

Ruijie Reyee RG-EG Series Router

Implementation Cookbook



Document Version: V1.2 Date: 2022-12-07 Copyright © 2022 Ruijie Networks

Copyright

Copyright © 2022 Ruijie Networks

All rights are reserved in this document and this statement.

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



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 Reyee: https://www.ruijienetworks.com/products/reyee
- Technical Support Website: <u>https://www.ruijienetworks.com/support</u>
- Case Portal: https://caseportal.ruijienetworks.com
- Community: <u>https://community.ruijienetworks.com</u>
- Technical Support Email: service_rj@ruijienetworks.com

Conventions

1. GUI Symbols

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

2. Signs

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

U 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

PrefaceI
1 Product Introduction9
1.1 Models9
1.2 LED Indicators
1.3 Button13
2 Getting Started14
2.1 Network Planning14
2.2 Installing the Router15
2.2.1 Safety Suggestions15
2.2.2 Installation Site Requirement16
2.2.3 Installation Steps18
2.3 Quick Provisioning
2.3.1 Quick Provisioning Through Ruijie Cloud App18
2.3.2 Quick Provisioning Through Reyee Eweb25
3 Device Management
3.1 Login
3.2 Configuring the Login Password29
3.3 Configuring the System Time
3.4 Configuring Upgrade
3.4.1 Online Upgrade32
3.4.2 Local Upgrade
3.5 Backing Up or Restoring the Configuration
3.6 Configuring Restart

3.6.1 Restarting the Current Device	
3.6.2 Restarting All Devices on the Network	
3.6.3 Restarting Specified Devices	
3.6.4 Configuring Scheduled Restart	
3.7 Restoring Factory Settings	
4 Common Settings	
4.1 Network Access Setting	
4.1.1 PPPoE Configuration Through a WAN Port	
4.1.2 Static IP Address Configuration Through a WAN Port	41
4.1.3 DHCP Configuration Through a WAN Port	42
4.2 AP Management	43
4.2.1 Switching the Working Mode	43
4.2.2 Configuring AP Groups	45
4.2.3 Configuring Wi-Fi	47
4.2.4 Configuring Guest Wi-Fi	50
4.2.5 Adding More Wi-Fi Networks	51
4.2.6 Healthy Mode	52
4.2.7 RF Settings	52
4.2.8 Configuring a Wi-Fi Blacklist or Whitelist	54
4.2.9 Configuring AP Load Balancing	56
4.2.10 Wireless Network Optimization in One-Click Mode	59
4.2.11 Enabling Reyee Mesh	61
4.2.12 Configuring a LAN Port of a Downlink AP	62
4.3 Switch Settings	64

4.4 Diagnostics	
4.4.1 Network Check	65
4.4.2 Alarms	66
4.4.3 Network Tools	67
4.4.4 Packet Obtaining	69
4.4.5 Fault Collection	71
4.5 WAN Load Balancing	71
4.6 Port VLAN	74
4.7 VPN	76
4.7.1 PPTP VPN	76
4.7.2 L2TP VPN	
4.7.3 IPsec VPN	
4.7.4 L2TP Over IPsec VPN	
4.7.5 Open VPN	119
4.8 Port Mapping	
4.8.1 Configuring Port Mapping	
4.8.2 Configuring NAT-DMZ	
4.9 Dynamic DNS	
4.10 Authentication	
4.10.1 Application Scenario	
4.10.2 Cloud Authentication	
4.10.3 Local Account Authentication	
4.10.4 Authorized Authentication	
4.10.5 QR Code Authentication	

4.10.6 Whitelist	
4.10.7 Online Clients	145
4.10.8 WeChat Authentication	146
4.10.9 Enterprise WeChat Authentication	
4.11 Behavior	
4.11.1 Application Scenario	
4.11.2 App Control	
4.11.3 Website Management	
4.11.4 Access Control	
4.12 Flow Control	
4.12.1 Application Scenario	
4.12.2 Smart Flow Control	
4.12.3 Custom Policies	
4.12.4 Application Priority	176
4.13 Security	
4.13.1 Application Scenario	
4.13.2 Configuring the ARP List and ARP Guard	
4.13.3 Configuring MAC Address Filtering	
4.13.4 Configuring Device Security	
4.14 Configuring the PPPoE Server	
4.14.1 Application Scenario	
4.14.2 Global Settings	
4.14.3 Configuring a PPPoE User Account	
4.14.4 Configuring a Flow Control Package	

4.14.5 Configuring Exceptional IP Addresses	190
4.14.6 Checking Online Users	191
4.15 IPTV	
4.15.1 Application Scenario	
4.15.2 Dual-WAN Configuration	
4.15.3 Single-WAN Configuration	
4.16 UPnP	
5 Advanced Solution	
5.1 Reyee Flow Control Solution	
5.1.1 Application Scenario	
5.1.2 Configuration Example	
5.1.3 Configuration Verification	
5.2 Reyee Cloud Authentication Solution	
5.2.1 Working Principle	
5.2.2 Application Scenario	
5.2.3 Configuration Example	
5.2.4 Configuration Verification	216
5.3 Reyee Guest Wi-Fi Solution	217
5.3.1 Working Principle	217
5.3.2 Application Scenario	217
5.3.3 Configuration Example	217
5.4 Reyee Economic Hotel Network Solution	
5.4.1 Application Scenario	
5.4.2 Configuration Example	

5.4.3 Configuration Verification	241
6 FAQ	
6.1 Reyee Password FAQ (Collection)	
6.2 Ruijie Cloud Reyee EG authentication FAQ (Collection)	
6.3 Reyee Mesh FAQ (Collection)	
6.4 Reyee IPTV FAQ (Collection)	
6.5 Reyee Authentication FAQ (Collection)	
6.6 Reyee Behavior Strategy FAQ (Collection)	
6.7 Reyee DDNS FAQ (Collection)	
6.8 Reyee VPN FAQ ((collection))	
6.9 Reyee Flow Control FAQ (Collection)	
6.10 Reyee Guest Wi-Fi FAQ (Collection)	
6.11 Reyee Wireless Configuration FAQ (Collection)	
6.12 Reyee Self-Organizing Network (SON) FAQ (Collection)	
6.13 Reyee series Devices Parameters Tables	
6.14 Reyee Parameter Consultation FAQ (Collection)	
7 Appendix: Surveillance	
7.1 Device Info	
7.2 Wi-Fi Information	
7.3 Network Status	
7.4 Real-Time Flow	
7.5 Flow History	
7.6 URL Logs	
7.7 Online Clients	

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 Mbit/s 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	5 (PoE supported)	100	500 Mbit/s asymmetric bandwidth (flow control disabled) 300 Mbit/s asymmetric bandwidth (flow control enabled)	AC mode: 300 Router mode: 32
RG- EG105G-P V2	5 (PoE supported)	100	500 Mbit/s asymmetric bandwidth (flow control disabled) 600 Mbit/s asymmetric bandwidth (flow control enabled)	AC mode: 300 Router mode: 32

Model	10/100/1000 Base-T Ethernet Port	Maximum Number of Concurrent Clients	Recommended Bandwidth	Management Capacity
RG- EG105G	5	100	500 Mbit/s asymmetric bandwidth (flow control disabled) 300 Mbit/s asymmetric bandwidth (flow control enabled)	AC mode: 300 Router mode: 32
RG- EG105G V2	5	100	600 Mbit/s asymmetric bandwidth (flow control disabled) 500 Mbit/s asymmetric bandwidth (flow control enabled)	AC mode: 300 Router mode: 32
RG- EG105GW	5	100 (recommend ed number of wireless terminals: 60)	500 Mbit/s asymmetric bandwidth (flow control disabled) 300 Mbit/s asymmetric bandwidth (flow control enabled)	Router mode: 32
RG- EG210G-E	10	200	 Gbit/s asymmetric bandwidth (flow control disabled) Gbit/s asymmetric bandwidth (flow control enabled) 	AC mode: 500 Router mode: 150

Model	10/100/1000 Base-T Ethernet Port	Maximum Number of Concurrent Clients	Recommended Bandwidth	Management Capacity
RG- EG210G-P	10 (PoE supported)	200	600 Mbit/s asymmetric bandwidth (flow control disabled) 500 Mbit/s asymmetric bandwidth (flow control enabled)	AC mode: 500 Router mode: 150
RG- 105GW(T)	5	100	600 Mbit/s (1500 bytes, NAT + flow audit) 400 Mbit/s (1500 bytes, NAT + authentication, application identification, flow audit, and flow control)	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

1.2 LED Indicators

LED Indicator	Status	Description	
		Fast flashing (at 8 Hz): The router is starting up.	
		Slow flashing (at 0.5 Hz): The network is unreachable.	
	Flashing	One long flash followed by three short flashes (at 0.8 Hz): The router is faulty.	
SYS		Flashing twice consecutively (at 0.8 Hz):	
		 The router is restoring factory settings. The router is upgrading the software. Note: Do not power off the router in this case. 	
	Solid on	The router is functioning properly.	
	Off	The router is not powered on.	
	Flashing	The port is connected and is sending/receiving traffic.	
Port	Solid on	The port is connected and is not sending/receiving traffic.	
	Off	No link is detected for this port.	
	Off	Mesh pairing is not implemented.Wireless relay is not set up.	
	Flashing alternately	Mesh pairing is in progress.	
Mesh	Three bars on	 The mesh signal strength is high. The wireless relay signal strength is high. 	
	Two bars on	 The mesh signal strength is medium. The wireless relay signal strength is medium. 	
	One bar on	 The mesh signal strength is low. The wireless relay signal strength is low. 	

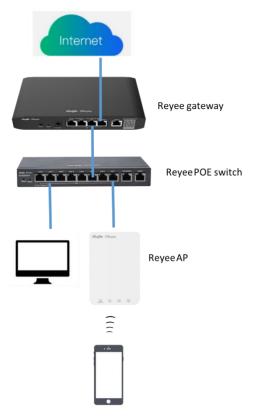
1.3 Button

Button	Description
	Press the Reset button for less than 2 seconds to restart the device.
Reset	Press the Reset button for over 5 seconds to restore the router to factory
	settings. (Release the button when the system status LED blinks).
	The default management IP address is http://192.168.110.1.
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.ruijienetworks.com	35.197.150.240	devicereg.ruijienetworks.com	35.190.10.141	80,443	
ryrc.ruijienetworks.com	35.197.150.240	ryrc.ruijienetworks.com	35.234.108.108	80,443	
stunrc.ruijienetworks.com	35.197.150.240	stunrc.ruijienetworks.com	35.234.108.108		34,783,479
stunsvr-as.ruijienetworks.com	34.126.80.150	stunsvr-eu.ruijienetworks.com	35.246.237.78		34,783,479
stunb-as.ruijienetworks.com	34.126.80.150	cwmpsvr-eu.ruijienetworks.com	34.159.112.239		34,783,479
stunc-as.ruijienetworks.com	34.87.169.209	cwmpcp-eu.ruijienetworks.com	34.120.73.71		34,783,479
cwmpsvr-as.ruijienetworks.com	35.197.136.171	cwmpb-eu.ruijienetworks.com	34.159.112.239	80, 443	
cwmpcp-as.ruijienetworks.com	34.160.143.162				
cwmpb-as.ruijienetworks.com	35.197.136.171				
Log Upload:		Log Upload:			
34.87.93.12	34.87.93.12	cloudlog-eu.ruijienetworks.com	35.246.247.49	80,443	
Advanced Service:		Advanced Service:			
firmware.ruijienetworks.com 34.87.32.36		firmware.ruijienetworks.com	34.89.153.55	80,443	
cloudweb.ruijienetworks.com	34.87.32.36	cloudweb.ruijienetworks.com	34.89.153.55	80,443	
fastonline.ruijienetworks.com	34.87.32.36	fastonline.ruijienetworks.com	34.89.153.55	80,443	
cloudapi.ruijienetworks.com	35.197.150.240	cloudapi.ruijienetworks.com	35.234.108.108	80,443	
cdn.ruijienetworks.com	35.201.94.110	cdn.ruijienetworks.com	35.190.93.193	80,443	
ES Series Switch		ES Series Switch			
iotrc.ruijienetworks.com	34.87.101.31	iotrc.ruijienetworks.com	34.107.106.56		7683
iotsvr-as.ruijienetworks.com	35.247.161.22	iotsvr-eu.ruijienetworks.com	35.242.228.40		5683
iotlog-as.ruijienetworks.com	35.240.167.168	iotlog-eu.ruijienetworks.com	35.198.144.180		6683
iotdl-as.ruijienetworks.com	34.87.141.45	iotdl-eu.ruijienetworks.com	35.234.118.145		8683
MQTT Devices with P206 version		MQTT Devices with P206 version			
ryrcmq.ruijienetworks.com	34.120.84.165	ryrcmq.ruijienetworks.com	34.149.186.87	25857	
ehrrcmq.ruijienetworks.com	34.120.84.165	ehrrcmq.ruijienetworks.com	34.149.186.87	25857	
mgclt001-as.rj.link	34.160.191.165	mgclt001-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

- o 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

- o Do not frequently move devices.
- When moving devices, keep the balance and avoid hurting legs and feet or straining the back.
- o 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.
- o 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.
- o 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.

o 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.

o 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.
- o Take measures to shield static electricity.
- o 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 Reyee router is often used with a Reyee PoE switch and a Reyee RAP.



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

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

17:54 🖪 🗂 🗖	··· 3.5KB/s ₽	🗿 🕅 🛗 🖬 🐨
Ruijie Cloud	Q Search	E E
Speed Test	Tech Support	Demo
My (9) Shared	(85)	+ Create a Project
Project Type -	Alarm -	Creation Time -
On-site	Time: 2022-01-28 09:3	
Creation On-site	etwork Time: 2022–01–21 11:38 Cloud e. Only Cloud managem	
	ned Wireless Bri Time: 2022-01-07 18:16 I Cloud	
×	Create Project	0
н	lave Reyee AP	s?
No. Scan QR-cor		Yes. nnnect to Wi-Fi
		_

b After you click Yes, Ruijie Cloud App will ask you to connect SSID @Ruijie-mxxxx.

17:54 🖪 🖸 📮 ··· 3.1KB/s 🛠 🏵 🖬 🕍 🖬 🖽
< Create Project
Connect to Wi-Fi
1.Please connect to the Wi-Fi starting with "@Ruijie-m".
WLAN
@Ruijie-mxxxx 🗢
2.Wait until 充 appears, and return to Ruijie Cloud to continue.
12:53 ⋪ all २ ■
Tips: " If there is only one AP in the network, please connect to the Wi-Fi starting with "@Ruijie-s".
Connect

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.

c Click Connect and access SSID @Ruijie-mxxxx.

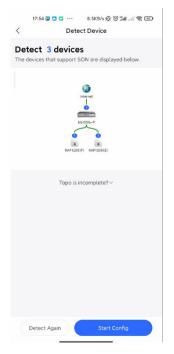
17:54 🗳 💁 🚥 · · · 19.0KB/s 🌾 🎯	
\leftarrow	8
WLAN	
WLAN	
WLAN assistant	>
	۲
Available networks	0
	â 🗲
qwert (2.4G/5G)	>
	>
@Ruijie-s1F0A (2.46/56)	>
< IT department 240/50	\rightarrow
PPSKtesttime 24G/5G	>
중 test1 2.46/56	>

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



	17:54 🖪 🖸 📮 ··· 4.7KB/s 🌾 🎯 🖫 🖽 🚓 🚳
<	Detect Device
	\sim
	30s
	Detecting
	Please wait.

e After all devices are detected, Cloud App will display them and show the topology.

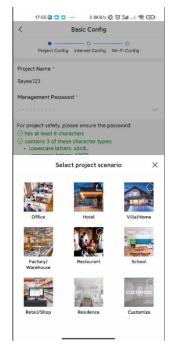


- (2) Click Start Config to perform basic configuration of this project.
 - a Set Project Name and Management Password.

Cookbook

	17:55 🚨 🖸 🖸 ··· 2.8KB/s 🚀 🗑 📶 🕁 📚 🐼
<	Basic Config
	Project Config Internet Config Wi-Fi Config
Proje Reyer	rct Name * e123
Mana	gement Password *
	🕲 🛩
⊘ ha ⊘ co • 1 • 1 • 1	roject safety, please ensure the password: s at least 8 characters Intains 3 of these character types: lowercase letters: abcd uppercase letters: ABCD puppercase letters: <a>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
Scen	ario *
	Next

b Select the scenario of this project based on your requirement.

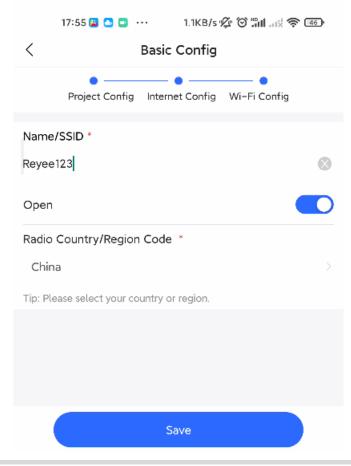


(3) Configure the Internet.

For WAN configuration, you can choose **PPPoE**, **DHCP**, or **Static IP**.

Project Config Internet Config Wi-Fi Config Single ISP Link: WAN0 Internet Connection of Link 1 (connect to WAN0) PPPOE DHCP Static IP Network parameters are automatically assigned. You don't need to configure. 802.10 Tag Dual ISP Links: WAN0 and WAN1			Basic Config	
Single ISP Link: WAN0 Internet Connection of Link 1 (connect to WAN0) PPPOE OHCP Static IP Network parameters are automatically assigned. You don't need to configure. 302.10 Tag				
Single ISP Link: WAN0 Internet Connection of Link 1 (connect to WAN0) PPPoE DHCP Static IP Network parameters are automatically assigned. You don't need to configure. 802.10 Tag		Project Config	Internet Confin	Ni=Ei Confin
Internet Connection of Link 1 (connect to WAND) PPPoE DHCP Static IP Network parameters are automatically assigned. You don't need to configure. 8002.10 Tag		roject comig	interior coring	in theoring
PPPoE DHCP Static IP Network parameters are automatically assigned. You don't need to configure. 802.10 Tag	💿 Sii	ngle ISP Lini	k: WAN0	
Network parameters are automatically assigned. You don't need to configure.	Interne	t Connectio	n of Link 1 (conne	t to WANO)
assigned. You don't need to configure.	Р	PPoE	DHCP	Static IP
	assigr	ned. You do	on't need to con	figure.
Dual ISP Links: WAN0 and WAN1	302.1Q	Tag		
	0 р.	ual ISP Links	WAN0 and WAN1	
	O DI	ual ISP Links	WAN0 and WAN1	
	0 DI	ual ISP Links	WANO and WANT	
	0 D.	ual ISP Links	WANO and WANT	
	O DI	ual ISP Links	WANO and WAN1	
	() D.	ual ISP Links	WANO and WAN1	
	O Du	ual ISP Links	WAN0 and WAN1	
		ual ISP Links	: WANO and WANT	
		ual ISP Links	: WANO and WANT	
		ual ISP Links	WANO and WANT	
		ual ISP Links	WAND and WANT	
	OD	ual ISP Links	WANO and WANT	

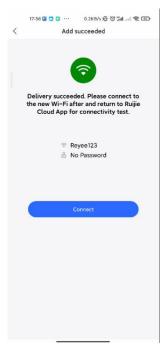
- (4) Configure the SSID.
 - a Enter the name of the SSID.
 - b Configure it as open to allow clients to access this SSID.
 - c Configure the password for this SSID.
 - d Select the region code.



e The configuration will be synchronized to the network.



f After about 3s, Ruijie Cloud App will prompt that the configuration is delivery succeed.

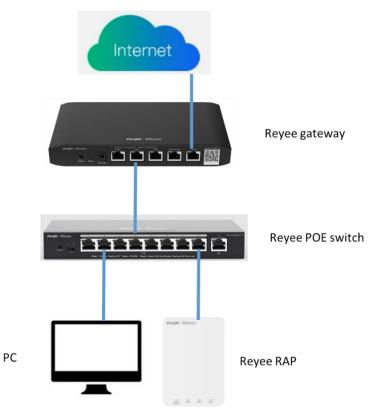


g Connect to the SSID created just now to manage the whole network on Cloud App.

17:56 🗳 🖸 🖸 🚥	0.0K8/s 🕼 🗑 🖫 🖽
\leftarrow	5
WLAN	
WLAN	
WLAN assistant	>
Reyee123 (2.40/50 Connected Connected Connected	
@Ruijie-m393E Saved	2.46/56
Available network:	s O
	ń. (>)
	\rightarrow
	2.4G/5G
PPSKtesttime 2	2.46/56
	ê 5

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.

						English
Total Devices: 3. Please make sure that the device count and top	ology are correct. The unmanaged swit	ch will not appear in the lis	t.			0
Net Status (Online Devices / Total)	DHCP	Router 1 Router	Switch 1/1 Switches	- 京 1/1 APs		Refresh ©
My Network						
New Device (3 devices) Model	SN	IP	MAC		Software Ver	~
Router EG105G-P-V2 [Master]		192.168.110.1			914	
AP RAP1200(E)		192.168.110.203	3		14	
Switch RG-ES209GC-P	0	192.168.110.44		ſ	3se(07200415)	
	D	ediscover	Start Setup			

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

* Network Name ReyeeNetwork Network Settings Network Settings Internet PP05 DHCP Static IP Connert IP Checking P assignment "IP T2266.162 * Subnet Mask 255.255.25.2 * Gateway 172.264.1 * DNS Server 192.168.58.94 192.168.58.110 * SSID @Ruijie-m0643 Wi-Fl Password Security Open		
Internet PPP0E DHCP Static IP Current IP © Checking IP assignment *IIP 172.266.162 * * Subnet Mask 255.255.252.0 * * * Gateway 172.264.1 * * * DNS Server 192.168.58.94 192.168.58.110 * * SSID @Ruijie-m0843 * *	* Network Nam	* ReyeeNetwork
© Checking IP assignment * IP 172.26.6.162 * Subnet Mask 255.255.20 * Gateway 172.26.4.1 * DNS Server 192.168.58.94 192.168.58.110 * SSID @Ruijie-m0043	Network Setting	<u>js</u>
* IP 17226.6.162 * Subnet Mask 255.255.252.0 * Gateway 17226.4.1 * DNS Server 192.168.58.94 192.168.58.110 * SSID @Ruijie-m0643	Interne	
* Galteway 172264.1 * DNS Server 192.168.58.94 192.168.58.110 * SSID @Ruijie-m0643	*1	
* DNS Server 192.168.58.94 192.168.58.110 * SSID @Ruijie-m0843	* Subnet Masi	255.255.252.0
* SSID @Ruijie-m0643	* Gateway	/ 172.26.4.1
	* DNS Serve	192.168.58.94 192.168.58.110
WI-Fi Password 🔘 Security 🔹 Open	* \$\$10	@Ruijie-m0843
	Wi-Fi Password	I Security Open
Country/Region/Time Zone	Country/Region	n/Time Zone

- 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.

Internet O PPPOE DitCP Static IP Converti Settions PRESENTE SETION PRE	

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

Ruffe &RCyCC Greate Network	English ~ (3) Exit
- N.	Operation succeeded. Froject Name: ReyeeNetwork
	• SSID: @Ruijie-m0843
Subort Ma	Redirecting
* Gatewa	172.26.4.1
* DNS Serv	or 192.168.58.94 192.168.58.110
* 55	D @Ruijie-m0843
Wi-Fi Passwo	të 🔿 Security 🔹 Open
Country/Regio	n/Time Zone V
	Yrevious Create Nichwork & Connect

Ruijie Rcycc	ReyeeNetwork > Ruijie Manter 0	English 🗸 🛆 Ruijie Cloud	d	twork Check - <u>満</u> Warn - 日 Log Out
& Overview	Device Info	Wi-Fi		Setup>
Online Clients	Hostname: Ruijie			Sector
(#) Router	SN: 119 IP: 172.26.6.162	Primary Wi-Fi: ReyeeNetwork Security: No	Guest Wi-Fi: Security: No	
	EG105G-P-V2 MAC: 508:43 Software Ver: 55.1914			
Switches				
-e-Network	Net Status (Online Devices / Total)	↓ 3.09Kbps	- (r) 1	Refresh &
	DHCP 1 Internet Router	1/1 Switches	1/1 1 APs Online Clients	
	Real-Time Flow (Kbps)	Uplink Flow Downlink Flow		Kbps 🗸 🤍 WAN 🗸
	8	oparity i town of the operation of the		
	6-			
	4			
	3-			
	2			
«Collapse			· · · · · · · ·	

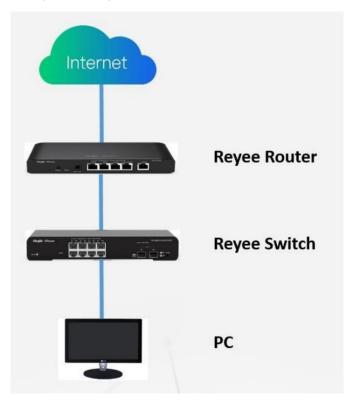
3 Device Management

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.
- Enter the password on the login page and click Login.
 The default password is admin.

RUJJE Hi, EG205G	
命 Password	
Login Forgot Password? English V	

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 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 System > Login > Login Password.
- (3) Enter the old password and new password.
- (4) Click Save.

Ruíjie Rcy	C gw_eg310g-e > Ruij	jie 🖸		English ~ 🛆 Ruijie Cloud	鬷Download App	🖨 Wizard	@Network Check	<u>満</u> Alert	⊡Log Out
🖧 Overview	Login Password	Session Timeout							
Online Clients	Change the la	login password. Please log in again with the new password l	ater						0
Network	~		MICH.						0
⊘ Security	 Old Passwo 	ord							
ന് Behavior	 New Passwo 	ord							
😨 VPN	 Confirm Passwo 	brd							
🗄 Advanced		Save							
② Diagnostics									
😨 System									
System Time									
Login									
Management									
Upgrade									

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.

3.3 Configuring the System Time

Choose System > System Time.

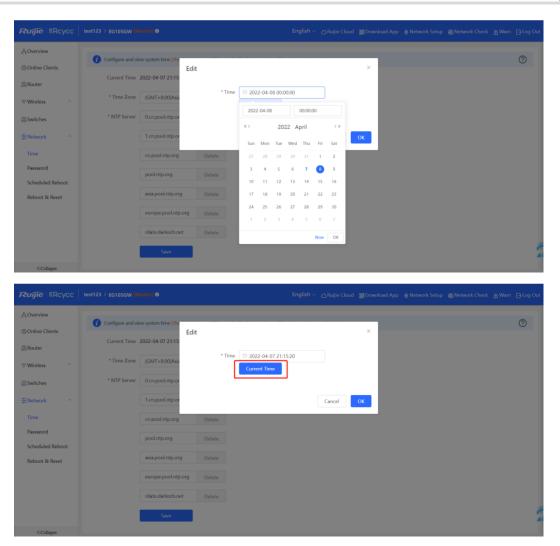
You can view the current system time. If the time is incorrect, check and select the local time zone. If the time zone is correct but the time is still incorrect, click **Edit** to manually set the time. In addition, the device supports Network Time Protocol (NTP) servers. By default, multiple servers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

<i>i</i> Configure and vie	ew system time (The device	has no RTC mo	odule. The time settings will not be saved upon reboot).	?
Current Time	2022-04-27 12:38:30	Edit		
* Time Zone	(GMT+8:00)Asia/Shang	jhai 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		
	europe.pool.ntp.org	Delete		
	rdate.darkorb.net	Delete		
	Save			

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

Edit			×
* Time	() Select a time.	Current Time	
		Cancel	Ж

• 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.

Ruíjie Rcycc	test123 > EG105GW [Minstor] 0	English 🗸 🛆 Ruijie Cloud	l 📓 Download App	🚖 Network Setup	Network Check	<u>満</u> Warn Log Out
중Overview	Configure and view system time (The device has no RTC module. The time setting)	ngs will not be saved upon reboot).				0
Online Clients	Current Time 2022-04-07 21:16:18	ge open recently				O
🖽 Router						
⇔Wireless ~	* Time Zone (GMT+8:00)Asia/Shanghai					
	* NTP Server (GMT+8:00)Asia/Hong_Kong (GMT+8:00)Asia/Irkutsk					
恋Network 个	(GMT+8:00)Asia/Kuala_Lumpur					
Time	(GMT+8:00)Asia/Kuching (GMT+8:00)Asia/Macau					
Password	(GMT+8:00)Asia/Makasar					
Scheduled Reboot	(GMT+8:00)Asia/Manila					
Reboot & Reset	(GMT+8:00)Asia/Shanghai					
	europe.pool.ntp.org Delete					
	rdate.darkorb.net Delete					
	Save					e
«Collapse						1

• Add or delete the NTP server.

ເວັບເງົາຍ ເສັດແລະ ເຊິ່ງ ເຊິ	test123 > EG105GW Mannes 🔍 English ~Ruijie Cloud 📓 Download App 🔶 Network Setup @ Network Check 🚊 Warn E	- Log Out
© Overview	Configure and view system time (The device has no RTC module. The time settings will not be saved upon reboot).	0
Online Clients Answer	Current Time 2022-04-07 21:15:39 Edit	
⇔Wireless ~	* Time Zone (GMT+8:00)Asia/Shanghai \checkmark	
Switches	* NTP Server 0.cn.pool.ntp.org Add	
*Network ^	1.cn.pool.ntp.org Delete	
Time Password	cn.pool.ntp.org Delete	
Scheduled Reboot	pooLntp.org Delete	
Reboot & Reset	asia.pool.ntp.org Delete	
	europe.pool.ntp.org Delete rdate.darkorb.net Delete	
	Turite Collin Actional Leventer	-
«Collapse		

3.4 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.

3.4.1 Online Upgrade

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

Log in to the Eweb of the device.

(1) Choose Gateway > System > Upgrade > Online Upgrade.

Ruíjie &Rcycc	Network	Navigatio	n Q English ~ c	🛆 Ruijie Cloud 🛛 📓 Download Ap	p 🐣 Network Setup 🝭 Net	work Check _ 滋 Alert 日 Log Out
Q Navigation	Hostname: III SN: MACC202205091 IP: 1	92.168.210.103 MA	C 00:D0:C8:75:A8:45			
 Overview 	EG310GH-P-E Software Ver: ReyeeOS 1.202.2023					(U) Reboot
$_{\delta}^{\theta_{0}}$ Network	Overview Network \vee Security \vee Behavior \vee VPN \vee Advanced \vee Diagnostics \vee	System				
Devices	Online Upgrade Local Upgrade	Login				
Gateway		Management				
	Online upgrade will keep the current configuration.	Upgrade				
Clients Management	Current Version ReyeeOS 1.202.2023 (It is the latest version.)	Reboot				
≆ System ~						

- 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 up	grade will keep the current configuration. Please do not refresh the page or close th
Current Version	ReyeeOS 1.86.
New Version	ReyeeOS 1.
Description	1, 2,
Tip	 If your device cannot access the Internet, please click Download File. Choose Local Upgrade to upload the file for local upgrade.
	Upgrade Now

3.4.2 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 Gateway > System > Upgrade > Local Upgrade.

Overview Ne	etwork × Security × Behavior × VPN × Advanced × Diagnostics × System ×
Online Upgrade	Local Upgrade
i Please do	not refresh the page or close the browser.
Model	EG105G-P-V2
Current Version	ReyeeOS 1.86.1929
Keep Config	If the target version is much later than the current version, it is recommended not to keep the configuration.)
File Path	Please select a file. Browse Upload

- (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** > **Overview** and check whether the current version is consistent with the target version in the **Device Details** pane.
- If versions are consistent, the upgrade is successful.
- If versions are inconsistent, the upgrade fails. Try again or contact RITA.

Overview Network ~ Security ~ Behavio	or ~ VPN ~ Advanced	✓ Diagnostics ✓ Syste	m ~	
Overview				
Memory Usage 65 %	Online Clients	3	Status: Online Uptime: 3 days 5 hours 42 minutes 49 seco Systime: 2022-09-13 16:32:55	nds
Device Details				
Model: EG105G-P-V2 MAC: 00:D0:F8:15:08:43 Hardware Ver: 1.00	Work Mode:	EG105G-P-V2 & Router & ReyeeOS 1.86.1929	SN: M. Role: Master AC	

3.5 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 Gateway > System > Management.

Ruíjie Rcycc	Network	Navigation Q	English ~	CRuijie Cloud	💐 Download App	Network Setup	Network Check	盐Alert 日Log Out
Q Navigation	Roster Hostname: 工位 SN: MACC202205091 IP: 192.168.210.103	MAC: 00:D0:0	C8:75:A8:45					
	EG310GH-P-E Software Ver: ReyeeOS 1.202.2023							(U) Reboot
🖧 Network	Overview Network - Security - Behavior - VPN - Advanced - Diagnostics - System -							
🖄 Devices	Backup & Import Reset							
🖪 Gateway								0
Clients Management	If the target version is much later than the current version, some configuration may be missing. It is recommended to choose Reset before importing the configuration. The device will be rebooted automatically later.							0
∑ System ∨	Backup Config							
	Backup Config Backup							
	Import Config							
	File Path Please select a file. Browse Import							

- (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.

3.6 Configuring Restart

3.6.1 Restarting the Current Device

• Switch to the **Local Device** mode.

Choose System > Reboot.

Ruijie ERcycc	Local Device(FG2 >>	English ~	△ Remote O&M	Network Setup	Network Check	凿 Alert	🕒 Log Out
🖧 Overview	Reboot Scheduled Reboot						
③ Online Clients	Please keep the device powered on during reboot.						0
Network	Reboot						
⊘ Security ~							
₽ VPN ~							
🖹 Advanced 🛛 🗸							
≗ System							
System Time							
Management							
Upgrade							
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.

Reboot	Scheduled Reboot
I	Please keep the device powered on during reboot.
	Reboot

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

Reboot	Scheduled Reboot
	recommended to set the scheduled time to a network idle time, e.g., 2 A.M downlink device will also be rebooted as scheduled.
	Enable
	Day 🗹 Mon 🗹 Tue 🗹 Wed 🗹 Thu 🗹 Fri 🗹 Sat 🗹 Sun
	Time 03 ~ : 00 ~
	Save

- Switch to the **Network** mode.
 - Choose System > Reboot > Reboot. Select Local to restart the current device.

Reboot Scheduled Reboot			
<i>i</i> Please keep the device power	ed on during reboot.		
Select O Local	O All Devices	O Specified Devices	
Reboot			

3.6.2 Restarting All Devices on the Network

Switch to the **Network** mode. Choose **System** > **Reboot** > **Reboot**.

Ruíjie I & Rcycc		Navigation Q English ~	CRuijie Cloud 📓 Download App	ခ္ခံ Network Setup 🛛 @ Netw	work Check 一 <u>漸</u> Alert	🕞 Log Out
Q Navigation	Reboot Scheduled Reboot					
☆ Overview	Please keep the device powered on during reboot.					0
🖧 Network	Select O Local All Devices	Specified Devices				U
Devices		Specified Devices				
🖹 Gateway	Reboot					
⊗ Clients ∨						
🚼 System 🗠						
System Time						
Login Password						
Management						
Reboot						
						e
(Collapse						Ai ai

Select All Devices, and click Reboot All Device to restart all devices on the network.

Reboot	Scheduled Reboot	
i Plea	ase keep the device powered on during reboot.	
S	elect O Local O All Devices	O Specified Devices
	Reboot All Device	

🛕 Caution

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

3.6.3 Restarting Specified Devices

Switch to the Network mode. Choose 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.

Reboot	Sche	eduled Reboot							
0	Please kee	p the device power	ed on during reboot.						?
	Select	🔾 Local	 All Devices 		• Specified Devic	es			
		🖌 Available Devi	ces	1/1		Selected Device	'S	0/0	
		Q Search by SN	I/Model			Q Search by SN/	Model		
		1234567891	234 - EG210G-P		< Delete	I	No data		
		Reboot							

3.6.4 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 3.3 Setting and Displaying System Time.

Choose System > 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.

