter	Description
Peer Gateway	Enter the IP address or domain name of the peer device.
Interface	Select a WAN port used locally from the drop-down list box. In the multi-line scenario, you are advised to set this parameter to Auto .
Key Exchange Version	<p>Select the IKE version for SA negotiation. There are two options available:</p> <ul style="list-style-type: none"> ● IKEv1: The negotiation of SA in IKEv1 primarily consists of two phases. <ul style="list-style-type: none"> ○ Phase 1: The purpose is to establish an IKE SA using one of two negotiation modes: Main Mode and Aggressive Mode. Main Mode requires six ISAKMP (Internet Security Association and Key Management Protocol) messages to complete the negotiation, while Aggressive Mode only requires three ISAKMP messages. Aggressive Mode offers faster IKE SA establishment. However, it combines key exchange and identity authentication, which means it does not provide identity protection. ○ Phase 2: The purpose is to establish an IPsec SA for data transmission, utilizing a fast exchange mode that requires only three ISAKMP messages to complete the negotiation. ● IKEv2: In IKEv2, the negotiation process for SA is simplified. The establishment of one IKE SA and one pair of IPsec SAs can be accomplished using two exchanges with four messages. If there is a need to establish more than one pair of IPsec SAs, only one additional exchange is needed for each pair. This enables the negotiation to be completed with just two messages per pair.
Local Subnets	Specify the local subnet address range for the data flows to be protected, that is, the LAN port network segment of the server. The value is the combination of IP address and subnet mask.
Peer Subnets	Specify the peer subnet address range for the data flows to be protected, that is, the LAN port network segment of the client. The value is the combination of IP address and subnet mask.
Pre-shared Key	Configure the pre-shared key the same as that on the IPsec server.
Status	Specify whether to enable the security policy.

You can configure advanced parameters by referring to the corresponding settings on the IPsec server. For details, see [Advanced Settings \(Phase 1\)](#) and [Advanced Settings \(Phase 2\)](#).

6.1.4 Viewing the IPsec Connection Status

Choose **One-Device > Gateway > Config > VPN > IPsec > IPsec Connection Status**.

You can view the IPsec tunnel connection status on the current page.

IPSec Security Policy [IPSec Connection Status](#)

IPSec Connection Status Refresh

Name	SPI	Direction	Tunnel Endpoint	Flow	Status	Security Protocol	Algorithm
test	32569111 34	in	172.26.1.200<--172.26.30.192	192.168.120.0/24 <-- 192.168.110.0/24	OK	ESP	AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128
test	32874839 13	out	172.26.1.200-->172.26.30.192	192.168.120.0/24 --> 192.168.110.0/24	OK	ESP	AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128

Table 6-5 IPsec tunnel connection status information

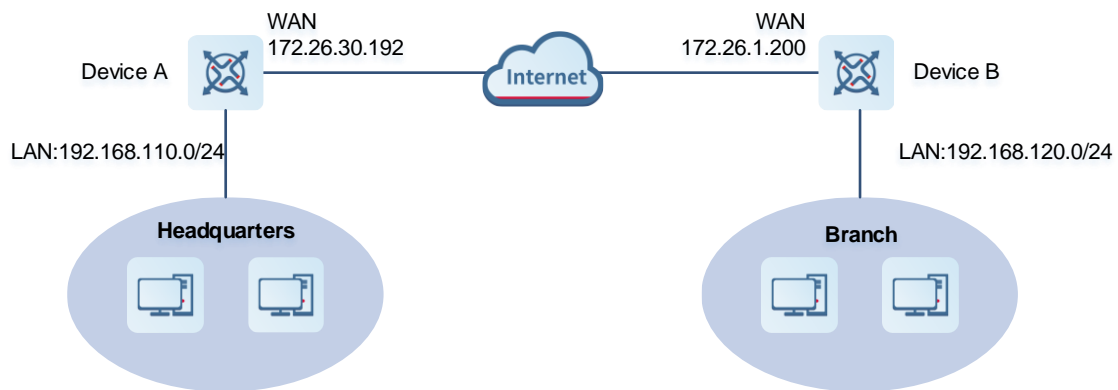
Parameter	Description
Name	Indicate the security policy name on the IPsec server or client.
SPI	Indicate the Security Parameter Index (SPI) of the IPsec connection, used to associate the received IPsec data packets with the corresponding SA. The SPI of each IPsec connection must be unique.
Direction	Indicate the direction of the IPsec connection. The value in indicates inbound, and the value out indicates outbound.
Tunnel Client	Indicate the gateway addresses on two ends of the IPsec connection. The arrow indicates the direction of data flows to be protected by the current tunnel.
Flow	Indicate the subnet range on two ends of the IPsec connection. The arrow indicates the direction of data flows to be protected by the current tunnel.
Status	Indicate the IPsec tunnel connection status.
Security Protocol	Indicate the security protocol used by the IPsec connection.
Algorithm	Indicate the encryption algorithm and authentication algorithm used by the IPsec connection.

6.1.5 Typical Configuration Example

1. Networking Requirements

The HQ and branch of an enterprise are connected through the Internet. An IPsec tunnel needs to be established between the HQ gateway and branch gateway to ensure the confidentiality of transmitted data.

2. Networking Diagram



3. Configuration Roadmap

- Configure the HQ gateway Device A as the IPsec server.
- Configure the branch gateway Device B as the IPsec client.

4. Configuration Steps

(1) Configure the HQ gateway.

- a Log in to the web management system and choose **One-Device > Gateway > Config > VPN > IPsec > IPsec Security Policy** to access the IPsec Security Policy page.

Note: Example: IP address/number of subnet mask bits.
Tips: If it is set to 192.168.110.x/24, the address range is from 192.168.110.1 to 192.168.110.254.
 Up to 3 entries with the policy type of client can be configured.
 Up to 1 entry with the policy type of server can be configured.
 The server and client cannot be configured at the same time.

Policy List + Add

Policy Type ?	Policy Name ?	Peer Gateway ?	Key Exchange Version	Local Subnet ?	Peer Subnet ?	Status	Action
No Data							

Total 0 < 1 > 10/page

- b Click Add. In the dialog box that appears, set Policy Type to Server, enter the policy name, select the bound interface, and configure the local subnet to be accessed through IPsec and the pre-shared key. If the device connects to other EG devices in the Reyee network, you are advised to keep the default settings in IKE phase 1 and phase 2. If the device connects to devices from another vendor, keep the parameter settings consistent on the connected devices.

Add



i If clients want to access from different WAN ports, please set Local ID Type to Name. Otherwise, all clients will access from the same one WAN port.

Policy Type Client Server

Internet IPv4 IPv6

* Policy Name

Interface

Key Exchange Version IKEv1 IKEv2



* Subnets

[+ Local Subnets](#)


* Pre-shared Key

Status

(2) Configure the branch gateway.

- a Log in to the web management system and access the IPsec Security Policy page.
- b Click Add. In the dialog box that appears, set Policy Type to Client, enter the policy name, select the peer gateway (WAN port address or domain name of the HQ gateway), and configure the local subnet that needs to access the peer subnet and the pre-shared key the same as that on the HQ gateway. Keep the other phase 1 and phase 2 parameters consistent with those on the IPsec server.

Add

Policy Type  Client ServerInternet  IPv4 IPv6* Policy Name  * Peer Gateway  Interface  Key Exchange Version IKEv1 IKEv2* Subnets

Local Subnets



Peer Subnets

* Pre-shared Key  Status

----- 1. Set IKE Policy -----

----- 2. Connection Policy -----

Cancel

OK

5. Verifying Configuration

- (1) Log in to the web management system of the HQ or branch gateway and choose **One-Device > Gateway > Config > VPN > IPsec > IPsec Connection Status**. You can view the IPsec connection status between the HQ and branch.

IPSec Security Policy IPSec Connection Status

IPSec Connection Status Refresh

Name	SPI	Direction	Tunnel Client	Flow	Status	Security Protocol	Algorithm
test	3483169338	in	172.26.30.192<--172.26.1.200	192.168.110.0/24 <-- 192.168.120.0/24	OK	ESP	AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128
test	3281459512	out	172.26.30.192-->172.26.1.200	192.168.110.0/24 --> 192.168.120.0/24	OK	ESP	AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128

- Perform ping test between clients on the two ends that need to access each other. The clients can successfully ping and access each other.

6.1.6 Solution to IPsec VPN Connection Failure

- Run the ping command to test the connectivity between the client and server. For details, see Section [4.5.3 Network Tools](#). If the ping fails, check the network connection settings. Check whether the branch EG can ping to HQ EG. If the ping fails, check the network connection between the two EGs.

Click **One-Device > Gateway > Config > Diagnostics > Network Tools**. Then, you can start the ping operation. For details, see Section [4.5.3 Network Tools](#).

- Confirm that the configurations on the IPsec server and IPsec client are correct.

Choose **One-Device > Gateway > Config > VPN > IPsec > IPsec Security Policy** and confirm that the security policies configured on the two ends are matching.

Policy List + Add

Up to 1 entries can be added.

Policy Type	Policy Name	Peer Gateway	Local Subnet	Peer Subnet	Status	Action
Server	test	0.0.0.0	192.168.110.0/24	0.0.0.0/0	Enable	Edit Delete

Policy List + Add

Up to 1 entries can be added.

Policy Type	Policy Name	Peer Gateway	Local Subnet	Peer Subnet	Status	Action
Client	test	172.26.30.192	192.168.120.0/24	192.168.110.0/24	Enable	Edit Delete

- Check whether the WAN IP address of your HQ EG is a public IP address. If not, you need to configure DMZ or port mapping (UDP 500 and 4500 used as IPsec VPN port) on your egress gateway and set **Local ID Type to NAME** on HQ and branch gateways.

1. Set IKE Policy

Authentication-Encryption-DH Group

IKE Policy 1

IKE Policy 2

IKE Policy 3

IKE Policy 4

IKE Policy 5

Negotiation Mode Main Mode Aggressive Mode

Local ID Type IP Name

* Local ID

Peer ID Type IP Name

* Peer ID

* Lifetime

DPD Enable Disable

* DPD Interval
seconds

1. Set IKE Policy

Authentication-Encryption-DH Group

IKE Policy 1

IKE Policy 2

IKE Policy 3

IKE Policy 4

IKE Policy 5

Negotiation Mode Main Mode Aggressive Mode

Local ID Type IP Name

* Local ID

Peer ID Type IP Name

* Peer ID

* Lifetime

DPD Enable Disable

* DPD Interval
seconds

6.2 Configuring L2TP VPN

6.2.1 Overview

Layer Two Tunneling Protocol (L2TP) is a virtual tunneling protocol, usually used in virtual private networks.

The L2TP protocol does not provide encryption and reliability verification functions, but it can work with a security protocol to implement encrypted data transmission. L2TP is frequently used with IPsec to encapsulate packets using L2TP before encapsulating packets using IPsec. This combination implements user verification and address allocation through L2TP and ensures communication security through IPsec.

L2TP VPN can be used to establish secure tunnels between the enterprise HQ and branches and allow traveling employees to access the HQ. Currently, the device can be deployed as the L2TP server or client.

6.2.2 Configuring the L2TP Server

1. Basic Settings of L2TP Server

Choose **One-Device > Gateway > Config > VPN > L2TP > L2TP Settings**.

Turn on the L2TP function, set **L2TP Type** to **Server**, set L2TP server parameters, and click **Save**.

Enable

L2TP Type Server Client

* Local Tunnel IP

* IP Range (?)

* DNS Server

Tunnel Authentication Disable Enable

IPSec Security Open Security


Flow Control Disable Enable

* PPP Hello Interval (?) seconds

Table 6-6 L2TP server configuration

Parameter	Description
Local Tunnel IP	Specify the local virtual IP address of the L2TP server. Clients can dial up to access the L2TP server through this address.
IP Range	Specify the address pool used by the L2TP server to allocate IP addresses to clients.
DNS Server	Specify the DNS server address pushed by the L2TP server to clients.

Parameter	Description
Tunnel Authentication	<p>Specify whether to enable L2TP tunnel authentication. If you enable this function, you need to configure a tunnel authentication key. By default, tunnel authentication is disabled.</p> <p>The tunnel authentication request can be initiated by clients. If tunnel authentication is enabled on one end, a tunnel to the peer can be established only when tunnel authentication is also enabled on the peer and consistent keys are configured on the two ends. Otherwise, the local end will automatically shut down the tunnel connection. If tunnel authentication is disabled on both ends, no authentication key is required for tunnel establishment.</p> <p>When a PC functions as the client to access the L2TP server, you are advised not to enable tunnel authentication on the L2TP server.</p>
IPsec Security	<p>Specify whether to encrypt the tunnel. If you select Security, the device encrypts the L2TP tunnel using IPsec, indicating the L2TP over IPsec mode.</p> <p>If an IPsec security policy is enabled on the current device, you cannot enable IPsec encryption for the L2TP tunnel. If you want to configure L2TP over IPsec, disable the IPsec security policy first.</p> <p>The IPsec encryption configuration on the L2TP server and client must be consistent. For details, see Configuring the L2TP over IPsec Server.</p>
Flow Control	<p>The VPN server has a lower priority to control the traffic of the client than the custom policy. The VPN server can only limit the maximum uplink and downlink bandwidth per user for the client. For details, see 4.14.2 Smart Flow Control.</p>
PPP Hello Interval	<p>Specify the interval for sending PPP Hello packets after L2TP VPN is deployed. You are advised to retain the default configuration.</p>

 **Caution**

The local tunnel address and IP address range of the address pool cannot overlap the network segment of the LAN port on the device.

2. Configuring the L2TP over IPsec Server

Choose **One-Device > Gateway > VPN > L2TP > L2TP Settings**.

After you complete [Basic Settings of L2TP Server](#), enable IPsec encryption on the L2TP server to guarantee communication security. For details on the IPsec configuration, see Section [6.1 Configuring IPsec VPN](#).