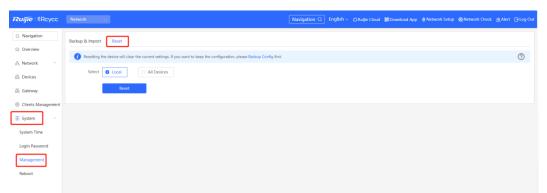
Reboot	Scheduled Reboot
	recommended to set the scheduled time to a network idle time, e.g., 2 A.M downlink device will also be rebooted as scheduled.
	Enable
	Day 🗹 Mon 🔽 Tue 🗹 Wed 🔽 Thu 🔽 Fri 🔽 Sat 🔽 Sun
	Time 03 ~ : 00 ~
	Save

3.7 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 System > Management > Reset.



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

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 **Wizard** to access the configuration wizard page.

gw_eg310g-e > Ruijie 🛛

Set	Internet	to	PPPoE	in	the	Network	Settings	pane.
	* Network Name	gw_eg3	10д-е					
	Network Settings	;						
		_	O DHCP O	Static IP				
	* Username	135591	tings: DHCP 63002					
	* Password	•••••			****			
	Service Name	(Option	al) Provided by IS	Р				
	Forgo	t Account	? Obtain Account	from Old De	vice			
	Country/Region/	Time Zo	one			\sim		
	* Country/Region	China (CN)		~			
	* Time Zone	(GMT+	3:00)Asia/Shangha	ai	~			
		Create	e Network & Conr	nect				

- (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 Create Network & Connect. The router initiates a connection with the Internet.
- (5) After connecting the router to the Internet, you can manage the router on Ruijie Cloud or Eweb.

Create Network		English 🗸 🕒 Exit
	Obtain PPPoE Account from Old Router <	
	Country/Region/Time Zone V	

4.1.2 Static IP Address Configuration Through a WAN Port

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

gw_eg310g-e ≻ Ruijie O		English ~	C Ruijie Cloud	證Download App	∲ Wizard @Ne	etwork Check – <u>満</u>	Alert 🕒
Set Internet to Static	IP in the Network Settings pane.						
* Network Name	gw_eg310g-e						
Network Settings							
Internet	PPPoE DHCP Static IP Current IP						
* IP	Checking IP assignment						
* Subnet Mask	255.255.255.0						
* Gateway	Example: 1.1.1.1						
* DNS Server	Example: 8.8.8.8, each separated by a space.						
Country/Region/	Fime Zone						
* Country/Region	China (CN)						
* Time Zone	(GMT+8:00)Asia/Shanghai						
	Create Network & Connect						

- (3) Configure an IP address, a subnet mask, a gateway IP address, and a DNS server address.
- (4) Click Create Network & Connect. The router initiates a connection with the Internet.
- (5) 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 **Wizard** to access the configuration wizard page.

	gw_eg310g-e > Ruijie O		English 🗸 🕜 Ruijie Clou	id 讃Download App	∂ Wizard	@Network Check	<u>尚</u> Alert	🕒 Log Out
(2)	Set Internet to DHCP in	n the Network Settings pane.						
	* Network Name	gw_eg310g-e						
	Network Settings	:						
		O PPPOE O DHCP O Static IP Current Settings: DHCP						
	Country/Region/	Time Zone	\sim					
	* Country/Region	China (CN)	~					
	* Time Zone	(GMT+8:00)Asia/Shanghai	~					
		Create Network & Connect						

(3) 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 Gateway > Network > WAN.

Rujje SRcycc	Network 🗸	Navigation Q English ~ @Ruijie Cloud 🏼 Download App 🔞 Network Setu	p @Network Check
Q Navigation	Router	Hostname: EG105G-P-V2 SN: M. 019 IP: 17226.5.127	(¹) Reboot
Overview	• EG105G-P-V2	MAC: 00:1 B:43 Software Ver; ReyeeOS 1.86.1929	O heboor
A Network	Overview Network	Security × Behavior × VPN × Advanced × Diagnostics × System ×	
Devices	<i>i</i> Configure WA	N settings.	0
🕮 Gateway	Single Line Du	al-Line	
Olients V			
:=- System	WAN WAN1	ISP/Load Settings	
	* Internet	DHCP ~	
		No username or password is required for DHCP clients.	
	IP	172.26.5.127	
	Subnet Mask	255.255.252.0	
	Gateway	172.264.1	
	DNS Server	192.168.58.110 192.168.58.94	
«Collapse			

4.2 AP Management

🚺 Note

- To manage the downlink AP, enable self-organizing network (SON) discovery (see section 错误!未找到引用源。错误!未找到引用源。). 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

o 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.

o 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. For details, see section <u>1.7 Switching Between Management Pages.</u>

3. Configuration Steps

Choose Overview > Device Details.

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.

Overview Real Time Flow Flow History URL L	og Client List	
Overview		
Memory Usage 19%	Online Clients 9	Status: Online Uptime: 41 days 21 hours 58 minutes 20 seconds Systime: 2022-10-10 14:22:56
Device Details		
Model: EG310G-E MAC: 00:D0:F8:18:28:38 Software Ver: ReyeeOS 1.206.2029	Hostname: Ruijie 2 Work Mode: Router 2	SN: MACCMR1250X01 Hardware Ver: 1.00

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.

Description:

- 1. The device IP address may change upon mode change.
- 2. Change the endpoint IP address and ping the device.
- Enter the new IP address into the address bar of the browser to access EWEB.
- The system menu varies with different work modes.

Work Mode	Router \vee 🕐
Self-Organizing Network	💽 🕐 🚺 Tip
AC	0
	Save

4. Viewing the Self-Organizing Role

Choose Local Device > Overview > Device Details.

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

Master AP/AC: The device functions as an AC to manage downlink devices.

Slave AP: The device connects to the AC in self-organizing mode and is managed by the AC. Slave APs are uniformly managed by the master AP or AC. Some wireless network configurations cannot be modified separately in local mode, and must be delivered by the master AP or AC.

Overview		
Memory Usage 46 %	Online Clients 1	Status: Online Uptime: 1 hour 6 minutes 16 seconds Systime: 2022-04-24 15:03:22
Device Details		
Model: EG	Но	ostname: Ruijie 🖉
SN: MACCEGWELYY01		MAC: 00:D0:F8:15:79:45
Work Mode: Router 🖉		Role: Master AC 🕖
Hardware Ver: 1.00	Softw	vare Ver: ReyeeOS 1.86.1611

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.

0 Note

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

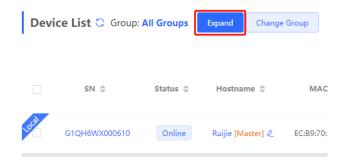
2. Configuration Steps

Switch to the Network mode. Choose 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.

Ruíjie l ®Rcycc	Network 🗸	Navigation Q	English 🗸 🛆 Ruijie C	loud _ 鼢Download App _ 合 Net	work Setup @Network Check	☆Alert Log Out
Q Navigation	All (3) Gateway (1) AP (2)	Switch (0) AC (0) Router (0)				
☆ Overview	<i>i</i> Device List					
유 Network ~	Device List 🔾 Group: All Groups	Expand Change Group Basic Inf	RF Information M	lodel		
Devices	1			IP/MAC/hostname/SN/S	Q Delete Offline Devices	Batch Upgrade
 Gateway Clients ~ 	SN ≎ Status ≎	Hostname $\ensuremath{\hat{\varphi}}$	IP \$	Clients 🗢 Device Group	Relay Information	Software Ver
: System	M.)21 Online	Ruijie 🖉 00:0 8:48	192.168.110.152 🖉	1 tests/Default	중 5G View Details	ReyeeOS 1.86.2019
	G1)534 Online	RAP2260(E) 🖉 EC: 14:97	192.168.110.200 🖉	0 tests/Default	Wired View Details	ReyeeOS 1.86.2019
	< 1 > 10/page >					Total 2
≪Collapse						

(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 *l* to modify the group name or click is to delete the group. You cannot modify the name of the default group or delete the default group.



 Device List C Group: All Groups
 Collapse

 Search by Group
 SN ≑

 ✓ All Groups
 +

 Default
 2

 Image: State of the state of

(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.

Device List	Group: A	ll Groups	Collapse	Change Group	Basic Info F	F Information Model	IP/MAC/hostna	me/SN/S Q	🗈 Delete Offline Devic	es Batch Upgrade
Search by Group	+	✓	SN 🔶	Status ≑	Hostname 🍦	MAC 💠	IP 🔶	Clients ≑	Device Group	Relay Information \$
Default) I	G1QH6WX000610	Online	Ruijie [Master] 🖉	EC:B9:70:23:A4:BF	172.26.1.32 🖉	0	test/默认组	Wired View Details
			_					_		

Change Group		
Select Group	Select ^	
	Default test	el

4.2.3 Configuring Wi-Fi

Switch to the Network mode. Choose Network > Wi-Fi > Wi-Fi Settings.

Enter the SSID and Wi-Fi password, select the frequency band used by the Wi-Fi signal, and click Save.

Click Advanced Settings to configure Wi-Fi parameters.

🛕 Caution

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

<i>i</i> Tip: Changing c	onfiguration requires a reboot and clients will be reconnected.
Wi-Fi Settings	Device Group: Default
* SSID	test
Band	2.4G + 5G ~
Security	Open ~
	Collapse
Wireless Schedule	All Time 🗸
VLAN	Default 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 his IP address unchanged in this Wi-Fi network.)
Wi-Fi6	(802.11ax High-Speed Wireless Connectivity.) 🕥
	Save

Table 4-1 Wireless Network Configuration

Parameter	Description
SSID Enter the name displayed when a wireless client searches for a wireless network.	
SSID Encoding	If the SSID does not contain Chinese, this item will be hidden. If the SSID contains Chinese, this item will be displayed. You can select UTF-8 or GBK.
Band	Set the band used by Wi-Fi signals. 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 as needed. The default value is 2.4G + 5G , indicating that the device provides signals at both 2.4 GHz and 5 GHz bands.

Parameter	Description				
Security	 Select an encryption mode for wireless network connections. The options are as follows: Open: The device can associate with Wi-Fi without a password. WPA-PSK/WPA2-PSK: Wi-Fi Protected Access (WPA) or WPA2 is used for encryption. WPA_WPA2-PSK (recommended): WPA2-PSK or WPA-PSK is used for 				
encryption. Wi-Fi Password Specify the password for interconnection with the wireless network. The password is a string of 8 to 16 characters.					
Wireless Schedule	Specify the period during which Wi-Fi is enabled. When this parameter is set, users can only connect to Wi-Fi during this period.				
VLAN	Set the VLAN to which Wi-Fi signals belong. You can select a VLAN from the available VLANs, or click Add New VLAN and go to the LAN Settings page to add a VLAN.				
Hide SSID	Enabling SSID hiding can prevent unauthorized users' 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.				
Client Isolation With client isolation enabled, clients associated with Wi-Fi are isolated fro other, and end users connected to the same AP (in the same network sec cannot access each other. This improves security.					
Band Steering Band steering allows 5G-capable clients to select 5 GHz Wi-Fi preferent You can enable this function only when Band is set to 2.4G + 5G.					
XPress	XPress enables the device to send game packets preferentially, providing more stable wireless network for games.				
Layer-3 Roaming	Layer 3 roaming enables clients to keep their IP addresses unchanged when the clients are associated with the same Wi-Fi. This function improves the roaming experience of users in the cross-VLAN scenario.				
Wi-Fi6	 Wi-Fi 6 provides wireless users with faster network access speed and optimized network access experience. This function is valid only on 802.11ax-capable APs and routers. Clients must also support 802.11ax to experience high-speed network access empowered by Wi-Fi 6. If clients do not support Wi-Fi 6, disable this function. 				

4.2.4 Configuring Guest Wi-Fi

Switch to the Network mode. Choose Network > Wi-Fi > Guest Wi-Fi.

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.

Enable guest Wi-Fi and set the guest SSID and password. Click **Advanced Settings** to configure the wireless schedule of guest Wi-Fi and more Wi-Fi parameters. For details, see section <u>4.2.2 Configuring Wi-Fi</u>. Click **Save**. Guests can access the Internet through Wi-Fi after entering the SSID and password.

Wi-Fi Settings	Guest Wi-Fi	Wi-Fi List	Healthy Mode	Load Balancing
i Tip: Changing	g configuration re	quires a reboot	and clients will be	reconnected.
Guest Wi-Fi	Device Group:	Default	~	
Enab	ole 🛑			
* SS	ID @Ruijie-g	uest-2277		
_				
Bar	nd 2.4G + 5G		\sim	
Securi	ity Open		~	

		Collapse
Wireless Schedule	Neve	er Disable ~
VLAN	Defa	ult 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 his IP address unchanged in this Wi-Fi network.)
Wi-Fi6		(802.11ax High-Speed Wireless Connectivity.) ⑦
		Save

4.2.5 Adding More Wi-Fi Networks

Switch to the **Network** mode. Choose **Network** > **Wi-Fi** > **Wi-Fi** List, and select the device group which you want to add more Wi-Fi networks.

Click **Add**, enter the SSID and password, and click **OK** to create a Wi-Fi network. Click **Advanced Settings** to configure more Wi-Fi parameters. For details, see section <u>4.2.2 Configuring Wi-Fi</u>. After a Wi-Fi network is added, clients can find this Wi-Fi network, and Wi-Fi information is displayed in the Wi-Fi list.

Wi-Fi Settings	Guest Wi-Fi	Wi-Fi List	Healthy Mode	Load Balancing		
i Tip: Chang	ging configuration re	equires a reboo	t and clients will be re	econnected.		0
Wi-Fi List	Device Group:	Default 🗸 🗸				+ Add
Up to 8 SSIDs	s can be added.					
SSID	Band	I	Security	Hidden	VLAN ID	Action
test	2.4G +	5G	OPEN	No	Default VLAN	Edit Delete

Add		×
i The configurati	on will take effect after being delivered t	o AP.
* SSID		
Band	2.4G + 5G ~	
Security	WPA_WPA2-PSK ~	
* Wi-Fi Password	**	
	Expand	
	Cancel	ОК

4.2.6 Healthy Mode

Switch to the Network mode. Choose Network > Wi-Fi > Healthy Mode.

Enable the healthy mode and select a wireless schedule 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.

Wi-Fi S	ettings	Guest Wi-Fi	Wi-Fi List	Healthy Mode	Load Balancing
0		1 C C C C C C C C C C C C C C C C C C C		ase its transmit powe and clients will be red	er to reduce radiation. connected.
Hea	lthy Mod	e Device Grou	p: Default	~	
	Enal	ble 🔵			
Wir	eless Sched	ule All Time		~	
		Sav	/e		

4.2.7 RF Settings

Switch to the Network mode. Choose Network > Radio Frequency.

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.

<i>i</i> Tip: Changing cor	figuration requires a reboot and clien	s will be reconnected.	
Radio Frequency	Device Group: Default		
Country/Region	China (CN)		
2.4G Channel Width	Auto	5G Channel Width	Auto ~
lulticast Rate (Mbps)	Auto	Multicast Rate (Mbps)	Auto
0		0	
Client Count Limit	32	Client Count Limit	32
Disconnection	-	Disconnection	
Di Threshold	sable -85dBm -5	IdBm Threshold	Disable -85dBm -50dBm
0		0	
	Save		

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.

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.

4.2.8 Configuring a Wi-Fi Blacklist or Whitelist

1. Overview

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

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

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

🛕 Caution

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

2. Configuring a Global Blacklist or Whitelist

Switch to the Network mode. Choose Clients Management > Blacklist/Whitelist > Global Blacklist/Whitelist.

Select the blacklist or whitelist mode and click Add to add a client to the blacklist or whitelist. 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 blacklist are forced offline and not allowed to access the Wi-Fi network. The global blacklist and whitelist settings take effect on all Wi-Fi networks of the router.

Global Blacklist/Whitelist	SSID-Based Blacklist/Whitelist				
• All STAs except blackliste	d STAs are allowed to access Wi-Fi.	O Onl	y the whitelisted STAs are	e allowe	ed to access Wi-Fi.
Blocked WLAN Client	ts		+ Add		Delete Selected
Up to 64 members can be a	added.				
MA	IC	Remark		Ac	tion
AE:4E:11	OUI			Edit	Delete
11:22:33:4	44:55:66			Edit	Delete
Add			×		
Match Type	• Full OPrefix (OUI)				
* MAC	Example: 00:11:22:33:44:5	5			
Remark					
		Cancel	ОК		

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

• All STAs exce	ept blacklisted STAs are allow	ved to access Wi-Fi. Only the	whitelisted STAs are allowed to access Wi-Fi.
Blocked WL	AN Clients		+ Add 🗇 Delete Selected
Up to <mark>64</mark> men	nbers can be added.		
	MAC	Remark	Action
	AE:4E:11 OUI		Edit Delete
	11:22:33:44:55:66		Edit Delete

3. Configuring an SSID-based Blacklist or Whitelist

Switch to the Network mode. Choose Clients Management > Blacklist/Whitelist > SSID-Based Blacklist/Whitelist.

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

Global Blacklist/Whitelist	bal Blacklist/Whitelist SSID-Based Blacklist/Whitelist					
<i>i</i> Note: OUI matching re Rule: 1. In the Black	ule and SSID-based blackli ist mode, the clients in the	e blacklist are not allowed	o the Wi-Fi network. by only RAP Net and P32 (and to connect to the Wi-Fi networl d to connect to the Wi-Fi netwo	k.		
Device Group: Default	/hitelist		As are allowed to access Wi- allowed to access Wi-Fi.	FI.		
123	Blocke	ed WLAN Clients	+ Add	Delete Selected		
	Up to	64 members can be adde	d.			
		MAC	Remark	Action		
		11:22:33:44:55:66		Edit Delete		

4.2.9 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

Switch to the **Network** mode. Choose **Network** > **Wi-Fi** > **Load Balancing**.

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

Wi-Fi Settings	Guest Wi-Fi	Wi-Fi List	Healthy Mode	Load Balancing			
Load Balancir	ng					+ Add	i Delete Selected
AP with lighter lo Example: Add AP	ea into a group ar ad. 1 and AP2 into a clients and AP2 i	group and select s associated with	client load balancing 2 clients, triggering l	s unbalanced in the gro . Set both the client co oad balancing. New cli	unt threshold	and differenc	e to 3. AP1 is
Group I	Name	Туре	F	Rule	N	lembers	Action
			No [Data			
Add						×	
* Group Nam	ne						
* Тур	Client L	.oad Balancii	ng		~		
* Rul	When an difference client cou 3 group. A 10	unt on the A , clients fter a client a	he currently asso P with the lighte can associate or association is de the client will be	Clients ociated client cou est load reaches aly to another AP nied by an AP for allowed to assoc	int and in the r		
* Member	rs Enter a	n AP name o	or SN.		~		

Table 4-3 Client Load Balancing Configuration

Parameter	Description	
Group Name	Enter the name of the AP load balancing group.	
Туре	Select Client Load Balancing.	

Cancel

Parameter	Description
Rule	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. 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 associated with the AP for 10 times, the client will be allowed to associate with the AP upon the next attempt.
Members	Specify the APs to be added to the AP load balancing group.

3. Configuring Traffic Load Balancing

Switch to the Network mode. Choose Network > Wi-Fi > Load Balancing.

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

Wi-Fi Setting	s Guest Wi-Fi	Wi-Fi List	Healthy Mode	Load Balancing		
Load Ba	lancing				+ Add	Delete Selected
Add APs i AP with li Example: associated	ghter load. Add AP1 and AP2 into a	group and selec is associated wit	t client load balancing h 2 clients, triggering	is unbalanced in the grou g. Set both the client coun load balancing. New clien	it threshold and differend	ce to 3. AP1 is
	Group Name	Туре		Rule	Members	Action
			No	Data		



dd	
Group Name	
* Type	Traffic Load Balancing
* Rule	When the traffic load on an AP reaches 5
	*100Kbps and the difference between the current traffic and
	the traffic on the AP with the lightest load reaches
	5 *100Kbps, clients can associate only to another
	AP in the group. After a client association is denied by an AP
	for 10 times, the client will be allowed to associate
	to the AP upon the next attempt.
* Members	Enter an AP name or SN.
* Members	Enter an AP name or SN. \sim

Cancel OK

Table 4-4 Traffic Load Balancing Configuration

Parameter	Description
Group Name	Enter the name of the AP load balancing group.
Туре	Select Traffic Load Balancing.
Rule	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. By default, when the traffic load on an AP reaches 500 kbit/s and the difference between the current traffic and the traffic on the AP with the lightest load reaches 500 kbit/s, 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.
Members	Specify the APs to be added to the AP load balancing group.

4.2.10 Wireless Network Optimization in One-Click Mode

Switch to the **Network** mode. Choose **Network** > **WIO**.

On the **Network Optimization** tab, select **I have read the notes** and click **Network Optimization** to perform automatic wireless network optimization in the networking environment. 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 an idle period.

🛕 Caution

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

Vetwork Optimization	Optimization Record		
\odot ———	Q,	<u>5</u> 9	
Start	Scanning	Optimizing	Finish
	Description: This feature will optimize the self-organize that all APs have been online.	ing network to maximize the W	LAN performance. Please make sure
	Notes: 1. During network optimization, the APs w will last for a while, subject to the quantity night. 2. If dynamic channel allocation is running later. 3. The configuration cannot be rolled back	y of devices. It is recommended g in the backend, network optim	you enable network optimization at
Scheduled Opti	I have read the notes. Network Optimization mization		
<i>Scheduled Op</i> Optimize the ne	timization twork performance at a scheduled time	for a better user experience.	
Ena	ble 🚺		
C	Day Sun ~		
Tir	me 03 ~ : 00 ~		
	Save		

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

Click View Details or the Optimization Record tab to view the latest optimization record details.

⊘ —— Start			- ⊘ ——— Scanning			⊘ <u> </u>		F	⊘ Finish
\bigcirc	Opti Time	nish imiation finished e: 31 seconds /iew Details	on 20 Back	Cancel Optim	nization				
etwork Optimiza	ized:2022-04-26 1	5:26:22 d improved the perfo	rmance by 12.50%!						
<i>i</i> Last Optim You have o	ized:2022-04-26 1	5:26:22	rmance by 12.50%!						
<i>i</i> Last Optim You have o	nized:2022-04-26 1 optimized 1 APs an	5:26:22	rmance by 12.50%! Channel (Before/After)	Channel Width (Before/After)	Transmit Power (Before/After)	Sensitivity (Before/After)	CCI (Before/After) \$	ACI (Before/After) \$	Interference (Before/After \$
Last Optim You have o	nized:2022-04-26 1 optimized 1 APs an Details	5:26:22 d improved the perfo	Channel	Width	Power		(Before/After)	(Before/After)	(Before/After

4.2.11 Enabling Reyee Mesh

Switch to the **Network** mode. Choose **Network** > **Reyee Mesh**.

Ruíjie I : Reycc	Network ✓
Q Navigation	👔 After enabling Reyee Mesh, you can set up a Mesh network through Mesh pairing between the devices that support Reyee Mesh.
DHCP Snooping	Enable
WIO	Save
Radio Frequency	
Reyee Mesh LAN Ports	
LED	
Alerts	
Batch Config	

After Reyee mesh is enabled, you can set up a mesh network through mesh pairing between the devices that support Reyee 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.

4.2.12 Configuring a LAN Port of a Downlink AP

🛕 Caution

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

Switch to the Net	work mode. Choose Network > LA	N Ports.		
	ngs n takes effect only for the AP with a LAN port, e.g., EAP gured LAN port settings prevail. <mark>The AP device with no</mark> I		h default settings	
Default Setting	5			
VLAN ID		Add VLAN		
Applied to	(Range: 2-232 and 234-4090. A blank value indicat WAN port.) AP device with no LAN port settings O Save gs	es the same VLAN as	+ Add	Delete Selected
Up to <mark>8</mark> VLAN IDs or	32 APs can be added (1 APs have been added).			
VLAN	ID 🗢 Ap	plied to		Action
□ 2	2	Ruijie		Edit Delete

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				0
* Applied to	Enter an AP name or SN.		~	
		Cancel		ок

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

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

Ruíjie	test123 > EG105GW Ma	asterj ()			English ~ _	合 Ruijie Cloud 🏾 🎇 Downlo	ad App 🛭 👌 Network Setup 🖉 Network Cher	ck ∦ğWarn ⊡gLogOu
ै Overview ® Online Clients क्षि Router	i Switch ListSwitch List				IP/	/MAC/hostname/SN/SoftW	are Ver Q Delete Offline Devices	Batch Upgrade
ି Wireless ଁ	Action	Hostname \$	IP \$	MAC \$	Status ≑	Model \$	Software Ver	SN \$
昼 Switches	Manage	ES209GC-P 🖉 19	2.168.110.3 CO:E	3:):77	Online	RG-ES209GC-P	ESW_1.0(1)B1P3,Release(07200415)	CAP 37
-Network V	Manage	NBS5200 192	2.168.110.74 54:1		Offline	NBS5200- 24SFP/8GT4XS	ReyeeOS 1.54.1818	G1I
	Manage	NB53100 🖉 19	2.168.110.2 CO:B	JD	Online	NBS3100- 24GT4SFP-P	ReyeeOS 1.83.1511	G1F 47
	< 1 > 10/	/page v						Total 3
«Collapse								

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

ຂັບເງົາເອ ີ ເສັດຊາດດ	test123	8 > EG105GW	[Master] 🕜			English 🗸 🛆	Support VLAN	Settings 🔵 🔇	Basic Settings Panel View	C Upg) Rebo
유 Overview 의 Online Clients	Ø	Switch List					1.2	3 4 5	6 7 8 9		_
Router	Sw	itch List									
ङ Wireless ৺		Action	Hostname \$	IP ‡	MAC \$	Status ≑	-0- -0-	Ruijie Cloud S	: ES209GC-P 🖉 Status: Connected : RG-ES209GC-P		
a Switches		Manage	ES209GC-P 🖉	192.168.110.3	C0:88 :77	Online F	SYS	Software Ver SN	RG-ES209GC-P ESW_1.0(1)B1P3,Release(07200415) C 1237 CL		
Network 🗸				192.168.110.74	54 A:8F	Offline	•	IP Subnet Mask	192.168.110.3 255.255.255.0		
		Manage	NBS3100 🖉	192.168.110.2	C0:13:0D	Online	WAN	DNS Server	: 192.168.110.1 : 192.168.110.1		
		1 > [10/page 🗸				Monitor Inf				
							Cable Diagn	nostics			
							MAC List				

• Edit Hostname: Modify the host name of switch.

Ruíjie #Rcycc	test123	> EG105GW	(Master) O			English	∽ Ruijie Cloud 🎇 Do	wnload App – 👌 Network Setup – 🔘 Network Che	ck <u>m</u> iWarn [–]LogOu
ింOverview (ల్రి Online Clients	() Swit	Switch Liet	Edit Hostname					ftWare Ver. Q	Batch Upgrade
⊞ Router		A	Edit Hostname	₽ ≑	MAC \$	Status ≑	Model \$	Software Ver	SN ¢
Switches		Manage	ES209GC-P &	192.168.110.3	C0:8° 7:77	Online	RG-ES209GC-P	ESW_1.0(1)B1P3,Release(07200415)	C ?37
Network 🗸		Manage	NBS5200	192.168.110.74	54: \:8F	Offline	NBS5200- 24SFP/8GT4XS	ReyeeOS 1.54.1818	G1 7B
		Manage	NBS3100 &	192.168.110.2	CO.E	Online	NBS3100- 24GT4SFP-P	ReyeeOS 1.83.1511	G1Pi 47
		1 >	10/page 🗸						Total 3
≪ Collapse									

4.4 Diagnostics

4.4.1 Network Check

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

(1) Switch to the Local mode. Choose Diagnostics > Network Check. Click Start and click OK in the displayed

dialog	box	to	start	checking	the	network	status.
Ruíjie MRcy		al Device(EG2 \vee					
🐣 Overview		i) Network Check					
Ø Online Clients							
Network	~	Start					
Security	~						
វារ៍ Behavior	× l						
VPN	~						
🖹 Advanced	~						
Ø Diagnostics	^						
Network Check							
Alerts							
Network Tools							
Packet Capture							
Fault Collection							
💱 System	~						

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

1 Network Check	
Racheck	
	100%
WAN/LAN Cable	0
Auto-Negotiated Speed	0
WAN Port	•
DHCP-Assigned IP Address	0
LAN & WAN Address Conflict	•
Loop	0
DHCP Server Conflict	0
IP Address Conflict	0
Route	0
Next Hop Connectivity	0
DNS Server	0
IP Session Count	•
DHCP Capacity	0
Flow Control	0
Ruijie Cloud Server	0

4.4.2 Alarms

The Alerts page allows you to query and manage alarms.

(1) Switch to the Local mode. Choose Diagnostics > Alert.



(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.

Alert L	ist					View Unfollowed Alert
Expand	Alerts		Sug	ggestion		Action
~	There is more th LAN network.	an one DHCP server i	n the Ple	ase disable the extra DHC	P server in the LAN network.	Delete Unfollow
	Hostname	SN	Туре	Time	Details	Action
	Ruijie	1234567891234	EG210G-P	2022-04-24 09:39:08	A DHCP server conflict occurs in LAN network: MAC:58:69:6c:00:00:01,1 P:192.168.11.1,VLAN ID:233; MAC:UNKNOWN,IP:192 .168.112.1,VLAN ID:233	Delete

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

 \times

/iew Unfollowed Alert		
There is more than one DHCP server in the LAN network.		
Re-follow		

Cancel

4.4.3 Network Tools

Switch to the Local mode. Choose Diagnostics > Network Tools.

i Network Tools					?
Tool	• Ping	e 🔿 DNS L	ookup		
* IP Address/Domain	172.26.1.1				
* Ping Count	4				
* Packet Size	64		Bytes		
	Start	Stop			
PING 172.26.1	.1 (172.26.1.1): 64 data byt	es			
	172.26.1.1: seq=0 ttl=64 ti				
72 bytes from	172.26.1.1: seq=1 ttl=64 ti				
72 bytes from					
72 bytes from 172.26.1.1: seq=3 ttl=64 time=2.212 ms					
172.26.1.1	172.26.1.1 ping statistics				
4 packets tran	4 packets transmitted, 4 packets received, 0% packet loss				
round-trip min/avg/max = 2.199/2.822/4.675 ms					
			//	2	

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.

i Network Tools					
Tool	Ping	O Traceroute	O DNS Loo	kup	
* IP Address/Domain	8.8.8.8				
* Ping Count	4				
* Packet Size	64		B	ytes	
	St	tart	Stop		
PING 8.8.8.8 (8.8.8.8): 64 data bytes 72 bytes from 8.8.8.8: seq=0 ttl=112 time=42.277 ms 72 bytes from 8.8.8.8: seq=1 ttl=112 time=43.100 ms 72 bytes from 8.8.8.8: seq=2 ttl=112 time=43.862 ms 72 bytes from 8.8.8.8: seq=3 ttl=112 time=41.880 ms 8.8.8.8 ping statistics 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 41.880/42.779/43.862 ms					

2. Traceroute Tool

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

i Network Tools		
Tool	O Ping O Traceroute	e 🔿 DNS Lookup
P Address/Domain	172.26.4.1	
* Max TTL	20	
	Start	Stop
packets	172.26.4.1 (172.26.4.1), 20 (172.26.4.1) 1.860 ms 1.62	

3. DNS Lookup Tool

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

i Network Too	ls		
Тоо	I 🔿 Ping	 Traceroute 	O DNS Lookup
* IP Address/Domair	www.go	oogle.com	
		Start	Stop
Server: 12 Address 1: 1		alhost	
Name: w Address 1: 2 Address 2: 1	2001::6ca0:a	7a7	
			1.

4.4.4 Packet Obtaining

Switch to the Local mode. Choose 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.

A Caution

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

<i>i</i> Packet Capture			?
Interface	ALL	~	
Protocol	ALL	~	
IP Address]
File Size Limit	2M	\sim	Available Memory 177.63 M
Packet Count Limit	500	\sim	
	Start	Stop	

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.

<i>i</i> Packet Capture			?
Interface	ALL	~	
Protocol	ALL	~	
IP Address			
File Size Limit	2M	~	Available Memory 177.63 M
Packet Count Limit		e: 78.02K	
PCAP file	Click to download the PC	ed on: 2022-04-27 12:50:07	
	Click to delete the file.		
	Start	Stop	

- 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.

4.4.5 Fault Collection

Switch to the Local mode. Choose Diagnostics > Fault Collection.

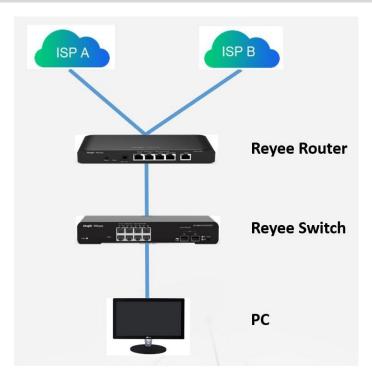
When the device fails, you need to collect fault information. Click **Start**. Configuration files of the device are packaged into a compressed file. Download the compressed file locally and provide it to R&D personnel for fault locating.



Compress the configuration file for engineers to identify faults.

4.5 WAN Load Balancing

If there is more than one WAN port, some traffic is routed over the ISP route, and the remaining traffic is balanced according to the load mode.



Prepare two uplink cables for Internet access before configuration.

(1) Switch to the **Local** mode. Choose **Network** > **WAN**.

Ruíjie #Rcycc	gw_eg310g-e > Ruijie 🜒
🖧 Overview	
Ø Online Clients	1 WAN
Hetwork	network.lines Three Lines Four Lines
WAN	WAN0 WAN1 ISP/Load Settings
LAN	* Internet PPPoE ~
IPv6 Address	* Username 13559163002
Port VLAN	Forgot Account? Obtain Account from Old Device
Port Settings	* Password > _{>r} <
IPTV	Service Name (Optional) Provided by ISP
⊘ Security 🗸 🗸	⊘ PPPoE connection succeeded. View PPPoE Records
m Behavior 🗸 🗸	IP 100.62.90.190
I VPN V	Subnet Mask 255.255.255
🖹 Advanced 🗸 🗸	Gateway 100.68.128.1
Diagnostics	DNS Server 211.138.151.161 211.138.156.66
-e System V	Advanced Settings
	Save

(2) Configure WAN accordingly.

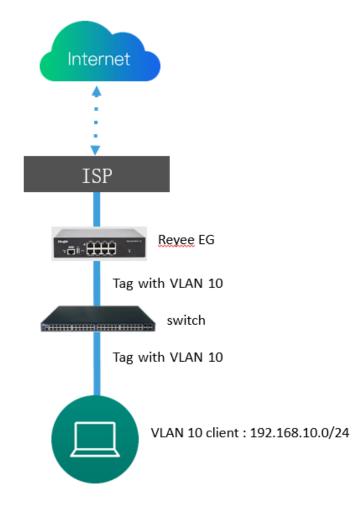
WANO	WAN1	ISP/Load Settings	
	* Internet	PPPoE	~
*	Username	13559163002	
0	Forgot A	ccount? Obtain Account from	Old Device
*	Password	•••••	×≮
Serv	vice Name	(Optional) Provided by IS	Ρ
Q	PPPoE cor	nnection succeeded. View PP	PoE Records
	IP	100.62.90.190	
Sub	onet Mask	255.255.255.255	
	Gateway	100.68.128.1	
D	NS Server	211.138.151.161 211.138.15	6.66
		Advanced Settings	
		Save	

(3) Select ISP/Load Settings, and configure the load mode and interface weight.

WAND	WAN1	ISP/Load Settings
Load Balar	ncing S	Settings
🥡 1. Balanc	ced mode:	suted based on ISP settings preferentially. The remaining traffic will be managed according to load mode. The traffic will be spread across multiple links according to the weight of each WAN port. For example, if WAN and WAN1 weight are set to 3 and 2 respectively, 60% of the total traffic will be routed over WAN and 40% over WAN1. Inder y mode: All traffic is routed over the primary interface. The traffic will be switched over to the secondary interface. If there are multiple primary and secondary interfaces, please configure their weight (See balanced mode).
Load	Mode	Primary & Secondary v
Balancing	Policy	Based on Src and Dest IP Address
	WAN	Set as Prim \sim * Weight 1
,	WAN1	Set as Secc. V * Weight 1

- Balanced mode: Traffic will be transmitted across multiple links according to the weight of each WAN port. For example, if weights of WAN and WAN1 are set to 3 and 2 respectively, 60% of the total traffic will be routed over WAN and 40% over WAN1.
- **Primary & secondary mode:** All traffic is routed over the primary interface. Once the primary interface fails, traffic will be switched over to the secondary interface. If there are multiple primary and secondary interfaces, configure the weights.

4.6 Port VLAN



(1) Switch to the Local mode. Choose Network > LAN to create a VLAN first.

Ruijie IRcycc	gw_cg310g-c > a	huğle 🛛					L	inglish ~ 🛆 Ruijie Cloud 🛛 🔠 Dowr	iload App 🔞 Wizard 🍭 Network C	heck <u>as</u> Alert ⊡Log 0
	LAN Settings	DHCP Clients Static IP Ad	dresses DHCP Option DNS I	Ртоку						
Online Clients	🕧 LAN Sett	lings								0
WAN	LAN Setting	gs							+ Add	© Delete Selected
LAN	Up to 8 entri	ies can be added.								
IPv6 Address		P	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
Port VLAN		192.168.111.1	255.255.255.0	Default VLAN		Enabled	192.168.111.1	254	3	Edit Delete
Port Settings										
PTV										
Security ~										
Behavior ~										
VPN ~										
Advanced ~										
E System										

Add		×	
* IP			
* Subnet Mask	255.255.255.0		
* VLAN ID			
Remark	Remark		
MAC	80:D0:F8:1A:8A:7A		
DHCP Server			
* Start			
* IP Count	254		
* Lease Time(Min)	30		
DNS Server	- 0		
	Cancel	ОК	

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



(2) Choose Network > Port VLAN to tag VLAN. By default, the tagged mode is used for VLANs.

Ruíjie I & Royco	Local Device(EG2 >>				
음 Overview ⑧ Online Clients	Port VLAN Please choose LAN Settin	gs to create a VLAN first and configure	port settings based on the VLAN.		
Network ^ WAN	Connected	nected			
LAN				-	-
IPv6 Address		LANO	LAN1/WAN3	LAN2/WAN2	LAN3/WAN1
Port VLAN Port Settings	Default VLAN			UNTAG 🗸	UNTAG 🗸
IPTV	VLAN 11 VLAN 12	TAG V	TAG \lor	TAG ~	TAG v
) Security 🗸 🗸	VLAN 13	TAG \lor	TAG ~	TAG V	TAG ~
Behavior 🗸	11111				
Advanced					
Diagnostics					
System ~					

• UNTAG: If VLAN 10 is set to UNTAG 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

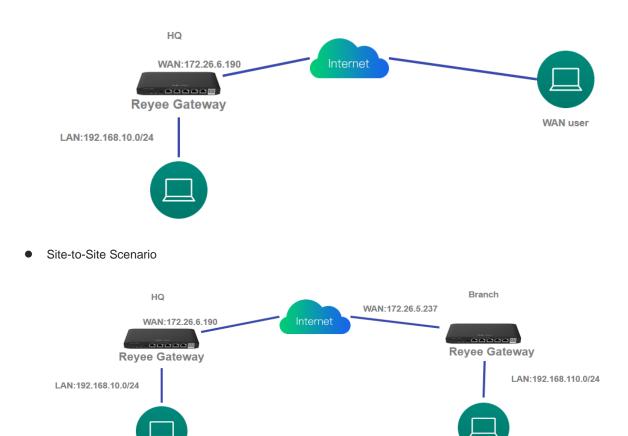
port 2 are considered as the packets from VLAN 10.

- o Each port can be configured with only one untagged VLAN.
- The native VLAN of port 1 is the default VLAN and cannot be edited.
- TAG: If both VLAN 10 and VLAN 20 are set to TAG on port 2, packets from VLAN 10 and VLAN 20 are forwarded through port 2.
- Not Join: If both VLAN 10 and VLAN 20 are set to Not Join on port 2, port 2 will not receive or transmit packets from VLAN 10 or VLAN 20.

4.7 VPN

Application Scenario

Client-to-Site Scenario



4.7.1 **PPTP VPN**

PPTP VPN is typically used in client-to-site and site-to-site scenarios. For example, clients work from home and need to access company servers through PPTP VPN tunnels; a company has three branches that are distributed in three different places, and each branch needs to establish a tunnel with each other through a router.

1. Client-to-Site Scenario Configuration

- (1) Headquarters side:
 - a Log in to the Reyee EG with the default IP address of 192.168.110.1.
 - b Switch to the **Local** mode. Choose **VPN** > **PPTP** and enable PPTP.

Ruíjie I #Rc	усс	Local Device(EG2 V
A Overview		PPTP Settings Tunnel List
Ø Online Clients		
		() PPTP Settings
Network	~	
⊘ Security	~	Enable
∰ Behavior	~	Save
VPN	^	
IPSec		
L2TP		
рртр		
OpenVPN		
VPN Clients		
🗄 Advanced	~	
Diagnostics Diagno	~	
🚆 System	~	

c Perform PPTP configuration and click **Save**.

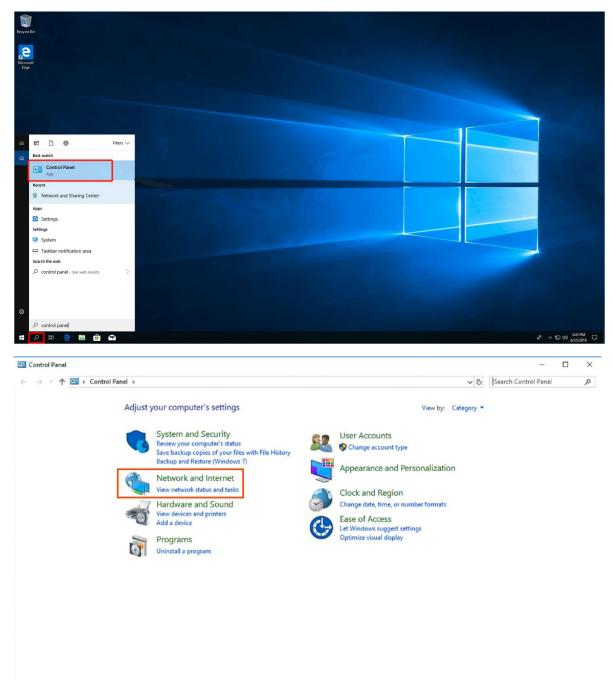
PPTP Settings Tunnel	List	
PPTP Settings		
Enable		
РРТР Туре	Server O Client	
* Local Tunnel IP	Example: 1.1.1.1	
* IP Range	Example: 1.1.1.2-1.1.1.100	0
* DNS Server	Example: 1.1.1.1	
MPPE	O Disable 🔿 Enable	
Flow Control	O Disable 🔿 Enable	
* PPP Hello Interval	10	
	Save	

d Choose Network > VPN Clients and configure VPN clients.

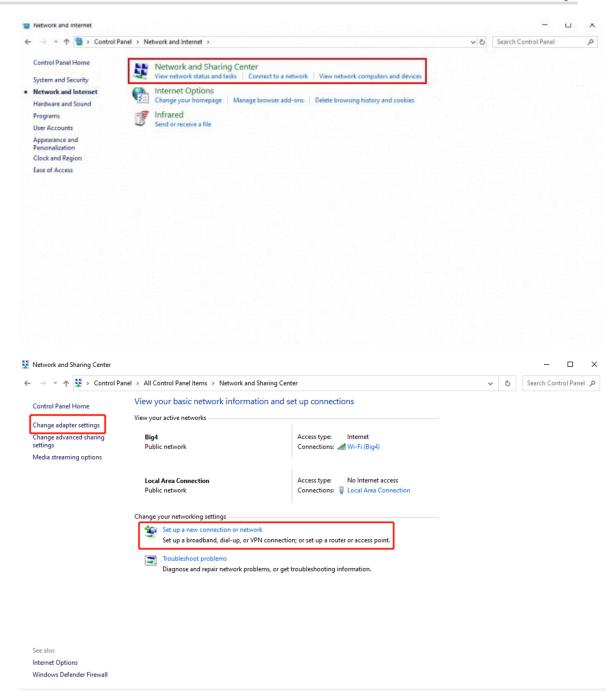
Rujje IRcycc	Local Device(EG2 ~	1					English ~ 🔘 Remote D&M 👋 Netwo	rk Setup 🚳 Network Check 🚊 Alert 🕒 Log Out
Overview Online Clients	VPN Clients							Ø
	VPN Client Lis	t					Usamama/#assword	C + Add Celete Selected
⊖ Security ~	Up to 100 entries	can be added.						
tti Behavior 🗠		Username	Password 🐱	Service Type	Network Mode	Client Subnet	Status	Action
VPN ^					No Data			
L2TP	< 1 >	10/page -						Total 0
8979								
OpenVPN								
VPN Clients								
 Diagnostics ~ ~ 								
🕃 System 🗸 🗸								
Add Use	٥r			×				
Aug 030	-1							
Service	Type	ALL	~					
* User	name	Please enter a user	name.					
* Pass	sword	Please enter a pass	word.					
Network I								
INETWORK I	Iviode	PC to Router	× .					
5	Status (
			Cancel	ОК				

(i) Note

- Service type: Select PPTP.
- Network Mode: Select Router to Router.
- **Peer Subnet**: Fill in the internal network segment of the branch. The value and the internal network segment of the headquarters cannot overlap.
- (2) Client side (Windows 10 is used as an example):
 - a Choose Control Panel > Network and Internet > Network and Sharing Center.



Common Settings



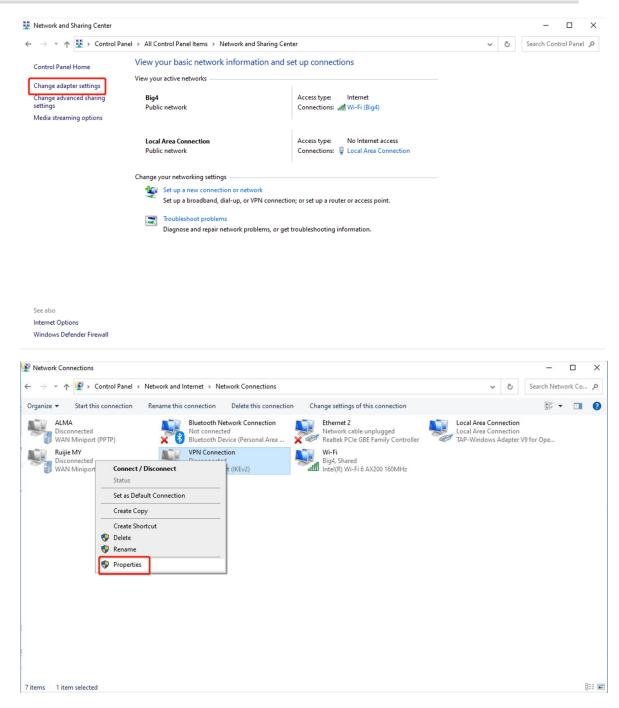
b Configure a VPN connection.

 \times

_ \leftarrow 🕎 Set Up a Connection or Network Choose a connection option Connect to the Internet Set up a broadband or dial-up connection to the Internet. Set up a new network Set up a new router or access point. Manually connect to a wireless network Connect to a hidden network or create a new wireless profile. Connect to a workplace Set up a dial-up or VPN connection to your workplace Next Cancel \times Connect to a Workplace ← Do you want to use a connection that you already have? No, create a new connection ○ Yes, I'll choose an existing connection Ruijie MY WAN Miniport (PPTP) Ruijie Demo WAN Miniport (PPTP) ALMA WAN Miniport (PPTP) Next Cancel

				-		\times
←	🌆 Connect to a Workplac	e				
	How do you want to	connect?				-
	→ Use my Interne Connect using a virt		(VPN) rork (VPN) connection through the In	ternet.		
	i	- 🥘	I			
	→ Dial directly Connect directly to a	a phone numbe	r without going through the Internet.			-
	I	_				
					Can	cel
				_		×
÷	Connect to a Workplace	2				~
	Type the Internet add	lress to conn	lect to			
	Your network administrator	r can give you th	is address.			
	Internet address:	172.26.6.190	The WAN IP of HQ			
1	Destination name:	VPN Connect	tion			
	Use a smart card					
	Remember my cred	lentials				
	Allow other people This option allows a		ection ess to this computer to use this conne	ection.		
			E	Create	Canc	el

c Change settings of the adapter.

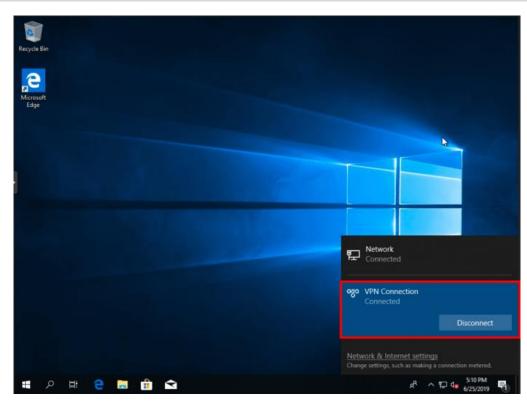


eneral Opt	ions Se	curity	Networking	Sharin	g	
Type of VPN	l:					
Point to Poi	nt Tunneli	ing Prot	ocol (PPTP)			~
Data encryp	ion:			Ad	vanced s	settings
Optional en	cryption (d	connect	even if no e	encryptio	n)	~
Authentica	tion					
O Use Ext	ensible A	uthentic	ation Protoc	ol (EAP)		
						\sim
					Proper	ties
Allow the second sec	ece proto	cole				
C / NOW U	ese proto	0013				
🗸 Une	ncrypted p	asswor	d (PAP)			
Chal	lenge Har	ndshake	Authentica	tion Prot	ocol (CH/	AP)
Micr	osoft CHA	P Versi	on 2 (MS-CH	HAP v2)		
			my Window main, if any)		ame and	
1						

d Check the VPN connection status.

Regist Bo		andhang xwix yr cyfr
Contract line		
A REAL PROPERTY OF		
		Re Network
		age VHsConnection
		Convet
4 月田 2 田 台 白		Notwork & Internet settings Charge odlings, with an existing a suscentions restricts. xP ∧ T2 61 \$22,761 □
Windows Security	×	
Sign in		
User name		

Password	
ОК	Cancel



e If your PC cannot access internal devices (192.168.10.0/24) of the headquarters after the VPN connection is set up, add the following static route on your PC. The IP address 192.168.100.2 is the PC's IP address obtained from the headquarters. Then the PC can access internal devices of the headquarters.

C:\Users\Daisy>route add 192.168.168.10.0 mask 255.255.255.0 192.168.100.2

2. Site-to-Site Scenario Configuration

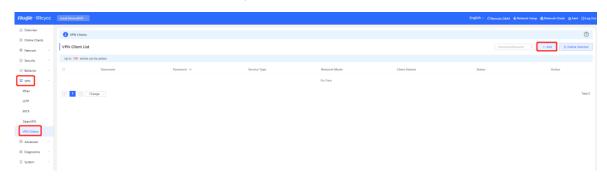
- (1) Headquarters side:
 - a Log in to the Reyee EG with the default IP address of 192.168.110.1.
 - b Switch to the Local mode. Choose VPN > PPTP.

Ruíjie &Rc	усс	Local Device(EG2 V
🖧 Overview		PPTP Settings Tunnel List
Ø Online Clients		PPTP Settings
Network	~	
Security	~	Enable 🕥
៣៍ Behavior	~	Save
🕏 VPN	^	
IPSec		
L2TP		
рртр		
OpenVPN		
VPN Clients		
🖻 Advanced	~	
Diagnostics Diagno	~	
🚉 System	~	

c Enable PPTP, set **PPTP Type** to **Server**, perform PPTP configuration, and click **Save**.

PPTP Settings Tunnel	List	
<i>i</i> PPTP Settings		
Enable		
РРТР Туре	 Server	
* Local Tunnel IP	192.168.100.1	
* IP Range	192.168.100.2-192.168.100.254	0
* DNS Server	8.8.8.8	
MPPE	Disable	
Flow Control	 Disable Enable 	
* PPP Hello Interval	10	
	Save	

d Choose Network > VPN Clients and configure VPN clients.



Add User		×
Service Type	ALL v	
* Username	Please enter a username.	
* Password	Please enter a password.	
Network Mode	PC to Router \checkmark	
Status		
	Cancel	к
Caution		

The value of **Peer Subnet** is the local IP address range of its branch.

(2) Branch side:

- a Log in to the Reyee EG with the default IP address of 192.168.110.1.
- b Switch to the Local mode. Choose VPN > PPTP, enable PPTP, and set PPTP Type to Client.

PPTP Settings Tunnel	List	
<i>i</i> PPTP Settings		
Enable		
РРТР Туре	Server O Client	
* Username	test	
* Password	•••••	
Interface	WAN ~	
Tunnel IP	• Dynamic O Static	
* Server Address	172.26.6.190	
* Server Subnet	192.168.110.0/24	+
MPPE	O Disable O Enable	
Work Mode	NAT O Router	
* PPP Hello Interval	10	
	Save	

A Caution

- PPTP Type: Select Client.
- Username and Password: Fill in the username and password that have been added in the headquarters.
- Tunnel IP: Select the address in the IP address range of the address pool filled in by the headquarters. If Dynamic is selected, the IP address of the address pool is assigned randomly. If Static is selected, any address in the address pool can be entered without conflicts.
- Server Address: Fill in the WAN port address of the headquarters. The public network IP address is required. Here, a private network address is just for reference.
- Peer Subnet: Specify the internal network segment of the headquarters. The value and internal network segment of the branch cannot overlap.
- Work Mode: Specify whether the headquarters is allowed to access the branch intranet. If so, select Router. If not, select NAT.
- c Check the VPN connection status.

PTP Set	tings Tunnel List							
() T	unnel List							(
								Delete Selecte
	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action

4.7.2 L2TP VPN

L2TP VPN is typically used in client-to-site and site-to-site scenarios. For example, clients work from home and need to access company server through L2TP VPN tunnels; a company has three branches that are distributed in three different places of the Internet, and each branch needs to establish a tunnel with each other through a router.

1. Client-to-Site Scenario Configuration

- (1) Headquarters side:
 - a Log in to the Reyee EG with the default IP address of 192.168.110.1.
 - b Switch to the Local mode. Choose VPN > L2TP.

Ruíjie	усс	Local Device(EG2 V
overview		L2TP Settings Tunnel List
Ø Online Clients		1 L2TP Settings
Network Network	~	
⊘ Security	×	Enable
☆i Behavior	~	Save
S VPN	^	
IPSec		
L2TP		
PPTP		
OpenVPN		
VPN Clients		
🖻 Advanced	ř	
Ø Diagnostics	ř	
:g= System	ř	

c Enable L2TP, perform L2TP configuration, and click **Save**.

L2TP Settings Tunnel	List	
<i>i</i> L2TP Settings		
Enable		
L2TP Type	• Server O Client	
* Local Tunnel IP	1.1.1.1	
* IP Range	1.1.1.2-1.1.1.100	0
* DNS Server	8.8.8.8	
Tunnel Authentication	• Disable 🔿 Enable	
IPSec Security	• Open Security ⊘	
Flow Control	• Disable 🔿 Enable	
* PPP Hello Interval	10	
	Save	

d Choose Local Device > VPN > VPN Clients and configure VPN clients.

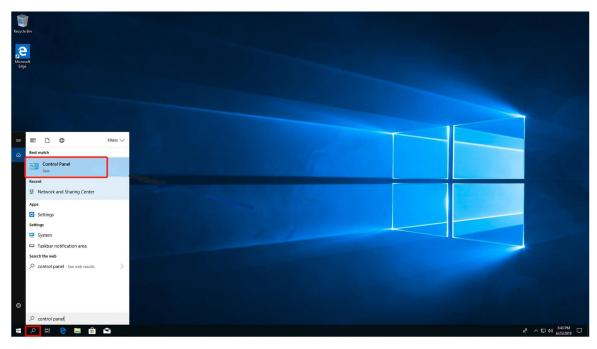
Cuijie ERcycc	Local Device(EG3 >	Currently in Local	Device mode.			English ∽ ∩ Remote C	86M 🔮 Network Setup @ Net	work Check
🖧 Overview	VPN Clients							0
Online Clients								
Network	VPN Client Lis	t				Username/Password C	+ Add 🗊 Delete	All Delete Selected
Security ~	Up to 300 entries	s can be added.						
11 Behavior 🗸		Username	Password 🥌	Service Type	Network Mode	Client Subnet	Status	Action
VPN ^					No Data			
IPSec	< 1 >	10/page V						Total 0
L2TP								
РРТР								
OpenVPN								
VPN Clients								
Advanced 🗸								
) Diagnostics 🗸 🗸								
🗄 System 🗸 🗸								

 \times

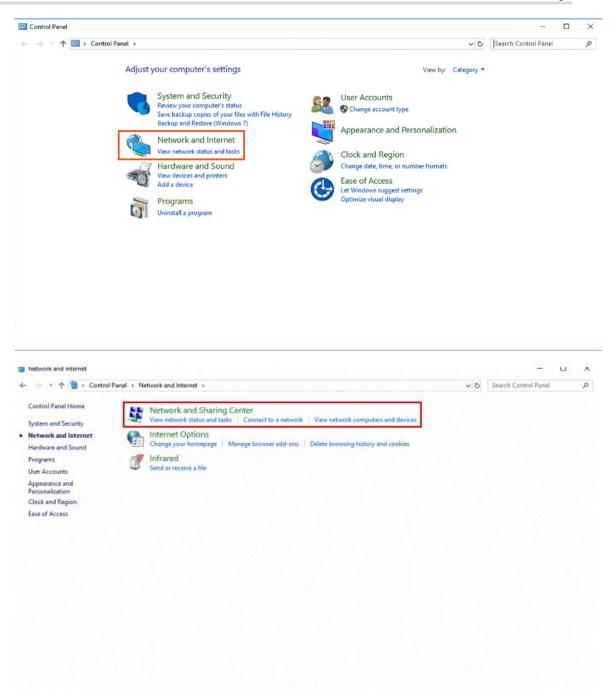
Add User

Service Type	OpenVpn ~	
* Username	admin	
* Password	Please enter a password.	
Status		
	Cancel	ОК

- (2) Client side (Windows 10 is used as an example):
 - a Choose Control Pane > Network and Internet > Network and Sharing Center.

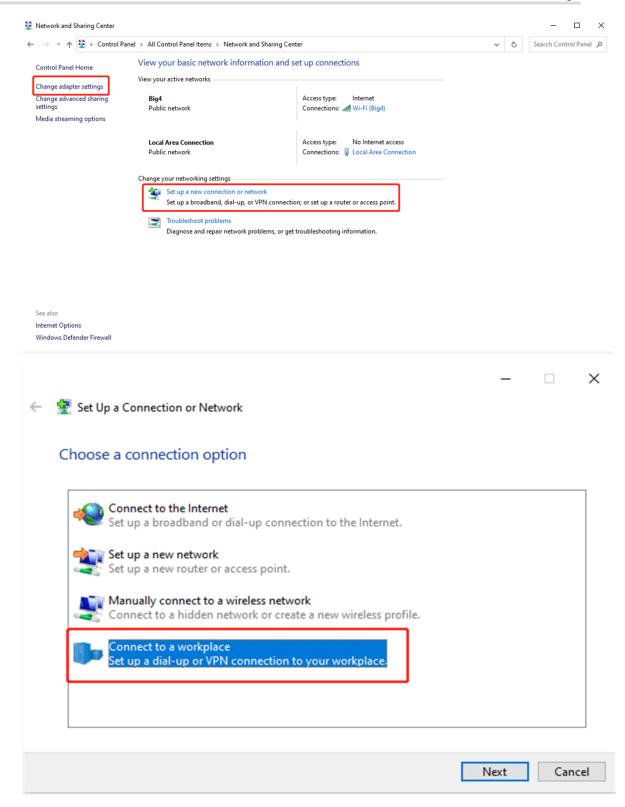


Common Settings



b Configure a VPN connection.

Common Settings



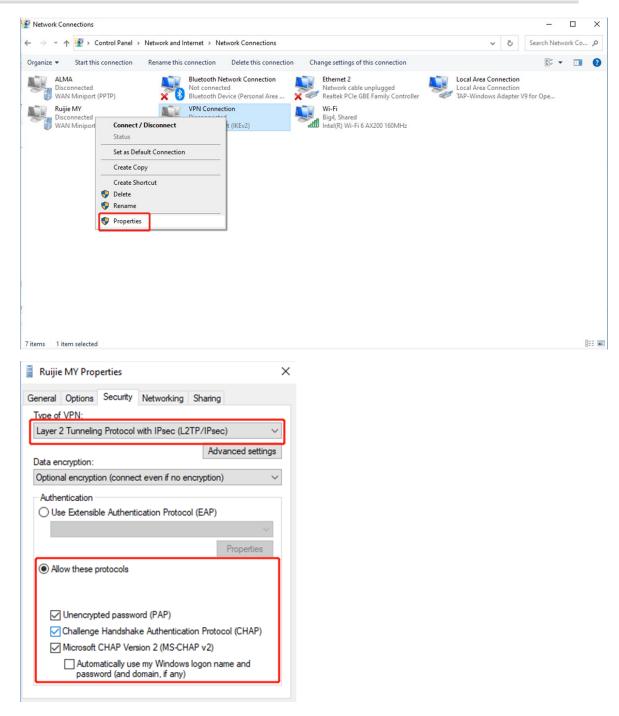
← 🔤 Connect to a Workplace	-		×
Do you want to use a connection that you already have?			
 No, create a new connection Yes, I'll choose an existing connection 			
Ruijie MY WAN Miniport (PPTP)			
ALMA WAN Miniport (PPTP)			
	Maria	6-7]
	Next	Can	cel
	_		×
🔶 🔣 Connect to a Workplace			
How do you want to connect?			
→ Use my Internet connection (VPN) Connect using a virtual private network (VPN) connection through the Intern	et.		
ių — 🎱 — ip			
 → Dial directly Connect directly to a phone number without going through the Internet. 			J
		Canc	

			-		×
🔶 🔚 Connect to a Workplace	e				
Type the Internet add	dress to conn	ect to			
Your network administrato	r can give you th	is address.			
Internet address:	172.26.6.190	The WAN IP of HQ			
Destination name:	VPN Connect	ion			
Use a smart card					
Remember my cree	dentials				
Allow other people					
This option allows	anyone with acce	ss to this computer to use this conn	ection.		
		Г	Create	Can	icel

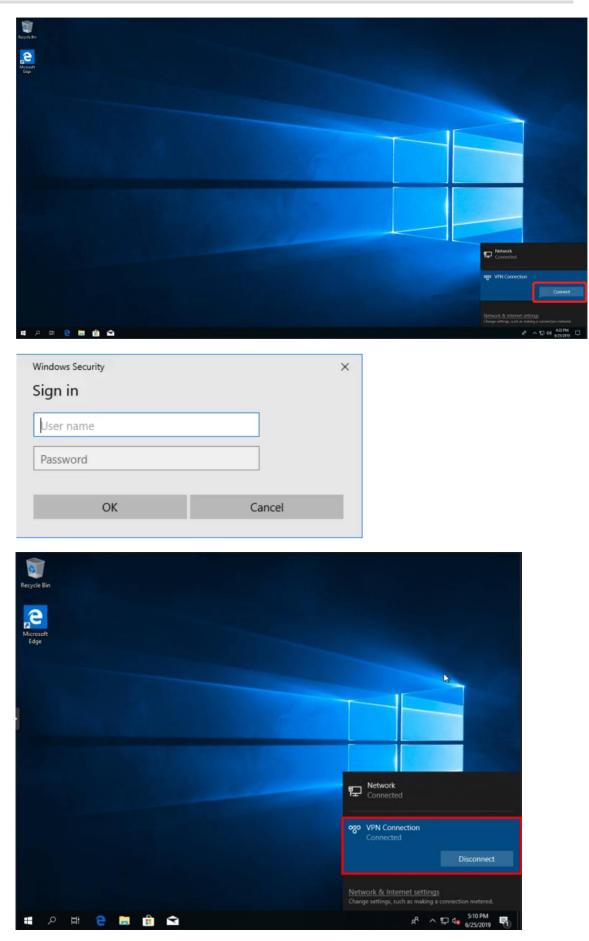
c Change adapter's settings.

Network and Sharing Center					- 0	×
\leftarrow \rightarrow \checkmark \uparrow 🛂 \Rightarrow Control Par	nel > All Control Panel Items > Network and Sharing Cent	er	~	õ	Search Control Pane	e p
Control Panel Home	et up connections					
Change adapter settings	View your active networks					
Change advanced sharing settings Media streaming options	Big4 Public network	Access type: Internet Connections: aff Wi-Fi (Big4)				
inclus scenning options	Local Area Connection Public network	Access type: No Internet access Connections: Use Local Area Connection				
	Change your networking settings					
	Set up a new connection or network Set up a broadband, dial-up, or VPN connection	n; or set up a router or access point.				
	Troubleshoot problems Diagnose and repair network problems, or get	troubleshooting information.				
See also Internet Options						
Windows Defender Firewall						

Common Settings



d Check the VPN connection status.



If your PC cannot access internal devices (192.168.10.0/24) of the headquarters after the VPN connection is set up, add the following static route on your PC. The IP address 192.168.100.2 is the PC's IP address obtained from the headquarters. Then the PC can access internal devices of the headquarters.

C:\Users\Daisy>route add 192.168.168.10.0 mask 255.255.255.0 192.168.100.2

2. Site-to-Site Scenario Configuration

- (1) Headquarters side:
 - a Log in to the Reyee EG with the default IP address of 192.168.110.1.
 - b Switch to the Local mode. Choose VPN >L2TP.

Ruíjie I Р	/CC	Local Device(EG2 V
용 Overview	1	
and Overview		L2TP Settings Tunnel List
③ Online Clients		
		1 L2TP Settings
Network	×	
⊘ Security	~	Enable
៣ Behavior	~	Save
🖶 VPN	^	
IPSec		
L2TP		
РРТР		
OpenVPN		
VPN Clients		
🗄 Advanced	~	
Diagnostics	~	
📰 System	~	

c Enable L2TP, set L2TP Type to Server, perform L2TP configuration, and click Save.

2TP Settings Tunnel	List	
1 L2TP Settings		
Enable		
L2TP Type	Server O Client	
* Local Tunnel IP	Example: 1.1.1.1	
* IP Range	Example: 1.1.1.2-1.1.1.100	0
* DNS Server	Example: 1.1.1.1	
Tunnel Authentication	Disable Enable	
IPSec Security	Open OSecurity	
Flow Control	O Disable O Enable	
* PPP Hello Interval	10	
	Save	

d Choose Network > VPN Clients and configure VPN clients.

TR TROYCE Local Device E02					English 🗸 🛆 Remote O&M 🔞) Network Setup 🔞 Network Check 🚊 Alert 🕞 Log
VPN Clients						Ø
VPN Client List					Username/Ra	oword O + Add @ Delete Selected
Up to 100 entries can be added.						
r 🗸 🔲 Userni	ame Password 🗸	Service Type	Network Mode	Client Subnet	Status	Action
			No Data			
< 1 > 10/page ~						Total 0
5						
• ·						

Add User	×
Service Type	ALL ~
* Username	Please enter a username.
* Password	Please enter a password.
Network Mode	Router to Router V
* Client Subnet	Example: 192.168.110.0/24
Status	
	Cancel

A Caution

The value of $\ensuremath{\text{Peer Subnet}}$ is the local IP address range of its branch.

- (2) Branch side:
 - a Log in to the Reyee EG with the default IP address of 192.168.110.1.
 - b Switch to the Local mode. Choose Gateway > VPN > L2TP, enable L2TP, and set L2TP Type to Client.

Ruíjie ARcycc	Local Device(EG2 \vee
Cverview	L2TP Settings Tunnel List
Online Clients	12TP Settings
 Network Security 	Enable
ាំា Behavior 🗸 🗸	L2TP Type 🔿 Server 💿 Client
🕏 VPN 🗠	* Username of L2TP user
IPSec	* Password of L2TP user
L2TP PPTP	Interface WAN \checkmark
OpenVPN	Tunnel IP O Dynamic 🔿 Static
VPN Clients	* Server Address IP/Domain
🗄 Advanced 🛛 🗸	* Server Subnet 192.168.110.0/24 +
	Tunnel Authentication O Disable O Enable
System	IPSec Security O Open O Security
	Work Mode 💿 NAT 🔷 Router
	* PPP Hello Interval 10
	Save

A Caution

- NAT: NAT is applied to incoming L2TP packets (the source IP address is replaced with the local virtual IP address).
- Router: Only incoming L2TP packets are routed.
- c Check the VPN connection status.

2TP Setti	ngs Tunnel List							
() Tu	innel List							0
								Delete Selected
	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
	test1	Client	l2tp	192.168.30.1	172.26.6.190	192.168.30.254	8.8.8	Delete

4.7.3 IPsec VPN

IPsec VPN is used for site-to-site scenarios. For example, three branches of a company are distributed in three different places of the internet; each branch uses a router to establish tunnels with each other; data between the company intranets (several PCs) is securely interconnected through the IPsec VPN tunnels established by through these routers.

IPsec VPN only applies to site-to-site scenarios.

- (1) Headquarters side:
 - a Log in to the Reyee EG with the default IP address of 192.168.110.1.
 - b Switch to the Local mode. Choose VPN > IPSec > IPSec Security Policy.

Rugie : IReyce	Local Device(002 V					English - Collemote OBM & Netwo	ek Setup 🔹 Network Check 🚊 Alert 🕞 Log Out
A Overview	Plac Security Policy Plac Connection	n Startus					
Online Clients							
© Network ~	IPSec Security Policy Note: Example: IP address/number of Tips If it is set to 132.168.110.j/24, the	subnet mask bits. address range is from 152.168.110.1 to 192.168.110.25	и				Ø
Security ~							_
til Behavior — ~	Policy List						+ Add
UPN -	Up to 1 entries can be added.						
_	Policy Type	Policy Name	Peer Gateway	Local Subnet	Peer Subnet	Status	Action
IPSec							
L2TP				No Data			
9979	< 1 > 10page -						Total 0
OpenVPN							
VPN Clients							
🖹 Advanced 🗸 🗸							
 Diagnostics 							
± System ~							

c Configure an IPsec VPN security policy.

Add		×
Policy Type	Client O Server	
* Policy Name	Length: 1-28 characters long.	
Interface	Auto \checkmark	0
* Local Subnet	Example: 192.168.110.0/24	
* Pre-shared Key		
Status		
	1. Set IKE Policy 2. Connection Policy	
	Cancel	ОК

1. Set IKE Policy								
	Authentication	Encryptio	n	DH Grou	h			
IKE Policy 1	sha1 V	3des	~][dh1	~			
IKE Policy 2	sha1 v	des	~	dh1	~			
IKE Policy 3	sha1 v	3des	~	dh2	~			
IKE Policy 4	md5 \vee	des	~	dh1	\sim			
IKE Policy 5	md5 \vee	3des	~	dh2	~			
	O Main Mode	🔿 Aggr	essive	Mode				
Mode								
Local ID Type	O IP 🔿 NA	ME						
Peer ID Type	OIP O NA	ME						
* Lifetime	86400							
DPD	• Enable C	Disable						
* DPD Interval	10							
	seconds							
	2. Connec	tion Policy -						
Transform Set 1	esp-sha1-aes	128						
Transform Set 2	esp-md5-3de	S		· · · · ·	~			
Perfect Forward	none			· · ·	~			
Secrecy								
* Lifetime	3600							
			Can	cel	ОК			

(2) Branch side:

- a Log in to the Reyee EG with the default IP address of 192.168.110.1.
- b Switch to the Local mode. Choose VPN > IPSec > IPSec Security Policy.

Ruffie IReyce	Local Device002						
A Overview	IFSec Security Policy IFSec Connection	n Status					
Online Clients Network	IPSec Security Policy	subnet mask bits.					Ø
© Security		address range is from 192.168.110.1 to 192.168.110.2	54.				_
rfl Behavior ~~~~	Policy List						+ Add
IPSec	Policy Type	Policy Name	Peer Gatemay	Local Subnet	Peer Subnet	Status	Action
LITP				No Data			
PPTP	< 1 > 10/page ~						Total D
OpenVPN VPN Clients							
Advanced ~							
R Diagnostics ~ ~							
🕃 System 🗸							

c Configure an IPsec policy. Ensure that the IKE policy and connection policy are the same on both sides.