* DNS Server

Tunnel Authentication Disable Enable

IPSec Security Open Security

* Pre-shared Key

IKE Policy

Transform Set

Negotiation Mode Main Mode Aggressive Mode

Local ID Type IP Address NAME

Flow Control Disable Enable

* PPP Hello Interval seconds

Table 6-7 L2TP over IPsec server configuration

Parameter	Description
Pre-shared Key	Specify the same unique pre-shared key as the credential for mutual authentication between the server and client.

Parameter	Description
IKE Policy	<p>Select the encryption algorithm, hash algorithm, and DH group ID used by the IKE protocol. To ensure successful IKE negotiation, the two parties engaged in IKE negotiation must have at least one set of consistent IKE policy. The IKE policies on the server and client must be consistent.</p> <ul style="list-style-type: none"> ● Hash algorithm: <ul style="list-style-type: none"> ○ sha1: SHA-1 algorithm ○ md5: MD5 algorithm ● Encryption algorithm: <ul style="list-style-type: none"> ○ des: DES algorithm using 56-bit keys ○ 3des: 3DES algorithm using 168-bit keys ○ aes-128: AES algorithm using 128-bit keys ○ aes-192: AES algorithm using 192-bit keys ○ aes-256: AES algorithm using 256-bit keys ● DH group ID: <ul style="list-style-type: none"> ○ dh1: 768-bit DH group ○ dh2: 1024-bit DH group ○ dh5: 1536-bit DH group
Transform Set	<p>Specify the set of security protocol and algorithms. During IPsec SA negotiation, the two parties use the same transform set to protect specific data flow. The transform set on the server and client must be the same.</p> <ul style="list-style-type: none"> ● Security protocol: The Encapsulating Security Payload (ESP) protocol provides data source authentication, data integrity check, and anti-replay functions for IPsec connections and guarantees data confidentiality. ● Verification algorithm: <ul style="list-style-type: none"> ○ sha1: SHA-1 HMAC ○ md5: MD5 HMAC ● Encryption algorithm: <ul style="list-style-type: none"> ○ des: DES algorithm using 56-bit keys ○ 3des: 3DES algorithm using 168-bit keys ○ aes-128: AES algorithm using 128-bit keys ○ aes-192: AES algorithm using 192-bit keys ○ aes-256: AES algorithm using 256-bit keys

Parameter	Description
Negotiation Mode	<p>Select Main Mode or Aggressive Mode. The negotiation mode on the server and client must be the same.</p> <ul style="list-style-type: none"> ● Main Mode: This mode is applicable to communication between fixed public network IP addresses and point-to-point communication between devices. In this mode, the peer identity is authenticated to provide high security. ● Aggressive Mode: The public network IP addresses obtained by ADSL dial-up users are not fixed and an NAT device may exist. Therefore, the aggressive mode is used to implement NAT traversal. In this mode, you need to set the local and peer ID type to NAME as the IP address is not fixed. The aggressive mode does not authenticate the peer identity, so it has low security.
Local ID Type	<p>Specify the ID type of the local device. The peer ID of the client must be the same as local ID of the server.</p> <ul style="list-style-type: none"> ● IP: The IP address is used as the identity ID. The ID of the local device is generated automatically. ● NAME: The host character string is used as the identity ID. The ID of the local device is generated automatically. In this case, you also need to configure the host character string that is used as the identity ID. <p>When the WAN port IP address of the server is a private network address, you need to set Local ID Type to NAME and configure DMZ on the external device.</p> <p>When the IP address is not fixed, you need to set Local ID Type to NAME and modify the peer device settings accordingly.</p>
Local ID	<p>When Local ID Type is set to NAME, the host character string is used as the identity ID. The peer ID of the client must be the same as local ID of the server.</p>

3. Configuring L2TP User

Choose **One-Device > Gateway > Config > VPN > VPN Account**

Only user accounts added to the VPN client list are allowed to dial up to connect to the L2TP server. Therefore, you need to manually configure user accounts for clients to access the L2TP server.

Click **Add**. In the dialog box that appears, set **Service Type** to **L2TP** or **ALL**. (If you select **ALL**, the created account can be used to establish all types of VPN tunnels.) Enter the username, password, and peer subnet, select a network mode, and click **OK**.

VPN User List

<input type="checkbox"/>	Username	Password	Service Type ?	Network Mode ?	Client Subnet ?	Status	Action
<input type="checkbox"/>	pptp@branch	****	PPTP	Router to Router	192.168.12.0/24	Enable	Edit Delete
<input type="checkbox"/>	pptp@pc	****	PPTP	PC to Router	-	Enable	Edit Delete
<input type="checkbox"/>	OpenVpnUser1	****	OpenVpn	-	-	Enable	Edit Delete

Up to 300 entries can be added. Total 3 1 10/page

Add User



Service Type (?)

* Username

* Password


Network Mode (?)

Status

Cancel

OK

Table 6-8 L2TP user configuration

Parameter	Description
Username/Password	Specify the name and password of the L2TP user allowed to dial up to connect to the L2TP server. The username and password are used to establish a connection between the server and client.
Network Mode	<ul style="list-style-type: none"> ● PC to Router: The dial-up client is an individual. Select this mode when a PC wants to dial up to communicate with the remote PC through the LAN. ● Router to Router: The dial-up client is a user in a network segment. Select this mode when the LANs on two ends of the tunnel need to communicate through router dial-up.
Client Subnet	<p>Specify the IP address range used by the LAN on the peer end of the L2TP tunnel. Generally, the Client Subnet is the IP address network segment of the LAN port on the device. (The LAN network segments of the server and client cannot overlap.)</p> <p>For example, when a branch dials up to connect to the HQ, enter the LAN network segment of the router.</p> <p>Note: When the Network Mode is set to Router to Router, you can click  to set multiple pairs of peer subnets for scenarios where multiple clients are connected to the same server.</p>
Status	Specify whether to enable the user account.

6.2.3 Configuring the L2TP Client

1. Basic Settings of L2TP Client

Choose **One-Device > Gateway > Config > VPN > L2TP > L2TP Settings**.

Turn on the L2TP function, set **L2TP Type** to **Client**, set L2TP client parameters, and click **Save**.

Enable

L2TP Type Server Client

* Username

* Password

Interface

Tunnel IP Dynamic Static

* Server Address

* Server Subnet +

Route All Traffic over VPN

Tunnel Authentication Disable Enable

IPSec Security Open Security

Working Mode NAT Router

* PPP Hello Interval seconds

Table 6-9 L2TP client configuration

Parameter	Description
Username/Password	Specify the username and password for identity authentication for communication over the L2TP tunnel. The values must be the same as those configured on the L2TP server.
Interface	Specify the WAN port used by the client.
Tunnel IP	Specify the virtual IP address of the VPN tunnel client. If you select Dynamic , the client obtains an IP address from the server address pool. If you select Static , manually configure an idle static address within the range of the server address pool as the local tunnel IP address.
Server Address	Enter the WAN port IP address or domain name of the server. This address must be a public network IP address.
Server Subnet	Enter the LAN network segment in which clients want to access the server. The value cannot overlap with the LAN network segment of the client.
Route ALL Traffic over VPN	Once this feature is enabled, all traffic will be directed through the VPN connection, that is, VPN is configured as the default route.
Tunnel Authentication	Specify whether to enable L2TP tunnel authentication. If you enable this function, you need to enter tunnel authentication key the same as that configured on the server. By default, tunnel authentication is disabled. To protect tunnel security, you are advised to enable tunnel authentication.
IPsec Security	Specify whether to encrypt the tunnel. If you select Security , the device Enable the L2TP tunnel using IPsec, indicating the L2TP over IPsec mode. The IPsec encryption configuration on the server and client must be consistent. For details, see Configuring the L2TP over IPsec Client .
Working Mode	<ul style="list-style-type: none"> ● NAT: Perform NAT traversal on the data packet passing through the L2TP tunnel. That is, replace the source IP address of the data packet with the local virtual IP address of the L2TP tunnel. In NAT mode, the server cannot access the LAN where the client resides. ● Router: Only route the data packet passing through the L2TP tunnel. In router mode, the server can access the LAN where the client resides.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after L2TP VPN is deployed. You are advised to retain the default configuration.

2. Configuring the L2TP over IPsec Client

Choose **One-Device > Gateway > Config > VPN > L2TP > L2TP Settings**.

After you complete [Basic Settings of L2TP Client](#), enable IPsec encryption on the L2TP client to guarantee communication security. The IPsec encryption configuration on the server and client must be consistent. For details, see [Configuring the L2TP over IPsec Server](#).

Tunnel Authentication Disable Enable

IPSec Security Open Security

* Pre-shared Key

IKE Policy

Transform Set

Negotiation Mode Main Mode Aggressive Mode

Peer ID Type IP Address NAME

Working Mode NAT Router

* PPP Hello Interval seconds

[Save](#)

6.2.4 Viewing the L2TP Tunnel Information

Choose **One-Device > Gateway > Config > VPN > L2TP > Tunnel List**.

It takes some time to establish a VPN connection between the server and client. After the configuration of the server and client is completed, wait for 1 to 2 minutes to refresh the page and view the L2TP tunnel establishment status.

[Export Log File](#)

[Delete Selected](#)

<input type="checkbox"/>	Username <input type="text"/>	Server/Client <input type="text"/>	Tunnel Name <input type="text"/>	Virtual Local IP <input type="text"/>	Access Server IP <input type="text"/>	Peer Virtual IP <input type="text"/>	DNS <input type="text"/>	Status	Action
No Data									

Total 0 < 1 > 10/page

Table 6-10 L2TP tunnel information

Parameter	Description
Username	Indicate the username used by the client for identity authentication.
Server/Client	Indicate the role of the current device, which is client or server.
Tunnel Name	Indicate the name of the vNIC generated by L2TP.
Virtual Local IP	Indicate the local virtual IP address of the tunnel. The virtual IP address of the L2TP client is allocated by the L2TP server.
Access Server IP	Indicate the real IP address of the peer connecting to the L2TP tunnel.
Peer Virtual IP	Indicate the peer virtual IP address of the tunnel. The virtual IP address of the L2TP client is allocated by the L2TP server.
DNS	Indicate the DNS server address allocated by the L2TP server.

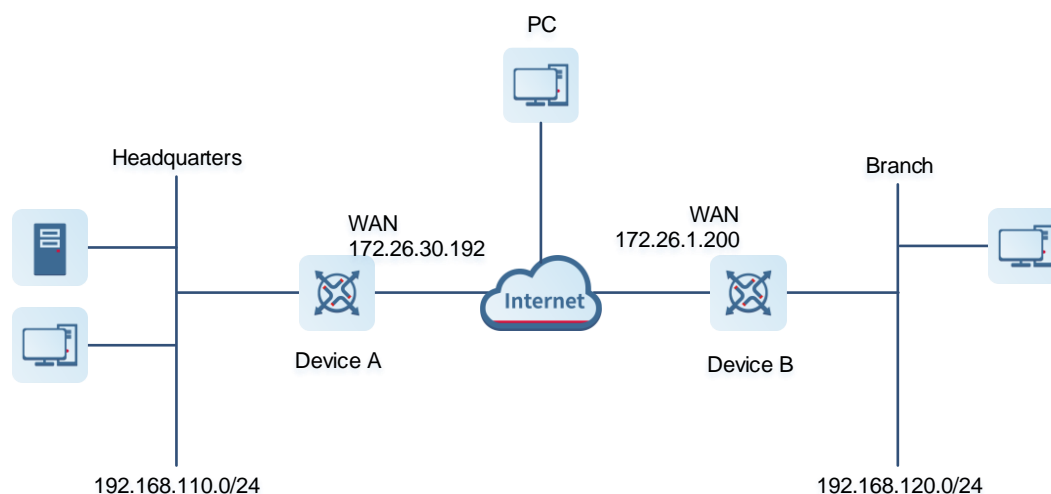
6.2.5 Typical Configuration Example

1. Networking Requirements

An enterprise wants to establish an L2TP tunnel to allow its traveling employees and branch employees to access the servers deployed in the HQ LAN.

- Traveling employees want to access the HQ servers from their PCs through L2TP VPN.
- Branch employees need to frequently access documents on the HQ servers. The enterprise wants to deploy the branch router (Device B) as the L2TP client, so that branch employees can dial up to transparently and directly access documents on the HQ servers, as if they are accessing servers inside the branch.

2. Networking Diagram



3. Configuration Roadmap

- Configure the HQ gateway Device A as the L2TP server.
- Configure the branch gateway Device B as the L2TP client.
- Configure the PC of the traveling employee as the L2TP client.

4. Configuration Steps

- (1) Configure the HQ gateway.

 Note

The LAN address of the HQ cannot conflict with that of the branch. Otherwise, resource access will fail.

- a Log in to the web management system and choose **One-Device > Gateway > Config > VPN > L2TP > L2TP Settings** to access the L2TP Settings page.
- b Turn on the L2TP function, set L2TP Type to Server, enter the local tunnel address, address pool IP address range, and DNS server address, specify whether to enable IPsec encryption and tunnel authentication, and click Save.

Enable

L2TP Type Server Client

* Local Tunnel IP

IP Range

* DNS Server

Tunnel Authentication Disable Enable

IPSec Security Open Security

* Pre-shared Key

IKE Policy

Transform Set

Negotiation Mode Main Mode Aggressive Mode

Local ID Type IP Address NAME

Flow Control Disable Enable

* PPP Hello Interval seconds

Table 6-11 L2TP server configuration


Parameter	Description
Local Tunnel IP	Enter an IP address not in the LAN network segment. The PC can dial up to access the server through this IP address.
IP Range	Enter an IP address range not in the LAN network segment, which is used to allocate IP addresses to clients.
DNS Server	Enter an available DNS server address.

Parameter	Description
Tunnel Authentication	By default, tunnel authentication is disabled. After this function is enabled, the server and client can be connected only when they use the same tunnel key. You can keep tunnel authentication disabled.
IPsec Security	Specify whether to encrypt the L2TP tunnel using the IPsec protocol. You are advised to select Security to guarantee data security. If an IPsec security policy is enabled on the current device, you cannot enable IPsec encryption for the L2TP tunnel. If you want to configure L2TP over IPsec, disable the IPsec security policy first.
Pre-shared Key	Enter the key for IPsec authentication. The client can access the server only when the same pre-shared key is configured on the client.
IKE Policy Transform Set Negotiation Mode Local ID Type Local ID	Keep the default settings unless otherwise specified.
PPP Hello Interval	Keep the default settings unless otherwise specified.