Add		×
Policy Type	O Client O Server	
* Policy Name	test	
* Peer Gateway	172.26.6.93	+
Interface	Auto ~	0
* Local Subnet	192.168.10.0/24	
* Peer Subnet	192.168.113.0/24	+
* Pre-shared Key	ruijie123	
Status		

	1. Set IK	E Policy			
	Authentication	Encryption	DH Group		
IKE Policy 1	sha1 V	3des 🗸	dh1 V		
IKE Policy 2	sha1 v	des \lor	dh1 v		
IKE Policy 3	sha1 v	3des \vee	dh2 v		
IKE Policy 4	md5 v	des \vee	dh1 v		
IKE Policy 5	md5 v	3des 🗸	dh2 ∨		
Negotiation Mode	 Main Mode 	 Aggressiv 	ve Mode		
Local ID Type	IP O NAME				
Peer ID Type	OIP O NA	ME			
* Lifetime	86400				
DPD	• Enable 🔿 Disable				
* DPD Interval	10				
	seconds				
	2. Connect	tion Policy			
Transform Set 1	esp-sha1-aes1	28	~		
Transform Set 2	esp-md5-3des	5	~		
Perfect Forward	none		\sim		
Secrecy					
* Lifetime	3600				

d Check the IPsec connection status.

Ruíjie IRcycc	RyceNetwork	1⊃ ruijieEG	(Master) 🛈		English 🗸 💡	_ Ruijie Cloud	2 Download App	Network	k Setup	@Network Check	<u>洪</u> Warn	🕒 Log Out
2 Overview	Factor		Hostname: N	ijieEG 5N: EG3494257001	9	p: 17226.6.93						
(3) Online Clients	• EG105G-			2:D0:F8:15:08:43							0	Reboot
Router	Overview	$Basics ^{\vee}$	Security ~	Behavior \simeq Advanced \simeq	Diagnostics ~	System ~						
\heartsuit Wireless \checkmark	IPSec Security	Policy	PSec Conne	ction Status								
Switches	IPSec	Connection	Status									0
等Network ~	IPSec Co	nnection	Status								Q R	lefresh
	Name	SPI	Direction	Tunnel Endpoint		Flow		Status	Security Protoco		orithm	
	test	32285484 80	in	172.26.6.93<172.26.6.190	192.168.1	13.0/24 « 19	2.168.10.0/24	ОК	ESP	AH Authenti ESP Authenti ESP Se		
	test	32564381 10	out	172.26.6.93>172.26.6.190	192.168.1	13.0/24> 19	2.168.10.0/24	ОК	ESP	AH Authenti ESP Authenti ESP Se		
Collapse												

A Caution

If your headquarters EG has no public IP address configured for other external devices, you need to configure port mapping on external devices and configure **Local ID Type** as **NAME** on devices of the headquarters and branches.

4.7.4 L2TP Over IPsec VPN

L2TP over IPsec VPN is typically used in site-to-site and client-to-site scenarios. For example, three branches of a company are distributed in three different places of the Internet, each branch uses a router to establish tunnels with each other, and data between the company intranets (several PCs) is securely interconnected through L2TP over IPsec VPN tunnels established by these routers, the staff who work at home can access company data through L2TP over IPsec VPN tunnels.

- (1) Headquarters side:
 - a Log in to the Reyee EG with the default IP address of 192.168.110.1.
 - b Switch to the Local mode. Choose VPN > L2TP and configure IPsec Security.

Rujje	20211224 > EG105G-P-V2 (Muster) 0	English 🗸 🕜 Ruijie Cloud	鍵Download App - 会 Network Setup @ Netw	rork Check _ <u>芮</u> Warn 日 Default Password
န္မီOverview	Device Info	Wi-Fi		Setup>
(8) Online Clients	Hostname: EG105G-P-V2	J		
A Router	SN: F IP: 1/urcours EG105G-P-V2 MAC: 00:D0:F8:15:08:43	Primary Wi-Fi: 20211224 Security: Yes	Guest Wi-Fi: Security: No	
	Software Ver: ReyeeOS 1.55.1914			
E Switches				
Network	Net Status (Online Devices / Total)			Refresh Q
	Contraction → 0.00bps	↓ 0.00bps Switch - 0 / 0	····· ○ · · · · · · · · · · · · · · · · · · ·	0
	Internet Router	Switches		e Clients
	Real-Time Flow (Kbps)			Kbps \checkmark WAN \checkmark
	1	Uplink Flow Downlin	nk Flow	
	0.8			
	0.6			
				C.
	0.4			4
≪Collapse	0.2			

Ruíjie @Rcycc	Cloud_Auth_Test > EG1050	G-P [Master] 🛈	English ~	🛆 Ruijie Cloud	器Download App	ବ୍ଧ Network Setup	@Network Check	<u> </u>	🕞 Log Out
5° Overview		Hostname: EG105G-P	SN: H1PTATC0017	46	IP: 172.26.5.253				
(8) Online Clients	• EG105G-P	MAC: C0:B8:E6:35:28:3C							Reboot
Router	Overview Basics $^{\sim}$	Security \checkmark Behavior \checkmark	VPN ^ Advanced ~	Diagnostics	∨ System ∨				
	L2TP Settings Tunnel	List	IPSec						
🖻 Switches	<i>i</i> L2TP Settings		PPTP						0
$_{aa}^{*aa}$ Network	Enable		VPN Clients						
	L2TP Type	Server Client							
	* Local Address	10.0.0.1							
	* IP Range	10.0.0.2-10.0.0.254	0						
	* DNS Server	8.8.8.8							(? Ai
≪ Collapse									
Ruíjie I & Rcycc	Cloud_Auth_Test > EG1050	G-P [Master] 🛈	English ~	☐ Ruijie Cloud	靉Download App	会 Network Setup	@Network Check	<u>ក្តា</u> Warn	🕞 Log Out
Ruíjie கேcycc			English ~	🛆 Ruijie Cloud	器Download App	ବ୍ତ Network Setup	@ Network Check	<u> </u> Warn	🕞 Log Out
	Cloud_Auth_Test > EG1050 * DNS Server	G-P [Master] •	English ~	∩Ruijie Cloud	諁Download App	会 Network Setup	@ Network Check	<u>芮</u> Warn	ြ Log Out
overview			English ~	⊖Ruijie Cloud	諁Download App	骨 Network Setup	@Network Check	<u>ന്</u> Warn	₿Log Out
윤Overview ⑧Online Clients	* DNS Server	8.8.8.8	English ~	∩Ruijie Cloud	諸Download App		@Network Check	<u>ṁ</u> Warn	🔁 Log Out
ی Overview (© Online Clients) Router	* DNS Server	8.8.8.8 Security	English ~	⊂ Ruijie Cloud	譲Download App	€ Network Setup	@Network Check	<u>満</u> Warn	G Log Out
e [®] Overview ⊗ Online Clients ≧ Router ∻ Wireless ×	* DNS Server IPSec Security * Pre-shared Key	8.8.8.8 Security ruijie	English ~	⊖Ruijie Cloud	設Download App	မ္မွ Network Setup	@Network Check	<u>À</u> Warn	C Log Out
8 [°] Overview ® Online Clients ه Router ج Wireless ه Switches	* DNS Server IPSec Security * Pre-shared Key IKE Policy Transform Set	8.8.8.8 Security ruijie sha1-3des-dh1 esp-sha1-aes128		_ Ruijie Cloud	證Download App	∲ Network Setup	@Network Check	<u>済</u> Warn	⊖ Log Out
8 [°] Overview ® Online Clients ه Router ج Wireless ه Switches	* DNS Server IPSec Security * Pre-shared Key IKE Policy Transform Set Negotiation Mode	8.8.8.8 Security ruijie sha1-3des-dh1 esp-sha1-aes128 • Main Mode Ag	English ~	⊖Ruijie Cloud	證Download App	∲ Network Setup	@Network Check	<u>À</u> Warn	[] Log Out
8 [°] Overview ® Online Clients ه Router ج Wireless ه Switches	* DNS Server IPSec Security * Pre-shared Key IKE Policy Transform Set	8.8.8.8 Security ruijie sha1-3des-dh1 esp-sha1-aes128 • Main Mode Ag		_ Ruïjie Cloud	證Download App	ê Network Setup	@Network Check	<u>ਲ</u> ੱ Warn	⊖Log Out
8 [°] Overview ® Online Clients ه Router ج Wireless ه Switches	* DNS Server IPSec Security * Pre-shared Key IKE Policy Transform Set Negotiation Mode	8.8.8.8 Security ruijie sha1-3des-dh1 esp-sha1-aes128 • Main Mode Ag		_ Ruijie Cloud	諸Download App	Network Setup	@Network Check	<u>क</u> िं Warn	⊖ Log Out
8 [°] Overview ® Online Clients ه Router ج Wireless ه Switches	* DNS Server IPSec Security * Pre-shared Key IKE Policy Transform Set Negotiation Mode Local ID Type	8.8.8.8 Security ruijie sha1-3des-dh1 esp-sha1-aes128 Main Mode Ag IP NAME	y gressive Mode	⊖Ruijie Cloud	譲Download App	€ Network Setup	@Network Check	<u>ă</u> Warn	₽ Log Out

A Caution

- **PPP Hello Interval**: indicates the interval for sending hello messages on the PPP over IPsec connection.
- IPsec Security: indicates whether IPsec is used.
- **Pre-shared Key**: indicates the pre-shared key required for IPsec encryption.
- Local ID Type: When the WAN port of the headquarters is configured with the public IP address, select IP. When the WAN port of the headquarters is configured with the private IP address, select NAME and configure DMZ on the external device.
- c Configure VPN clients for the branch EG and PC.

Conversion Schware Winkies Conversion Winkies Conversion Conversion <t< th=""><th></th><th>Router</th><th>MAA</th><th>e: EG105G-P C: C0:B8:E6:35:28:3C</th><th>SN: H1PTATC001746</th><th>IP: 172.20</th><th>6.5.253</th><th></th><th>() Reboo</th></t<>		Router	MAA	e: EG105G-P C: C0:B8:E6:35:28:3C	SN: H1PTATC001746	IP: 172.20	6.5.253		() Reboo
Wirkels Bachabes Bachab					VPN ^ Advanced ~	Diagnostics ~ System	m ~		
Badaras Baranas Bar									
Network		<i>i</i> VPN Clier	nts						?
Version Personal Service Type Network Mode Pers Subart Sature Action is stat test L17P PC to Bours is sature Easter Easter <td></td> <td>VPN Client</td> <td>List</td> <td></td> <td></td> <td></td> <td></td> <td>+ Add</td> <td>Delete Selected</td>		VPN Client	List					+ Add	Delete Selected
isst ist L17 PC to Ruser Each Ed Deles isst ist ist P77 PC to Ruser Each Ed Deles isst ist ist P77 PC to Ruser Each Ed Deles isst ist ist P77 PC to Ruser Each Ed Deles isst ist ist P77 PC to Ruser Each Ed Deles ist ist ist P77 PC to Ruser Each Ed Deles ist ist ist P77 PC to Ruser Each Ed Deles ist ist ist ist P77 PC to Ruser Each Ed Deles ist ist ist ist P77 PC to Ruser Each Ed Deles ist ist ist ist ist P77 PC to Ruser Each Ed Deles ist ist ist ist ist P77 PC to Ruser Each Ed Deles ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist ist		Up to 32 entr	ries can be added.						
Nervice Collapse Collapse <td></td> <td>U</td> <td>sername</td> <td>Password</td> <td>Service Type</td> <td>Network Mode</td> <td>Peer Subnet</td> <td>Status</td> <td>Action</td>		U	sername	Password	Service Type	Network Mode	Peer Subnet	Status	Action
Collapse Collapse Col			test	test	L2TP	PC to Router		Enable	Edit Delete
			test1	test1	РРТР	PC to Router	-	Enable	Edit Delete
ZUTFC English _ Ohuyo Cloud @Download App @ Helenolt Stelps @ Welenolt Stelps @ Helenolt St			test2	test2	PPTP	PC to Router	-	Enable	Edit Delete
Bourier Bourier Wreiss Banke VPN Client List Upon 22 ontex can be addet Upon 22 on	≪Collapse								
Bourier Bourier Wreiss Banke VPN Client List Upon 22 ontex can be addet Upon 22 on									
Deniver Clears Besider Wirdeles Serice Type All Wirdeles Serice Type Username Besider VPN Client List Username Besider Center Besider VPN Client List Username Center Status Center VPN Client List Username Center Status Center Status Center Status Center VPN Client List Username VPN Client List Username Center VPN Client List Username Center Status Center VPN Client List Username VPN Client List Username Particle Status Service Type Ald User Service Type VPN Client List Username Particle Status Service Type VPN Client List Username Particle Status Service Type Username	Ruíjie i ⁽ Rcycc	Cloud_Auth_Test	> EG105G-P [Mas	iter] 0	English 🗸 📿	Ruijie Cloud 諁 Downl	oad App	etup @ Network Check	< <u> </u>
Sontine Clients Backer Wreises Backer VPN Client List Up to 32 entries can be abled. Backer Ugename Peer Subnet 192:158:10.002d Status Collage	Overview	Router	Hostnam				3		(1) Rehos
Wreiess Swite To Souther Boitches VPN Client List Up to 32 entites can be added Persound Network Username Retwork English - Obuje Cleud Retwork Kdd User Switches Formier Bouter VPN Client List Up to 32 entites can be added Personed Wreiess Service Type Bouter VPN Client List Up to 32 entites can be added Personed Wreiess Service Type Switches VPN Client List Up to 32 entites can be added Personed Wreiess Service Type Service Type AlL Username	Online Clients	EG105G-P		Add User			^		
Bavitches Bavitches VPN Client List Up to 32 entirs can be added Username Cancel OK Cancel OK	Router	Overview Ba	sics	Service Type	ALL				
E Network Wielers Status Action Courrier Basics Security Wreiess Bouter VPN Client List VPN Client List VPN Client List Courrier Basics Security Wreiess Bouter Courrier Basics Security Wreiess Bouter Courrier Basics Security Wreiess Bouter Courrier Basics Security Wreiess Bouter Courrier Basics Security Wreiess Bouter Courrier Basics Security Wreiess Bouter Courrier Basics Security Courrier Basics Security		🚺 VPN Clier	nts	* Username	Branch				0
Up to 32 entries can be added. Network Mode Revier to Router * Peer Subnet 132:168.10.0/24 Status Cancel OK Cancel OK Revier to Router Cancel OK Revier to Router English ~ @ Rujee Cloud @ Download App @ Network Check @ Wer Router Mark Add User Service Type ALL @ Revier @ VPN Clients * Username C * Username C * Username C @ VPN Clients Username C Service Type ALL * Username C @ VPN Clients Username C Service Type ALL * essond * essond <td>Switches</td> <td>VPN Client</td> <td>List</td> <td>* Password</td> <td></td> <td>\odot</td> <td></td> <td>+ Add</td> <td>Delete Selected</td>	Switches	VPN Client	List	* Password		\odot		+ Add	Delete Selected
Username * Peer Subnet \$status Action * Cellapue Cancel CK Retor Cancel CK Sonine Clients Fostname Add User Soviches VPN Client List Username PC Wrieless VPN Client List Username PC Username PC Username PC Switches Up to 32 entries can be added. Network Mode PC to Router Username PC Username PC Status Cto Router Status Cto Router	≟– ⊔-Network ⊻	Up to 32 entr	ries can be added.	Network Marke					
Kontere Cancel		Us	sername	Network Mode	Router to Router		Peer Subnet	Status	Action
Cancel Ox Currier Cound Auth, Test > EG105G-P English ~ Oragine Cloud Download App Antwork Check Marrier Contine Clients Image: Cound Auth, Test > EG105G-P Marrier Add User Image: Cound Auth, Test > EG105G-P Image: Cound Auth, Test				* Peer Subnet	192.168.10.0/24				
Source VPN Client List Up to 32 entries can be added. Up to 32 entries can be added. Status Status Status				Status					
Collapse Cloud Auth Test > EG105G-P Manael Courview © Online Clients Forther Basics Security Wireless © VPN Client List Wireless © VPN Client List Up to 32 entries can be added. Werview Username PC to Router Status Status									
Ruffe Cloud Coverview Souter Souter Wireless Wireless Wireless Wireless Wireless Wireless VPN Client List Up to 32 entries can be added. Username PC PC to Router Verview Mode PC to Router Status Status Status Status Status	// O. 11					Cancel OK			
% Overview © Online Clients © Overview Basics ~ Security © VPN Clients © VPN Clients © VPN Client List Up to 32 entries can be added. Up to 32 entries can be added. Network © Lisername Status	« Collapse								
Sonine Clients Bouter Coverview Basics & Security Switches VPN Client List Up to 32 entries can be added. Username Status Status Status	Reyce	Cloud_Auth_Test							
Online Clients EG105G-P Bouter Overview Basics & Security Wireless Ivpn Clients Switches VPN Client List Up to 32 entries can be added. Username Username Status Status Called PC and a status Called Add User Called Service Type ALL Called Service Type ALL Called PC Password Status Called Status Called Called Called Service Type ALL Called Service Type ALL Called Called Service Type Automatic Type Automatic Type Automatic Type Called Status Called Status Called Called Status Called	Overview		Hostname						
Service Type ALL Service Type ALL Service Type ALL Username PC Password + Add Delete Selected Network VPN Client List Up to 32 entries can be added. Username Username Status Status	Online Clients	EG105G-P		Add User			×		(U) Reboot
Switches Switches VPN Client List Password Up to 32 entries can be added. Network Mode PC to Router Status Status	Router	Overview Ba	sics 🌱 Security	Service Type	ALL				
VPN Client List Up to 32 entries can be added. Username Username Status Status	ি Wireless 🛛 👋	i VPN Clier	nts	* Username	PC				0
ENetwork V Up to 32 entries can be added. Username Status Status eer Subnet Status Action	Switches	VPN Client	List					+ Add	Delete Selected
Username Veer Subnet Status Action	Network	Up to 32 entr	ies can be added.	- Password	•••••	0			
		Us	ername	Network Mode	PC to Router	~	eer Subnet	Status	Action
Cancel				Status					
Cancel									
						Cancel			

PC to Router: A connection is established between a PC and a terminal.

<u>_</u>

• Router to Router: A direct, non-shared, and secure connection is set up between two terminals.

(2) Branch side:

- a Log in to the Reyee EG with the default IP address of 192.168.110.1.
- b Choose Setup > VPN > L2TP and enable IPsec Auth.

Ruíjie Rcycc	20211224 > EG105G-P-V2 (Mustor) 0	English ~ 🛛 Ruijie Cloud	歸Download App 🔮 Network Setup 🌘	資 Network Check 👸 Warn 🕞 Default Password
<mark>8</mark> Overview	Device Info	Wi-Fi		Setup>
Online Clients	Hostname: EG105G-P-V2			
A Router	SN: F IP: 17 Concession • EG105G-P-V2 MAC: 00:D0:F8:15:08:43	Primary Wi-Fi: 20211224 Security: Yes	Guest Wi-Fi: Security:	
	Software Ver: ReyeeOS 1.55.1914			
Switches				
:‰Network ∨	Net Status (Online Devices / Total)	↓ 0.00bps	令 0 / 0 APs	Refresh C 0 Online Clients
	Real-Time Flow (Kbps)			Kbps \checkmark WAN \checkmark
	1	Uplink Flow Downlinl	: Flow	
	0.8 -			
	0.5 -			
	0.4			
«Collapse	0.2			

Ruíjie l Rcycc	Cloud_Auth_Test > EG105G-P [Master] 0	English ~ _ CRuijie Cloud 뛟Download App	k Check <u> </u>
ం రాంగుల Clients	Hostname: EG105G-P MAC: C088:E6:35:28:34	SN: H1PTATC001746 IP: 172.26.5.253	() Reboot
A Router	EG105G-P MAC CUBCC0352034		
♥Wireless	L2TP Settings Tunnel List	IPSec	
Switches	<i>i</i> L2TP Settings	РРТР	0
-a- -a- -a- Network	Enable	VPN Clients	
	L2TP Type 🕓 Server 💽 Client		
	* Username Branch		
	* Password	\odot	
	Interface WAN		4
≪ Collapse			

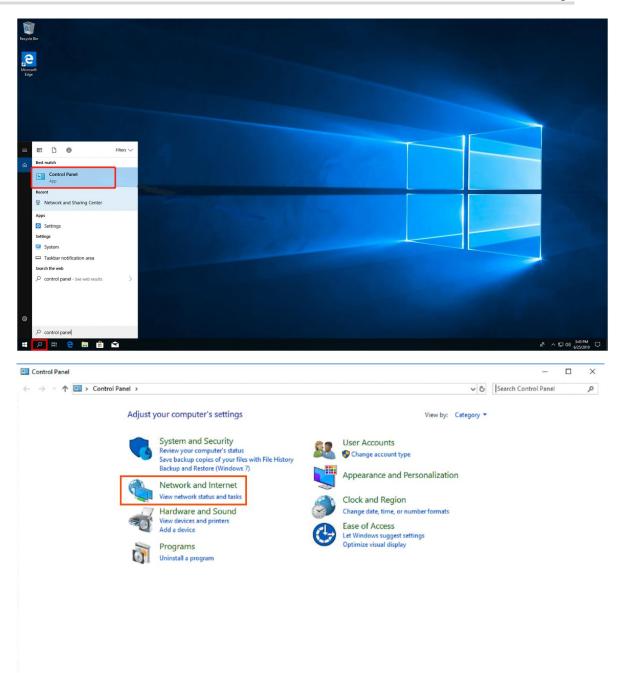
c Configure an IPsec security, and ensure that the values of **Pre-share Key**, **IKE Policy**, and **Transform Set** are the same on both sides.

ໄມເງົາຍ ໂຮຼດແດ	Local Device(EG2 >>
යි. Overview	Tunnel IP O Dynamic O Static
③ Online Clients	* Server Address IP/Domain
Network ·	* Server Subnet 192.168.110.0/24
⊘ Security ~	Tunnel Authentication O Disable O Enable
때 Behavior · ·	IPSec Security Open Security
😨 VPN 🔷	* Pre-shared Key ruijie
IPSec	IKE Policy sha1-3des-dh1 V
L2TP	
OpenVPN	Transform Set esp-sha1-aes128 ~
VPN Clients	Negotiation Mode O Main Mode O Aggressive Mode
Advanced	Peer ID Type O IP O NAME
Diagnostics	Work Mode 💿 NAT 🔗 Router
≟ System	PPP Hello Interval 10
	Save
	Save

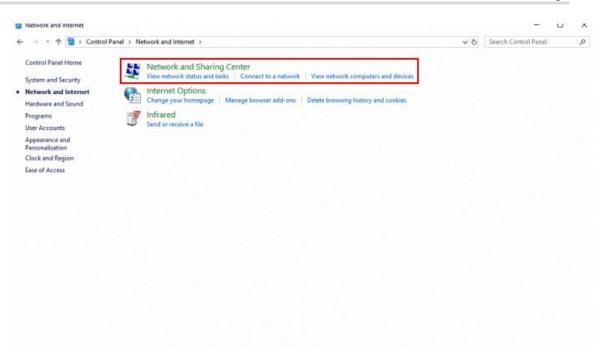
d Check the L2TP over IPsec connection status.

Rujje	GTAC_Reyee	ReyeeEG [Master	10		English ~	合 Ruijie Cloud 認Dow	mload App 🛛 🐣 Network S	Setup @Network Che	ck <u>済</u> Warn []Log
S Overview € Online Clients	Rout • EG10		ame: ReyeeEG //AC: EC:B9:70:17:39:35	SN: H1QH6RL04575	4 ip: 172.	26.5.46			(U) Reboot
Router	Overview	Basics ~ Secur	ity 🌱 Behavior 🌱 🚺	PN Y Advanced Y	Diagnostics ~ Syste	m ~			
≌Wireless ∨	L2TP Settin	gs Tunnel List							
≧ Switches	🥡 Tun	nnel List							0
Network									Delete Selected
		Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
		Branch	Client	l2tp	10.0.0.2	172.26.5.253	10.0.0.1	8.8.8	Delete
«Collapse									

- (3) Client side (Windows 10 is used as an example):
 - a Choose Control Panel > Network and Internet > Network and Sharing Center.



Common Settings



b Configure a VPN connection.

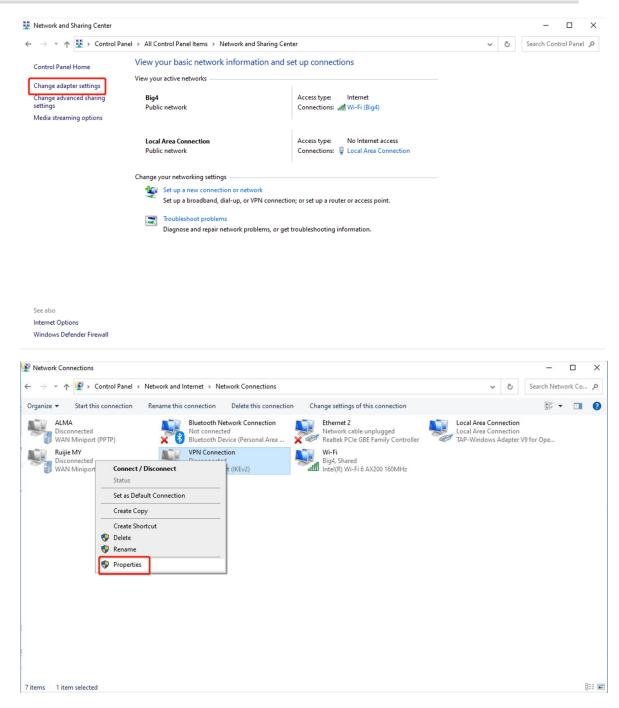
💱 Network and Sharing Center				– 🗆 ×
🗧 🔶 👻 🛧 💆 > Control Pa	anel > All Control Panel Items > Network and Sharing Co	enter	5 V	Search Control Panel 🔎
Control Panel Home	View your basic network information and	set up connections		
Change adapter settings	View your active networks			
Change advanced sharing settings Media streaming options	Big4 Public network	Access type: Internet Connections: and Wi-Fi (Big4)		
	Local Area Connection Public network	Access type: No Internet access Connections: Q Local Area Connection		
	Change your networking settings			
	Set up a new connection or network Set up a broadband, dial-up, or VPN connec	tion; or set up a router or access point.		
	Troubleshoot problems Diagnose and repair network problems, or g	et troubleshooting information.		
See also				
Internet Options				
Windows Defender Firewall				

_

 \leftarrow 💇 Set Up a Connection or Network Choose a connection option Connect to the Internet Set up a broadband or dial-up connection to the Internet. 📬 Set up a new network Set up a new router or access point. Manually connect to a wireless network Connect to a hidden network or create a new wireless profile. Connect to a workplace et up a dial-up or VPN connection to your workplace Next Cancel \times ← Connect to a Workplace Do you want to use a connection that you already have? No, create a new connection ○ Yes, I'll choose an existing connection Ruijie MY WAN Miniport (PPTP) Ruijie Demo WAN Miniport (PPTP) ALMA WAN Miniport (PPTP) Next Cancel

🗲 🛛 📊 Connect to a Workplace		_	
How do you want to	connect?		
→ Use my Internet Connect using a virtu	connection (VPN) al private network (VPN) connection through the Inter	net.	
I	- 🔮 — 🧊		
→ Dial directly Connect directly to a	phone number without going through the Internet.		
i 🦊 —	-		
			Cancel
← 🛛 🚛 Connect to a Workplace	2	-	
Type the Internet add	ress to connect to		
Your network administrator	can give you this address.		
Internet address:	172.26.6.190 The WAN IP of HQ		
Destination name:	VPN Connection		
Use a smart card			
Remember my cred	entials		
Allow other people This option allows a	to use this connection nyone with access to this computer to use this connec	tion.	
		Create	Cancel

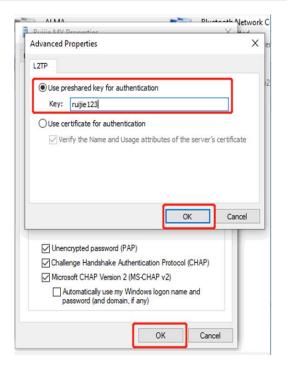
c Change adapter's settings.



neral Options	Security	Networking	Sharing)	
ype of VPN:					
Layer 2 Tunnelin	g Protocol	with IPsec (L2	TP/IPse	c)	~
			Ad	vanced settin	gs
)ata encryption:					
Optional encrypti	ion (connec	ct even if no e	ncryption	1)	~
Authentication					
	le Authent	ication Protoc	ol (EAP)		
				Properties	
Allow these r	protocols			Properties	
Allow these p	protocols			Properties	
Allow these p	protocols			Properties	
		ord (PAP)		Properties	
Unencryp	ted passw		ion Prote		
Unencryp	oted passwo e Handshak	ke Authenticat			
Unencryp Challenge Microsoft	oted passwo Handshak CHAP Ven	ke Authenticat sion 2 (MS-CH	AP v2)	ocol (CHAP)	
Unencryp Challenge Microsoft	oted passwo e Handshal CHAP Ven natically us	ke Authenticat	AP v2)	ocol (CHAP)	

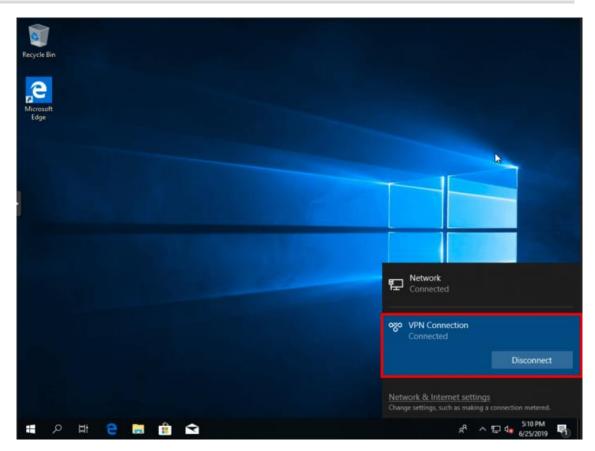
d Click Advanced Settings to configure the pre-shared password.

and a provide	Security Network	king Sharing	
Type of VPN:			
Layer 2 Tunnelin	g Protocol with IPse	ec (L2TP/IPsec)	~
Data encryption:		Advanced	settings
Optional encrypti	on (connect even if	no encryption)	~
Authentication			
O Use Extensib	le Authentication Pr	rotocol (EAP)	
		Proper	ties
Allow these p	protocols		_
Unencryp	ted password (PAP))	
Challenge	Handshake Auther	ntication Protocol (CH.	AP)
Microsoft	CHAP Version 2 (M	S-CHAP v2)	
	natically use my Win	dows logon name and any)	



e Set Network Mode to PC to Router.

Ruíjie ®Rcycc	Cloud_Auth_Test > EG105G-P Mass							
o Overview								
⊗ Online Clients	Roster Hostname EG105G-P MAC	Add User			×			() Reboot
Router	Overview Basics Y Security	Service Type	ALL		~			
ି Wireless 🗸 🗸	VPN Clients	* Username	PC					0
Switches	VPN Client List	* Password			\odot		+ Add	Delete Selected
-e-Network Y	Up to 32 entries can be added.	Network Mode	PC to Router		~			
	Username					eer Subnet	Status	Action
		Status						
				Cancel	ок			
								¢
≪ Collapse								



4.7.5 Open VPN

Open VPN is typically used in site-to-site and client-to-site scenarios. Open VPN is an application-layer VPN implementation based on the OpenSSL library. Compared with traditional VPN, open VPN is simple to use. VPN is a virtual private channel or a tunnel that provides secure data transmission between enterprises. Open VPN is full-featured SSL VPN that uses Layer 2 or Layer 3 secure network technology and industrial standard Secure Sockets Layer (SSL) or Transport Layer Security (TLS). SSL and TLS are security protocols that provide security and data integrity for network communications. Open VPN supports flexible client authorization modes, and supports certificates, usernames and passwords, allowing users to connect to the VPN through virtual interfaces. Open VPN is not the web proxy-based application or browser-based access.

- (1) Headquarters side:
 - a Log in to the Reyee EG with the default IP address of 192.168.110.1.
 - b Switch to the Local mode. Choose VPN > OpenVPN.

Ruijie I #Rc	ycc s	gw_eg310g-e > Ruijie 🜒
🖧 Overview		OpenVPN Tunnel List
③ Online Clients		() OpenVPN
Network	~	
⊘ Security	~	Enable
mi Behavior	~	Save
VPN	^	
IPSec		
L2TP		
РРТР		
OpenVPN		
VPN Clients		
🖴 Advanced	~	
Ø Diagnostics	~	
System	~	

c Enable **Open VPN** and configure VPN information.

		Collapse ·····	
TLS Authentication			
Allow Data Compression	Yes	~	0
Route All Traffic over VPN	Yes	~	0
Cipher	AES-128-CBC	~	0
Deliver DNS	192.168.5.28		€ +
Auth	SHA1		
Client Config	Export		
	Save		

OpenVPN Tunnel List			
Enable 🧲	D		
OpenVPN Type 💿	Server O Client		
Server Mode	Certificate \lor		
Protocol			
* Server Address	172.20.72.100		
* Port ID	1194	1-65535	
* IP Range	10.80.20.0/24	0	
Deliver Route	192.16.11.0	255.255.255.0	0+
Flow Control 💿	Disable O Enable		
	Expand		
Client Config	Export		
	Save		

- OpenVPN Type: Select Server or Client as needed
- Server Mode: Select an authentication mode.
 - o Account: You have to enter the correct account password, and import the CA certificate file on the client.
 - Certificate: You have to import the correct CA certificate, client certificate, and private key file on the client.
 - o Account & Certificate: You have to enter the correct account password and import the correct CA certificate, client certificate, and private key file on the client.
 - Protocol: Select TCP or UDP.
- Server Address: Enter the WAN IP address or domain name.
- Port ID: Use port 1194 by default.
- IP Range: Assign IP addresses in the range to clients.
- Deliver Route: The route of the client is used when the client accesses the intranet of the server.
- Advanced configuration:
- TLS authentication: A VPN connection is secured with the TLS key.
- Allow Data Compression: The value is Yes by default.

- Route All Traffic over VPN: The value is No by default.
- Cipher: You can select a data encryption algorithm. AES-128-CBC is used by default.
- **Deliver DNS**: A DNS address is assigned to a client.
- Auth: SHA1 is used by default.
 - d Click **Save** to save the configuration and click **Export** to export client configuration.

OpenVPN	Tunnel List				
🥑 Оре	enVPN				
	Enable 🧲	D			
0	penVPN Type 💿	Server O Client			
	Server Mode	Certificate	~		
	Protocol	UDP	~		
	* Server Address	172.20.72.100			
	* Port ID	1194		1-65535	
	* IP Range	10.80.20.0/24		0	
	Deliver Route	192.16.11.0		255.255.255.0	€+
	Flow Control 🧿	Disable O Enable			
	Client Config	Export			
		Save			

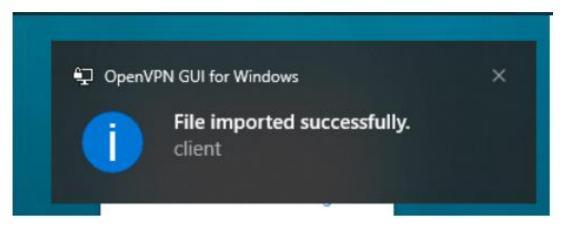
- (2) Client side (Windows 10 is used as example):
 - a Download and install OpenVPN application to your PC.

You can download OpenVPN client at <u>https://openvpn.net/community-downloads/</u>. Select a suitable version for your PC.

- b Import client configuration to the OpenVPN client after the OpenVPN client is installed on your PC.
- o Export the client configuration on the web page.
- Right-click **OpenVPN** and choose **Import** > **Import file...** to import the client configuration on the client.

Connect			
Disconnect			
Reconnect			
Show Status			
View Log			
Edit Config			
Clear Saved Passwords		-	
Import	>	Import file)
Settings		Import from A	ccess Server
Exit		Import from U	IRL
	🔶 💬	- 194 	

New fold	er			
ents 🖈 ^	Name	Date modified	Туре	Size
s 🖈	🧕 client.ovpn	3/10/2022 11:20 PM	OpenVPN Config	2 KB
e - Persor				



After the message "File Imported successfully" appears, you can connect to the VPN.

c Click **OpenVPN** and select **Connect**. If you use the account authentication method, enter your VPN account.