- c Choose **One-Device > Gateway > Config > VPN > VPN Account** and add L2TP user accounts for the traveling employee and branch employee to access the HQ.

For the traveling employee account, set **Network Mode** to **PC to Router**.

For the branch employee account, set **Network Mode** to **Router to Router** and **Peer Subnet** to the LAN network segment of the branch gateway, which is 192.168.120.0/24.

 **Caution**

The LAN network segments of the server and client cannot overlap.

Add User ×

Service Type:

* Username:

* Password:

Network Mode:

* Client Subnet: +

Status:

Add User ×

Service Type:

* Username:

* Password:

Network Mode:

Status:

VPN Client List Username/Password

Up to 100 entries can be added.

<input type="checkbox"/>	Username	Password	Service Type	Network Mode	Peer Subnet	Status	Action
<input type="checkbox"/>	test	test	ALL	PC to Router	-	Enable	Edit Delete
<input type="checkbox"/>	branch	branch	L2TP	Router to Router	192.168.120.0/24	Enable	Edit Delete
<input type="checkbox"/>	pc@l2tp	pc@l2tp	L2TP	PC to Router	-	Enable	Edit Delete

(2) Configure the branch gateway.

- a Log in to the web management system and access the L2TP Settings page.
- b Turn on the L2TP function, set L2TP Type to Client, enter the username and password configured on the server, server address, and LAN network segment of the peer, configure IPsec encryption parameters the same as those on the server, and click Save.

Enable

L2TP Type Server Client

* Username

* Password

Interface

Tunnel IP Dynamic Static

* Server Address

* Server Subnet +

Route All Traffic over VPN

Tunnel Authentication Disable Enable

IPSec Security Open Security

* Pre-shared Key

IKE Policy

Transform Set

Negotiation Mode Main Mode Aggressive Mode

Peer ID Type IP Address NAME

Working Mode NAT Router

* PPP Hello Interval seconds

Table 6-12 L2TP client configuration

Parameter	Description
Username/Password	Enter the username and password configured on the server.
Interface	Select the WAN port on the client to establish a tunnel with the server.
Tunnel IP	Select Dynamic to automatically obtain the tunnel IP address. You can also select Static and enter an IP address in the address pool of the server.
Server Address	Enter the WAN port address of the server, which is 172.26.30.192.
Server Subnet	Enter the LAN network segment (LAN port IP address range) of the server, which is 192.168.110.0/24.
Tunnel Authentication	The value must be the same as that on the server. In this example, you need to disable tunnel authentication.
IPsec Security	The value must be the same as that on the server. In this example, you need to set this parameter to Security .
Pre-shared Key	Enter the pre-shared key configured on the server.
IKE Policy Transform Set Negotiation Mode Peer ID Type Peer ID	The settings must be the same as those on the server. Set Peer ID Type to the same value as that of Local ID Type on the server.
Working Mode	If the HQ wants to access the LAN of the branch, set this parameter to Router .
PPP Hello Interval	Specify the interval for sending PPP Hello packets after L2TP VPN is deployed. Keep the default settings.

- (3) Configure the PC of the traveling employee.

 Note

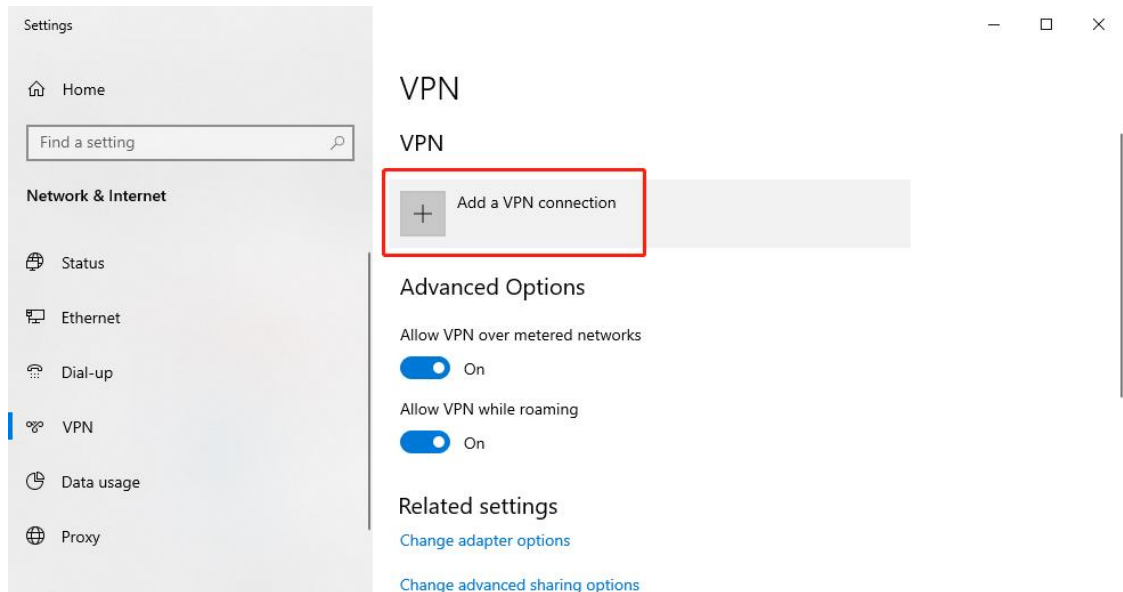
Configure the PC of a traveling employee as the L2TP client. The following uses the PC running Windows 10 operating system as an example.

The Windows XP (shorted as XP) system and Windows 7/Windows 10 (shorted as Win7/10) system differ in their support for L2TP VPN: To enable L2TP VPN in the XP system, you need to modify the service registries. L2TP is supported in the Win7/10 system by default, without the need to modify registries.

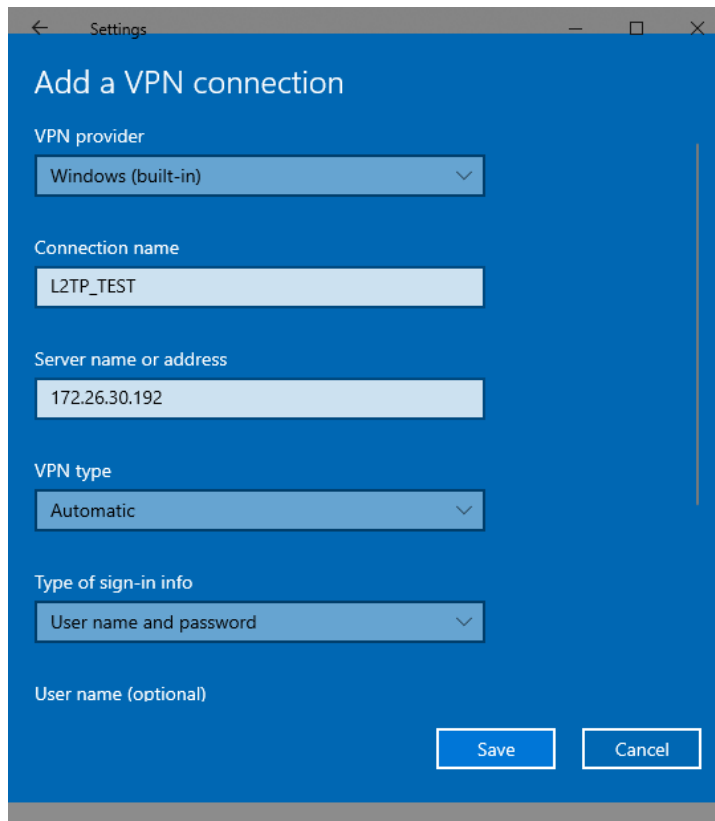
Neither the Win7/Win10 system nor the XP system supports L2TP tunnel authentication. Therefore, tunnel authentication must be disabled on the server.

Apple mobile phones support L2TP over IPsec but do not support IPsec encryption for L2TP dial-up.

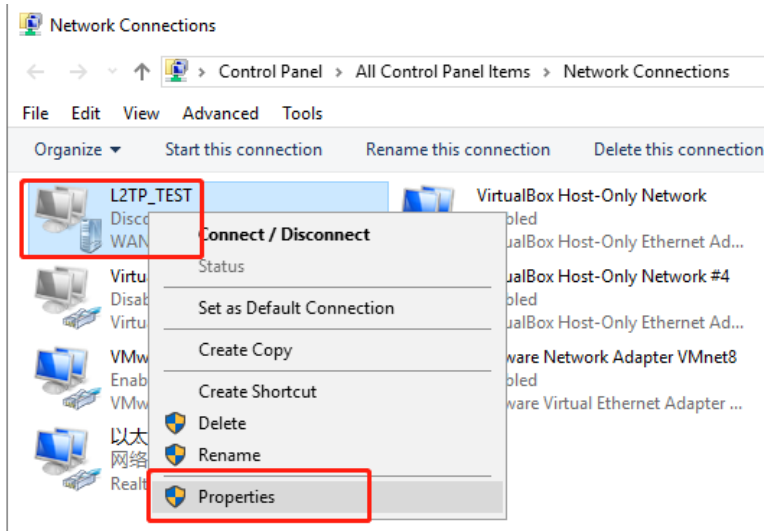
- a Choose **Settings** > **Network & Internet** > **VPN** to access the VPN page.



- b Click **Add a VPN connection**. In the dialog box that appears, set VPN provider to **Windows**, enter the connection name and server address or domain name, and click **Save**.



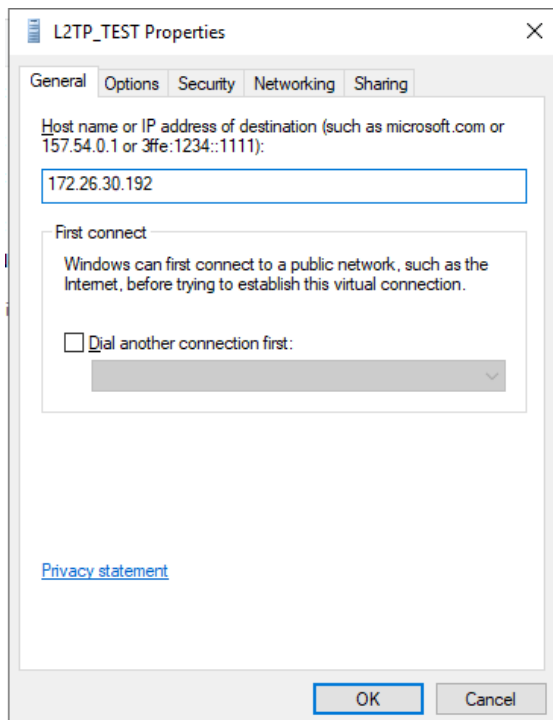
- c Right-click the created VPN connection named **L2TP_TEST** and select Properties to view the properties of the network connection.

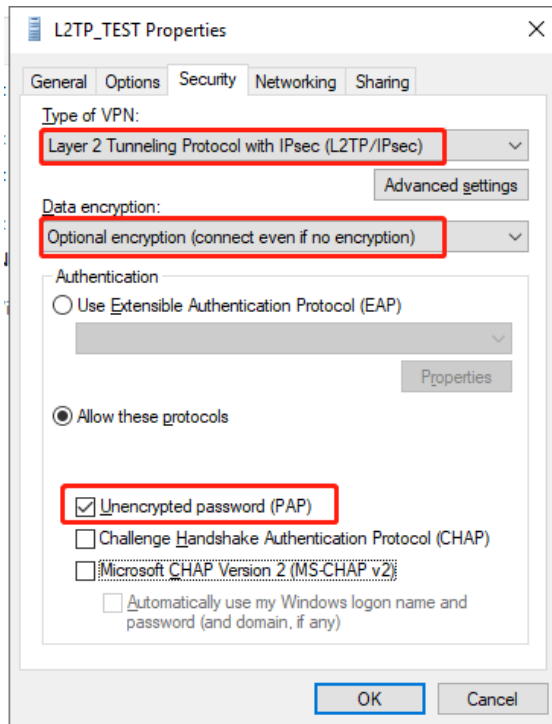


- d In the dialog box that appears, click the **Security** tab, and set **Type of VPN** to **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)** and **Data encryption** to **Optional encryption (connect even if no encryption)**.

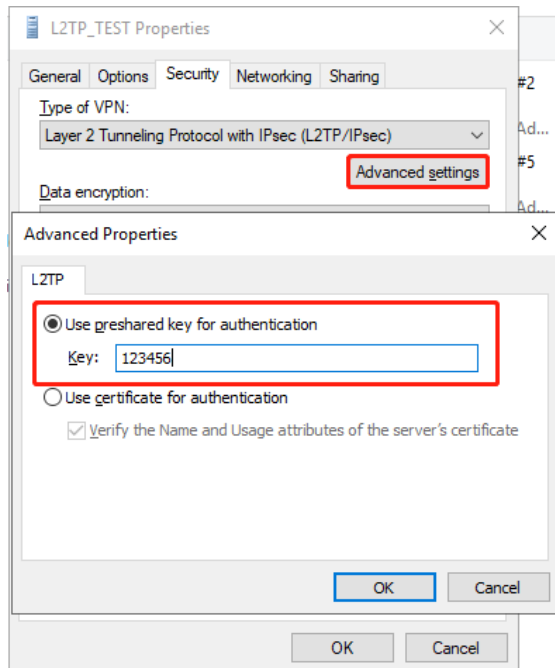
If IPsec encryption is not enabled on the L2TP server, select **Unencrypted password (PAP)** and click **OK**. Skip Step e .