Cookbook

🗐 OpenVPN Connec	tion (client)			_		\times
Current State: Connect	ling					
Thu Mar 10 23:38:20 Thu Mar 10 23:38:20 Thu Mar 10 23:38:20 Thu Mar 10 23:38:20	🕥 client	×	ed. Compression -128-CBC' but i	missing in	data-cip	hers
Thu Mar 10 23:38:20 Thu Mar 10 23:38:20 Thu Mar 10 23:38:20 Thu Mar 10 23:38:20	Usemame: u11		SSL)] [LZO] [L er) 64bit 1, LZO 2.10 F_INET]127.0.0			010
Thu Mar 10 23:38:20 Thu Mar 10 23:38:21 Thu Mar 10 23:38:21 Thu Mar 10 23:38:21	Password:		e, waiting INET]127.0.0.1			
Thu Mar 10 23:38:21 Thu Mar 10 23:38:21 Thu Mar 10 23:38:21 Thu Mar 10 23:38:21	<u>O</u> K <u>C</u> ancel					
Thu Mar 10 23:38:21 Thu Mar 10 23:38:21	Connecting automatically in 2 seconds					
<						>
			OpenVPN	I GUI 11.2	26.0.0/2.5	5.5
Disconnect	Reconnect				Hide	

Current State: Connected			
Thu Mar 10 23:38:28 20 Thu Mar 10 23:38:28 20	22 interactive service msg_channel=80	18	^
	22 tap-windows6 device [OpenVPN TA	P-Windows61 opened	
	22 TAP-Windows Driver Version 9.24	in thildeneog opened	
	22 Set TAP-Windows TUN subnet mod		
	22 Notified TAP-Windows driver to set		
	22 Successful ARP Flush on interface		0D24535
	22 MANAGEMENT: >STATE:1646930		
	22 IPv4 MTU set to 1500 on interface 4 22 TEST ROUTES: 1/1 succeeded ler		
Tha Mai 10 20.00.00 20			
Thu Mar 10 23:38:30 20	22 MANAGEMENT: >STATE:1646930 22 C:\WINDOWS\system32\route.exe	310,ADD_ROUTES	5.255.0
Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20	22 MANAGEMENT: >STATE:1646930 22 C:\WINDOWS\system32\route.exe 22 Route addition via service succeed	310,ADD_ROUTES ADD 192.168.100.0 MASK 255.25	55. 2 55.0
Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20	22 MANAGEMENT: >STATE:1646930 22 C:\WINDOWS\system32\route.exe 22 Route addition via service succeed 22 Initialization Sequence Completed	1310,ADD_ROUTES ADD 192.168.100.0 MASK 255.25 ed	
Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20	22 MANAGEMENT: >STATE:1646930 22 C:\WINDOWS\system32\route.exe 22 Route addition via service succeed	1310,ADD_ROUTES ADD 192.168.100.0 MASK 255.25 ed	
Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20	22 MANAGEMENT: >STATE:1646930 22 C:\WINDOWS\system32\route.exe 22 Route addition via service succeed 22 Initialization Sequence Completed	1310,ADD_ROUTES ADD 192.168.100.0 MASK 255.25 ed	
Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20	22 MANAGEMENT: >STATE:1646930 22 C:\WINDOWS\system32\route.exe 22 Route addition via service succeed 22 Initialization Sequence Completed	1310,ADD_ROUTES ADD 192.168.100.0 MASK 255.25 ed	
Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20	22 MANAGEMENT: >STATE:1646930 22 C:\WINDOWS\system32\route.exe 22 Route addition via service succeed 22 Initialization Sequence Completed 22 MANAGEMENT: >STATE:1646930	1310,ADD_ROUTES, ADD 192.168.100.0 MASK 255.25 ed 1310,CONNECTED,SUCCESS,10.8	0.12.2,12
Thu Mar 10 23:38:30 20 Thu Mar 10 23:38:30 20	22 MANAGEMENT: >STATE:1646930 22 C:\WINDOWS\system32\route.exe 22 Route addition via service succeed 22 Initialization Sequence Completed 22 MANAGEMENT: >STATE:1646930	1310,ADD_ROUTES ADD 192.168.100.0 MASK 255.25 ed	0.12.2,12

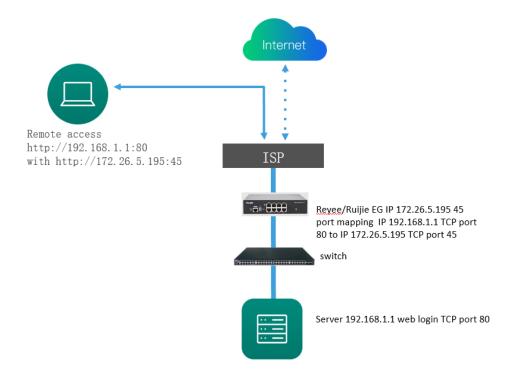
4.8 Port Mapping

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.

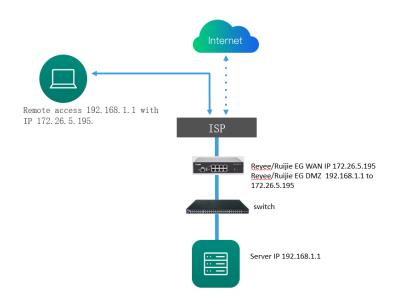
Port mapping enables users to access cameras or computers on their home networks when they are in companies or on a business trip.



• 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.



4.8.1 Configuring Port Mapping

- (1) Switch to the Local mode. Choose 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 Mappi	ng NAT-D	DMZ					
🪺 Por	t Mapping						?
Port M	apping List				(+ Add	Delete Selected
Up to 5	• entries can be	e added.					
	Name	Protocol	External IP Address	External Port	Internal IP Address	Internal Port	Action
	test	ТСР	172.26.1.200	3389	192.168.110.236	80	Edit Delete

Add		×
* Name		
Preferred Server	HTTP ~	
Protocol	TCP ~	
External IP Address	 Outbound Interface Enter or select an IP address. 	
	All WAN Ports \checkmark	
* External Port/Range	Example: X or X-X (Range: 1-6553	
* Internal IP Address	Example: 1.1.1.1	
* Internal Port/Range	80	
	Cancel	ж

Table 4-5 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.
External IP Address	Specify the host address used for accessing the external network. 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.

ОК

Parameter	Description
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.

4.8.2 Configuring NAT-DMZ

- (1) Switch to the Local mode. Choose 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.

Port Mapping	NAT-DMZ				
VAT-DMZ		and edit or delete the rule.			0
NAT-DMZ R	cule List			+ Add	Delete Selected
There are 3 ou	utbound interfaces. Up	to 3 rules can be added.			
	Name	Outbound Interface	Dest IP Address	Status	Action
	test	WAN1	192.168.110.222	Enable ⊘	Edit Delete

Add Rule			×
* Name			
* Dest IP Address	Example: 1.1.1.1		
Outbound Interface	WAN	~	
Status			
		Cancel	ОК

Table 4-1 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.

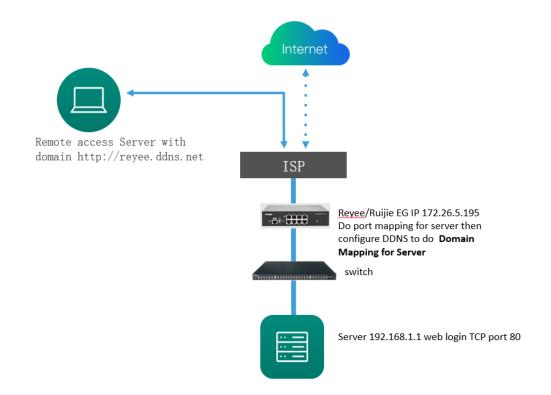
🛕 Caution

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

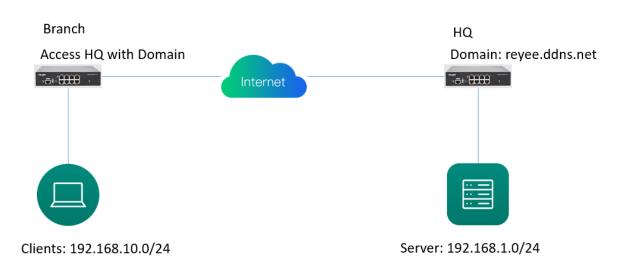
4.9 Dynamic DNS

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 Local mode. Choose Advanced > Dynamic DNS.

There are three DDNS servers you can choose to connect: Peanut Shell DDNS, NO-IP DNS, and DynDNS.

Ruíjie Rcycc	gw_eg310g-e > Ruijie Ø	English 🗸 🛆	Ruijie Cloud	設Download App	♦ Wizard	Network Check	述 Alert 🕞	Log Out
중 Overview	No-IP DNS DynDNS							
③ Online Clients	7 DynDNS							
Network	Uynuns							
⊘ Security ~	* Service Interface WAN \checkmark							
mî Behavlor ∨	* Username freelancedxb Register							
₩ VPN ~	* Password 🛛 💿							
🖻 Advanced 🗠	* Domain rulijedemo.dyndins.org							
Routing	Log in Delete							
PPPoE Server	Link Status Connecting ©							
Authentication	cinx status connecting to							
Session Limit								
Port Mapping								
Dynamic DNS								1
UPnP Settings								
Local DNS								

- (2) When Peanut Shell DDNS is used, you are advised to use WeChat or Peanut Shell to scan the QR code to register an account.
- (3) You can use the value of Domain to access the intranet server or headquarters device.

<i>Dynamic DNS</i> It is recommend	ed to use Peanut Shell for NAT, including 1	CP, UDP, HTTP and HTTPS mapping.
Dynamic DNS		
* Preferred Interface	WAN ~	0
* Username	15396042844	
* Password	•••••	
	Log In Delete	
Link Status	Connection success.	
Domain	emptynamea.vicp.net	

4.10 Authentication

4.10.1 Application Scenario

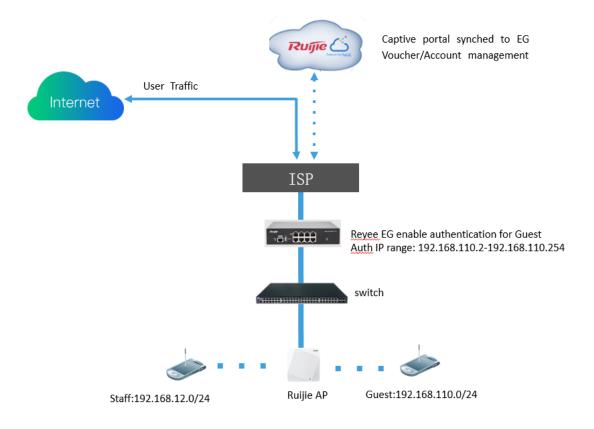
As wireless networks become popular, Wi-Fi has become one of the marketing means for merchants. Users can connect to Wi-Fi provided by the merchants to surf the Internet after watching advertisements or following WeChat official accounts. In addition, to defend against security vulnerabilities, a wireless office network usually allows only employees to associate with Wi-Fi, so identities of clients need to be verified.

The device uses portal authentication to implement information display and user management. After users connect to Wi-Fi, traffic is not routed to the Internet. Wi-Fi users must pass authentication at 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.

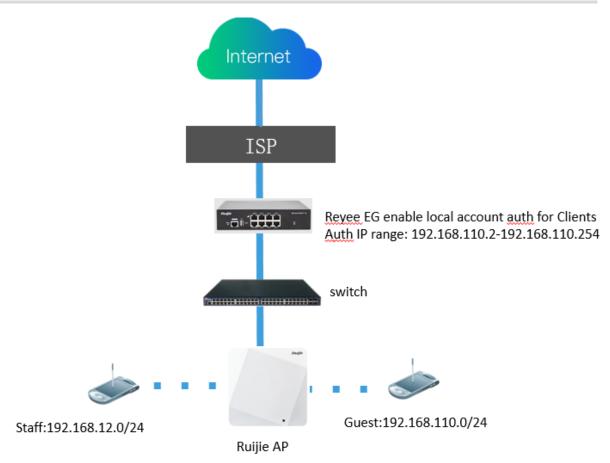
- (1) Before you enable Wi-Fi authentication, ensure that wireless signals are stable and users can connect to Wi-Fi and surf the Internet normally. The wireless SSID used for authentication on a network should be set to open. Encryption may lead to exceptions during Wi-Fi interconnection through authentication.
- (2) If the IP address of an AP on a network is within the authentication scope, add the AP as the authenticationfree user. For details, see section <u>4.2.10.7 Authentication-Free</u>.

- o On a Layer 2 network, add the MAC address of the AP to the authentication-free MAC address whitelist.
- o On a Layer 3 network, add the IP address of the AP to the authentication-free IP address whitelist.

• Cloud authentication scenario



• Local account authentication scenario



4.10.2 Cloud Authentication

Reyee EG devices support cloud portal authentication, including one-click, voucher, account, SMS (integration with Twilio) authentication modes.

(1) Configure cloud authentication on the cloud, and click the SN of the EG to access the page of EG details.



(2) Choose Config > Cloud Portal Auth.

Ruíjie 🝊		000
The second secon	Cloud Portal Auth ×	
A abcdefg@111.com V	AL	Take over Network Unbind Device
DASHBOARD	Auth @ O Arer you enable Cloud Portal Auth, it will be synced to the Reyee EG automatically.	
& TOPOLOGY	Save	0 S
逝 ALARM		
REPORT	Not EG1006-P	
Network	Operation Mode: Route Egress IP 120.35.11.195	Search
	Actual Master Device: H1QH6RL045754 MGMT IP 172.265.46 Network Master Device: IP11QH6RL045754 Firmware Version: ReveolS 1.55.1325	Action
E DEVICE	Description	Re-authorize. Delete
AP	Overview Config	5 🔺 1 in total
AC	Device Config	6
Switch		tefresh: 💽 😌 🖄 📰 = 😒
Gateway	Web CLI eWeb TELNET SSH Tunnel Reboot Cloud Portal Auth	SN, Alias, Description Q
Home Router		Sin, Alias, Description
Bridge	I IPTV	Model Description Action
A CAMERA		G105G-P Empty 1
	IPTV/VLAN IPTV/IGMP	10 🔺 1 in total
NVR	WAN LAN Disconnected Disabled PPPoE Static IP DHCP Copper SFP	
^(R) CLIENT	WAN LAW Disconnected Disabled Private Law	
	Dynamic DNS 🛛	

(3) Enter the value of Auth IP/Range for the user that needs to be authenticated before Internet access.

Ruíjie	MONITORING CONFIGURATION MAINTENANCE	e e e e
A abcdelg@111.com V	Cloud Portal Auth ×	Take over Network Unbind Device
DASHBOARD	Auth 🛛 🔍 After you enable Cloud Portal Auth, it will be synced to the Reyee EG automatically.	
8 TOPOLOGY	Portal Escape 🛛 🔍	0 X
逝 ALARM	Ng Auth IPiRange 192 168 120 2-192 168 120 254 +	
REPORT		Search
Network	Seamless Online @	
Voucher	User Offline Detection	Action Re-authorize_Delete
E DEVICE	Please select a portal or add a new portal.	
AP		5 * 1 in total
AC		<u></u>
Switch		tefresh: 💽 ↔ 🖄 📰 + 💥 🗍
Gateway	1	SN, Alias, Description Q
Home Router		Model Description Action
Bridge	1	G105G-P Empty
🕰 CAMERA		10 a 1 in total
Cameras		10 x Throat
NVR		
/R CLIENT		

Portal Escape: When the cloud server goes Down, this function enables clients to access the Internet directly without authentication.

Seamless Online: Users only need to pass the authentication once. If they want to go online again, authentication is not required. After users go online, they do not need to log in again in the specified period. You can choose **1 Day, 1 Week, 1 Month**, or **Always**.

User Offline Detection: Users do not access the Internet after the validity period.

(4) Click add a new portal to add a portal page.

Cookbook

Common Settings

Ruíjie 🝊	MONITORING CONFIGURATION MAINTENANCE	<mark>6</mark> 000	
Present for BACE	Captive Portal > Add	×	٩
	A	Take over Network Unbind Device	
DASHBOARD	Name test		
希 TOPOLOGY	Description	efresh: 🌉 다 🖄 🗮 👯	
濟 ALARM	Login Options 🖉 One-click Login 🖉 Voucher 🦉 Account 🗌 SMS 📄 Registration	cebook Account SN, Alias, Description Q	I
REPORT	The twillio account is not configured. Please click here to configure.	Model Description Action	I
		stosg-P Empty II	
	Show Balance Page 🖉 🔍	10 - 1 in total	
B DEVICE	Post-login URL @ https://www.ruijienetworks.com	8	-
	Portal Page 🛛		Ð
			2
	Basic Advanced Mobile	Desktop O Reset Style	
	Logo Picture @ Default Logo Upload		
	Background o Image O Solid Color	Ruffe 🖒	
A CAMERA	Background Image Default Image Upload		
	Voucher L	ogin	
	Languages English × + Access Cod	fe	
A CLIENT	Welcome Message • Text Image @	Logn	
	Text 60 characters remaining		
		One-click Login	

(5) Click the portal page to apply it and click **Save**.

Ruíjie	MONITORING CONFIGURATION MAINTENANCE	🗳 a e ® e•
A abcdeltp@111.com ~	Cloud Portal Auth	
	AL	Take over Network Unbind Device
DASHBOARD	Auth @ C After you enable Cloud Portal Auth, it will be synced to the Reyee EG automatically.	
希 TOPOLOGY	1 Portal Escape 🔞 🔍	lefresh: 💽 🤤 🖄 🏭 + 😫
逝 ALARM	Auth IPIRange 192.168.120.2-192.168.120.254 +	SN, Alias, Description Q
REPORT	1982 1991 1991 1991 1991 1991 1991 1991	Model Description Action
Network	Seamless Online 🛛 🔍 1 Day 🗸	G105G-P Empty II
Voucher	User Offline Detection	10 a 1 in total
B DEVICE	Please select a portal or add a new portal.	
AP	test	Ę
AC		Ę
Switch		
Gateway Home Router		
Bridge	O Voucher Login	
CAMERA	Access Code	
Cameras		
风 CLIENT	O Over dial (app	
INS GEIENT	Konet tage	

(6) If you use voucher or account authentication, choose Configuration > Voucher/Account to add a voucher or an account used for clients. Click Manage Package to add a package.

Ruíjie		0 3 8
A abcdefg@111.com ∨	Rulije-Hotel V Search Network Q (GMT+8:00)Asia/Shanghai Manage Project Take over Network	Unbind Device
PROJECT		
WIRELESS	Note: Reyee AP requires authentication on Reyee gateway. Please enable Cloud Auth on EG for Reyee devices. How to enable Cloud Auth on Reyee EG?	
Basic	Voucher O	₫ #+3
Layout Radio	Print Voucher Manage Package More Total Vouchers: 0 Activated Vouchers: 0 Depleted Vouchers 0: 0 Voucher Code, Alias, Packa Q Advant	anced Search \vee
Wi-Fi Optimization Ibeta	Voucher Code Alias Package Name Price Period Created at Activated at Expired at Devices Bind MAC Download Speed Upload Speed	Status
Roaming	No Data	
Bluetooth	First Previous Page 0 of 0 Next Last 10	0 in tota
Load Balancing		
AUTHENTICATION		
Captive Portal		
PPSK		
Voucher		
Account		
Easy Sharing		
ADVANCED		
Batch CLI Config		
Customize CLI Set		
AP VLAN		

(7) Click Add Package and fill in Price, Concurrent Devices, Bind MAC, Period, Download Speed, and Upload Speed.

Ruíjie	MONITORING CONFIGURATION				🗳 D 🛛 😵 🕒
A abcdelg@111.com ~	Ruijie-Hotel V Search Network Q	Add Package	X	T+8:00)Asia/Shanghai Manage Project	Take over Network Unbind Device
PROJECT		Package Name	test ·		
	Note: Reyee AP requires authentication on	Description			
Basic Lavout	Voucher > Manage Package	Price			⊕ #+ S
Radio	Add Package	Concurrent Devices	3 ~		Package Name Q
Wi-Fi Optimization	Package Name Des	Bind MAC		Download Speed	Upload Speed Action
Roaming		Period	30 Minutes V		
Bluetooth Load Balancing		Download Speed	1 Mbps v		10 🔺 0 in total
AUTHENTICATION		Upload Speed	1 Mbps v		10 • 0 in total 🕅
Captive Portal					
PPSK			CHERCH		
Voucher					
Account Easy Sharing					
ADVANCED					
Batch CLI Config					
Customize CLI Set					
AP VLAN					

(8) Click **Print Voucher** to add a voucher. Fill in **Quantity** and choose the package you add just now. Then click **Print.**

Common Settings

	MONITORING CONFIGURATION MAINTENANCE*	•e ® e a 🎴
 A abcdefg@111.com ∨ PROJECT WIRELESS 	Note: Neyee AP fegures authentication on Reyee gateway. Please enable Cloud Auth on EC for Reyee devices. <u>How to enable Cloud Auth on Reyee EC2</u> Voucher > Print Voucher	
Basic Layout Radio Wi-Fi Optimization	Print Configuration Profile Information on Voucher • Quantity You can select at most 4 parameters for the voucher. 1 Package Name Bind MAC Alias 020 Period • Package 2 Manage Package Voucher Code	
Cast Satariang AUTHENTICATION Captive Portal PPSK Voucher Account Easy Sharing	test ````````````````````````````````````	Ę C
ADVANCED Batch CLI Config Customize CLI Set AP VLAN	Print Method Print in 2 Columns (A4)	
Print Voucher Manage	Package More - • Total Vouchers: 1 • Activated Vouchers: 0 • Depleted Vouchers • : 0 Voucher Code, Alias, Packa Q	d Status
37tc7g	- test - 30 Minutes 2022-04-14 21:50:31 0/3 Yes 1.00 Mbps 1.00 Mbps	Not Activated
	First Previous Page 1 of 1 Next Last	10 🔺 1 in total

(9) Click **One-Click** to log in and perform authentication on the PC.

	auth	× +		-	٥	×
÷	\rightarrow C	🛦 不安全 portal.ruijienetworks.com/download/static/advertisement/maccauth/src/index.html?RES=//expand/res/mftzux6hv9xgic6 A 🏠	≨	Ē		
		Descisk Login or @ Account Login @ Voucher Login				

4.10.3 Local Account Authentication

Reyee EG devices provide local account authentication. The portal page and account are all created locally.

(1) Switch to the Local mode. Choose Advanced > Authentication > Local Account Auth, enable local account authentication, fill in Auth IP/IP Range, and click Save.

Rujje &Rcycc	Local Device(EG2 >>
A Overview	Cloud Auth Local Account Auth Authorized Auth QR Code Auth Whitelist Online Clients
Online Clients	Local Account Auth
Network	1. Enable account authentication and create an account.
⊘ Security ~	2. A user logs in with the account created in step 1 and will be allowed to access the Internet. Make sure that the device can access the Internet.Otherwise, the Portal page may not pop up on the terminal.
mî Behavior ∨	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 whitelist of Whitelist. 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 whitelist of Whitelist.
₽ VPN ✓	Local Account Auth
🖻 Advanced	Accounts 0
Routing	
PPPoE Server	* Network Type Layer-2 Network
Authentication	* Auth IP / IP Range 192.168.120.2-192.168.120 Add
Session Limit	Save

Auth IP/IP Range: The IP address of a client who needs to be authenticated. The value and other IP addresses for authentication cannot overlap.

(2) Add the account used by clients. Up to 200 accounts can be added.

Cloud Auth Local Account Auth Authorized Auth QR Code Auth Whitelist Online Clients				
Local Account Auth 1. Enable account suthentication and create an account.				
2. A user log in with the account created in typ: 3 and will be allowed to access the internet. Make sure that the device cara access the internet.Otherwise, the Portal page may not pop up on the terminal. In a layer-2 network, if the Packets of the EAM device is in the submiciation if many, please add its MAC address to the MAC address.	Add Account	×		0
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 w	t Usernami	Username		
Local Account Auth	* Password	d Password		
Accounts 0	At most o			
* Network Type Layer 2 Network V	Concurrent User	5		
* Augh # / # Range 192.148.1102-192.188.120 Add		Cancel OK		
Account Settings				+ Add 👔 Delete Selected
Up to 200 accounts can be added.				
Username Password		At most of Concurrent Users	MAC	Action

A Caution

The account can be used by multiple clients.

(3) Perform authentication on the PC. Generally, the portal page is displayed automatically. If the page is not displayed, try to enter 1.1.1.1 to redirect to the portal page. The page is displayed based on your browser language setting.

> C 🔺 Not secure http://192.168.120.1/guest_auth/pwdpage_en.html?gw_id=ecb970173935&gw_sn=H1QH6RL045754&gw_address=192.168	QK	☆ ☆		÷
R				
Please enter your username and password~				
Please enter username				
Please enter password				
Change Password				
Login				ł
Reset				Ţ

- ॰ ९ 🖻 🛧 🖪 😩 : $\leftarrow \ \ \, \rightarrow \ \ \, {\bf C} \quad \ \ \, {\bf A} \quad Not \ secure \ \ \, | \ \ http://192.168.120.1/guest_auth/pwdmodify_en.html?dis=0$ test1 ••••• Submit Reset Back ГІЕАЗЕ ЕПІЕГА ПЕМ РАЗЗМОГИ. Please enter the new password agair **Change Password Succeeded** Cubmit
- (4) Enter **username** and **password** obtained from a manager. To change the password, click **Change Password**.

(5) Enter the new username and password to log in. The page will appear automatically after you log in, and then you can access the Internet.

Ŗ,	
Please enter your username and password~	
test1	
Change Password	
Login	
Reset	

(6) Check online information on the EG.

RCYCC	Ruijie-Hotel > Ruijie (Martar) O						English ~	CRuijie Cloud	Download App	Network Setup	Q Network Chec	ck <u>∦i</u> Warn ⊡Log O
A Overview	• EG105G-P Overview Basics ~ Security ~		SN: H1		IP: 1 System ~	MAC: I	EC 35					() Reboot
⇔Wireless	Cloud Auth Local Account Auth	Authorized Auth	QR Code Auth	Whitelist	Online Clients]						
Switches	Online Clients											
≟Network ~	Auth Settings											
	Idle Client Timeout 15 N	tin (Range: 5-65535)					Search by IP Addre	15	~ Enter	Q	© Refresh	Delete Selected
	Save	tin (Range: 5-65535)		MAC		Up on		is tion(Sec)	C Enter Auth Tyr		© Refresh Status	Delete Selected Action
	Save		8 (MAC 2H	20		Dur			pe		
	Online Clients Username	IP	a (20	Up on	Dur	tion(Sec)	Auth Ty	pe	Status	Action

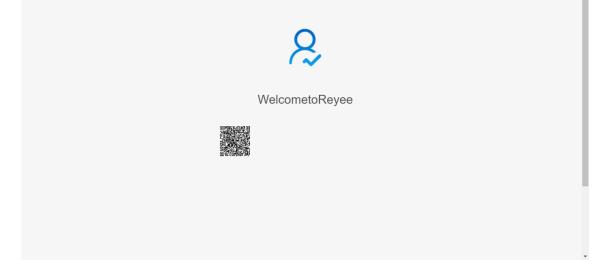
4.10.4 Authorized Authentication

Reyee EG devices supports **Authorized Auth**. When this function is enabled, an authenticated user can authorize guests by scanning the QR code.

 Switch to the Local mode. Choose Advanced > Authentication > Authorized Auth, and enable Authorized Auth.

Ruijie ເສັດຊາວດ	Local Device(EG2 🛇
ို Overview	Cloud Auth Local Account Auth Authorized Auth QR Code Auth Whitelist Online Clients
Ø Online Clients	Authorized Auth
Network ✓	An authenticated user can authorize guests by scanning his QR code.
⊘ Security ~	() 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 whitelist of Whitelist.
∭ Behavior 🗸	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 whitelist of Whitelist.
₽ VPN ~	Authorized Auth
🖹 Advanced	Popup Message
Routing	
PPPoE Server	* Auth IP / IP Range 192.168.110.2-192.168.110 Add
Authentication Session Limit	Limit Online Duration
Port Mapping	Duration Limit 60 minute
Dynamic DNS	* Authorization IP/IP 192.168.12.2-192.168.12.254 Range
UPnP Settings	- conge
Local DNS	Save

- Auth IP/IP Range: indicates the guest's IP address to be authenticated or range of guests' IP addresses to be authenticated.
- Limit Online Duration: indicates the online duration of a guest.
- o Authorization IP/IP: indicates the IP address of the authenticated user.
- (2) The following authentication portal page is displayed automatically after the guest is connected to the Internet.



(3) After the authorized client scans the QR code, the guest is authorized to access the Internet.

	8	
	Tips	
Authorization succeeded.		
	ОК	
		l

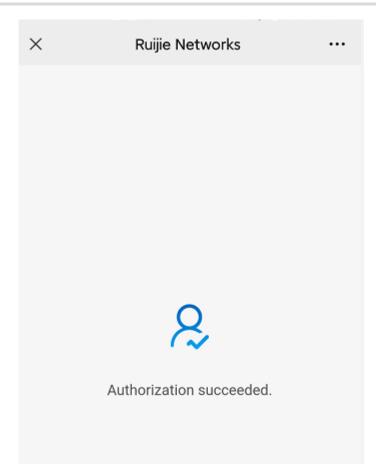
4.10.5 QR Code Authentication

Reyee EG devices support QR code authentication. This function enables a user to access the Internet by scanning the specified QR code.

 Switch to the Local mode. Choose Advanced > Authentication > QR Code Auth, and enable QR Code Auth.

Ruíjie &Rcycc	Local Device(E62 🗸
Cverview	Cloud Auth Local Account Auth Authorized Auth OR Code Auth Whitelist Online Clients
Ø Online Clients	QR Code Auth
Network	A user can access the Internet by scanning the specified QR code. Make sure that the device can access the Internet. Otherwise, the Portal page may not pop up on the terminal.
⊘ Security ∨	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 whitelist.
៣ Behavior ビ	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 whitelist of Whitelist.
👳 VPN 🗸	QR Code Auth
🗄 Advanced	* Auth IP / IP Range 192.168.110.2-192.168.110 Add
Routing	Limit Online Duration
PPPoE Server	* Duration Limit 60 minute
Authentication	QR Code Generator
Session Limit	* Dynamic QR defgrcode
Port Mapping	Popup Welcome to Revee
Dynamic DNS	Message
UPnP Settings	
Local DNS	Please print and paste the QR code for guests to scan.
TTL Rule	Save
Other Settings	

- Auth IP / IP Range: indicates the IP address of a guest.
- Limit Online Duration: indicates the online duration of a guest.
- o **QR Code Generator**: indicates the QR code used for guests to scan.



(2) The guest scan the QR code, and then can access the Internet.

4.10.6 Whitelist

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

Switch to the Local mode. Choose Advanced > Authentication > Whitelist, and add User Whitelist, IP
 Whitelist, URL Whitelist, MAC Whitelist, or MAC Blacklist.

Ruijie ເສັດຊາວດ	Local Device(62 -	English ~ 🛆 Remote O&M	I 会 Network Setup @ Network Check
\mathcal{E}_{δ} Overview	Cloud Auth Local Account Auth Authorized Auth QR Code Auth Whitelist Online Clie	nts	
③ Online Clients	A user configured with whitelisted IP or MAC address can access the Internet without authentication	yn.	
Network Security	User Whitelist		+ Add 🗈 Delete Selected
♂ Behavior	Up to 50 entries can be added.		
🗑 VPN 🗸	IP / I	IP Range	Action
🖻 Advanced		No Data	
Routing	< 1 > 10/page ~		Total 0
PPPoE Server Authentication	IP Whitelist		+ Add 🗊 Delete Selected
Session Limit	Up to 50 entries can be added.		
Port Mapping	IP / I	IP Range	Action
Dynamic DNS		No Data	
UPnP Settings	< 1 > I0/page ~		Total 0
1			

Ruijie I Rcycc	Local Device(EG2 ->		English 🗸 🛆 Remote O&M 🔮 Network Set	up @Network Check 凿Alert ⊟Log Out
a Overview	Cloud Auth Local Account Auth Authorized Auth QR Code Auth	Whitelist Online Clients		
Online Clients	A user configured with whitelisted IP or MAC address can access the	Add ×		
Network × Security ×	User Whitelist	* IP / IP Range Example: 1.1.1.1-1.1.100		+ Add 🗈 Delete Selected
ার্শ Behavior 🗸	Up to 50 entries can be added.			
🐺 VPN 🗸 🗸		Cancel		Action
🖻 Advanced 🔷 🔿		No Data		
Routing	< 1 > 10/page ~			Total 0
PPPoE Server	IP Whitelist			+ Add 🖻 Delete Selected
Session Limit	Up to 50 entries can be added.			
Port Mapping		IP / IP Range		Action
Dynamic DNS		No Data		
UPnP Settings	< 1 > 10/page >			Total 0

- User Whitelist: indicates that users can access the Internet without authentication. Up to 50 entries can be added.
- **IP Whitelist:** indicates that users can access an external IP address without authentication. Up to 50 entries can be added.
- URL Whitelist: indicates that users can access a URL without authentication. Up to 100 entries can be added.
- The following URL is the default URL added for cloud authentication.

URL Whitelist		+ Add 🖹 Delete Selected
Up to 100 entries can be added.		
	URL	Action
	ruijienetworks.com	Edit Delete

- **MAC Whitelist:** indicates that a user with the whitelisted MAC address can access the Internet without authentication. Up to 250 accounts can be added.
- MAC Blacklist: indicates that a user with the blacklisted MAC address is prevented from accessing the Internet.

4.10.7 Online Clients

1. Configuring the Idle Client Timeout

Switch to the Local mode. Choose Local Device > Advanced > Authentication > Online Clients.

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

Cloud Auth	Local Account Auth	Authorized Auth	QR Code Auth	Whitelist	Online Clients
i Online (Clients				
Auth Setti	ngs				
Idle Client Ti	meout 15	Min (Range: 5-65535)			
	Sav	e			

Idle Client Timeout: The idle client will be disconnected after 15 minutes. The value ranges from 5 to 65535, in minutes.

2. Disconnecting a User

The online client list displays information about all the current online clients, including the client IP address, client's MAC address, login time, and authentication mode. You can find 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 delete the client and end the Wi-Fi connection of the client.

Onlin	e Clients	Search by IP	Address	~ En	ter	Q	C Refresh	🗇 🗇 Dele	ete Selected
	Username	IP	MAC	Up on	Duration(Sec)) Au	th Type	Status	Action
				No Data					

4.10.8 WeChat 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 is displayed. Users need to switch to WeChat and follow the WeChat official account before they can access the Internet. WeChat authentication is applicable to the shopping mall scenario, where merchants guide customers to follow their WeChat official accounts through WeChat authentication.

2. Getting Started

- Connect Wi-Fi through WeChat that is a Layer 2 protocol. Ensure that the authentication device can obtain MAC addresses of the wireless users.
 - o The gateway address of wireless users to be authenticated is deployed on the authentication device.
 - If the gateway address is not deployed on the authentication device, the device functions as a DHCP server to allocate IP addresses to 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 WeChat Official Account platform and Ruijie Cloud platform before you enable authentication on the device. Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication, and one-click authentication. Log in to Ruijie Cloud to enable authentication.

Cloud /	Auth	Local Account Auth	Authorized Auth	QR Code Auth	Whitelist	Online Clients
	into Ruiji In a laye address In a laye	e Cloud to enable authentic r-2 network, if the IP addre whitelist of Whitelist.	ation View	in the authentication	ı IP range, pleas	d one-click authentication. Please log se add its MAC address to the MAC ⑦ se add its IP address to the IP

3. Configuration Steps

- (1) Switch to the Local mode. Choose Advanced > Authentication > Cloud Auth.
- (2) Enable WeChat authentication for Internet access.

Enable authentication, set Server Type to Connect Wi-Fi via WeChat, configure Network Type, Auth Server URL, Redirect IP, and Client Escape, and click Save.