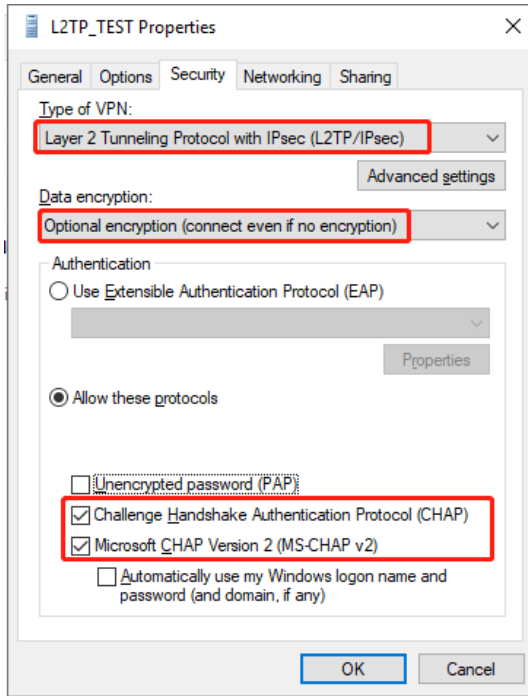
If IPsec encryption is enabled on the L2TP server, perform Step e .






- e If IPsec encryption is enabled on the server, select **CHAP** and **MS-CHAP v2** as the identity authentication protocols and click **Advanced settings**. In the dialog box that appears, configure the pre-shared key the same as that on the server. After completing the configuration, click **OK**.

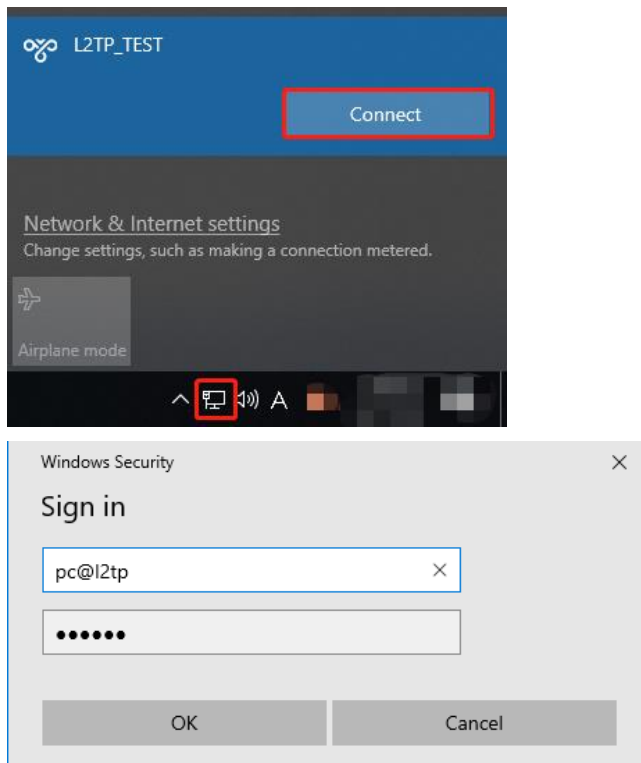




Note

The device does not support EAP for identity authentication. Therefore, you cannot select EAP-related identity authentication options in the Windows client. Otherwise, the VPN connection fails.

- f After the L2TP client configuration is completed on the PC, initiate a VPN connection on the PC. Click the network icon  in the task bar, select the created L2TP VPN connection, and click Connect. In the dialog box that appears, enter the username and password configured on the server.



5. Verifying Configuration

- (1) After the server and client are configured, wait for about 1 minute. If you can view the L2TP tunnel connection information on the HQ server and branch client, the connection is successful.

HQ:

L2TP Settings [Tunnel List](#)

Tunnel List								
<input type="checkbox"/>	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
<input type="checkbox"/>	pc@l2tp	Server	ppp2	20.0.0.1	172.26.1.200	20.1.1.3	114.114.114.114	Delete
<input type="checkbox"/>	branch	Server	ppp0	20.0.0.1	172.26.1.200	20.1.1.2	114.114.114.114	Delete

Branch:

Tunnel List

<input type="checkbox"/>	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
<input checked="" type="checkbox"/>	branch	Client	l2tp	20.1.1.2	172.26.30.192	20.0.0.1	114.114.114.114	Delete

- (2) Ping the LAN address of the peer from the HQ or branch. The HQ and branch can successfully communicate. The PC of the traveling employee and the PC of the branch employee can access the HQ server.

```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>ping 192.168.110.1

Pinging 192.168.110.1 with 32 bytes of data:
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.110.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
  
```

6.2.6 Solution to L2TP VPN Connection Failure

- (1) Run the ping command to test the connectivity between the client and server. For details, see Section [4.5.3 Network Tools](#). If the ping fails, check the network connection settings. Check whether the branch EG can ping to HQ EG. If the ping fails, check the network connection between the two EGs.

Choose **One-Device > Gateway > Config > Diagnostics > Network Tools**. Then, you can start the ping operation. For details, see Section [4.5.3 Network Tools](#).

- (2) Check whether the username and password used by the client are the same as those configured on the server.
- (3) Check whether the WAN port IP address of your HQ EG is a public network IP address. If not, you need to configure DMZ on your egress gateway.

6.3 Configuring PPTP VPN

6.3.1 Overview

Point-to-Point Tunneling Protocol (PPTP) is an enhanced security protocol designed based on the Point-to-Point Protocol (PPP). It allows an enterprise to use private tunnels to expand its enterprise network over the public network. PPTP relies on the PPP protocol to implement security functions such as encryption and identity authentication. Generally, PPTP works with Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv1/v2), or Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) for identity authentication and Microsoft Point-to-Point Encryption (MPPE) for encryption to improve security.

Currently, the device can be deployed as the PPTP server or client. It supports MPPE for encryption MSCHAP-v2 for identity authentication, and does not support EAP authentication.

6.3.2 Configuring the PPTP Service

1. Configuring the PPTP Server

Choose **One-Device > Gateway > Config > VPN > PPTP > PPTP Settings**.

Turn on the PPTP function, set **PPTP Type** to **Server**, configure PPTP server parameters, and click **Save**.

Enable

PPTP Type Server Client

* Local Tunnel IP

* IP Range (?)

* DNS Server

MPPE Disable Enable

Flow Control Disable Enable

* PPP Hello Interval (?) seconds

Table 6-13 PPTP server configuration

Parameter	Description
Local Tunnel IP	Specify the local virtual IP address of the L2TP server. Clients can dial up to access the L2TP server through this address.
IP Range	Specify the address pool used by the PPTP server to allocate IP addresses to clients.
DNS Server	Specify the DNS server address pushed by the PPTP server to clients.
MPPE	<p>Specify whether to use MPPE to encrypt the PPTP tunnel.</p> <p>After MPPE is enabled on the server: If Data encryption is set to Optional encryption on the client, the server and client can be connected but the server does not encrypt packets. If Data encryption is set to Require encryption on the client, the server and client can be connected and the server encrypts packets. If Data encryption is set to No encryption allowed on the client, the server and client cannot be connected.</p> <p>If MPPE is disabled on the server but the client requires encryption, the server and client connection fails.</p> <p>By default, MPPE is disabled on the server. After you enable MPPE, the bandwidth performance of the device degrades. You are advised to keep MPPE disabled if there are no special security requirements.</p>
Flow Control	The VPN server has a lower priority to control the traffic of the client than the custom policy. The VPN server can only limit the maximum uplink and downlink bandwidth per user for the client. For details, see 4.14.2 Smart Flow Control .
PPP Hello Interval	Specify the interval for sending PPP Hello packets after PPTP VPN is deployed.

 **Caution**

The local tunnel address and IP address range of the address pool cannot overlap the network segment of the LAN port on the device.

2. Configuring PPTP User

Choose **One-Device > Gateway > Config > VPN > VPN Account**.

Only user accounts added to the VPN client list are allowed to dial up to connect to the PPTP server. Therefore, you need to manually configure user accounts for clients to access the PPTP server.

Click **Add**. In the dialog box that appears, set **Service Type** to **PPTP** or **ALL**. (If you select **ALL**, the created account can be used to establish all types of VPN tunnels.) Enter the username, password, and peer subnet, select a network mode, and click **OK**.

VPN User List Username/Password

<input type="checkbox"/>	Username	Password	Service Type	Network Mode	Client Subnet	Status	Action
<input type="checkbox"/>	pptp@branch	****	PPTP	Router to Router	192.168.12.0/24	Enable	Edit Delete
<input type="checkbox"/>	pptp@pc	****	PPTP	PC to Router	-	Enable	Edit Delete

Add User ×

Service Type

* Username


* Password

Network Mode

Status

Table 6-14 PPTP user configuration

Parameter	Description
Username/Password	Specify the name and password of the PPTP user allowed to dial up to connect to the PPTP server. The username and password are used to establish a connection between the server and client.
Network Mode	<ul style="list-style-type: none"> PC to Router: The dial-up client is an individual. Select this mode when a PC wants to dial up to communicate with the remote PC through the LAN. Router to Router: The dial-up client is a user in a network segment. Select this mode when the LANs on two ends of the tunnel need to communicate through router dial-up.

Parameter	Description
Client Subnet	<p>Specify the IP address range used by the LAN on the peer end of the PPTP tunnel. Generally, the peer subnet is the IP address network segment of the LAN port on the device. (The LAN network segments of the server and client cannot overlap.)</p> <p>For example, when a branch dials up to connect to the HQ, enter the LAN network segment of the router.</p> <p>Note: When the Network Mode is set to Router to Router, you can click  to set multiple pairs of peer subnets for scenarios where multiple clients are connected to the same server.</p>
Status	Specify whether to enable the user account.

6.3.3 Configuring the PPTP Client

Choose **One-Device > Gateway > Config > VPN > PPTP > PPTP Settings**.

Turn on the PPTP function, set **PPTP Type** to **Client**, configure PPTP client parameters, and click **Save**.

Enable

PPTP Type Server Client

* Username

* Password

Interface

Tunnel IP Dynamic Static

* Server Address

* Server Subnet +

Route All Traffic over VPN

MPPE Disable Enable

Working Mode NAT Router

* PPP Hello Interval seconds

Table 6-15 PPTP client configuration

Parameter	Description
Username/Password	Specify the username and password for identity authentication for communication over the PPTP tunnel. The values must be the same as those configured on the PPTP server.
Interface	Specify the WAN port used by the client.
Tunnel IP	Specify the virtual IP address of the VPN tunnel client. If you select Dynamic , the client obtains an IP address from the server address pool. If you select Static , manually configure an idle static address within the range of the server address pool as the local tunnel IP address.

Parameter	Description
Server Address	Enter the WAN port IP address or domain name of the server. This address must be a public network IP address.
Server Subnet	Enter the LAN network segment in which clients want to access the server. The value cannot overlap with the LAN network segment of the client.
Route All Traffic over VPN	Once this feature is enabled, all traffic will be directed through the VPN connection, that is, VPN is configured as the default route.
MPPE	Specify whether to use MPPE to encrypt the PPTP tunnel. The value must be the same as that on the server.
Working Mode	NAT: The client can access the server network, but the server cannot access the client network. Router: The server can access the client network.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after a PPTP tunnel is established. You are advised to retain the default configuration.

6.3.4 Viewing the PPTP Tunnel Information

Choose **One-Device > Gateway > Config > VPN > PPTP > Tunnel List**.

It takes some time to establish a VPN connection between the server and client. After the configuration of the server and client is completed, wait for 1 to 2 minutes to refresh the page and view the PPTP tunnel establishment status.

<input type="checkbox"/>	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Status	Action
No Data									

Table 6-16 PPTP tunnel information

Parameter	Description
Username	Indicate the username used by the client for identity authentication.
Server/Client	Indicate the role of the current device, which is client or server.
Tunnel Name	Indicate the name of the vNIC generated by PPTP.

Parameter	Description
Virtual Local IP	Indicate the local virtual IP address of the tunnel. The virtual IP address of the PPTP client is allocated by the PPTP server.
Access Server IP	Indicate the real IP address of the peer connecting to the PPTP tunnel.
Peer Virtual IP	Indicate the peer virtual IP address of the tunnel. The virtual IP address of the PPTP client is allocated by the PPTP server.
DNS	Indicate the DNS server address allocated by the PPTP server.

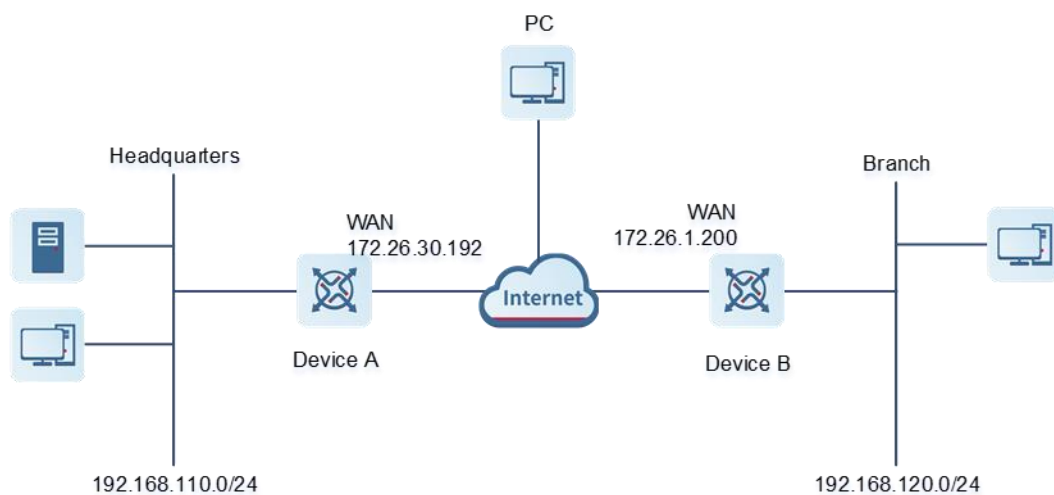
6.3.5 Typical Configuration Example

1. Networking Requirements

An enterprise wants to establish a PPTP tunnel to allow its traveling employees and branch employees to access the servers deployed in the HQ LAN.