Cloud Auth	Local Account Auth	Authorized Auth	QR Code Auth	Whitelist	Online Clients
into Rui into Ina lay address In a lay	ijie Cloud to enable auther rer-2 network, if the IP ad s whitelist of Whitelist.	ntication. View dress of the EAP device	is in the authenticati	on IP range, plea	nd one-click authentication. Please log use add its MAC address to the MAC (?) use add its IP address to the IP
	_				
Authen	tication				
* Netwo	ork Type Layer-2 Netw	vork	~		
* Serv	rer Type Connect Wi-	Fi via WeChat	~		
* Auth Serv	ver URL maccauth.rui	jie.com.cn			
Rec	direct IP 118.31.178.1	37			
Client	: Escape 🔽 Enable				
	Save				

Table 4-6 WeChat Authentication Configuration

Parameter	Description
Network Type	The default value is Layer-2 Network. Select a network type based on the actual network environment. Interconnection between Wi-Fi and the WeChat platform is performed on a Layer 2 network. On a Layer 3 network, you need to connect downlink devices to the current authentication device through the DHCP relay agent and deploy the DHCP address pool for authentication-engaged network segments on the authentication device. In this way, the authentication device can obtain MAC addresses of wireless users through DHCP. In this scenario, set this parameter to Layer-3 Network.
Server Type	Select Connect Wi-Fi via WeChat.
Auth Server URL	After you complete MACC server configuration, the MACC server returns a URL. The device sends an authentication request to this URL.
Redirect IP	The value corresponds to a menu or link address configured in the official account. The default value is 118.31.178.137. In most cases, you do not need to change the value. When a user is redirected to the WeChat official account, the user needs to visit this IP address before subsequent authentication.
Client Escape	After this function is enabled, the authentication function is disabled on the device if the authentication server fails, so that all the users can directly access the Internet. After the server recovers, the authentication function is enabled automatically.

(3) Configure the authentication scope.

Click **Add** on the current page. In the dialog box that appears, enter the SSID and IP address range that requires authentication, and click **OK**.

For clients (such as printers, computers, or some users) that do not require authentication, set **IP/IP Range** to authentication-free, so that these clients can directly access the Internet.

Wi-Fi List		+ Add 🗇 Delete Selected
Up to 8 entries can be added.		
SSID	IP/IP Range	Action
test	192.168.110.2-192.168.110.254	Edit Delete

 \times

Add

* SSID				
* IP/IP Range	Example: 1.1.1.1-1.1.1.00		Add	
		Car	ncel	ОК

4. Verifying Configuration

When a mobile phone connects to the specific Wi-Fi, the portal authentication page pops up automatically. The user visits the WeChat page under instructions on the portal authentication page, follows the WeChat official account, clicks the menu or auto reply link to complete authentication. Then the user can normally access the Internet. After successful user authentication, you can choose **Advanced > Authentication > Online Clients** to view information about this authenticated user. For details, see section 错误!未找到引用

源。错误!未找到引用源。

5. Troubleshooting

• When a user clicks the authentication menu or link in the official account during WeChat authentication, the message "**This page cannot be accessed now.**" is displayed, leading to an authentication failure.



This page cannot be accessed

now.

Cause: The link address configured in the official account authentication entry on the official account Platform is regarded as insecure by Security Center of the WeChat client. When a client sends a request to this address, WeChat blocks this request.

Solution: Change the forced redirection address and the address in the official account authentication menu or link to an IP address not used on the LAN. For example, if the network segment 172.29.0.0 is not used on the LAN, set both the official account redirection IP address and the link address in the official account to 172.29.1.140.

🛕 Caution

If the official account redirection IP address is set to an IP address in a network segment used on the LAN, WeChat authentication will fail.

Authentication		
* Network Type	Layer-2 Network	~
* Server Type	Connect Wi-Fi via We	Chat ~
* Auth Server URL	maccauth.ruijie.com.c	n
Redirect IP	172.29.1.140	
Client Escape	Enable	
	Save	

4.10.9 Enterprise WeChat Authentication

1. Overview

Similar to WeChat authentication, Wi-Fi users need to switch to the enterprise WeChat after connecting to Wi-Fi and complete applet authentication in the workspace before they can access the Internet. Enterprise WeChat authentication can be used to manage Internet access of employees and guests in the enterprise environment.

2. Getting Started

The operations are the same as those in section 错误!未找到引用源。_错误!未找到引用源。_.Before you enable enterprise WeChat authentication, complete relevant configurations on the enterprise WeChat console and Ruijie Cloud platform.

3. Configuration Steps

Switch to the Local mode. Choose Advanced > Authentication > Cloud Auth.

The configuration steps are similar to those in WeChat authentication. The major difference is that the official account redirection IP address in enterprise WeChat authentication must be set to 47.104.189.180:81. For details, see section <u>错误!未找到引用源。错误!未找到引用源。</u>.

Cloud Au	uth Local A	ccount Auth	Authorized Auth	QR Code Auth	Whitelist	Online Clients
		orts voucher authe to enable authentic		authentication, SMS a	uthentication an	d one-click authentication. Please log
	n a layer-2 netw Iddress whitelist		ess of the EAP device is	in the authentication	n IP range, plea	se add its MAC address to the MAC?
	n a layer-3 netw ddress whitelist		ess of the EAP device is	in the authentication	n IP range, plea	se add its IP address to the IP
A	uthentication					
* N	Network Type	Layer-2 Networ	k	~		
	* Server Type	Connect Wi-Fi v	ria WeChat	~		
* Aut	th Server URL	maccauth.ruijie	com.cn			
	Redirect IP	47.104.189.180:	81			
	Client Escape	Enable				
	l	Save				

Employee Authentication

Make sure that employees have joined the enterprise WeChat organization. When an employee connects a mobile phone to Wi-Fi, the employee is automatically redirected to the enterprise WeChat for authentication. After the employee opens the enterprise WeChat, the employee needs to access the **Workspace** menu of the enterprise WeChat and click the authentication app created by the administrator to obtain an Internet access permission. After the authentication success message is displayed, the employee can access the Internet normally.

The enterprise WeChat may not be started on the portal authentication page on some mobile phones due to low compatibility. In this case, users can manually open the enterprise WeChat and continue follow-up operations.

Guest Authentication

When a guest visits an enterprise, the employee can authorize the guest to connect to the Wi-Fi network of the enterprise. After the guest connects to the guest Wi-Fi, the authentication QR code is displayed. At this time, the authenticated employee scans the QR code using the enterprise WeChat on the mobile phone and enters the guest name. Then the guest can pass authentication and access the Internet normally.

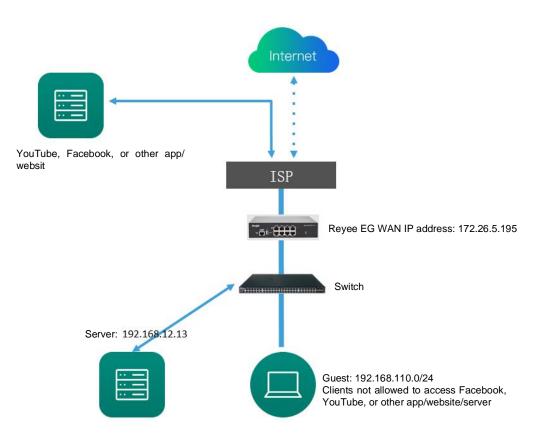
When configuring guest authentication, you need to configure at least two Wi-Fi SSIDs and corresponding network segments in the Wi-Fi list, which are used for employee and guest connections, respectively.

Wi-	Fi List		+ Add Delete Selected
Up t	o 8 entries can be added.		
	SSID	IP/IP Range	Action
	test	192.168.110.2-192.168.110.254	Edit Delete
	@Ruijie-guest-2277	192.168.111.2-192.168.111.254	Edit Delete

4.11 Behavior

4.11.1 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.



4.11.2 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 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.

A 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.

i App Control					0
App Control				+ Add	Delete Selected
Up to 50 entries can be added.					
IP Address Group	Time	Blocked App	Status	Remark	Action
		No Data			

(3) Configure App Control.

Click Add to create an App control policy.

	App Control					?
Арр	Control	⑦ App	lication Library Version:	International	- + Add	Delete Selected
Up to	50 entries can be adde	d.				
	User Group	Time	Blocked App	Status	Remark	Action
	1.1.1.1-1.1.1.254	All Time 🛗	Play	Enable ⊘		Edit Delete

Add App			×
IP Address Group	test user	~	
Time	test	~	
* Blocked App	Select	•	
Remark	Please select at least one test		
Status			
		Cancel	ОК

Add				>
	Туре	User Group		
	* User Group	Select	-	0
	Time	All Time	~	
	* Blocked App	Select	-	
	Remarks			
	Status			

Cancel

OK

Parameter	Description
Туре	 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. For details on how to configure a user group list, see section <u>6.2 User Management</u> . 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.

Parameter	Description
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.
Blocked App	Specify the apps or app groups to be blocked.
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 Behavior > App Control > Application Library Update.

A 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.

App Control	Application Library Upda	Custor	m			
<i>i</i> There is s	sufficient flash memory a	and system m	emory for upd	ating the application	on library.	
Current Version	2022.08.17.22.08.17(V2.0)				
File Path	Please select a file.	Browse	Upload			

- (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.

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 Behavior > App Control > Custom.
- (2) Switch the application library.

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.

A 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.

App Control	Application Library Update	Custom					
🥖 Custon	n						
Custom				Application Library Version	n: International	p Q + Add	Delete Selected
Up to 500	entries can be added.				China		
	Арр	Protocol Type	Source IP	Destination IP	International	Destination Port	Action
				No Data			
< 1	> 10/page V						Total 0

(3) Click Add. Enter information about a custom app.

App Control	Application Library Update	Custom						
🥡 Custom			Add App		×			
Custom			* App			۲ International ۲ App	Add + Add	Delete Selected
Up to 500 en	tries can be added.		Protocol Type	TCP \lor				
	Арр	Protocol Type	Control Type	Dest IP + Dest Port ~		Source Port	Destination Port	Action
_			* Destination IP	Enter Manually Auto Assign				
< 1 >	10/page 🗸			Example: 1.1.1.1 or 1.1.1.1-1.1.1.10	0			Total 0
			* Destination Port	Enter Manually Auto Assign Example: X or X-X (Range: 1-6553!				
				Cancel	ОК			

Parameter	Description
Арр	Configure the app name (the name must be unique in the app list).
Protocol Type	Select a protocol type based on the protocol used by obtained packets. It can be set to TCP, UDP, or IP.
	Select a rule type based on 5-tuple information of extracted packets. It can be set to the following:
Control Type	Src IP + Src Port
	Dest IP + Dest Port
	Src IP + Dest IP
Source/Destination IP	Enter the source or destination IP address.

Parameter	Description
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 错误!未找到引用源。错误!未找到引用

<u>源。</u>.

Try to access Facebook on the guest PC. Then you will find the access failure.

8	
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

4.11.3 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 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.

A 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 Filterin	ng Website Group			
	te Group oup member can be a complete	URL (example: www.baidu.com) or a domain (example:	*.56.com).	0
Website G	Group		+ Add	Delete Selected
Up to 20 e	ntries can be added.			
	Group Name	Member	Ac	tion
	Games	duowan.com More	Edit	Delete
	Finance	*.10jqka.com.cn More	Edit	Delete
	Social	*.baihe.com More	Edit	Delete
	Shopping	*.taobao.com More	Edit	Delete
	Life	*.55bbs.com More	Edit	Delete

Add Group

 \times

* Group Name	test		
* Member	*.56.com www.google.com		
			li
		Cancel	ОК

Parameter	Description
Group Name	Configure a unique name for a website group. The name can be a string of 1 to 64 characters.

Parameter	Description
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 Gateway > 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.

Website F	Filtering We	bsite Group					
<i>i</i> w	/ebsite Filtering						?
Webs	ite Filtering					+ Add	Delete Selected
Up to	20 entries can b	e added.					
	IP Address Group	Control Type	Blocked Website	Time	Status	Remark	Action
	test user 🕧	Your request is forbidden.	Games	test 🚞	Enable ⊘	test	Edit Delete

 \times

ЭK

Add Website Filtering

IP Address Group	test user	~	
Time	test	~	
* Blocked Website	Games ×	× •	
Remark	test		
Status			
		Cancel	(

Parameter	Description
Туре	 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. For details on how to configure a user group list, see section <u>6.2 User Management</u> . 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. For details on how to create or modify a website group, see 错误!未找到引用源。.
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.

Details

Ĥ		
This	••	

This site can't be reached
www.facebook.com took too long to respond.

Try:
Checking the connectionChecking the proxy and the firewall
Running Windows Network Diagnostics
ERR_CONNECTION_TIMED_OUT
Reload

4.11.4 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 Behavior > Access Control.

The access control rule list displays the created access control rules. Click **Add** to add an access control rule.

	ACL Configure ACL based on IP addresses. Reverse flow mismatches. The policy cannot take effect on the WAN port to block the traffic among the internal users between an L2TP server and an L2TP client. The policy only takes effect in the LAN 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								
	Fip: Configure one more deny ACL entr	y containing source	- Fraddiess (52.100.2.0) E		The address TSE. For	_			
ACL	 50 entries can be added. 						+ Add	J Delete Selected	
	Rule	Control Type	Wireless Schedule	Interface	Effective State	Remark	Match Order	Action	
	Src IP Address 192.168.1.1/24 : 20 Dest IP Address 192.168.2.2 : 30 Protocol TCP	Block	test	WAN	Inactive 9		1	Edit Delete	
	MAC 11:11:11:11:11	Block	All Time	WAN	Active		1	Edit Delete	

Table 4-9 Access Control Rule Information

Parameter	Description
Effective State	Indicate whether a rule takes effect. If Inactive is displayed, the current system time may be not in the effective time range. Move the cursor to ⁹ to view the detailed cause.
Match Order	All the created ACL rules are displayed in the ACL list, with the latest rule listed on the top. The device matches 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			×
Based on	MAC O IP		
* MAC	Enter a MAC address.		
Control Type	Block	~	
Wireless Schedule	All Time	~	
Remark	Enter the ACL purpose.		
		Cancel	ОК

Table 4-10 MAC Address-based ACL Configuration

Parameter	Description
MAC	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. Allow: Permit the data packets matching the conditions. Block: Drop the data packets matching the conditions.
Wireless Schedule	You can select a time range from the drop-down list box, or select Custom and manually enter the specific time range.
Remark	Enter the rule description, which is used to uniquely identify a rule.

(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**.

A 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
Auu	nuic

Based on	O MAC 💿 IP				
Src IP Address: Port	Net:192.168.1.1/24 : 1-65535				
Dest IP Address: Port	Net:192.168.1.1/24	1-65535			
Protocol Type	All Protocols ~				
Control Type	Block (Reverse flow mismatches) \sim				
Wireless Schedule	All Time		\sim		
Interface	WAN		~		
Remark	Enter the ACL purpose.				

Table 4-11 IP Address-based ACL Configuration

Parameter	Description
Src IP Address: Port	Enter the source IP address and port number 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).
Dest IP Address: Port	Enter the destination IP address and port number 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 TCP , UDP , and ICMP .
Control Type	 Specify the method for processing data packets matching conditions. 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.

Cancel

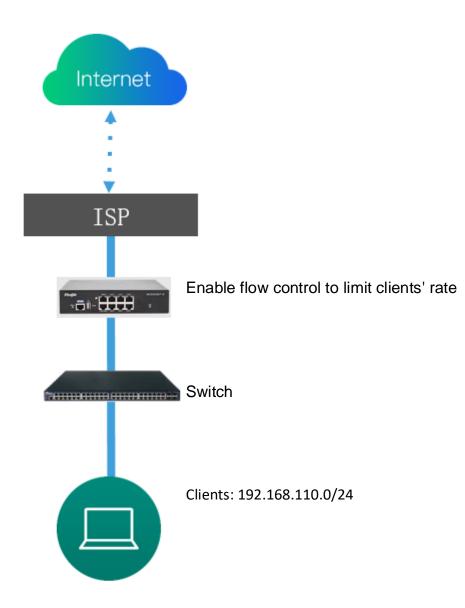
 \times

Parameter	Description
Wireless Schedule	You can select a time range from the drop-down list box, or select Custom and manually enter the specific time range.
Interface	 Select the port to which the rule applies. LAN: The rule takes effect on a LAN port to control data packets to the LAN. WAN: The rule takes effect on a WAN port to control data packets received from or sent to the Internet.
Remark	Enter the rule description, which is used to uniquely identify a rule.

4.12 Flow Control

4.12.1 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.



4.12.2 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 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

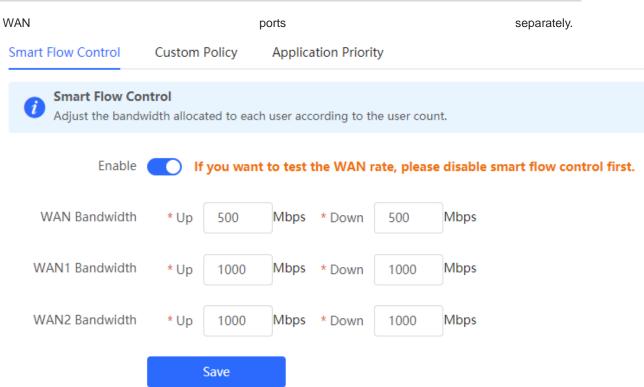


Table 4-7 Smart Flow Control Configuration

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 Mbit/s.

(3) Click **Save** to make the configuration take effect.

🛕 Caution

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 Mbit/s.

		Apps Analysis	Network De	evelopers	Enterprise A	sbout 은 Log In
	Speedtest M Try Speedtes		d Androic	×		× Sept 28−30, 2022 #SpiceWorldHybrid
	SHARE Ø Ø f Result ID			SETTINGS	Tech-ric network	h sessions, ing. and
	S PING ms		⊕ UPLOAD Mbp 1 9∩		best pra	ctices.
	14 1.	/0	1.70			rson or online!
	Connections Multi		YOUR PROVIDER		REGISTER	iow N
	GO China Unicom FuJian Fuzhou Change Server		****			
	China Telecom 120.35.11.195					
Waiting for securepubads.g.doub	×	Having Internet Prob Popular services with				

4.12.3 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 <u>错误!未找到引用源。</u> <u>错误!未找到引用源。</u>.

3. Configuration Steps

Choose Gateway > Behavior > Flow Control > Custom Policy.

(1) Set **Policy Type**.

Smart Flow Control Custom Policy Application Priority							
Cestern Rvley O Altone bandwards to the specific of a softward as relates as range The priority is some as follows: Cestern Rvley & Centern Rv							
Policy Type Normal Policy VPN Policy Policy List						Application Library Version: China	+ Add Belete Selected
Up to 30 entries can be added.							
Policy Name User Group	Bandwidth Channel Application Type Priority List	Uplink Bandwidth	Downlink Rate	Interface	Enabled	Effective State	Action

Note

The **Cloud Policy** option is displayed in **Policy Type** only after a MACC policy is configured on the MACC.

(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 template of the application priority will be reset (see section_ <u>6.6.4 Application Priority</u>), and the old application control policy may take ineffective (see section<u>6.4</u> <u>App Control</u>). Proceed with caution.

Smart F	Tow Control Custom Policy	Application Priority									
0	Custom Policy Allocate bandwidth to the specified IP as When custom policy and template are ap			om Policy >	Smart Flow Cont	rol.					?
Poli	cy List							[+ Add	🗎 Dele	ete Selected
Up	to 30 entries can be added. 1 entries a	ire already added.									
	Policy Name	IP / IP Range	Bandwid th Type	Channel	Applicati on List	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
	test	1.1.1.1-1.1.1.1	Shared	4	All Applicati ons	No Limit	No Limit	WAN	Enable ⊘	Active	Edit Delete

- (1) Set a custom policy.
- Set a custom normal policy.
 - a 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		
Туре	User Group O Custom	
* User Group	Select *	
Bandwidth Type	• Shared O Independent	
Application	All Applications Custom	
Channel Priority	4 ~ ⑦	
Bandwidth Limit	O Limit Kbps 🔿 No Limit	
Uplink Bandwidth	* CIR Kbps * PIR Kbps ⑦	
Downlink Rate	CIR Kbps * PIR Kbps	
* Interface	All WAN Ports	
Enabled		
	Cancel	ОК

b 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.					
Туре	 Type of a flow control policy: 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	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. The IP address range must be within a LAN segment. You can choose Overview > 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.
Bandwidth Type	 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	 When Bandwidth Type is set to Shared, the flow control policy can be configured to take effect only on specified applications. 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. 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. For the models, contact technical support engineers.
Application List	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.
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 错误!未找到引用源。错误!未找到引用源。.
Bandwidth Limit	 Configure whether to limit the bandwidth. 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.

Parameter	Description
Uplink Bandwidth Downlink Rate	 Configure the uplink or downlink data transmission rate, in kbit/s. CIR: Specifies the minimum bandwidth that can be shared by all users when the bandwidth is insufficient. PIR: Specifies the total maximum bandwidth that can be occupied by all users when the bandwidth is sufficient. PIR 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		
Туре	User Group O Custom	
* User Group	Select 👻 💿	
Effective User	Internal IP/User C External IP/External User	
Application	All Applications Custom	
Max Uplink Rate per	No Limit by Default	
User		
Max Downlink Rate	No Limit by Default	
per User		
* Interface	All VPN Ports	
Enabled		
	Cancel OK	

Parameter	Description
Policy Name	A policy name uniquely identifies a custom flow control policy. It cannot be modified.
	Type of a flow control policy:
Туре	• 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.
	Select a user to be managed by the policy from the user group list.
User Group	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).
	Specify the type of effective users:
	• 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.
	Configuration suggestions are as follows:
Effective User	 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.
	When Bandwidth Type is set to Shared, the flow control policy can be configured to take
	effect only on specified applications.
	• All Applications: The flow control policy takes effect on all applications in the current application library.
Application	• Custom : The flow control policy takes effect only on specified applications in the application list.
	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.
	For the models, contact technical support engineers.
Application	When Application is set to Custom, it specifies the applications on which the policy takes
List	effect. The traffic of the selected applications is limited by the policy.
Max Uplink	Configure the maximum uplink or downlink data transmission rate when multiple users
Rate per User	share the bandwidth, in kbit/s.
Max Downlink	It is optional and can be configured only when Bandwidth Type is set to Independent . The
Rate per User	rate is not limited by default.
	Specify the VPN port on which the policy takes effect. When it is set to All VPN Ports, the

b Configure items related to a VPN policy.

Parameter	Description
Enabled	Set whether to enable the flow control policy. If it is disabled, the policy does not take effect.

- c Click OK.
- (3) 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

Smart Flow (Control Custom Policy	Application Priority									
🧃 Alloc		address or range.The priority is sorte applied to an application, the custor		tom Policy >	Smart Flow Cont	trol.					0
Policy L	ist entries can be added. 1 entries	are already added.							+ Add	🗈 Dele	ete Selected
	Policy Name	IP / IP Range	Bandwid th Type	Channel	Applicati on List	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
	test	1.1.1.1-1.1.1.1	Shared	4	All Applicati ons	No Limit	No Limit	WAN	Enable ⊚	Active	Edit Delete

o VPN policy list

Policy	Type 🔿 Normal Policy 💽	VPN Policy O Cloud Policy								
Polic	cy List				App	lication Library Ver	sion: China		+ Add	Delete Selected
Upt	o 10 entries can be added. 3 ent	ries are already added.								
	Policy Name	User Group	Application List	Uplink Bandwidth	Downlink Rate	Interface	Enabled	Effective State	Match Order	Action
	PPTP_SERVER_74624	1.1.1.1-255.255.255.255	All Applications	PIR per User No Limit	PIR per User No Limit	PPTP	Disable 🖨	Inactive	4	Edit Delete
	L2TP_SERVER_49952	1.1.1.1-255.255.255.255	All Applications	PIR per User No Limit	PIR per User No Limit	L2TP	Disable 🖨	Inactive	1 4	Edit Delete
	OPENVPN_SERVER_15522	1.1.1.1-255.255.255.255	All Applications	PIR per User No Limit	PIR per User No Limit	OpenVPN	Disable 🖨	Inactive	P.	Edit Delete

Table 4-8 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, Custom 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.

Parameter	Description
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 $\sqrt[1]{10}$ in the list.
Action	You can modify and delete a custom policy.

4.12.4 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.

A Caution

If one application exists in both the custom policy list and application priority list, the custom policy takes effect.

2. Getting Started

o Before you configure an application priority, enable smart flow control. For details, see section 错误!未

找到引用源。错误!未找到引用源。

 Confirm that the appropriate application library is selected on the Custom Policy page (see section <u>6.6.3</u> Custom Policies).

3. Configuration Steps

Switch to the Local mode. Choose 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.

Smart Flow Control	Custom Policy	Application Priority	
U I I I I	·	ill reset the application group list. ck Group	
Application Priority	Default	^	
	Default		
	Office		
	Home		
	Entertainment		

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:

- o 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.

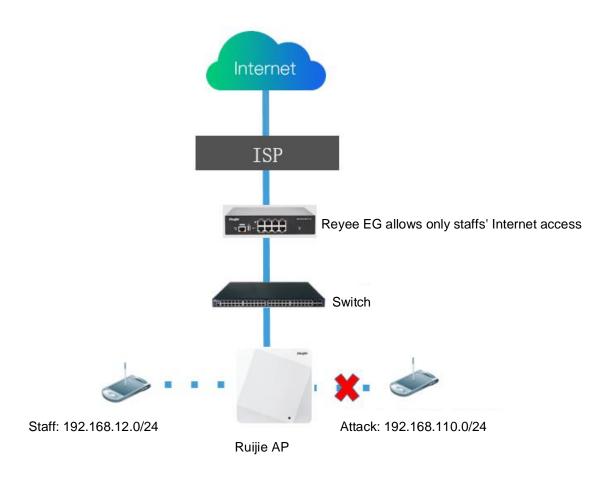
Smart Flow Control Cu	istom Policy Applicatio	on Priority			
Application Priority Changing the application priority will reset the application group list. Application priority: Key Group > Block Group					
Application Priority C	Office	\sim			
Application Group	List				
Group Nam	e	Application List	t	Action	
Key Group		Communication		Edit	
Block Group	0	Play More	Application List(2) Play Video	Edit	
Normal Grou	р	Other		Edit	
Edit			×		
Group Name	抑制通道				
Application List	Play × Video × Communication Video Shopping Play Databank	X A Car	ncel OK		
Key Group	 P2PSoftware AppStore Payment 				

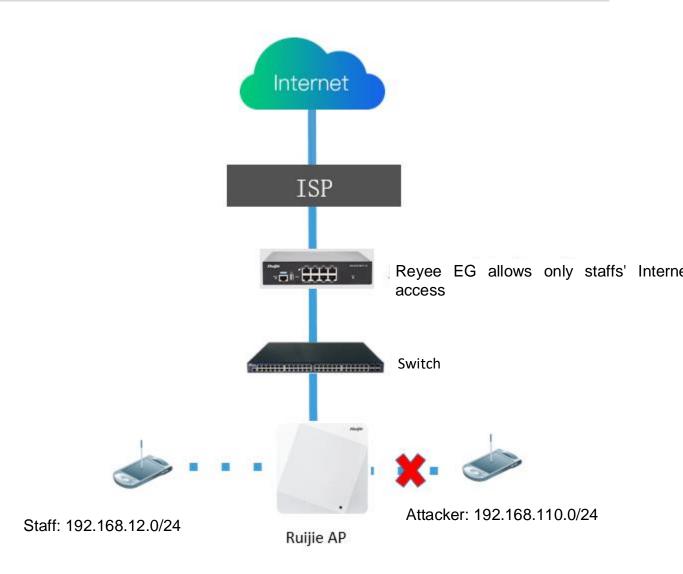
🛕 Caution

- If you switch the application library, the application list will change.
- The application list will be reset after you switch the application priority template.

4.13 Security

4.13.1 Application Scenario





4.13.2 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 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.

		levices connected to its interfaces. You ca binding to improve network security.	n bind or filter the MAC address.	0
ARP Guard				
Ena	ble Only the devic	es configured with IP-MAC binding a	re allowed to access the Internet.	
ARP List		Search by IP/MAC Q	+ Add Ø Bind Selected	Delete Selected
Up to 256 IP-N	IAC bindings can be added.			
- No.	MAC	IP	Туре	Action
1	00:e0:4c:36:0b:ea	192.168.110.236	Static	Edit Delete
2	30:0d:9e:7e:13:a1	172.26.1.1	Dynamic	

• 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	×
* [[Enter or select an IP address.
* MAC	Enter or select a MAC address.
	00:e0:4c:36:0b:ea (192.168.110.236)
	Cancel OK

(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.
Outbound Interface	 Select All Default VLAN VLAN 333
	Keep Config

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.

4.13.3 Configuring MAC Address Filtering

You can enable MAC address filtering and configure a whitelist or blacklist to effectively control Internet access from LAN hosts.

- Whitelist: Allow only hosts whose MAC addresses are in the filter rule list to access the Internet.
- Blacklist: Prevent hosts whose MAC addresses are in the filter rule list from accessing the Intern
- (1) Switch to the Local mode. Choose 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.

<i>i</i> MAC Filtering Enable MAC add	dress filtering a	nd configure the filtering type to control the host's access to the Internet.	0
MAC Filtering			
MAC Filtering	Click	to enable MAC address filtering.	
Filtering Type	Blacklist	~	
	Sav	e	
Filtering Rule Li	ist		+ Add 🗇 Delete Selected
Up to 80 rules can	be added.		
	MAC	Remark	Action
		No Data	
Add			×
	* MAC	Enter or select a MAC address.	
(Remark		
		Cancel	

(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	Blacklist	\sim
	Save	

4.13.4 Configuring Device Security

🚺 Note

This feature is supported by only R202 and later versions.

1. Overview

Prohibit Ping: This function identifies and directly discards ping packets in the traffic sent to the device, so as to prohibit the ping operation on the device. The device can be pinged from the administrative IP address only.

Admin IP Address: Packets sent from the administrative IP address are allowed to pass through.

2. Enabling the Ping Prohibition Function

Switch to the Local mode. Choose Security > Local Safety.

The ping prohibition function includes the following:

- o If you select **Prohibit LAN**, ping packets sent from all clients on the LAN to the device will be discarded.
- If you select Prohibit WAN, ping packets sent from all clients on the WANs to the device will be discarded.
 Ping packets sent from a client to the device will be responded only after the IP address of the client is contained in Admin IP Address. For details on how to configure admin IP addresses, see Configuring an Admin IP Address.

NFPP				
Prohibi	t Ping 🔽 Prohibit LAN 🛛 🗹 Prohibit WAN			
	Save			
Admin IP #	Address			+ Add 🛛 🕀 Delete Selected
Up to 32 ent	tries can be added.			
	Username	IP Range	Outbound Interface	Action
		No D	ata	
< 1 ⊃	10/page V			Total 0

3. Configuring an Admin IP Address

Switch to the Local mode. Choose Security > Local Safety.

<pre>kmin P dates is a string of 1 to 32 characters. Set Specific Mode to IP Range. Configure an name for the admin IP address. Set Specific Mode to IP Range. Configure an name for the admin IP address. Set Specific Mode to IP Range. Cancel Kmin Min Min Min Min Min Min Min Min Min M</pre>	Drobikit Dina 🖂 D. 1				
Amine Forder Plane of the address Configuring an admin IP address (based on an IP address) Add Add Cancel Configure a name for the admin IP address. Cancel Cancel Configure a name for the admin IP address. Cancel Cancel Configure a name for the admin IP address. Cancel Cancel Configure a name for the admin IP address. Cancel Cancel Configure an ame for the admin IP address. Cancel Cancel Cancel Cancel Configure an ame for the admin IP address. Cancel Cancel Cancel Cancel Cancel Cancel Cancel Configure an ame for the admin IP address. Cancel Cancel Cancel Configure an IP address. Configure an IP address or range. Configure an IP address. Configure an IP address	Prohibit Ping 🔄 Proh				
Image: Brance Image: Define define define and the set of		Save			
Image: transme of the admin IP address. Configure a name for the admin IP address. Configure a name for the admin IP address. The name is a string of 1 to 32 characters. Sepecified Mode to IP Range. Configure an IP address. (a can be address.) (b can be address.) (c can be address.) </th <th></th> <th></th> <th></th> <th></th> <th>+ Add 🖻 Delete Selec</th>					+ Add 🖻 Delete Selec
<pre>vector vector vect</pre>			IP Range	Outbound Interface	Action
Configuring an admin IP address (based on an IP address) Add Username Specified Mode IP Range Outbound Interface Please enter an IP address or range. Configure a name for the admin IP address. Configure a name for the admin IP address. Set Specific Mode to IP Range. Configure an IP address. Configure an IP address. Configure an IP address. Configure an IP address. Configure an IP address or an IP address range. Configure an admin IP address or an IP address range. Configure an admin IP address (based on a port) d Vusername Specified Mode IP Range Outbound Interface Configure an admin IP address (based on a port) Configure an admin IP addre					
Add * Usemane Specified Mode IP Range Outbound Interface Please enter an IP address or range. Configure a name for the admin IP address. Configure a name for the admin IP address. Configure an ane is a string of 1 to 32 characters. Set Specified Mode to IP Range. Configure an IP address. Configure an IP address. Configure an ange IP address or an IP address range. Configure an ange IP address or an IP address range. Configure an ange IP address (based on a port) Configure an admin IP address (based on a por	< 1 > 10/page				Та
Add * Usemane Specified Mode IP Range Outbound Interface Please enter an IP address or range. Configure a name for the admin IP address. Configure a name for the admin IP address. Configure an ane is a string of 1 to 32 characters. Set Specified Mode to IP Range. Configure an IP address. Configure an IP address. Configure an ange IP address or an IP address range. Configure an ange IP address or an IP address range. Configure an ange IP address (based on a port) Configure an admin IP address (based on a por	Configuring an a	dmin IP address (ba	ased on an IP address)		
*Username Specified Mode IP Range Ottound Interface Please enter an IP address or range. Cancel Ottout Configure a name for the admin IP address. The name is a string of 1 to 32 characters. Set Specific Mode to IP Range. Configure an IP address. You can specify a single IP address or an IP address range. Configuring an admin IP address (based on a port) d d *Username specified Mode IP Range Outbound Interface	Configuring an a				
Specified Mode • IP Range • Outbound Interface Please enter an IP address or range. Cancel • K Cancel • K Configure a name for the admin IP address. The name is a string of 1 to 32 characters. Set Specific Mode to IP Range. Configure an IP address. You can specify a single IP address or an IP address range. Configuring an admin IP address (based on a port) d	Add			×	
Specified Mode • IP Range • Outbound Interface Please enter an IP address or range. Cancel • K Cancel • K Configure a name for the admin IP address. The name is a string of 1 to 32 characters. Set Specific Mode to IP Range. Configure an IP address. You can specify a single IP address or an IP address range. Configuring an admin IP address (based on a port) d					
Please enter an IP address or range. Cancel Cancel Cancel Cancel Cancel Cancel Cancel Cancel Coc Coc Configure a name for the admin IP address. Configure an IP address. Set Specific Mode to IP Range. Configure an IP address. Configure an IP address or an IP address range. Configuring an admin IP address (based on a port) d Coc	* Use	rname			
Please enter an IP address or range. Cancel Cancel Cancel CK Configure a name for the admin IP address. The name is a string of 1 to 32 characters. Set Specific Mode to IP Range. Configure an IP address. You can specify a single IP address or an IP address range. Configuring an admin IP address (based on a port) d Yusemame Specified Mode IP Range Outbound Interface					
Configure a name for the admin IP address. The name is a string of 1 to 32 characters. Set Specific Mode to IP Range . Configure an IP address. You can specify a single IP address or an IP address range. Configuring an admin IP address (based on a port) d × *Username Specified Mode IP Range Outbound Interface	Specified	Mode O IP Range	 Outbound Interface 		
Configure a name for the admin IP address. The name is a string of 1 to 32 characters. Set Specific Mode to IP Range . Configure an IP address. You can specify a single IP address or an IP address range. Configuring an admin IP address (based on a port) d × *Username Specified Mode O IP Range O tubound Interface		Please enter	r an IP address or range.		
Configure a name for the admin IP address. The name is a string of 1 to 32 characters. Set Specific Mode to IP Range . Configure an IP address. You can specify a single IP address or an IP address range. Configuring an admin IP address (based on a port) d × *Username Specified Mode O IP Range Outbound Interface					
Configure a name for the admin IP address. The name is a string of 1 to 32 characters. Set Specific Mode to IP Range . Configure an IP address. You can specify a single IP address or an IP address range. Configuring an admin IP address (based on a port) d × *Username Specified Mode O IP Range Outbound Interface					
The name is a string of 1 to 32 characters. Set Specific Mode to IP Range . Configure an IP address. You can specify a single IP address or an IP address range. Configuring an admin IP address (based on a port) d × * Username Specified Mode O IP Range O Outbound Interface			Cancel	ОК	
The name is a string of 1 to 32 characters. Set Specific Mode to IP Range . Configure an IP address. You can specify a single IP address or an IP address range. Configuring an admin IP address (based on a port) d × * Username Specified Mode O IP Range O Outbound Interface	0 "				
Set Specific Mode to IP Range. Configure an IP address. You can specify a single IP address or an IP address range. Configuring an admin IP address (based on a port) d					
Configure an IP address. You can specify a single IP address or an IP address range. Configuring an admin IP address (based on a port) d × *Username Specified Mode O IP Range Outbound Interface			acters.		
You can specify a single IP address or an IP address range. Configuring an admin IP address (based on a port) d × *Username Specified Mode O IP Range Outbound Interface					
Configuring an admin IP address (based on a port) d *Username Specified Mode O IP Range Outbound Interface					
d × * Username Specified Mode O IP Range Outbound Interface					
* Username Specified Mode O IP Range Outbound Interface	Configuring an a	dmin IP address (ba	ased on a port)		
* Username Specified Mode O IP Range Outbound Interface	ld		×		
Specified Mode O IP Range Outbound Interface					
	* Username				
Select ~		IP Range Out	tbound Interface		
	Specified Mode		\sim		
			tbound Interface		
	Specified Mode	Select			

The name is a string of 1 to 32 characters.

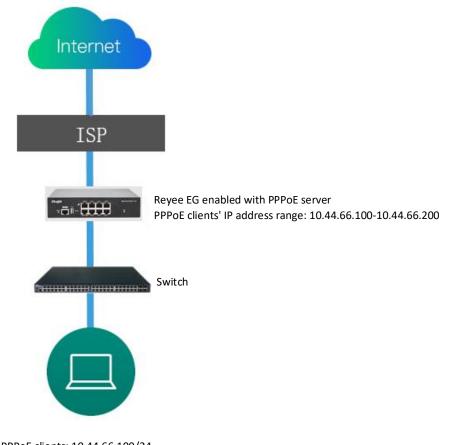
- (2) Set Specific Mode to Outbound Interface.
- (3) Specify the port.

You can select a LAN port or WAN port as the outbound interface.

4.14 Configuring the PPPoE Server

4.14.1 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.



PPPoE clients: 10.44.66.100/24

4.14.2 Global Settings

Switch to the Local mode. Choose Advanced > PPPoE Server > Global Settings.

Set **PPPoE Server** to **Enable** and configure PPPoE server parameters.

Global Settings	Account Settings	Account Management	Exceptional IP Address	Online Clients
2. The IP add	ing and MAC filtering ar	e not valid for PPPoE clients. r cannot overlap with any inte valid for PPPoE clients.	rface IP range.	
PPPoE S	Server 🔿 Enable	• Disabled		
Mandatory PPPoE [Dialup 🔿 Enable	Disable		
* Local Tun	nel IP 10.44.66.99			
* IP F	Range 10.44.66.100	-10.44.66.200		
	VLAN Default VLAI	N ~		
Primary DNS S	Server Example: 1.1	.1.1		
Secondary DNS S	Server Example: 1.1	.1.1		
* Unanswere			Range: 1-60	
Packet	: Limit			
Auth	Mode 🗹 PAP 🗹	CHAP MSCHAP2		
	Save			

 Table 4-7
 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.

Parameter	Description
Auth Mode	Select at least one authentication mode among PAP, CHAP, MSCHAP, and MSCHAP2.

4.14.3 Configuring a PPPoE User Account

Switch to the Local mode. Choose 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.

Global Settings	Account Setting	Account Manageme	nt Exceptional	IP Address Onlin	e Clients	
i Account	Settings					?
Account Li	st			[+ Add	Delete Selected
Up to 15 en	tries can be added. Clie	nts 1				
Use	ername Pass	word Expire Date	Status	Account Management	Remark	Action
	test te	st 2022-04-30	Enable	-		Edit Delete

Add		×
* Username	Please enter a username.	
* Password	Please enter a password.	
Expire Date	🗐 Select a time.	
Remark	Length: 1-50 characters long.	
Status		
Flow Control		
* Account	Select ~	
Management		
	Cancel	ОК

Table 4-8 PPPoE User Account Configuration

Parameter	Description		
Username/Password	Set the username and password of the authentication account for Internet access through PPPoE dialing.		
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.		

Parameter	Description			
Flow Control	Specify whether to apply flow control on the account. If flow control is enabled, you need to configure flow control policies for PPPoE authentication users. If smart flow control is disabled, Flow Control must be disabled. To enable Flow Control , enable smart flow control first. For details on how to configure smart flow control, see section <u>6.6.2</u> 错误!未找到引 用源。.			
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 <u>3.12.4</u> 错误!未找到引 用源。.			

4.14.4 Configuring a Flow Control Package

Switch to the Local mode. Choose 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 <u>6.6.2</u> 错误!未找到引用源。.

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.

Global Settin	igs Account Settir	ngs Account Manageme	nt Exceptional IP Address	Online Clients	
Account	t Management Li	st		+ Add	Delete Selected
Up to 10	entries can be added.				
Ac	count Name	Uplink Rate	Downlink Rate	Interface	Action
	test PII	CIR 100000Kbps PIR 100000Kbps R per User No Limit	CIR 100000Kbps PIR 100000Kbps PIR per User No Limit	WAN	Edit Delete

Add							×
* Account Name							
Uplink Rate	* CIR	Kbps	* PIR	Kbps	PIR per User	No Limit Ł	
Downlink Rate	* CIR	Kbps	* PIR	Kbps	PIR per User	No Limit Ł	
* Interface	WAN			~			

Table 4-9	PPPoE User Flow Control Package Configuration
	FFFOL User Flow Control Fackage 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/Downlink CIR	Specify the uplink and downlink committed information rate (CIR) for an authentication account when the bandwidth is insufficient.
Uplink/Downlink PIR	Specify the uplink and downlink peak information rate (PIR) that can be used by an authentication account when the bandwidth is sufficient.
Uplink/Downlink PIR per User	Specify the PIR that can be consumed by each user. This parameter is optional. By default, the PIR per user is not limited.
Interface	Specify the interface to which the flow control package applies.

Cancel

4.14.5 Configuring Exceptional IP Addresses

Switch to the Local mode. Choose 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.

Global Se	ettings	Account Set	ttings A	ccount Mana	gement	Exceptional	IP Address	Onl	ine Clients	
🪺 E	xceptional	IP Address								?
Ехсер	otional IF	P Address	List				+	Add	🗇 Delete Sele	cted
Up to	5 entries o	an be added.								
	Start IP	Address	End IP A	ddress	Rema	rk	Statu	5	Action	
	172.2	26.1.2	172.26	.1.100			Enabl	е	Edit Delet	e
					~ " .					
Add						×				
	* Start IP									
	Address									
	* End IF Address									
	Address	5								
	Remark	۲								
	Status	s ()								
				Ca	incel	ОК				

4.14.6 Checking Online Users

Switch to the Local mode. Choose 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.

Global Settings	Account Settings	Account Manageme	ent Exceptional IP	Address	Online Clients	
i Online Cli	ents					?
Account List	t			🗊 Dis	sconnect	C Refresh
Online Clients	0					
Us	ername	IP	MAC	Up on		Action
		No	Data			

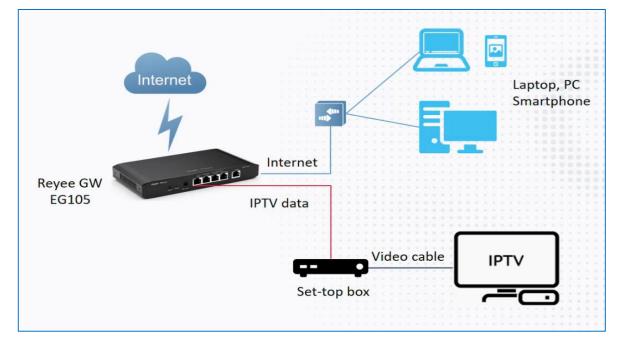
Table 4-10 PPPoE Online User Information

Parameter	Description
Username	Total number of online users that access the Internet through PPPoE dialing.
IP	IP address of the client.
MAC	MAC address of the client.
Up on	Time when the user accesses the Internet.

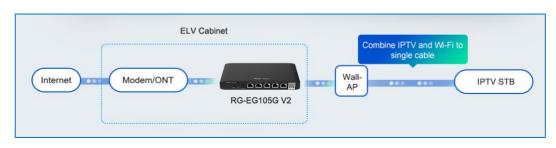
4.15 IPTV

4.15.1 Application Scenario

• Scenario 1: Dual-WAN Scenario



• Scenario 2: Single-WAN Scenario



4.15.2 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) Switch to the Local mode. Choose Network > IPTV > IPTV/VLAN.

Ruíjie l @Rc	усс	gw_eg310g-e > Ruijie (•			
😤 Overview		IPTV/VLAN IPTV/I	GMP			
Online Clients	^	i IPTV/VLAN set	tings.			
Hetwork WAN		IPTV/VLAN				
LAN		* Mode	Custom	~		
IPv6 Address		* AG	Internet	~		
Port VLAN		* AG	Internet	~		
Port Settings		* LAN0	Internet			
PTV ⊘ Security	~	* LAN1	Internet	\sim		
∰ Behavior	~	* LAN2	Internet	~		
VPN	~	* LAN3	Internet	~		
🖶 Advanced	~	* LAN4/WAN3	Internet	~		
Diagnostics Diagno	~	Internet VLAN (WAN)	802.1Q Tag			

- (3) Configure IPTV VLAN ID or IP-Phone VLAN ID.
 - o If you are in following regions listed in the red box, you can choose the mode directly.

IPTV/VLAN IPTV/IGMP						
<i>i</i> PTV/VLAN settings.						
IPTV/VLAN						
* Mode	Custom ^]				
* AG	Singapore-Singtel					
* AG	Malaysia-Unifi Malaysia-Maxis-l					
* LANO	Maylaysia-Maxis-2					
* LAN1	Vietnam-Viettel Australia-NBN					
	Custom					
* LAN2	Internet ~					
* LAN3	Internet ~					
* LAN4/WAN3	Internet \vee					
* LAN5/WAN2	Internet ~					
Internet VLAN (WAN)	802.1Q Tag					
	Save					

 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>i</i> IPTV/VLAN settings.						
IPTV/VLAN						
* Mode	Custom	~				
* LAN0	Internet	~				
* LAN1/WAN3	IPTV	~				
* LAN2/WAN2	IP-Phone	~				
* LAN3/WAN1	Internet	~				
* IPTV VLAN ID	100					
* IP-Phone VLAN ID	200					
Internet VLAN (WAN)	802.1Q Tag					
* Internet VLAN ID	300					
	Save					

4.15.3 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 **Network** > **IPTV** > **IPTV/IGMP** and enable **IPTV/IGMP**.

움 Overview	IPTV/VLAN IPTV/IGMP
Ø Online Clients	
Hetwork	IPTV/IGMP (For FPT Service Provider)
WAN	IPTV/IGMP
LAN	Enable 🔵
IPv6 Address	Save
Port VLAN	
Port Settings	
IPTV	
Security ~	
슈 Behavior · ·	

(2) Log in to the web management system of a wall AP. Choose Wireless > LAN Ports > Add.

Ruíjie &Rcycc	Cloud_Auth_Test > EG105G-P (Maxter) 0	English ~Ruijie Cloud	號Download App 🛭 용 Network Setup	@ Network Check <u>m</u> Warn ⊟ Log Ou
ි Overview ම Online Clients	LAN Port Settings The configuration takes effect only for the AP with a LAN port, e.g., EAI Note: The configured LAN port settings prevail. The AP device with no	2101. LAN port settings will be enabled with default settin	gs.	
Router	Default Settings	Add VLAN		
APs Wi-Fi Clients	(Range: 2-232 and 234-4090. A blank value indica WAN port.)	tes the same VLAN as		
Blacklist/Whitelist Radio Frequency	Applied to AP device with no LAN port settings			
LAN Ports LED	LAN Port Settings		[+ Add 🗇 Delete Selected
Network Optimization	Up to 8 VLAN IDs or 32 APs can be added (0 APs have been added).			
Switches	VLAN ID 🗢	Applied to		Action
Collapse		No Data		

Set the VLAN ID to 100, which is applied to the wall AP.

Ruijie	test123 > Ruijie (Master) 0		English - 〇 鼹 🖨 @ 道 🗗
	VLAN ID	Add VLAN	
APs	Edit	×	
Wi-Fi	VLAN ID 1	00 0	
Clients	Applied to		
Blacklist/Whitelist	* Applied to G	1Q 0534 🛞 🗸	
Radio Frequency			
LAN Ports	LAN Port Setti	Cancel	+ Add 🗇 Delete Selected
LED	Up to 8 VLAN IDs or 32 APs can be added (1	APs have been added).	
Network Optimization	VLAN ID 🗢	Applied to	Action
Switches			
Network	1236		Edit Delete
Collapse			
A Caution			

IPTV is supported by only Reyee OS 1.55 and later versions.

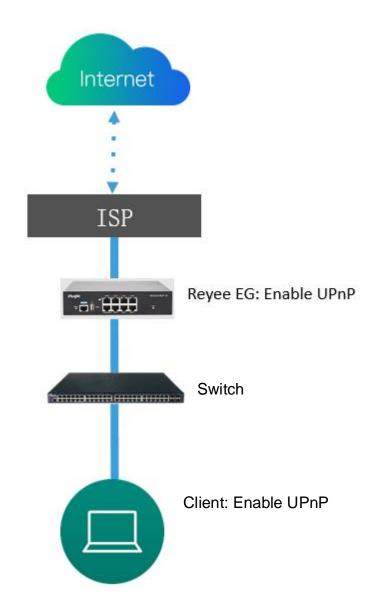
4.16 UPnP

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.



Procedure

- Switch to the Local mode. Choose Advanced > UPnP Settings > Enable to enable UPnP on your phone or PC.
- (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.

Ruijie HRoyco	Local DevicettG2			English v 💡	D Remote C&M 🔹 Network Setup 🎕 Network Check 🖹 Alert 🕞 Log 0
A Overview					
Online Clients	UPnP Settings UPnP (Universal Plug and Play) is a new Internet protocol aimed at improving comm.	nication between devices.			
@ Network ~	Enable 💽				
⊖ Security ~	Default Interface WAN ~				
ifi Behavior ∵	Saw				
UPN VPN V	UPnP List				
🖻 Advanced 🗠					
Routing	Protocol	App	Client IP Address	Internal Port	External Port
PPPoE Server			No UPoP Device		
Authentication					
Session Limit					
Port Mapping					
Dynamic DNS					
UPnP Settings					
Local DNS					
TTL Rule					
Other Settings					
Constitution Co					
🗄 System 🗸 🗸					

5 Advanced Solution

5.1 Reyee Flow Control Solution

5.1.1 Application Scenario

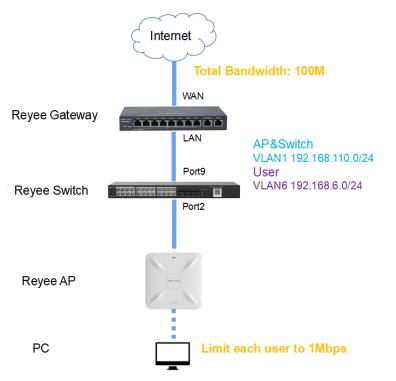
Flow control is used for setting rate limits of download and upload rates for the clients. With flow control configured, the router can protect the network bandwidth from being occupied by some clients.

5.1.2 Configuration Example

Requirement

The total bandwidth of the EG is limited to 100 Mbit/s and the rate of each user on the network segment of VLAN 6 is limited to 1 Mbit/s.

Network Topology



Network Description

- The EG works as a DHCP server to assign IP addresses to users, Reyee AP, and Reyee switch.
- The Reyee AP and switch obtain the IP address 192.168.110.0/24 on the network segment of VLAN 1 for Internet access.
- The users obtain the IP address 192.168.6.0/24 on the network segment in VLAN 6 for Internet access.

Configuration Steps

- (1) Perform basic network configuration.
 - a Switch to the Local mode. Choose Network > LAN > LAN Settings > Add and perform LAN settings and DHCP address pools of VLAN 1 and VLAN 6 on the router.

Ruijie IRcycc	Local Device(EQ2 -						English ~ 🛆 Remo	ne D&M 👋 Network Setup 🖓 Network O	heck 🚊 Alert 🕒 Log Out
A Overview		c IP Addresses DHCP Option DNS Proxy							
Online Clents Network	() LAN Settings								0
WAN	LAN Settings							+ Add	8 Delete Selected
UN	Up to 8 entries can be added.								
Pv6 Address	P	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
Port VLAN	192.168.110.1	285.285.285.0	Default VLAN		Enabled	192.168.110.1	254	30	Edit Delete
IPTV	92.168.11.3	255.255.255.0	11		Disabled				Edit Delete
⊖ Security ~	192,168,12,1	255.255.255.0	12		Disabled				Edit Delete
cti Behavior 🤍	192.168.116.1	255.255.255.0	13	11111	Disabled				Edit Delete
Advanced									
®: Diagnostics ~ ~									
🗉 System 🗸 🗸									
Add					×				
	:	IP 192.168.	120.1						
	* Subnet M	ask are are	255.0						
	Sublict M	ask 255.255.	255.0						
	* VLAN	ID							
	Rem	ark Remark							
	M	IAC 00:D0:18	:24:93:51						
		00.00.10							
	DHCP Ser								
	DHCP Ser	ver 💽							
	* 51	tart 192.168.	120.1						
	* IP Co	unt 254							
*	Lease Time(N	1in) 30							
	DNCC	10246242	01.0						
	DNS Ser	ver 192.168.12	0.1 10						

Cancel	ок

Ruijie	test123 >	EG105GW (Maste	el •		Engl	ish ∽ 🔄 Ruijie Clou	d 📓 Download App	Network Setup	@Network Check	<u>₩</u> Warn (
å Overview ⊗Online Clients		oser H	ostname: EG105GW MAC: 30:00:9E:E7:		PH745119402	IP: 172.26.5.2	37			C) R	eboot
Router	Overvie	w Basics ~ 5	ecurity ~ Behavio	r∼ VPN ∽ Adv	vanced ~ Diagr	iostics ~ System ~					
⇔Wireless ~	LAN Setti	DHCP Cli	ents Static IP A	ddresses DHCP	Option DNS	Ргоку					
Switches	() U	N Settings									0
ENetwork ~	LAN S	ettings							+ Add	1 Delete Sele	ected
	Up to	8 entries can be ad	ided.								
		IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action	
		192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	220	30	Edit Del	lete
		192.168.6.1	255.255.255.0	6		Enabled	192.168.6.1	254	30	Edit Del	ete
«Collapse											

A Caution

The network segment 192.168.110.0/24 is configured for VLAN 1.

(2) Switch to the **Network** mode. Choose **Device** > **Switch**.

Device Lis	t O					B(NHL/humars	a S2(S_G_) 2 Delete Offline Devices Banh Upgrade
	104 c	Status ±	Hostronie C	MAC =	P 2	Software Ver	Model =
	G11/W815200043	Onine	Refe Z.	384946782267	10216811042	ReperCS 1.206.2122	N353100-24G745FP-P
	MACENIESSOOM	Colles	Roje C	00000 FEFT 86.40	100.186.110.5 Z	ReperIDS 1.206.2118	NIR56002
	10/paga -						Total 2

- a Select a device from **Device List** and access the configuration page.
- b In the VLAN pane, select a VLAN and click Edit to configure the VLAN.

_	Hostname: Ruijie 🖉		Software Ver:ReyeeOS 1.206.2122	
MSW	Model:NBS3100-24GT4SFP-P		MGMT IP: 192.168.110.6 🖉	
	SN:G1NWB1S000043		MAC: 58:69:6C:FB:22:C7	
Port Status	Port Status			
VLAN Info				
Port				Panel View
RLDP	VLAN			Edit 💿
More	VLAN1 VLAN13			
	Interface	IP	IP Range	Remark
	Port			Edit 🕲
	Interface	Туре	VLAN	DHCP Pool
		TRUNK		
	Port List			
	Interface	Туре	VLAN	DHCP Pool
			No Data	
	Total 0 10/page 🗸 🤇 1	Go to page 1		

c Click Add VLAN to create VLAN 6 on the switch.

VLAN Info

Vlan ID	Remark VLAN0001
Vlan ID 13	Remark 11111
Vlan ID	Remark
6	

+Add VLAN	+Batch Add	-Delete Selected			
			Cancel	Save	

d In the **Port** pane, click **Edit**, configure port2 and port9 connected to the AP and EG as trunk ports and configure them to allow packets from VLAN 1 and VLAN 6 to pass through. Then check port settings on the switch.

rt			 		 	 	 		 	
1	-	-	-	11	 		 			
				1						
2								25		

Cancel

РО	rt															
	Ava	ailable	e 💼	Un	availa	able		6	Aggre	egate	1R	Uplink	ė	Cop	per	Fiber
	1	3	5	7	9	11	13	15	17	19	21	23				
	2	4	6	8	10	12	14	16	18	20	22	24	25	26	27	28
Not	Note: You can click and drag to select one or more ports. Select All Inverse Deselect															
		C - 1 -			1.10											
			cted I				orted	i								
		Roi		Port	Not	i2"] : Supp		1								
		Roi	uted I	Port ype	Not	Supp		1	~							
		Roi	uted I Port T	Port ype	Not	Supp		1								

(3) Switch to the Network mode. Choose Network > Wi-Fi > Wi-Fi Settings, configure the SSID named Reyee_test, and associate VLAN 6 with this SSID.

Ruíjie ARcycc	Network
Q Navigation	Wi-Fi Settings Guest Wi-Fi Wi-Fi List Healthy Mode Load Balancing
Overview	
A Network	Tip: Changing configuration requires a reboot and clients will be reconnected.
Network Planning	Wi-Fi Settings Device Group: Default v
Wi-Fi	* SSID @Ruijie-mBCFA
RLDP	Band 2.4G + 5G \lor
DHCP Snooping	Security Open V
WIO	Collapse
Radio Frequency	
Reyee Mesh	Wireless Schedule All Time 🗸
LAN Ports	VLAN 6
LED	Hide SSID (The SSID is hidden and must be manually entered.)
Alerts	Client Isolation Prevent wireless clients of this Wi-Fi from communicating with one another.
Batch Config	Band Steering (The 5G-supported client will access 5G radio preferentially.)
Devices	XPress (The client will experience faster speed.)
👜 Gateway	
🖻 Firewall	Layer-3 Roaming (The client will keep his IP address unchanged in this Wi-Fi network.)
Ilients Management	Wi-Fie 👥 (802.11ax High-Speed Wireless Connectivity.) ⊘
🚆 System 🗸 🗸	Save

Ruijie ERcycc	test123 > EG105GW [Master] (0	English ~ 🗠	Ruijie Cloud 🛛 😹 Download i	Npp 👃 Network Setup @	Network Check 📺 Warn	🕞 Log Out
∆ Overview							
@ Online Clients	Wi-Fi Settings Guest Wi-F	i Wi-Fi List Healthy M	ode				
@ Router	👔 Tip: Changing configurati	ion requires a reboot and clients wi	Il be reconnected.				0
⇔Wireless ^	Wi-Fi List Device Group	C Default V				+	Add
APs	Up to 8 SSIDs can be added						
Wi-Fi	SSID	Band	Security	Hidden	VLAN ID	Action	
Clients	Reyee_test	2.4G + 5G	OPEN	No	6	Edit Delete	
Blacklist/Whitelist Radio Frequency	1. January 100, 1	2.4G + 5G	WPA_WPA2-PSK	Yes	6	Edit Delete	
LAN Ports	T. dependencent	2.4G + 5G	OPEN	No	Default VLAN	Edit Delete	
LED Network Optimization	Const. ADD. 4	2.4G + 5G	WPA_WPA2-PSK	Yes	7	Edit Delete	
Switches							
李Network ~							-
«Collapse							

- (4) Configure smart flow control.
 - a Switch to the Local mode. Choose Behavior > Flow Control and enable Smart Flow Control.

Ruíjie I &Rcycc	Local Device(EG2 😒
o Overview	Smart Flow Control Custom Policy Application Priority
Ø Online Clients	
Network ~	Smart Flow Control Intelligently adjust the network speed to ensure that each user shares the network fairly.
⊘ Security ∨	Enable If you want to test the WAN rate, please disable smart flow control first.
☆ Behavior へ	WAN Bandwidth * Up 1000 Mbps * Down 1000 Mbps
App Control	Save
Website Management	
Flow Control	
Access Control	
User Management	
Time Management	
😨 VPN 🗸	
🖻 Advanced 🛛 🗸	
Ø Diagnostics	
🗄 System 🗸 🗸	

b Fill in the uplink and downlink WAN bandwidth as 100 Mbit/s and click **Save**.

Smart Flow Control	Custom Policy Application Priority
intelligently adju	ntrol st the network speed to ensure that each user shares the network fairly.
Enable	If you want to test the WAN rate, please disable smart flow control first.
WAN Bandwidth	* Up 1000 Mbps * Down 1000 Mbps
	Save

c After Step 2 is performed, Custom Policy will be displayed. Click Add to add a policy.

Smart F	low Control	Custom Policy							
	Custom Policy Allocate bandwidt	h to the specified IP i	address or range. The p	priority is sorted as follows: Cus	stom Policy > Smart Flow Control.				?
Polic	cy List							+ Add	+ Delete Selected
Up t	o 30 entries can	be added.							
	Policy Name	IP/IP Range	Bandwidth Type	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
					No Data				

Set Policy Name, IP Range, Bandwidth Type, Rate, and other parameters.

Edit					×
* Policy Name	test				
* IP/IP Range	192.16	68.6.2-192.16	68.6.254		
Bandwidth Type	Indep	endent		~	
Uplink Rate	* CIR	1000	* PIR	1000	Kbps
Downlink Rate	* CIR	1000	* PIR	1000	Kbps
Interface	WAN			~	
Status					
				Cancel	ОК

mart Flow	v Control	Custom Policy							
	stom Policy ocate bandwidt	th to the specified I	P address or range. Th	he priority is sorted as follows	:: Custom Policy > Smart Flow C	ontrol.			0
Policy	List							+ Add	+ Delete Selected
Up to 3	30 entries can	be added.							
P	Policy Name	IP/IP Range	Bandwidth Type	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
	test	192.168.6.2-1 92.168.6.254	Independent	CIR 1000 Kbps PIR 1000 Kbps	CIR 1000 Kbps PIR 1000 Kbps	WAN	Enable ⊘	Active	Edit Delete

- Bandwidth Type
 - Shared: indicates that the total bandwidth is shared by all IP addresses.
 - Independent: indicates that the rate limit is set for each IP address.
- **CIR**: indicates the committed information rate.
- **PIR**: indicates the peak information rate.

5.1.3 Configuration Verification

Use Speed test tool to check that each user is limited up to 1 Mbit/s.



5.2 Reyee Cloud Authentication Solution

5.2.1 Working Principle

Cloud authentication allows you to control users' access to the wireless network. The configuration will be synchronized from Ruijie Cloud to the local EG. In portal authentication, all the clients' HTTP requests are redirected to an authentication page first. The clients are required for authentication, payment, acceptance of the end-user license agreement, acceptable use policy, survey completion, or other valid credentials, so they can visit the Internet after successful authentication.

5.2.2 Application Scenario

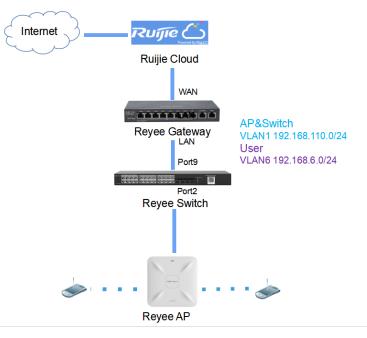
Portal authentication, also known as web authentication, is usually deployed in a guest-access network (such as a hotel or a coffee shop) to control clients' Internet access.

5.2.3 Configuration Example

Requirement

Users toned to be authenticated before accessing the Internet. Reyee AP does not support cloud authentication, and Reyee EG needs to authenticate users.

Network Topology



Network Description

- The EG works as a DHCP server to assign IP addresses to users, Reyee AP, and Reyee switch.
- The Reyee AP and switch obtain the IP address 192.168.110.0/24 on the network segment of VLAN 1 for Internet access.
- Users obtain the IP address 192.168.6.0/24 on the network segment of VLAN 6 for Internet access.
- Ruijie Cloud manages and monitors the device and client status and provides captive authentication for clients.

Configuration Steps

- (1) Configure the basic network.
 - a Switch to the Local mode. Choose Network > LAN > LAN Settings > Add, and configure LAN settings and DHCP pool of VLAN 1 and VLAN 6 on the router.

Ruijie IRcycc	Local Device(B	62						English ~ 🔿 Rema	ne DAM 👋 Network Setup 🙈 Network C	heck 🚊 Alert 🔂 Logi
& Overview	LAN Settings	DHCP Clants Static IP Add	resses DHCP Option DNS Proxy							
Online Clients	🚺 LAN Se	rttings								Ø
Network	LAN Setti	ngs							+ Add	Delete Selected
LAN	Up to 8 ent	tries can be added.								
IPv6 Address			Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
Port VLAN		192.168.110.1	255.255.255.0	Default VLAN		Enabled	192.168.110.1	254	30	Edit Delete
Port Settings		192.168.11.3	255.255.255.0	11		Disabled				Edit Delete
IFTV 3 Security ~		192.168.12.1	255.256.255.0	12		Disabled				Edit Delete
fi Behavior 🗠		192.168.116.1	255.255.255.0	13	11111	Disabled				Edit Delete
⊒ vpn –										
Advanced 🛛 👻										
il Diagnostics 🗠										
S System ~										

 \times

Edit

_			_
	* IP	192.168.110.1	
	* Subnet Mask	255.255.255.0	
	Remark	Remark	
	* MAC	30:0d:9e:e7:e9:15	
	DHCP Server		
	* Start	192.168.110.1	
	* IP Count	220	
* L	ease Time(Min)	30	
	DNS Server	192.168.110.1 🚺	

Ado	ł		
	* IP	192.168.6.1	
	* Subnet Mask	255.255.255.0	
	* VLAN ID	6	
	Remark	Remark	
	MAC	80:D0:F8:22:1B:B0	
	DHCP Server		
	* Start	192.168.6.1	
	* IP Count	254	
	* Lease Time(Min)	30	
	DNS Server	192.168.6.1 🕐	

Cancel OK

×

Rujje	test123	EG105GW [Mast			Eng	lish ∽ ⊔ 🛆 Ruijie Clou	d 🏭 Download App	A Network Setup	@Network Check	a≚Warn ⊡Log
& Overview		Router 105GW	Hostname: EG105GW MAC: 30:0D:9EE7:		PH745119402	IP: 172.26.5.2	37			() Reboot
Router	Overvi	ew Basics ~	Security ~ Behavio	or ~ VPN ~ Ad	vanced ~ Diagr	nostics ~ System ~				
⇔Wireless ~	LAN Set	tings DHCP C	lients Static IP A	ddresses DHCP	Option DNS	Praxy				
Switches	0	LAN Settings								0
∑Network ~	LAN	Settings							+ Add	1 Delete Selected
	Up to	a entries can be a	idded.							
		IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
		192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	220	30	Edit Delete
	•	192.168.6.1	255.255.255.0	6		Enabled	192.168.6.1	254	30	Edit Delete
«Collapse										

A Caution

The network segment 192.168.110.0/24 is configured for VLAN 1.

(2) Switch to the **Network** mode. Choose **Device** > **Switch**.

Device Lis	10					ID/MAC/Institutionaria/	SNS C Drive Office Drokes Bach Upgrade
	529 c	Status 1	Hostromie =	MAC =	P 2	Softward Wer	Model =
	G11/W815000043	Online	hope 2.	\$84940182207	152 148 110 # 2	Repertor 1.206.2122	N8551106-246745FP-P
	MACCNESSOON	Online	Nije C	000048773654E	110.168.110.3 Z.	ReperIDS 1.206.2118	1056602
	10/paga -						Total 2

- a Select a device from **Device List** and access the configuration page.
- b In the VLAN pane, select a VLAN and click Edit to configure the VLAN.

MSW	Hostname: Ruijie 🖉 Model:NBS3100-24GT45F SN:G1NWB15000043	:p.p	Software Ver:ReyeeOS 1.206.2 MGMT IP: 192.168.110.6 & MAC: 58:69:6C:FB:22:C7	2122
 Port Status VLAN Info 	Port Status			Panel View
Port RLDP	VLAN			Edit @
More	VLAN1 VLAN13			
	Interface	IP	IP Range	Remark
	Port			Edit ©
	Interface	Type TRUNK	VLAN	DHCP Pool
	Port List Interface	Туре	VLAN	DHCP Pool
		No	o Data	
	Total 0 10/page 🗸 🤇 1	Go to page		

c Click Add VLAN to create VLAN 6 on the switch.

VLAN Info

Vlan ID	Remark VLAN0001	
Vlan ID 13	Remark	
Vlan ID	Remark	
6		

+Add VLAN	+Batch Add	-Delete Selected		
			Cancel	Save

d In the **Port** pane, click **Edit**, configure port2 and port9 connected to the AP and EG as trunk ports and configure them to allow packets from VLAN 1 and VLAN 6 to pass through, and check port settings on the device.

rt									
1			11						
		 	÷						
2							25		

Cancel

PO	rt															
	Ava	ailable		Un	availa	able		6	Aggr	egate	18	Uplink		Cop	oper	Fiber
	1	3	5	7	9	11	13	15	17	19	21	23				
	2	4	6	8	10	12	14	16	18	20	22	24	25	26	27	28
No	te: Yo						elect	one	or ma	ore po	orts.	Selec	t All	Inv	erse	Deselect
		Sele	cted P	lort -		12" 1										
					-	-	orted	1								
		Roi		ort	Not	Supp		i		7						
	*	Roi	uted F	ort ype	Not	Supp		1	``````````````````````````````````````							
	*	Roi	uted F Port T	ort ype	Not	Supp		9								

(3) Switch to the Network mode. Choose Network> Wi-Fi > Wi-Fi Settings, and configure the SSID named Reyee_test and associate VLAN 6 with this SSID.

Ruíjie l &Rcycc	Network
Navigation	Wi-Fi Settings Guest Wi-Fi Wi-Fi List Healthy Mode Load Balancing
Coverview	Tip: Changing configuration requires a reboot and clients will be reconnected.
Network Planning	Wi-Fi Settings Device Group: Default 🗸
Wi-Fi	* SSID @Ruijie-mBCFA
RLDP	Band 2.4G + 5G \lor
DHCP Snooping	Security Open ~
WIO Radio Frequency	Collapse
Reyee Mesh	Wireless Schedule All Time 🗸
LAN Ports	VLAN 6
LED	Hide SSID (The SSID is hidden and must be manually entered.)
Alerts	Client Isolation Prevent wireless clients of this Wi-Fi from communicating with one another.
Batch Config	Band Steering (The 5G-supported client will access 5G radio preferentially.)
Gateway	XPress (The client will experience faster speed.)
Firewall	Layer-3 Roaming (The client will keep his IP address unchanged in this Wi-Fi network.)
8 Clients Management	Wi-Fi6 (802.11ax High-Speed Wireless Connectivity.) 🕜
😤 System 🗸 🗸	Save

Ruijie Reyce	test123 > EG105GW (Master)	•	English ×	Ruije Cloud - M Download	App 🖕 Network Setup 🗶 N	ebwerk Oberk - 16 Warn - 🕞	Joe Di
				nușe croau 📷 comincau i	and Automatical Sta	Construct Within G	
<i>8</i> ₀Overview	Wi-Fi Settings Guest Wi-F	i Wi-Fi List Healthy M	ode				
Online Clients							0
A Router	Tip: Changing configurat	ion requires a reboot and clients wi	I be reconnected.			(0
⊕Wireless ^	Wi-Fi List Device Group	K Default V				+ ^	dd
APs	Up to 8 SSIDs can be added	L.					
Wi-Fi	SSID	Band	Security	Hidden	VLAN ID	Action	
Clients	Reyee_test	2.4G + 5G	OPEN	No	6	Edit Delete	
Blacklist/Whitelist							
Radio Frequency	A demot ADD. 4	2.4G + 5G	WPA_WPA2-PSK	Yes	6	Edit Delete	
LAN Ports	C. Ingenteent.	2.4G + 5G	OPEN	No	Default VLAN	Edit Delete	
LED	Course ann a	2.4G + 5G	WPA, WPA2-PSK	Yes	7	Edit Delete	
Network Optimization							
Switches							
∑Network ~							
«Collapse							

- (4) Configure cloud authentication.
 - a Choose **CONFIGURATION** > **AUTHENTICATION** > **Captive Portal** to access the captive portal page, and click **Add** to create a portal template and edit the captive portal template.