- Traveling employees want to access the HQ servers from their PCs through PPTP dial-up.
- Branch employees need to frequently access documents on the HQ servers. The enterprise wants to deploy the branch router (Device B) as the PPTP client, so that branch employees can dial up to transparently and directly access documents on the HQ servers, as if they are accessing servers inside the branch.

2. Networking Diagram



3. Configuration Roadmap

- Configure the HQ gateway Device A as the PPTP server.
- Configure the branch gateway Device B as the PPTP client.
- Configure the PC of the traveling employee as the PPTP client.

4. Configuration Steps

(1) Configure the HQ gateway.

Note

The LAN address of the HQ cannot conflict with that of the branch. Otherwise, resource access will fail.

- a Log in to the web management system and choose **One-Device > Gateway > Config > VPN > PPTP > PPTP Settings** to access the PPTP Settings page.
- b Turn on the PPTP function, set PPTP Type to Server, enter the local tunnel address, address pool IP address range, and DNS server address, specify whether to enable MPPE encryption, and click Save.

Enable

PPTP Type Server Client

* Local Tunnel IP

* IP Range

* DNS Server

MPPE Disable Enable

Flow Control Disable Enable

* PPP Hello Interval seconds

Table 6-17 PPTP server configuration

Parameter	Description
Local Tunnel IP	Enter an IP address not in the LAN network segment. The PC can dial up to access the server through this IP address.
IP Range	Enter an IP address range not in the LAN network segment, which is used to allocate IP addresses to clients.
DNS Server	Enter an available DNS server address.

Parameter	Description
MPPE	Specify whether to use MPPE to encrypt the PPTP tunnel. The value must be the same as that on the client. After you enable MPPE, the device security is improved but the bandwidth performance of the device degrades. You are advised to keep MPPE disabled if there are no special security requirements.
Flow control	Flow control is disabled by default.
PPP Hello Interval	Keep the default settings unless otherwise specified.

- c Choose **One-Device > Gateway > Config > VPN > VPN Account** and add PPTP user accounts for the traveling employee and branch employee to access the HQ.

For the traveling employee account, set **Network Mode** to **PC to Router**.

For the branch employee account, set **Network Mode** to **Router to Router** and **Client Subnet** to the LAN network segment of the branch gateway.

 Caution

The LAN network segments of the server and client cannot overlap.

Add User



Service Type (?)

* Username

* Password

Network Mode (?)

* Client Subnet +

Status

Cancel

OK

Add User



Service Type PPTP

* Username pc@pptp

* Password *****

Network Mode PC to Router

Status

Cancel

OK

VPN User List

Username/Password

+ Add

Delete All

Delete Selected

<input type="checkbox"/>	Username	Password	Service Type	Network Mode	Client Subnet	Status	Action
<input type="checkbox"/>	branch	*****	L2TP	Router to Router	192.168.120.0/24	Enable	Edit Delete
<input type="checkbox"/>	pc@l2tp	*****	L2TP	PC to Router	-	Enable	Edit Delete
<input type="checkbox"/>	branch	*****	PPTP	Router to Router	192.168.120.0/24	Enable	Edit Delete
<input type="checkbox"/>	pc@pptp	*****	PPTP	PC to Router	-	Enable	Edit Delete

Up to 300 entries can be added.

Total 4



1



10/page

(2) Configure the branch gateway.

- a Log in to the web management system and access the PPTP Settings page.
- b Turn on the PPTP function, set PPTP Type to Client, enter the username and password configured on the server, server address, and LAN network segment of the peer, configure IPsec encryption parameters the same as those on the server, and click Save.

Enable

PPTP Type Server Client

* Username

* Password

Interface

Tunnel IP Dynamic Static

* Server Address

* Server Subnet +

Route All Traffic over VPN

MPPE Disable Enable

Working Mode NAT Router

* PPP Hello Interval seconds

Table 6-18 PPTP client configuration

Parameter	Description
Username/Password	Enter the username and password configured on the server.
Interface	Select the WAN port on the client to establish a tunnel with the server.
Tunnel IP	Select Dynamic to automatically obtain the tunnel IP address. You can also select Static and enter an IP address in the address pool of the server.
Server Address	Enter the WAN port address of the server.
Server Subnet	Enter the LAN network segment (LAN port IP address range) of the server.

Parameter	Description
Route All Traffic over VPN	Once this feature is enabled, all traffic will be directed through the VPN connection, that is, VPN is configured as the default route.
MPPE	The value must be the same as that on the server.
Working Mode	If the HQ wants to access the LAN of the branch, set this parameter to Router .
PPP Hello Interval	Specify the interval for sending PPP Hello packets after PPTP VPN is deployed. Keep the default settings.

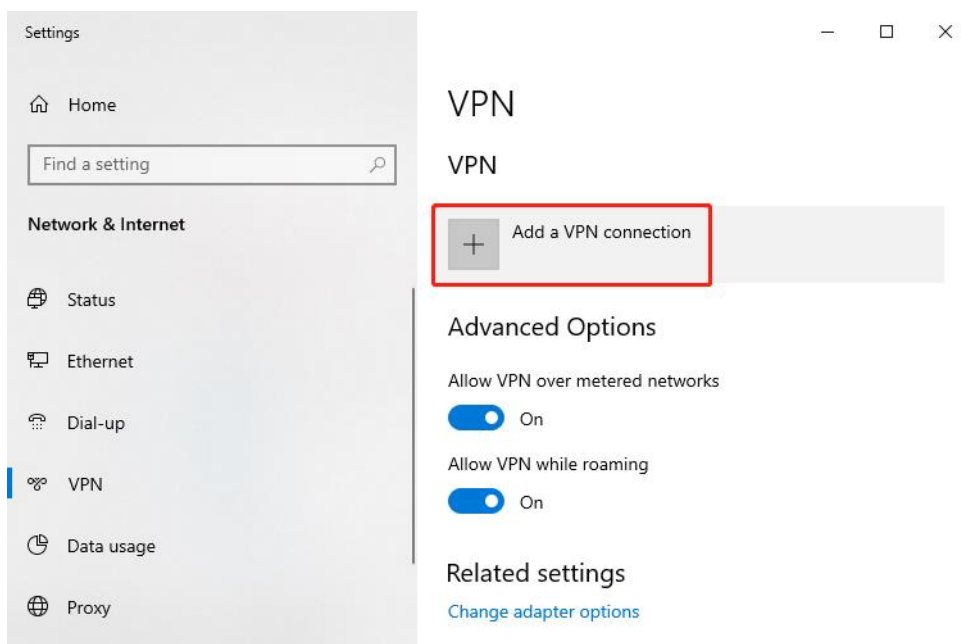
(3) Configure the PC of the traveling employee.

Note

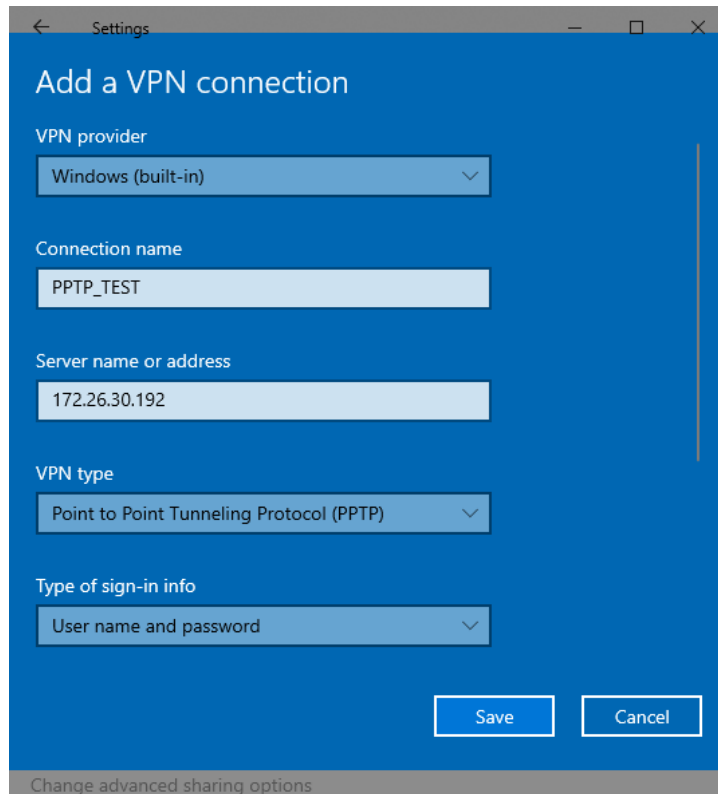
Configure the PC of a traveling employee as the PPTP client. The following uses the PC running Windows 10 operating system as an example.

Enable ports 1723 (PPTP) and 47 (GRE) on the PC firewall.

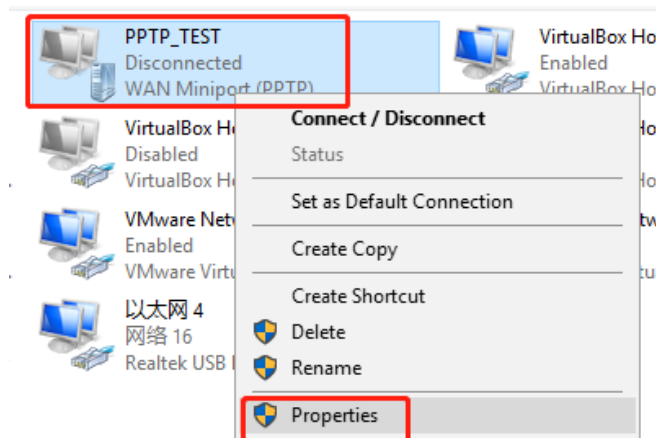
a Choose Settings > Network & Internet > VPN to access the VPN page.



b Click **Add a VPN connection**. In the dialog box that appears, set VPN provider to **Windows** and VPN type to **Point to Point Tunneling Protocol (PPTP)**, enter the connection name and server address or domain name, and click **Save**.



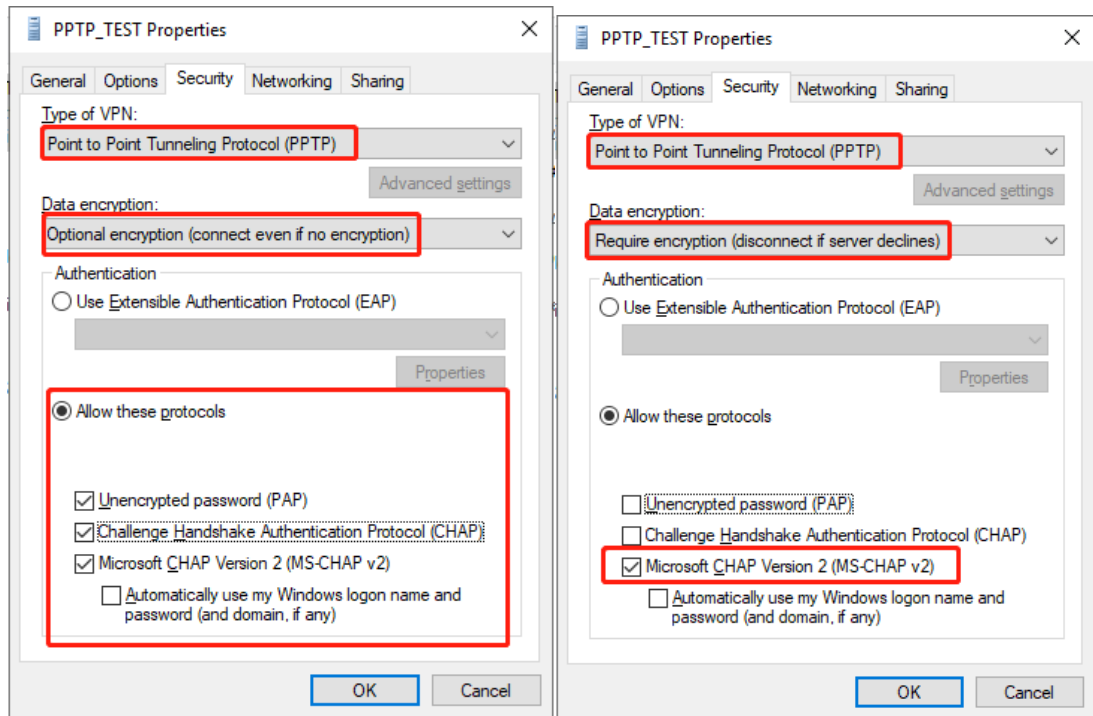
- c Right-click the created VPN connection named **PPTP_TEST** and select Properties to view the properties of the network connection.



- d In the dialog box that appears, click the **Security** tab.

If MPPE is not enabled on the PPTP server, set **Data encryption** to **Optional encryption** or **No encryption allowed** and use PAP, CHAP, or MS-CHAP v2 for identity authentication, as shown in the following figure on the left.

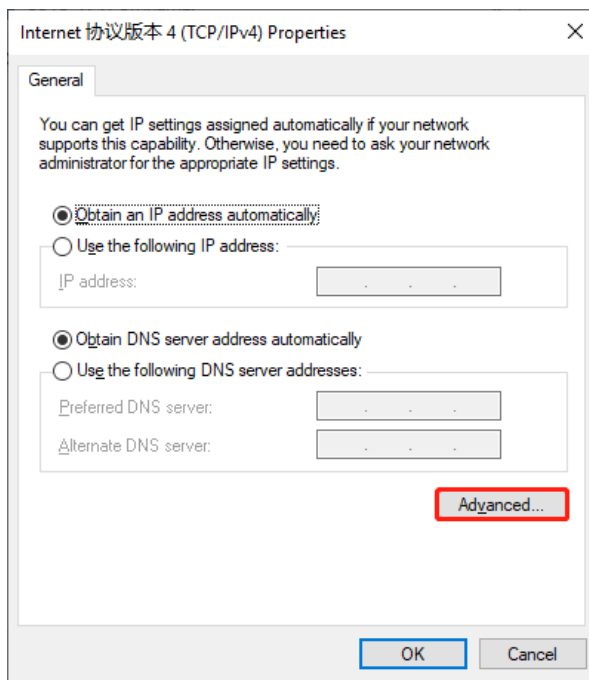
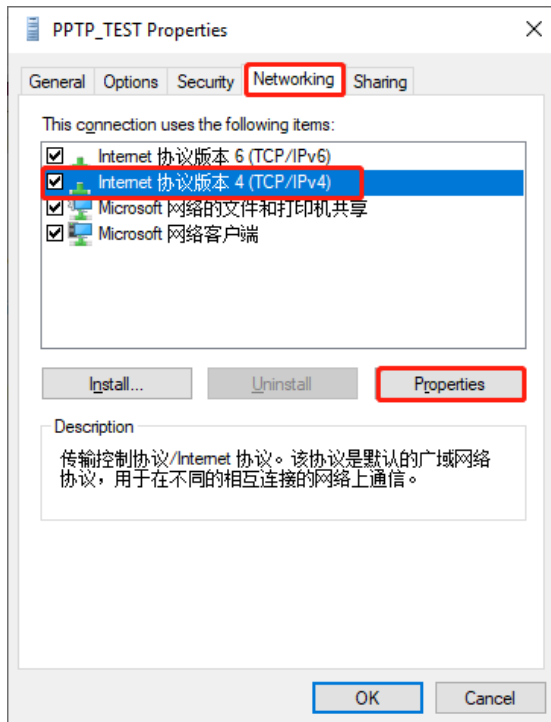
If MPPE is enabled on the PPTP server, set **Data encryption** to **Require encryption** or **Maximum strength encryption** and use MS-CHAP v2 for identity authentication, as shown in the following figure on the right.

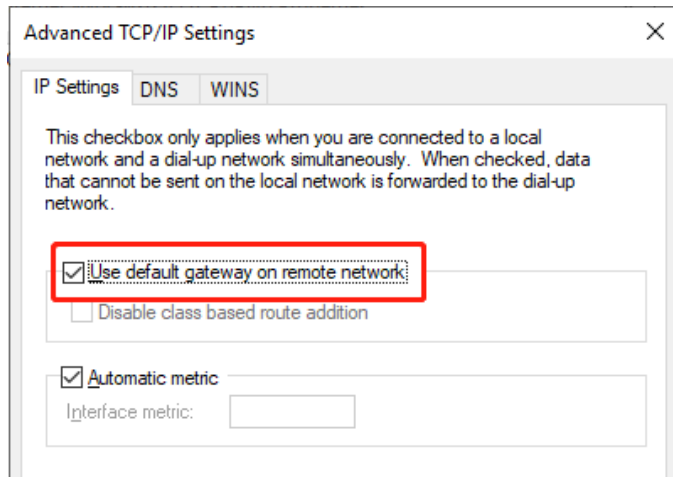



Note

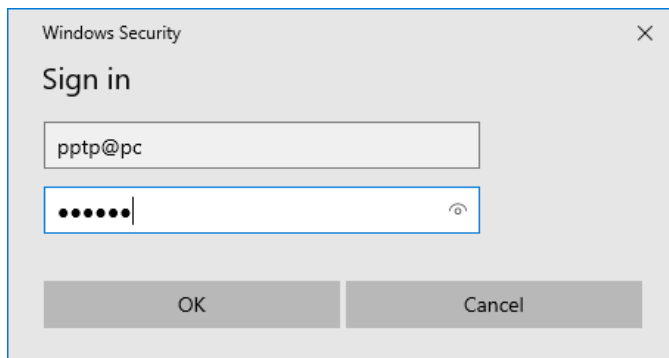
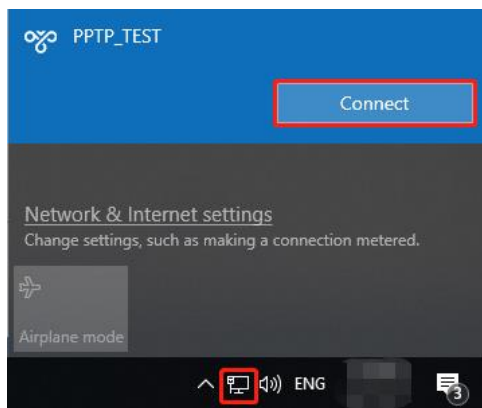
The device does not support EAP for identity authentication. Therefore, you cannot select EAP-related identity authentication options in the Windows client. Otherwise, the VPN connection fails.

- e When the PC functions as a dial-up client, configure the PC by using either of the following methods:
 - o Add a route to the VPN peer network segment on the PC as the administrator.
 - o In the **Properties** dialog box of the local VPN connection, select **Use default gateway on remote network**. After the VPN connection is successful, all data flows from the PC to the Internet are routed to the VPN tunnel. The following figures show the detailed configuration.





- f After the PPTP client configuration is completed on the PC, initiate a VPN connection on the PC. Click the network icon  in the task bar, select the PPTP VPN connection, and click **Connect**. In the dialog box that appears, enter the username and password configured on the server.



5. Verifying Configuration

- (1) After the server and client are configured, wait for about 1 minute. If you can view the L2TP tunnel connection information on the HQ server and branch client, the connection is successful.

HQ:

PPTP Settings [Tunnel List](#)

Tunnel List ?

[Delete Selected](#)

<input type="checkbox"/>	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
<input type="checkbox"/>	pc@pptp	Server	ppp2	10.1.1.1	172.26.1.200	10.2.2.3	114.114.114.114	Delete
<input type="checkbox"/>	branch	Server	ppp1	10.1.1.1	172.26.1.200	10.2.2.2	114.114.114.114	Delete

Branch:

Tunnel List ?

[Delete Selected](#)

<input type="checkbox"/>	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
<input checked="" type="checkbox"/>	branch	Client	pptp	10.2.2.2	172.26.30.192	10.1.1.1	114.114.114.114	Delete

- (2) Ping the LAN address of the peer from the HQ or branch. The HQ and branch can successfully communicate. The PC of the traveling employee and the PC of the branch employee can access the HQ server.

```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>ping 192.168.110.1

Pinging 192.168.110.1 with 32 bytes of data:
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.110.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
  
```

6.3.6 Solution to PPTP VPN Connection Failure

- (1) iPhones and other IOS devices do not support PPTP VPN. Please use L2TP VPN instead
- (2) Run the ping command to test the connectivity between the client and server. For details, see Section [4.5.3 Network Tools](#). If the ping fails, check the network connection settings. Check whether the branch EG can ping to HQ EG. If the ping fails. Check the network connection between the two EGs.
Choose **One-Device** > **Gateway** > **Config** > **Diagnostics** > **Network Tools**. Then, you can start the ping operation. For details, see Section [4.5.3 Network Tools](#).
- (3) Check whether the username and password used by the client are the same as those configured on the server.
- (4) Check whether the WAN port IP address of your HQ EG is a public network IP address. If not, please configure DMZ on your egress gateway.

6.4 Configuring OpenVPN

Caution

- The RG-EG105G does not support the OpenVPN function.
 - IPTV connection is not supported only in the Chinese environment. To connect to IPTV in the Chinese environment, switch the system language.
-

6.4.1 Overview

1. OpenVPN Overview

Due to security considerations or cross-NAT communication needs, private channels need to be established between enterprises or between individual and enterprise. OpenVPN is used to establish Layer 2 or Layer 3 VPN tunnels by using the vNIC. OpenVPN supports flexible client authorization modes, supports authentication through certificate or username and password, and allows users to connect to VPN virtual interfaces through the firewall. It is easier to use than other types of VPN technologies. OpenVPN can run in the Linux, xBSD, Mac OS X, and Windows 2000/XP systems. The device can establish VPN connections to PCs, Android/Apple mobile phones, routers, and Linux devices, and it is compatible with most OpenVPN products in the market.

OpenVPN connections can traverse most proxy servers and can function well in the NAT environment. The OpenVPN server can push the following network configuration to clients: IP address, routes, and DNS settings.

2. Certificate Overview

The major advantage of OpenVPN lies in its high security, but OpenVPN security requires the support of certificates.

The OpenVPN client supports certificates **ca.crt**, **ca.key**, **client.crt**, and **client.key** and the OpenVPN server supports certificates **ca.crt**, **ca.key**, **server.crt**, and **server.key**.

6.4.2 Configuring the OpenVPN Server

Choose **One-Device > Gateway > Config > VPN > OpenVPN**.

1. Basic Settings

Turn on **Enable** to enable the OpenVPN function, set **OpenVPN Type** to **Server**, set other parameters, and click **Save**. After the basic settings are completed, you can view the tunnel information of the server in the tunnel list.

i OpenVPN Client [Download Link](#)

Enable

OpenVPN Type Server Client

Server Mode Account

Protocol UDP

* Server Address 10.52.48.43

* Port ID 1194 1-65535

* IP Range 10.80.12.0/24

* Deliver Route 192.168.110.0 255.255.255.0 +

Flow Control Disable Enable

advanced Setting


Client Config Export

Save

Table 6-19 OpenVPN server basic settings

Parameter	Description
Server Mode	Select a server authentication mode. The options are Account , Certificate , and Account & Certificate . <ul style="list-style-type: none"> ● Account: Enter the correct username and password and upload the CA certificate on the client to connect to the server. The configuration is simple. ● Certificate: Upload the CA certificate and client certificate and enter the correct private key on the client to connect to the server. ● Account & Certificate: Upload the CA certificate and client certificate and enter the correct username, password, and private key. This mode is applicable to scenarios with high security requirements.
Protocol	Select a protocol for all OpenVPN communications based on a single IP port. The options are UDP and TCP . The default value is UDP , which is recommended. When you select a protocol, pay attention to the network status between two encrypted tunnel ends. If high latency or heavy packet loss occurs, select TCP as the underlying protocol.

Parameter	Description
Server Address	Specify the server address for client connection. You can set this parameter to a domain name.
Port ID	Specify the port used by the OpenVPN service process. Internet Assigned Numbers Authority (IANA) specifies port 1194 as the official port for the OpenVPN service. If the port is in use or disabled in the local network, the server log prompts port binding failure and you are asked to change the port number.
IP Range	Specify the network segment of the OpenVPN address pool. The first available in the address pool is allocated to the server, and the other addresses are allocated to clients. For example, if this parameter is set to 10.80.12.0/24 , the VPN virtual address of the server is 10.80.12.1.
Deliver Route	Specify the VPN dial-up line for clients to access the LAN network segment of the server. The server informs clients that want to access the server LAN of the route information. You can configure a maximum of three routes.
Flow Control	The VPN server has a lower priority to control the traffic of the client than the custom policy. The VPN server can only limit the maximum uplink and downlink bandwidth per user for the client. For details, see 4.14.2 Smart Flow Control .
Client Config	<p>Click Export to export the parameter configuration of the client connected to the server in the .tar compressed package. The decompressed information is used for setting the OpenVPN client.</p> <p>In account mode, the compressed package contains the configuration file client.ovpn, CA certificate ca.crt, and CA private key ca.key.</p> <p>If certificate authentication is configured, the compressed package contains the configuration file client.ovpn, CA certificate ca.crt, CA private key ca.key, client certificate client.crt, and client private key client.key.</p> <p>If TLS authentication is enabled, the compressed package contains the TLS identity authentication key tls.key apart from the preceding files. For details on TLS authentication, see Advanced Settings.</p>
Server Log	Click Export to export server log files, including the server start time and client dial-up logs.

 **Caution**

The IP address range of the device cannot overlap the network segment of the LAN port on the device.

OpenVPN [Tunnel List](#)

<input type="checkbox"/>	Username	Server/Client	Status	Real IP Address	Virtual IP Address
<input type="checkbox"/>	openvpn	Server	OK	172.26.30.192	10.80.12.1

2. Advanced Settings

Click **advanced Setting** to configure the advanced parameters. Keep the default settings unless otherwise specified.

TLS Authentication ?

Allow Data Compression ?

Route All Traffic over VPN ?

Cipher ?

Deliver DNS ? +

Auth

Table 6-20 OpenVPN server advanced settings

Parameter	Description
TLS Authentication	Specify the TLS key for enhanced OpenVPN security by allowing the communicating parties to possess the shared key before TLS handshake. After TLS authentication is enabled, you must import the TLS key on the client. (The version of the peer OpenVPN client must be higher than 2.40.)
Allow Data Compression	Specify whether to enable data compression. If this function is enabled, transmitted data is compressed using the LZO algorithm. Data compression saves bandwidth but consumes certain CPU resources. The setting on the client must be the same as that on the server. Otherwise, the connection fails.
Route All Traffic over VPN	Specify whether to route all traffic over VPN. After this function is enabled, all the traffic is routed over the VPN tunnel. This means that the VPN tunnel is the default route.

Parameter	Description
Cipher	Select the data encryption mode before data transmission to ensure that even data packets are intercepted during transmission, the leaked data cannot be interpreted. If this parameter is set to Auto on the server, you can set this parameter to any option on the client. If a specific encryption algorithm is configured on the server, you must select the same encryption algorithm on the client. Otherwise, the connection fails.
Deliver DNS	Specify the DNS server address pushed by the server to clients. Currently, the device can push the DNS server address to Windows clients only.
Auth	Specify the MD5 algorithm used by the server. The server will inform the clients of this information. The default value is SHA1 .

3. Configuring OpenVPN User

Choose **One-Device > Gateway > Config > VPN > VPN Account**.

Only user accounts added to the VPN client list are allowed to dial up to connect to the OpenVPN server. Therefore, you need to manually configure user accounts for clients to access the OpenVPN server.

Click **Add**. In the dialog box that appears, set **Service Type** to **OpenVpn**, enter the username and password, and click **OK**. The **Status** parameter specifies whether to enable the user account.

VPN User List Username/Password + Add Delete All Delete Selected

<input type="checkbox"/>	Username	Password	Service Type	Network Mode	Client Subnet	Status	Action
<input type="checkbox"/>	branch	*****	L2TP	Router to Router	192.168.120.0/24	Enable	Edit Delete
<input type="checkbox"/>	pc@l2tp	*****	L2TP	PC to Router	-	Enable	Edit Delete

Add User ×

Service Type

* Username

* Password

Status

6.4.3 Configuring the OpenVPN Client

Choose **One-Device > Gateway > Config > VPN > OpenVPN**.

Currently, you can configure the device as the OpenVPN client in either of the following methods:

Web Settings: Configure OpenVPN client on the web page. This method is used when the device is connected to a non-EG server.

Import Config: Manually import the configuration file. This method is used when the device is connected to a similar device. The client configuration file **client.ovpn** can be directly exported from the connected OpenVPN server.

Enable

OpenVPN Type Server Client

Client Config Import Config Web Settings

1. Import Config

Turn on **Enable** to enable the OpenVPN function, set **OpenVPN Type** to **Client** and **Client Config** to **Import Config**, select a server mode, set relevant parameters, and click **Browse** to import the client configuration file. Then, click **Save** to make the configuration take effect.

Enable

OpenVPN Type Server Client

Client Config Import Config Web Settings

Server Mode

* Username

* Password

Client Config [It already exists.](#)

Table 6-21 OpenVPN client configuration in Import Config method

Parameter	Description
Server Mode	<p>Select a server authentication mode. The options are Account, Certificate, Account & Certificate and Pre-Shared Key.</p> <ul style="list-style-type: none"> ● Account: Enter the correct username and password and upload the CA certificate on the client. The CA certificate information is embedded in the client configuration file. ● Certificate: Upload the CA certificate and client certificate and enter the correct private key on the client. All the information is embedded in the client configuration file. ● Account & Certificate: Enter the correct username, password, and private key and upload the CA certificate, and client certificate on the client. The information of the CA certificate, client certificate, and private key is embedded in the client configuration file. ● Pre-Shared Key: Upload the pre-shared key file apart from the client configuration file.
Username & Password	Enter the username and password configured on the server.
Client Config	Click Browse, select the client configuration file exported from the server, and upload the file.
Pre-Shared Key	Click Browse, select the pre-shared key file, and upload the file.
Working Mode	<p>This parameter is available only when Server Mode is set to Pre-Shared Key.</p> <p>NAT: The client can access the server network, but the server cannot access the client network.</p> <p>Router: The server can access the client network.</p>

2. Web Settings

Turn on **Enable** to enable the OpenVPN function, set **OpenVPN Type** to **Client** and **Client Config** to **Web Settings**, configure parameters such as **Device Mode** and **Device Mode**, and click **Save** to make the configuration take effect.

(1) Basic Settings

i OpenVPN Client [Download Link](#)

Enable

OpenVPN Type Server Client

Client Config Import Config Web Settings

Device Mode

Server Mode

* Username

* Password

Protocol

* Server Address

* Server Port ID 1-65535

advanced Setting

CA Certificate

Table 6-22 OpenVPN client configuration in Web Settings method

Parameter	Description
Device Mode	Specify the mode of the EG device that functions as a client. The options are TUN and TAP . The value must be the same as that configured on the server. When the EG device works as a server, it supports the TUN mode only.

Parameter	Description
Server Mode	<p>Select a client authentication mode. The options are Account, Certificate, and Account & Certificate.</p> <ul style="list-style-type: none"> ● Account: Enter the correct username and password and upload the CA certificate on the client. ● Certificate: Upload the correct CA certificate, client certificate, and private key file on the client. ● Account & Certificate: Enter the correct username and password, and upload the CA certificate, client certificate, and private key file on the client.
Username/Password	Enter the username and password configured on the server.
Protocol	Select the protocol running on the device. The options are UDP and TCP . The value must be the same as that configured on the server.
Server Address	Enter the address or domain name of the server to be connected.
Server Port ID	Enter the port number of the server to be connected.
CA Certificate	Click Browse , select the CA certificate file with the file name extension .ca , and upload the file.
Client Key	Click Browse , select the client private file with the file name extension .key , and upload the file.
Client Certificate	Click Browse , select the client certificate file with the file name extension .crt , and upload the file.
Client Certificate Key	Specify the client certificate key if the client certificate provided by the server (such as the MikroTik server) is encrypted twice.

(2) Advanced Settings

Click **advanced Setting** to configure the advanced parameters. Keep the default settings unless otherwise specified.

----- advanced Setting -----

Use Explicit Signature for Server Certificate [?](#)

TLS Authentication [?](#)

Cipher [?](#)

Auth [?](#)

Allow Data Compression [?](#)

Use Route Pushed by Server [?](#)

Table 6-23 OpenVPN client configuration in Web Settings method

Parameter	Description
Use Explicit Signature for Server Certificate	Specify whether to verify the server certificate using explicit signature. By default, this function is enabled. If the server certificate does not use explicit signature, for example, the MikroTik server, you need to disable this function. Otherwise, the connection fails.
TLS Authentication	Specify whether to enable TLS authentication for the server. If this function is enabled, you need to upload the TLS certificate file.
Cipher	Select a data compression algorithm. The value must be the same as that configured on the server. Otherwise, the connection fails.
Auth	Select an MD5 algorithm for data packet verification. The options are SHA1 , MD5 , SHA256 , and NULL . The value must be the same as that configured on the server. Otherwise, the connection fails.
Allow Data Compression	Specify whether to allow data compression. After this function is enabled, the transmitted data can be compressed by using the LZO algorithm. The value must be the same as that configured on the server.
Use Route Pushed by Server	Specify whether to use the routes pushed by the server. If this function is disabled, the device cannot accept the routes pushed by the server. If the server needs to access LAN devices, you must set this parameter to Yes .

6.4.4 Viewing the OpenVPN Tunnel Information

Choose **One-Device > Gateway > Config > VPN > OpenVPN > Tunnel List**.

After the server and client are configured, you can view the OpenVPN tunnel connection status. If the tunnel is established successfully, the client tunnel information is displayed in the tunnel list of the server.

<input type="checkbox"/>	Username	Server/Client	Status	Real IP Address	Virtual IP Address
<input type="checkbox"/>	openvpn	Server	OK	10.52.48.43	10.80.12.1

Total 1 < 1 > 10/page

Table 6-24 OpenVPN tunnel information

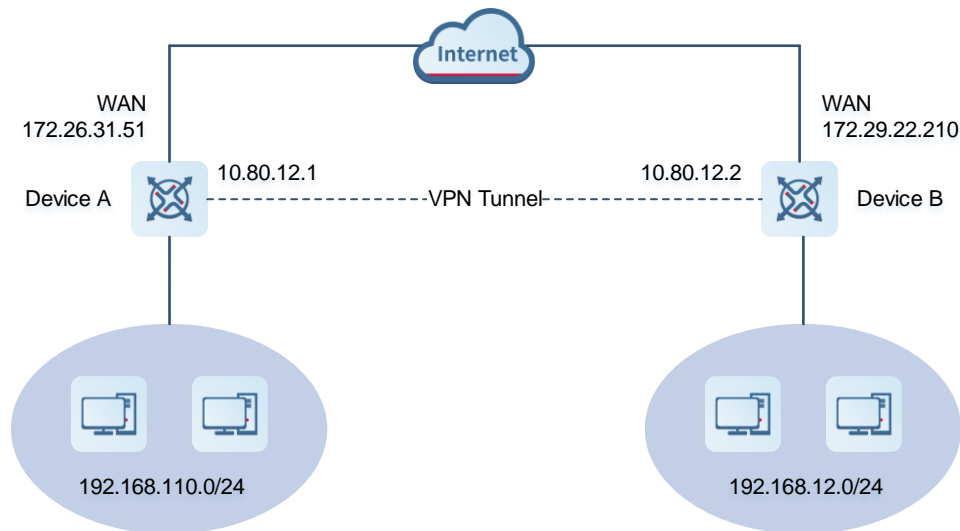
Parameter	Description
Username	Indicate the username used by the client for identity authentication. By default, the username displayed on the server is openvpn .
Server/Client	Indicate the role of the local end of the tunnel, which can be client or server.
Status	Indicate the tunnel establishment status.
Real IP Address	Indicate the real IP address used by the local end to connect to the VPN.
Virtual IP Address	Indicate the local virtual IP address of the tunnel. The virtual IP address of the OpenVPN client is allocated by the OpenVPN server.

6.4.5 Typical Configuration Example

1. Networking Requirements

The enterprise wants to allow the client network to dial up to the server through OpenVPN, implementing mutual access between the server and client.

2. Networking Diagram



3. Configuration Roadmap

- Configure Device A as the OpenVPN server.
- Configure Device B as the OpenVPN client.
- The server needs to push the local LAN network segment to the client to allow the client to access the server in the LAN.

4. Configuration Steps

(1) Configure Device A.

- a Log in to the web management system and choose **One-Device > Gateway > Config > VPN > OpenVPN > OpenVPN** to access the OpenVPN page.
- b Turn on Enable to enable the OpenVPN function, set OpenVPN Type to Server, select a server mode and protocol, enter the port number (1194 by default) and server address (external IP address of the local device), and click **Save**.

Enable

OpenVPN Type Server Client

Server Mode

Protocol

* Server Address

* Port ID 1-65535

* IP Range

* Deliver Route +

Flow Control Disable Enable

----- advanced Setting -----

Client Config

Table 6-25 OpenVPN server configuration

Parameter	Description
Server Mode	Select an authentication mode. In this example, select Account . In scenarios with high security requirements, select Account & Certificate .
Protocol	Select UDP unless otherwise specified. When the network status between two encrypted tunnel ends is poor, such as high latency or heavy packet loss, select TCP .
Server Address	Enter the WAN port address of the server, which is 172.26.31.51 .
Port ID	The default value is 1194 . Keep the default value unless otherwise specified. If the port is in use of disabled in the current network, change to an available port number.
IP Range	Specify the network segment of the OpenVPN address pool. The first available in the address pool is allocated to the server, and the other addresses are allocated to clients. For example, if this parameter is set to 10.80.12.0/24 , the VPN virtual address of the server is 10.80.12.1.

Parameter	Description
Deliver Route	Add routes to the corresponding network segment if the client wants to the LAN network segment where the server resides.

- c Click **Expand** to configure more advanced parameters. If the device connects to other EG devices in the Reeye network, you are advised to keep the default values for advanced settings. If the device connects to devices from another vendor, keep the parameter settings consistent on the connected devices.

TLS Authentication

Allow Data Compression

Route All Traffic over VPN

Cipher

Deliver DNS

Auth

- d Click **Export** to export the compressed package of the client parameter configuration. Download the compressed package to the local device and decompress it for setting the OpenVPN client in subsequent steps.



- e Choose **One-Device > Gateway > Config > VPN > VPN Account** and add an OpenVPN user account.

Add User ×

Service Type

* Username

* Password

Status

(2) Configure Device B.

- a Log in to the web management system and access the OpenVPN page.
- b Turn on Enable to enable the OpenVPN function and set OpenVPN Type to Client. Two methods are available for configuring the client. The Import Config method is recommended.

Import Config:

Enable

OpenVPN Type Server Client

Client Config Import Config Web Settings

Server Mode

* Username

* Password

Client Config It already exists.

Table 6-26 OpenVPN client configuration in Import Config method

Parameter	Description
Client Config	Select Import Config.
Server Mode	The value must be the same as that on the server. In this example, select Account .
Username & Password	Enter the username and password configured on the server.
Client Config	Click Browse , select the client configuration file exported from the server, and upload the file.

Web Settings:

Enable

OpenVPN Type Server Client

Client Config Import Config Web Settings

Device Mode

Server Mode

* Username

* Password

Protocol

* Server Address

* Server Port ID 1

----- advanced Setting -----

CA Certificate

Table 6-27 OpenVPN client configuration in Web Settings method

Parameter	Description
Client Config	Select Web Settings.
Device Mode	The value must be the same as that on the server. In this example, select TUN .
Server Mode	The value must be the same as that on the server. In this example, select Account .
Username & Password	Enter the username and password configured on the server.
Protocol	The value must be the same as that on the server. In this example, select UDP .

Parameter	Description
Server Address	Enter the public network IP address of the server, which is 172.26.31.51 .
Server Port ID	Enter the port number used by the server, such as 1194 .

Import the corresponding files according to the value of **Server Mode**.

If **Server Mode** is set to **Certificate** or **Account & Certificate**, you need to import the CA certificate file, client certificate file, and client private key file. If **Server Mode** is set to **Account**, you only need to import the CA certificate file. If the client certificate is encrypted, you also need to enter the pre-shared key specified by **Client Certificate Key**.

CA Certificate

Client Key

Client Certificate

Client Certificate Key

Click **advanced setting** to configure more parameters. Configure **Use Route Pushed by Server** to specify whether to accept routes pushed by the server. The value must be the same as that on the server. If the client is connected to a non-EG device, such as MikroTik server outside China, you need to turn off **Use Explicit Signature for Server Certificate**.

----- [advanced Setting](#) -----

Use Explicit Signature for

TLS Authentication

Cipher

Auth

Allow Data Compression

Use Route Pushed by

- c After the configuration is completed, click Save to make the configuration take effect.

5. Verifying Configuration

After the server and client are configured, view the two tunnel end information in the tunnel list.

Client:

Export Log File

Username	Server/Client	Status	Real IP Address	Virtual IP Address
OpenVpnUser1	Client	Connecting...	10.52.48.43	

Total 1 < 1 >

Server:

Export Log File

Username	Server/Client	Status	Real IP Address	Virtual IP Address
openvpn	Server	OK	10.52.48.43	10.80.12.1

Total 1 < 1 >

7 Appendix: Surveillance

Choose **Network-Wide > Workspace > Physical Topology**.

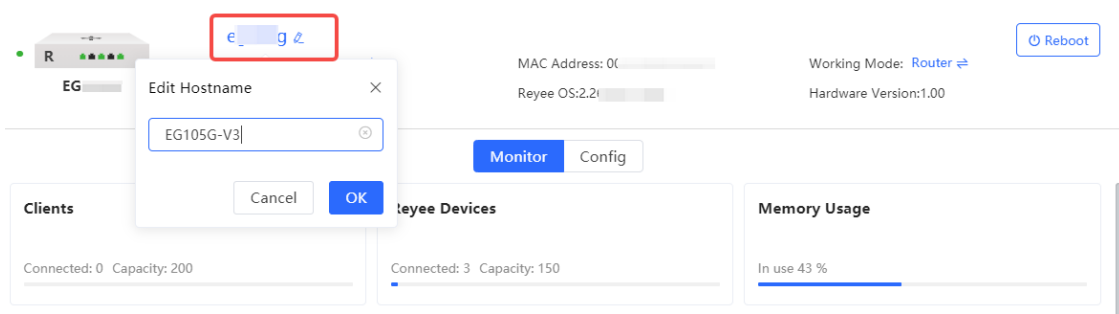
The **Workspace** page displays the current network topology, uplink and downlink real-time traffic, network connection status. On the current page, you can monitor, configure, and manage the network status of the entire network.

7.1 Device Info

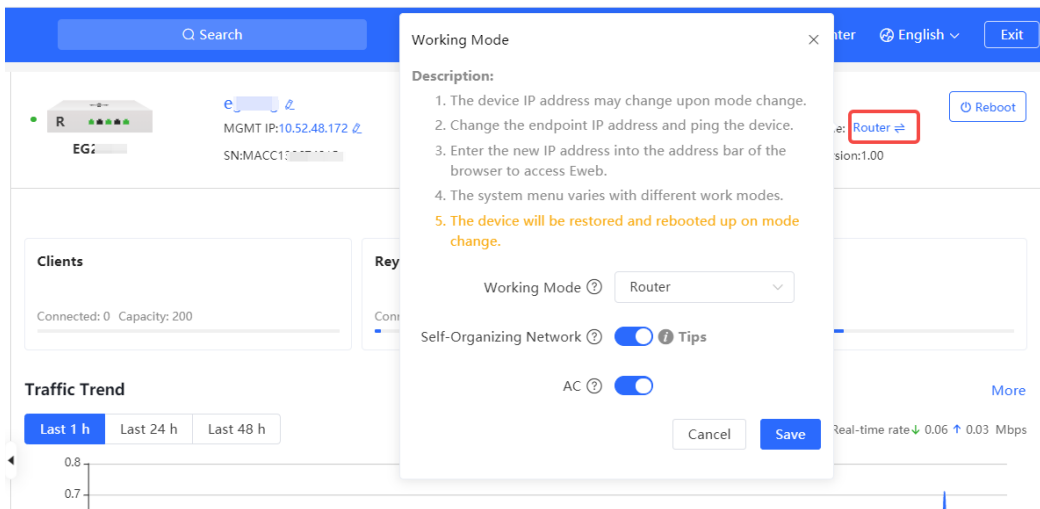
Choose **One-Device > Gateway > Monitor**. On the **Monitor** page, the model, host name, IP address, MAC address, software version, and SN of the router are displayed.

In the **Device Info** pane, the memory usage, online client count, status, uptime, and system time are displayed.

- The **Online** status indicates the SON status of the Reyee devices but not Ruijie Cloud.
- You can click **Device Name** to modify the device name.



- Click **Work Mode** to switch the device mode. Two modes are available: **Router** and **AC** modes. The default mode is **Router**.



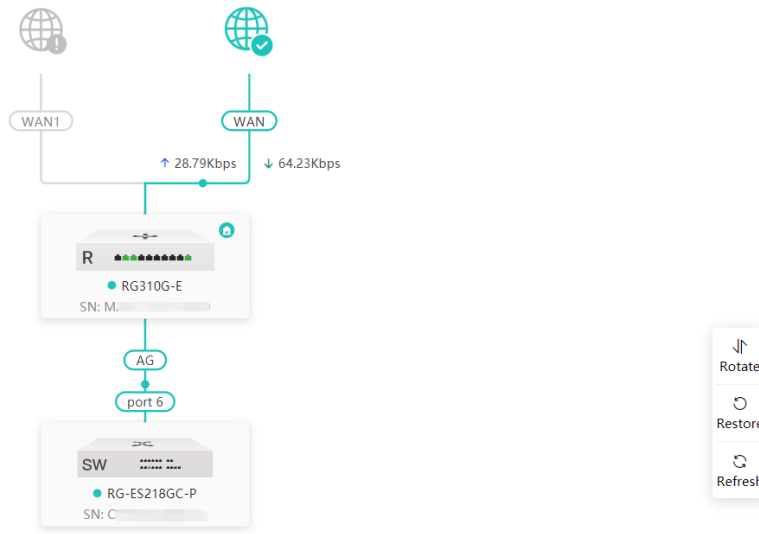
- **Router Mode:** indicates NAT forwarding.
- **AC Mode:** indicates bridge forwarding.
- SON:
 - -If SON is enabled, the device role is displayed.
 - -If SON is disabled, the device works in standalone mode.
 - - SON is enabled by default in AC mode.
- AC:
 - -It is enabled by default. The device works as a virtual AC to manage downlink devices.
 - -When it is disabled, the device must be elected as the AC before managing downlink devices.

7.2 Network Topology

The **Physical Topology** page displays the topology and connected status of the network.

Physical Topology

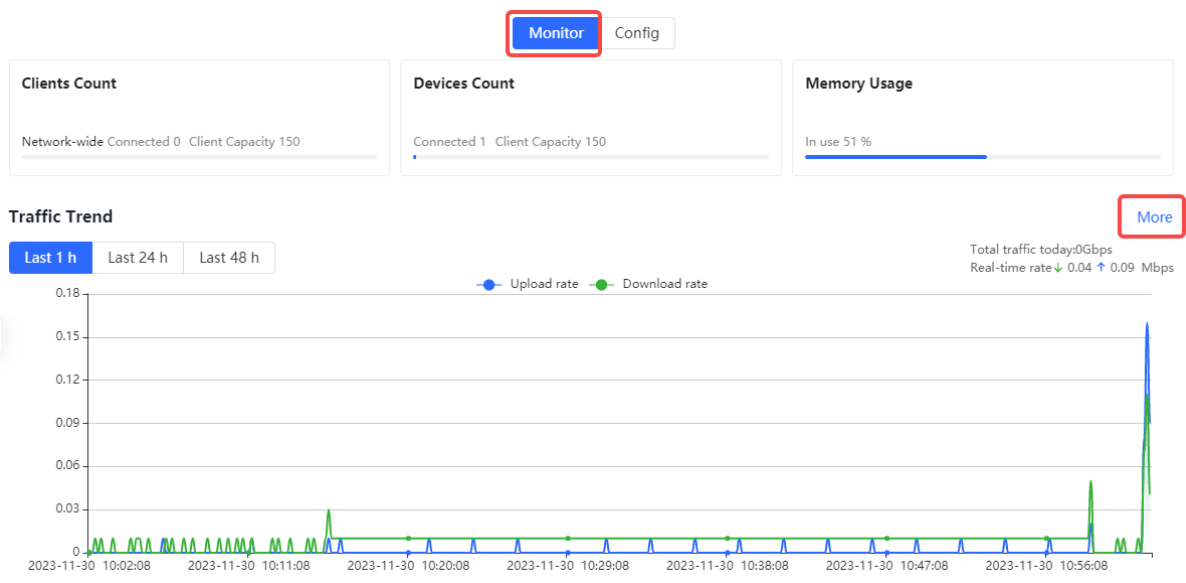
1 1 [+ Discover Devices](#)

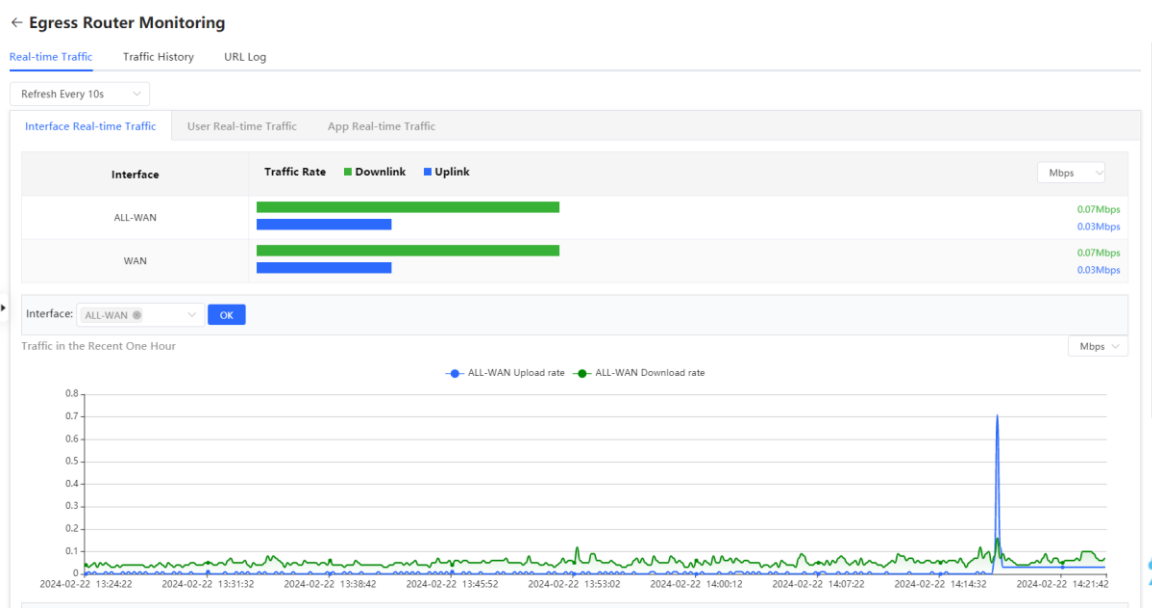


7.3 Real-Time Flow

Choose **One-Device > Gateway > Monitor**.

Click **More** to the right of **Traffic Trend** to access the gateway's monitoring details page. On the page that is displayed, click the **Real-time Traffic** tab.





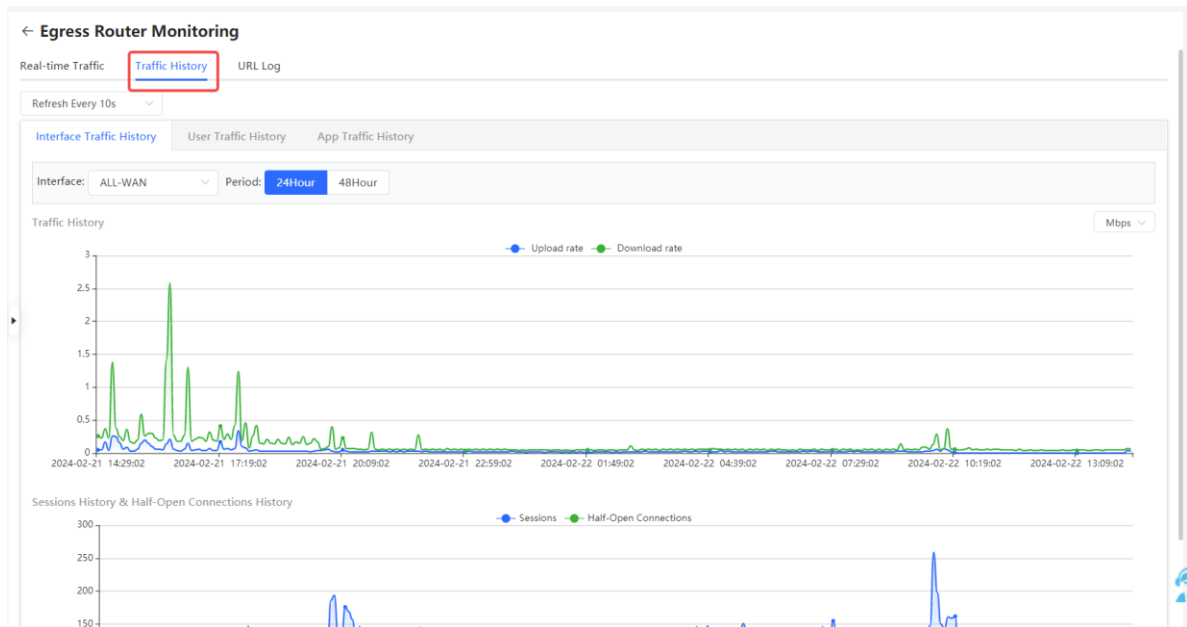
7.4 Traffic History

Note

This feature is supported by R202 and later versions.

Choose **One-Device > Gateway > Monitor**.

Click **More** to the right of the **Traffic Trend** tab. On the gateway monitoring details page, click the **Traffic History** tab.



7.5 URL Logs

URL logs record and display website domain names accessed by devices connected to LAN ports within a certain minute, access count, and audit results.

Choose **One-Device > Gateway > Monitor**.

Click **More** to the right of the **Traffic Trend** tab. On the page that is displayed, click the **URL Log** tab.

(1) Toggle on the **Enable** switch. On the pop-up dialog box, click **OK**.

Enable

Tips



Are you sure you want to enable the URL Log?

Cancel

OK

(2) (Optional) Configure **record IP**.

The system records access records of all devices connected to LAN ports by default. If you need to view access records of a single device, set **record IP**.

Enter the device IP address in **record IP** and click **Save**.

Enable Record IP Only ⓘ 192.168.110.11 Save

Time	IP	Access Count	URL	Action
2023-11-30 15:17	192.168.110.11	2	http://conf.wsm.360.cn	Allow
2023-11-30 15:17	192.168.110.11	2	http://qup.f.360.cn	Allow

Note

If you need to restore access records of all devices connected to LAN ports, clear information in **Record IP Only** and click **Save**.

(3) Check access records.

The system displays detailed access records, including the time, IP address.

You can search for access records by IP address or URL.

Enable Record IP Only ⓘ Example: 1.1.1.1 Save

Time	IP	Access Count	URL	Action
2023-11-30 15:20	192.168.110.11	2	http://conf.wsm.360.cn	Allow
2023-11-30 15:20	192.168.110.11	2	http://qup.f.360.cn	Allow
2023-11-30 15:20	192.168.110.11	1	https://msgmq.rj.link	Allow