Ruijie 🛆	MONITORING	CONFIGURATION MAINT	ENANCE *				ľ
A abcdelog(111.com ~		Captive Portal > Edit				×	1
	test123 V Sear	Name				Conflict Network Take over Network Unbind Device	
PROJECT							
	Note: There are R	Description	12				
Basic	Captie Portal	Login Options	One-click Login Voucher Account	SMS Registration		50	
Layout	Add Sync					Portal Name Q	
Radio		Show Balance Page Ø	CD				
WI-FI Optimization			https://www.ruljienetworks.com				
Bluetooth		Post-login URL	https://www.ruijienetworks.com			0.0	
Load Balancing	10000	Portal Page @				- ed SSID	8
	C Texperier Logis	Basic Advanced		Mobile Desktop	Reset Style		Ģ
Caplive Portal	Ernel Visal Norm	Logo Picture Ø Deta	will Logo Upload			ork of Synchronized EG	6
PPSK	(Contraction of the second sec					red on	
Voucher	O Oranda Lage	Background 🔵 k	mage 🔘 Solid Color	Progra 🛆		-01-18 13:59.05	
Account		Background image	ult Image Upload			xiption	
Easy Sharing		0	nu maže obrost	Noucher Login			
@ ADVANCED		Languages Englis	h × +				
Batch CLI Config			^	Access Code			1
Customize CLI Set		Welcome Message	Text Image	Lopin			
AP VLAN		Text	60 characters remaining	and the second s			
					1		
		Marketing Message	60 characters remaining				
		Torres & Constitution					
							~
		CONFIGURATION MAINT	ENANCE *			• 0 0 • a 🎕	~
A abcdefg@111.com ~	MONITORING		ENANCE *	(00.8+1ND)	Asia/Shanghai Manage Project		~
 A abcdefg@111.com ∨ PROJECT 	test123 V Sear	ch Network Q			Asia/Shanghai Manage Project		
 A abcdelg@111.com ✓ PROJECT WIRELESS 	test123 V Sear	ch Network Q	ENANCE *		Asia/Shanghai Manage Project		
A abcdr/g@111.com > PROJECT WIRELESS Basic	test123 V Sear	ch Network Q			AstarShanghai Manage Project		
A abdefg@111.com PROJECT WIRELESS Basic Layout	test123 V Sear Note: There are Re Captive Portal	ch Network Q			AsiaShanghar Manage Project	Conflict Network	
A abdolg@111.com PROJECT WIRELESS Basic Layout Radio	test123 V Sear Note: There are Re Captive Portal	ch Network Q			Aslathangha 🗌 Manage Project	Conflict Helmon Table over Helmonn United Device	
Acceleration	test123 V Sear Note: There are Re Captive Portal	ch Network Q			Aslathangha Manage Project	Conflict Helmon Table over Helmonn United Device	
A abdolg@111.com PROJECT WIRELESS Basic Layout Radio	test123 V Sear Note: There are Re Captive Portal	in Helenok Q	e enable Cloud Auth on EG for Reyee devices. <u>How to</u>	enable Coud Auth on Reyes EG2		Conflict Federary Table counterfeature () United Device Portal Factor Conflict Factor Conflict Factor Conflict Factor Conflict Federary Conflict Federary	
A abcategitti.com PROJECT WRELESS Basic Layout Radio WH-Fi Optimization Roaming	test123 V Sear Note: There are Re Captive Portal	ch Network Q	enable Cloud Auth on EG for Reyee devices. <u>How to</u>	enable Chost Auth on Reyes EG? (2) 8 645	5 S	Control Testeven Table over Factboork (United Deelca Period Harme Q S55	
A aboldgill tom A aboldgill tom PROJECT WRELESS Bask Layout Rado WHP Optimization Roaming Bustoch	test123 V Sear Note: There are Re Captive Portal	th Network Q	enable Cloud Auth on EG for Reyee devices. <u>How to</u>	enable Crost Auth on Reyes EG2 (2 645 Apple SBIO 2222 222		Control Testeven Table over Factboark (United Decka)	
A abcddg(111.con v A coddg(111.con v A coddg(111.con v WRELESS Basic Layout Radio WrFi Optimization Roaming Bisvelooth Load Balancing	test123 V Sear Note: There are Re Captive Portal	ventar	enable Cloud Auth on EG for Reyee devices. <u>How to</u>	enable Cloud Auth on Reyer EC2 C/ @ 645 Applied SSD 2222	Ownerstan Sector	Contractieneurs Tale over Network United Deeles	
A abcidge11.cm > A abcidge11.cm > PROJECT WRELESS Basic Layout Radio WH-Flopfmization Roaming Buetooth Lada Baancing Authentication	test123 V Sear Note: There are Re Captive Portal	ventia Test Appendiston Appendiston Masseculated with SSID Network of Synchronized to EG Created on	enable Cloud Auth on EG for Reyee devices. How to	enable Cloud Auth on Reyes EC2 G B Applied SISD 22222 Reteron of Shyrchronized EC3 hot procharacted EC3 consect on		Control freework Table over freetwork United Deckers Portial Flamme Q SS SS SS SS SG Sectors of synchronized ED Strated on	
A abcidge (111 com v A abcidge (111 com v PALECT WRELESS Basic Layout Radio WrFiC/Gemination Roaming Bushooth Load Balancing O AUTHENTICATION Captive Portal	test123 V Sear Note: There are Re Captive Portal	A hiterest Q yee devices in the network. Please writer Test Add associated with SBD Network of Systemicates D Not associated with SBD Network of SD Add SSD Not associated with SSD Not ass	enable Cloud Auth on EG for Reyee devices. <u>Hou to</u>	ensible Cloud Auth on Reyee E02 645 Applied SLID 22222 Hartoon to Stynchronaed EC3 Hold synchronaed EC3 Hold synchronaed EC3 Created on 2021-02.5 90:05:00		Control frieteen Tate over fasteen Channe Control Foreign Cont	
A abcidge (11 con v A abcidge (11 con v WreteEss Basic Layout Radio WreteOremization Roaming Biselooth Load Baarong Buefooth Load Baarong O Auth-MittiCatton Captive Portal Pisk Voucher Account	test123 V Saw Note: There are Re Captive Portal As3 Ond	ventia Test Appendiston Appendiston Masseculated with SSID Network of Synchronized to EG Created on	enable Cloud Auth on EC for Reyee devices. How to C	enable Cloud Auth on Reyes EC2 G B Applied SISD 22222 Reteron of Shyrchronized EC3 hot procharacted EC3 consect on		Control freework Table over freetwork United Deckers Portial Flamme Q SS SS SS SS SG Sectors of synchronized ED Strated on	
A aboldgi (11 con v A aboldgi (11 con v PALECT WRELESS Basic Layout Radio WH-Fi Openization Roaming Buetooth Load Balancing O AUTHENTICATION Captive Portal PPSK Youcher Account Easy Sharing	test123 V Saw Note: There are Re Captive Portal As3 Ond	A hiterest Q yee devices in the network. Please writer Test Add associated with SBD Network of Systemicates D Not associated with SBD Network of SD Add SSD Not associated with SSD Not ass	enable Cloud Auth on EG for Reyee devices. <u>Hou to</u>	ensible Cloud Auth on Reyee E02 645 Applied SLID 22222 Hartoon to Stynchronaed EC3 Hold synchronaed EC3 Hold synchronaed EC3 Created on 2021-02.5 90:05:00		Control Heleware Table Device Heleware United Devices Fortis Hamme SS SG Sector of Synchronized EC Sector of Synchronized EC Sector of Synchron	
A sheading (111 com v A sheading (111 com v PROJECT WRELESS Basic Layout Radio WHFI Optimization Roaming Burlsooth Lad Balancing O AUTHENTICATION Captive Portai PPSK Vusiter Account Easy Sharing WaySharing PAUANCED	test123 V Saw Note: There are Re Captive Portal As3 Ond	A hiterest Q yee devices in the network. Please writer Test Add associated with SBD Network of Systemicates D Not associated with SBD Network of SD Add SSD Not associated with SSD Not ass	enable Cloud Auth on EG for Reyee devices. <u>Hou to</u>	ensible Cloud Auth on Reyee E02 645 Applied SLID 22222 Hartoon to Stynchronaed EC3 Hold synchronaed EC3 Hold synchronaed EC3 Created on 2021-02.5 90:05:00		Control Heleware Table Device Heleware United Devices Fortis Hamme SS SG Sector of Synchronized EC Sector of Synchronized EC Sector of Synchron	
A aboling 111 con V A count E aboling 111 con V A count E aboling 111 con V Bable CLU Config Bable CLU Config	test123 V Saw Note: There are Re Captive Portal As3 Ond	A hiterest Q yee devices in the network. Please writer Test Add associated with SBD Network of Systemicates D Not associated with SBD Network of SD Add SSD Not associated with SSD Not ass	enable Cloud Auth on EG for Reyee devices. <u>Hou to</u>	ensible Cloud Auth on Reyee E02 645 Applied SLID 22222 Hartoon to Stynchronaed EC3 Hold synchronaed EC3 Hold synchronaed EC3 Created on 2021-02.5 90:05:00		Control Heleware Table Device Heleware United Devices Fortis Hamme SS SG Sector of Synchronized EC Sector of Synchronized EC Sector of Synchron	
A abrologi 11 com V A abrologi 11 com V Monecer Wreecess Basic Layout Radio WreFoOpenization Roaming Biselooth Lade Baarong Buerooth Lade Baarong O All'HEVITICATION Captive Portal P95K Voucher Account Easy Shaning Bakh Cu Zondh Easy Shaning Bakh Cu Zondh Easy Shaning	test123 V Saw Note: There are Re Captive Portal As3 Ond	A hiterest Q yee devices in the network. Please writer Test Add associated with SBD Network of Systemicates D Not associated with SBD Network of SD Add SSD Not associated with SSD Not ass	enable Cloud Auth on EG for Reyee devices. <u>Hou to</u>	ensible Cloud Auth on Reyee E02 645 Applied SLID 22222 Hartoon to Stynchronaed EC3 Hold synchronaed EC3 Hold synchronaed EC3 Created on 2021-02.5 90:05:00		Control Heleware Table Device Heleware United Devices Fortis Hamme SS SG Sector of Synchronized EC Sector of Synchronized EC Sector of Synchron	
A aboling 111 con V A count E aboling 111 con V A count E aboling 111 con V Bable CLU Config Bable CLU Config	test123 V Saw Note: There are Re Captive Portal As3 Ond	A hiterest Q yee devices in the network. Please writer Test Add associated with SBD Network of Systemicates D Not associated with SBD Network of SD Add SSD Not associated with SSD Not ass	enable Cloud Auth on EG for Reyee devices. <u>Hou to</u>	ensible Cloud Auth on Reyee E02 645 Applied SLID 22222 Hartoon to Stynchronaed EC3 Hold synchronaed EC3 Hold synchronaed EC3 Created on 2021-02.5 90:05:00		Control Heleware Table Device Heleware United Devices Fortis Hamme SS SG Sector of Synchronized EC Sector of Synchronized EC Sector of Synchron	
A abrologi 11 com V A abrologi 11 com V Monecer Wreecess Basic Layout Radio WreFoOpenization Roaming Biselooth Lade Baarong Buerooth Lade Baarong O All'HEVITICATION Captive Portal P95K Voucher Account Easy Shaning Bakh Cu Zondh Easy Shaning Bakh Cu Zondh Easy Shaning	test123 V Saw Note: There are Re Captive Portal As3 Ond	A hiterest Q yee devices in the network. Please writer Test Add associated with SBD Network of Systemicates D Not associated with SBD Network of SD Add Add Add Add Add Add Add Add Add Ad	enable Cloud Auth on EG for Reyee devices. <u>Hou to</u>	ensible Cloud Auth on Reyee E02 645 Applied SLID 22222 Hartoon to Stynchronaed EC3 Hold synchronaed EC3 Hold synchronaed EC3 Created on 2021-02.5 90:05:00		Control Heleware Table Device Heleware United Devices Fortis Hamme Q ISS special SSID G estina of synchronized EC estina of S2:-01-13.59.05 becketpion	
A abrologi 11 com V A abrologi 11 com V Monecer Wreecess Basic Layout Radio WreFoOpenization Roaming Biselooth Lade Baarong Buerooth Lade Baarong O All'HEVITICATION Captive Portal P95K Voucher Account Easy Shaning Bakh Cu Zondh Easy Shaning Bakh Cu Zondh Easy Shaning	test123 V Saw Note: There are Re Captive Portal As3 Ond	A hiterest Q yee devices in the network. Please writer Test Add associated with SBD Network of Systemicates D Not associated with SBD Network of SD Add Add Add Add Add Add Add Add Add Ad	enable Cloud Auth on EG for Reyee devices. <u>Hou to</u>	ensible Cloud Auth on Reyee E02 645 Applied SLID 22222 Hartoon to Stynchronaed EC3 Hold synchronaed EC3 Hold synchronaed EC3 Created on 2021-02.5 90:05:00		Control Heleware Table Device Heleware United Devices Fortis Hamme Q ISS special SSID G estina of synchronized EC estina of S2:-01-13.59.05 becketpion	
A abrologi 11 com V A abrologi 11 com V Monecer Wreecess Basic Layout Radio WreFoOpenization Roaming Biselooth Lade Baarong Buerooth Lade Baarong O All'HEVITICATION Captive Portal P95K Voucher Account Easy Shaning Bakh Cu Zondh Easy Shaning Bakh Cu Zondh Easy Shaning	test123 V Saw Note: There are Re Captive Portal As3 Ond	A hiterest Q yee devices in the network. Please writer Test Add associated with SBD Network of Systemicates D Not associated with SBD Network of SD Add Add Add Add Add Add Add Add Add Ad	enable Cloud Auth on EG for Reyee devices. <u>Hou to</u>	ensible Cloud Auth on Reyee E02 645 Applied SLID 22222 Hartoon to Stynchronaed EC3 Hold synchronaed EC3 Hold synchronaed EC3 Created on 2021-02.5 90:05:00		Control Heleware Table Device Heleware United Devices Fortis Hamme Q ISS special SSID G estina of synchronized EC estina of S2:-01-13.59.05 becketpion	

1 Note

One-click Login: indicates login without the username and password. Access Duration and Access Times per day can be configured.

Voucher: indicates login with a random eight-digit password.

Account: indicates login with the account and password.

b Make sure that the Reyee EG is online on Ruijie Cloud. Click its SN in the list to access the configuration page.

Ruijie 📥	MONITOR	ING CON	FIGURATION	MAINTENANCE								0 0	® 6
abcdefg⊜111.com ∨	ALL V	test123 V	Search Network	٩					(GMT+8:00)Asia/Shangh:	al Manage Project Conflict Ne	work Take over	Network Unb	ind Device
DASHBOARD													
TOPOLOGY	Gatewa	ay List									Auto Refresh:	000	11 - C
LARM	Add	Web CLI	eWeb More	+ 0 Selected							SN 4		n C
REPORT													
Network		Status	⊿ SN	Alias ¢	MGMT IP 172.26.5.237	MAC 300d.9ee7.e915	Egress IP 120.35.11.195	Network	Firmware Version ReveeOS 1.55.1915	Offline Time 2022-03-19 07:00:07	Model EG105GW	Description Empty	Actio
loucher		Online	1	Ruite	172.26.5.253	c0b8.e635.283c	0.0.0	test123	ReyeeOS 1.55.1325	-	EG105G-P	Emply	Û
EVICE			/										
р					First	Previous Page	1 0 of 1	Next				10 🔺	2 in 10
Switch													
Saleway													
Home Router													
Bridge													
AMERA													
Cameras													
IVR													
LIENT													

c Click **Cloud portal Auth** to configure authentication on Ruijie Cloud.

Ruíjie	MONITORING	CONFIGURATION MAINTENANCE*			×	<i>•</i>	000	9 8
A abcdefg@111.com v	ALL V Search N	Device Information				Take over Network	Unbind	Device
DASHBOARD		WAN LAN Disconnected Disabled PPPoE State: P DHCP PGE Abnormal Copper SPP	Basic					
A TOPOLOGY	Gateway List	VAN LAN Disconnected Usabled PPPOE Static P UHUP POE Adnormal Copper SPP	Alias: SN:	EG105GW	Auto R	efresh: 🔍 🕯	€ 2 8	R = 20
E ALARM	Add Web 0		MAC: Model:	300d.9ee7.e915 EG105GW				Q
Network	Status	Operation Mode: Route	MGMT IP:	172.26.5.237	Offline Time	Model EG2100-P	Descriptio	n Action
Voucher	Online	Actual Master Device: H1PH745119402 Network Master Device: G1PHCA4047747 G H1PH745119402 G H1PTATC001746	Sync: Hardware Version:	Synchronized 1.10	2-03-19 07:00:07	EG105GW	Empty	Û
B DEVICE	Online	SSID: Reyee_test, Internal_APP-1, IT department, Guest_APP-1	Firmware Version: Description	ReyeeOS 1.55.1915	- 2-03-28 10:43:07	EG105G-P EG105G-P	Empty	1 1
AP AC	 Online Offline 	Overview Config	o co		2-04-20 16:36:07	EG105G-P-V2		0
Switch	Cffline	Diagnose			1-09-08 19:01:07	EG2100-P EG105G-P	Empty Empty	10 - 10 -
Gateway Home Router	C) C Control	Web CLI eWeb SSH Tunnel Cloud Portal Auth					10 - 7	
Bridge		IPTV			_			
A CAMERA		IPTV/VLAN						
Cameras		WAN LAN Disconnected Disabled PPPoE Static IP DHCP	PoE Abnormal Copper	SFP				
R CLIENT								
		Dynamic DNS 🛛						
		No-IP DynDNS						
		Service Interface wan0 v						

d Enable Auth, and set Auth IP Range to 192.168.6.2-192.168.6.254 for authentication, and select a portal template to be used. Then click **Save** to save all configurations.

Advanced Solution

Ruíjie	MONITORING		0aa7 a015	🗳 🛛 😖	0 0
A abode(p@111.com ~	ALL ~ Search for	Cloud Portal Auth	× milici Network	Take over Network Unb	blad Davis
DASHBOARD	ALL - CONTRACT	Auth @			
A TOPOLOGY	Gateway List	Portal Escape 🕘 💽	Auto	Refresh 🔍 🖯 🖄	IT = 2
5 ALARM	Add Web G	Autn IPRange 192.168.6.2-192.168.6.254 +			n Q
REPORT	Status		Offine Time	Model Descrip	iption Actio
Network	O Online	Seamless Online 🔮 🛛 💭	504-20 09:29:07	EG2100-P Emply	. 0
Voucher	Online	User Offline Detection	-03-19 07:00:07		
8 DEVICE	Online		-	EG105G-P Emply	v (1)
	Online	Please select a portal or add a new portal.	-03-28 10:43 07	EG105G-P Emply	v 6
	C © Offine	Test 645 555	-04-20 16:36:07	EG105G-P-V2 Emply	
	C O Office		-09-08 19:01:07	EG2100-P Ensolv	v B
	C © Ottine	State of the second sec	-04-19 21:36:07	EG105G-P Empty	
		111		10.4	7 in tota
		O Register Login			
		Enal			
9. CAMERA		Your Name	>		
Cameras					
R CLIENT		O Decida Logo			
		0 -#D#			
			4		
			Close		

Note

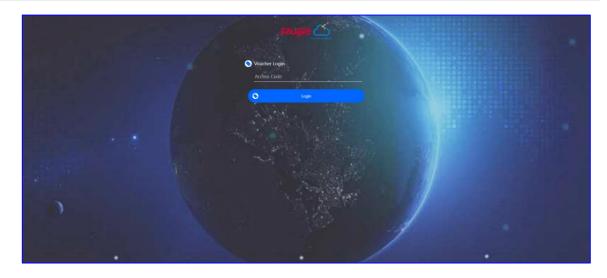
IP addresses of the EG, switch, and AP need to be excluded; otherwise, the switch cannot access the Internet.

5.2.4 Configuration Verification

 Choose Advanced > LAN > Authentication > Cloud Auth to check whether the configuration has been synchronized to the EG.

Ruijie Rcycc	test123 > EG105GW Maxtur O English ~ _ Ruijie Cloud 🏭 Download App 🔌 Network Setup @ Network Check 🖄 Warn 🕞 Log Out
နို့Overview	Roser Hostname: EG105GW SN: IP: 172265.237 O Reboot C Reboot • EG105GW MAC: 300D/9E/27:8:15 O C Reboot C
Online Clients	Overview Basics Security Behavior VPN Advanced Diagnostics System S
Router	Cloud Auth Whitelist Online Users
🖻 Switches	Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication and one-click authentication. Please log into Ruijie Cloud to enable authentication. View If the IP address of the EAP device is in the authentication IP range, please choose Whitelist to add the EAP MAC address to the MAC address whitelist.
\dot{a}_{a}^{a} . Network	Authentication
	* Server Type Cloud Integration \vee
	* Auth Server URL portal.ruijienetworks.com
	Client Escape 🗧 Enable
	* IP/IP Range 192.168.6.2-192.168.6.254 Add
	Save
Collapse	

(2) Users whose IP addresses are in the range of 192.168.6.2 to 192.168.6.254 need to be authenticated before accessing the Internet.



5.3 Reyee Guest Wi-Fi Solution

5.3.1 Working Principle

A single Internet entrance is created by using guest Wi-Fi. The devices that are allowed to access guest Wi-Fi can access the Internet but cannot access the home Wi-Fi.

5.3.2 Application Scenario

Guest Wi-Fi provides a secured Wi-Fi access for guests to share your home or office network. When someone visits your house, apartment, or workplace, you can enable the guest Wi-Fi for them. You can set different access options for guest users, which is very effective to ensure the security and privacy of your main network.

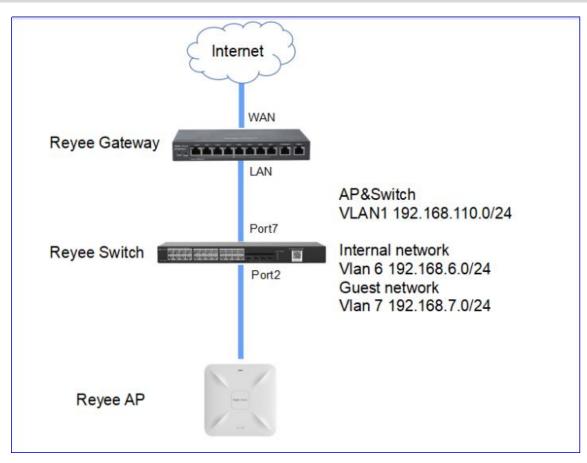
5.3.3 Configuration Example

1. Configuration Through EG's Eweb

Requirement

Guest Wi-Fi is configured for guests on the network segment of VLAN 7 and the guests are not allowed to access the internal network on the network segment of VLAN 6.

Network Topology



Network Description

- The EG works as a DHCP server to assign IP addresses to users, Reyee AP, and Reyee switch.
- The Reyee AP and switch obtain the IP address on the network segment of VLAN 1 for Internet access.
- Internal users obtain IP addresses in the network segment of VLAN 6 for Internet access and guests obtain IP addresses on the network segment of VLAN 7 for Internet access

Configuration Steps

- (1) Configure VLAN 6 and VLAN 7 on the router.
 - a Switch to the Local mode. Choose Network > LAN > LAN Settings >Add.

Ruijie IRcycc	Local Device(EGJ	2.0						English ~ 🛆 Ramot	ta O&M 👋 Network Setup 🎕 Network C	beck ≜Alert ⊝Log Du
A Overview	LAN Settings	DHCP Clients Static IP Addres	ses DHCP Option DNS Proxy							
Online Clients	🕧 LAN Sett	tings								0
Network WAN	LAN Setting	gs							+ Add	Colete Selected
LAN	Up to 🛢 entri	ies can be added.								
IPv6 Address		P	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
Port VLAN		192.168.110.1	255.255.255.0	Default VLAN		Enabled	192.168.110.1	254	30	Edit Delete
Port Settings		192.168.11.3	255.255.255.0	11		Disabled				Edit Delete
IFTV © Security ~		192.168.12.1	255.255.255.0	12		Disabled				Edit Delete
di Behevior		192.168.116.1	255.255.255.0	13	11111	Disabled				Edit Delete
💷 vpn 🧹										
🗎 Advanced 🛛 🗠										
R Diagnostics ~ ~										
🕸 System 🗠										

b Perform LAN settings and configure DHCP address pools of VLAN 6 and VLAN 7 on the router.

Add	ł	×
ſ	* IP	192.168.6.1
	* Subnet Mask	255.255.255.0
	* VLAN ID	7
	Remark	Remark
	MAC	80:D0:F8:0A:19:E7
	DHCP Server	
	* Start	192.168.6.1
	* IP Count	254
	* Lease Time(Min)	30
	DNS Server	192.168.6.1 🕖
		Cancel OK
Ac	ld	Cancel
Ac		
Ac	*	IP 192.168.7.1
Ac		IP 192.168.7.1
Ac	*	IP 192.168.7.1 sk 255.255.255.0
Ac	* * Subnet Ma	IP 192.168.7.1 sk 255.255.255.0 D 7
Ac	* * Subnet Ma * VLAN I	IP 192.168.7.1 sk 255.255.255.0 D 7 rk Remark
Ac	* * Subnet Ma * VLAN I Rema	IP 192.168.7.1 sk 255.255.255.0 D 7 rk Remark AC 30:0D:9E:A0:54:4A
Ac	* Subnet Mar * VLAN I Rema * MA	IP 192.168.7.1 sk 255.255.255.0 D 7 rk Remark C 30:0D:9E:A0:54:4A er
Ac	* Subnet Ma * VLAN I Rema * MA DHCP Serv	IP 192.168.7.1 sk 255.255.255.0 D 7 rk Remark C 30:0D:9E:A0:54:4A er 192.168.7.1
Ac	* Subnet Mar * VLAN I Rema * MA DHCP Serv * Sta	IP 192.168.7.1 sk 255.255.255.0 D 7 rk Remark AC 30:0D:9E:A0:54:4A er 192.168.7.1 nt 254

 \times

Ruíjie Rcycc	test123 >	EG105GW [Maste			ion succeeded.		i 웷Download App	Network Setup	Network Check	<u>∦äi</u> Warn ⊟Log (
ి _ద Overview	• EG	i 105GW ew Basics ~ S	MAC: SUUD.SECT.E: Security ~ Behavior		dvanced 🐃 Diag	nostics ~ System	~			
Online Clients Router	LAN Set	tings DHCP CI	lients Static IP Ad	dresses DHCF	P Option DNS	Ргоху				
	() I	AN Settings								0
🖻 Switches	LAN	Settings							+ Add	Delete Selected
-9- -9- Network	Up to	8 entries can be a	dded.							
		IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
		192.168.110.1	255.255.255.0	Default VLAN		Enabled	192.168.110.1	220	30	Edit Delete
		192.168.1.1	255.255.255.0	2	-	Enabled	192.168.1.1	254	30	Edit Delete
		192.168.6.1	255.255.255.0	6	-	Enabled	192.168.6.1	254	30	Edit Delete
		192.168.7.1	255.255.255.0	7		Enabled	192.168.7.1	254	30	Edit Delete

- (2) Configure VLANs for a switch.
 - a Switch to the **Network** mode. Choose **Device** > **Switch**.

Device List	o.					B19AAC/hostmarnel	SN(S_G_) Delete Office Devices Devices
	529 C	Status 2	Hostowie 2	MAC =	P 2	Softward Wer	Model =
	011/0815000043	Online	Refe Z	5849467822.67	5 1011 441 521	RepertOS 1.206.2122	NISS1100-24074579-9
	MACCNESSOON	Othe	Roje C	00005887736640	10.166.110.3.4	ReperID 1.206.2116	N856002
	10/paga -						Total 2

- b Select a device from **Device List** and access the configuration page.
- c In the **VLAN** pane, select a VLAN and click **Edit** to configure the VLAN.

MSW	Hostname: Ruijie 🖉 Model:NBS3100-24GT45FP-P SN:G1NWB1S000043		Software Ver:ReyeeOS 1.206.212 MGMT IP: 192.168.110.6 & MAC: 58:69:6C:FB:22:C7	2
Port Status VLAN Info	Port Status			
Port				Panel View
RLDP	VLAN			Edit 💿
More	VLAN1 VLAN13			
	Interface	IP	IP Range	Remark
	Port			Edit 🕲
	Interface	Туре	VLAN	DHCP Pool
		TRUNK		
	Port List	-		
	Interface	Туре	VLAN	DHCP Pool
		Ν	lo Data	
	Total 0 10/page 🗸 🤇 1	Go to page 1		

d Click Add VLAN to create VLAN 6 on the switch.

VLAN Info

Vlan ID	Remark VLAN0001
Vlan ID 13	Remark 11111
Vlan ID	Remark
6	

+Add VLAN	+Batch Add	-Delete Selected		
			Cancel	Save

e In the **Port** pane, click **Edit**, configure port2 and port9 connected to the AP and EG as trunk ports and configure them to allow packets from VLAN 1 and VLAN 6 to pass through, and check port settings on the device.

rt										 	 	
1 3	5 7	9	11	13	15	17	19	21	23			
		-										
	•								•			

Port				
Available 🚺 Ur	navailable 👘 Aggreg	gate 🔳 Uplink 📕	Copper Fiber	
1 3 5 7	9 11 13 15 17	19 21 23		
2 4 6 8	10 12 14 16 18	20 22 24 25 2	26 27 28	
lote: You can click and Selected Port	d drag to select one or mor	e ports. Select All I	nverse Deselect	
	Not Supported			
Port Type	Access Port \lor			
* Access VLAN:	1 ~			
				c

(3) Switch to the Network mode. Choose Network > Wi-Fi > Guest Wi-Fi, and configure a guest Wi-Fi SSID named Guest_Wi-Fi_Reyee and associate VLAN 7 with this SSID.

Wi-Fi Settings	Guest Wi-Fi	Wi-Fi List	Healthy Mode	Load Balancing
i Tip: Changin	g configuration i	equires a reboot	and clients will be re	connected.
Guest Wi-Fi	Device Group:	Default		
Enal	ble 🚺			
* 55	Guest_W	iFi_Reyee		
Ba	nd 2.4G + 5	G		
Secur	ity WPA_WF	A2-PSK		
* Wi-Fi Passwo	ord		>yyd	
		Collapse		
Effective Tir	me Never D	sable		
VL	AN 6		~	
Hide SS		e SSID is hidder	and must be man	ually entered.)
Client Isolati	ion 🔵 Pre	vent wireless cli	ents of this Wi-Fi fr	rom communicating with one another.
Band Steeri	ing 🔵 (Th	e 5G-supported	l client will access 5	5G radio preferentially.)
XPre	ess 🔵 (Th	e client will exp	erience faster speec	d.)
Layer-3 Roami	ing 🔵 (Th	e client will keep	p his IP address und	changed in this Wi-Fi network.)
Wi-	Fi6 🚺 (80	2.11ax High-Sp	eed Wireless Conne	ectivity.) ⑦
	S	ave		

(4) Choose **Network** > **Wi-Fi** > **Wi-Fi** List > **Add**, configure the internal user SSID named Internal_network_Reyee, associate VLAN 6 with this SSID, and check Wi-Fi settings in the Wi-Fi list.

Edit Dele

Edit Delete

Add				×	
i The configurat	ion will take effe	ect after being delive	red to AP.		
* SSID	Internet_netwo	ork_Reyee			
Band	2.4G + 5G		\sim		
Security	Open		\sim		
	Colla	pse			
Wireless Schedule	All Time		\sim		
VLAN	6		~		
Hide SSID Wi-Fi Settings Guest Wi-Fi Wi-Fi	entered.)	D is hidden and must	be manually		
ip: Changing configuration require	es a reboot and clients will b	e reconnected.			0
Wi-Fi List Device Group: Default					+ Add
Up to 8 SSIDs can be added.					
SSID	Band	Security	Hidden	VLAN ID	Action
RAP2	2.4G + 5G	WPA_WPA2-PSK	No	10	Edit Delete

(5) Switch to the Local mode. Choose Behavior > Access Control, configure an ACL to block traffic from guests on the network segment 192.168.7.0/24 of VLAN 7 to internal users on the network segment 192.168.6.0/24 of VLAN 6, and apply the ACL rule to the LAN interface on the EG.

No

No

WPA_WPA2-PSK

WPA_WPA2-PSK

2.4G + 5G

2.4G + 5G

st WiFi Reye

Ruijie IRcycc	Local Device(EG2 ->-						
A Overview © Online Clients © Network ~	ACL Configure ACL based on IP addresses. Reverse Bore The L2TB/PETB/Cpeni/RN VPN only supports the SH- Example: Candidagres as damy ACL entry containing or Try: Configure one more damy ACL entry containing	based ACL. The effective interface must be configurate IP address 192,168,1,0/24 and destination	m IP address 192.168.2.0/24. Device configur	ed with IP address 192,168.1.x will feil to acc ices will be mutually unreachable.	ees device 192,168.2.x. But slevice 192,168.2.x will be allowed to access device 192	2161.	Ø
⊖ Security ~	ACL List						+ Add 🛛 Delete Selected
ff Behavior	Up to 50 entries can be added.						
App Control	D Rate	Control Type	Effective Time	Interface	Effective State	Remark	Action
Website Management					No Data		
Row Control Access Control User Management	< 3 > 10/page ~						Total D
Time Management							
🗢 vøn 🗸							
Advanced ~ ~							
 Diagnostics ~ ~ 							
S System -							

Ado	d Rule				×			
	Based on	o mac 💿 IP						
Si	rc IP Address: Port	192.168.7.0/24	: 1	-65535				
De	st IP Address: Port	192.168.6.0/24	: 1	-65535				
	Protocol Type	All Protocols		\sim				
	Control Type	Block (Reverse f	low mismatches)	\sim				
	Effective Time	All Time		~				
	Interface	LAN		~				
	Remark	Black Guest						
			Cano	el	ж			
ACL	List						+ Add	📋 Delete Selecte
Up	to 50 entries can be added.	Control Type	Wireless Schedule	Interface	Effective State	Remark	Match	Action
	Src IP Address 192.168.7.0/24 : All Ports Dest IP Address 192.168.10.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active	VLAN 10_Intranet_isolation	Order J	Edit Delete
	Src IP Address 192.168.7.0/24 : All Ports Dest IP Address 192.168.6.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active	Block Guest	1 L	Edit Delete
	Src IP Address 192.168.7.0/24 : All Ports Dest IP Address 192.168.111.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active	_Intranet_isolation	1	Edit Delete

Configuration Verification

A guest at 192.1687.2 cannot access the internal network user at 192.168.6.2.

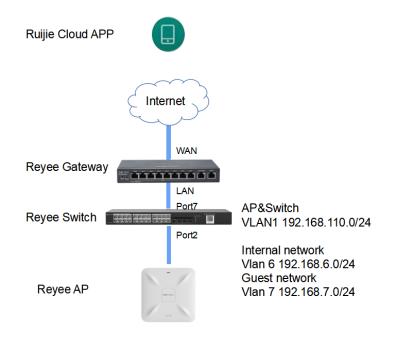


2. Configuration Through Ruijie Cloud APP

Requirement

Guest Wi-Fi through Ruijie Cloud App is configured for guests on the network segment of VLAN 7, who cannot access the internal network on the network segment of VLAN 6. Ruijie Cloud App will deliver the corresponding configuration to the device automatically.

Network Topology

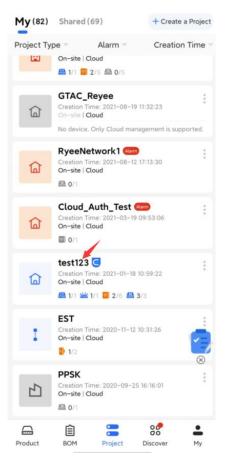


Network Description

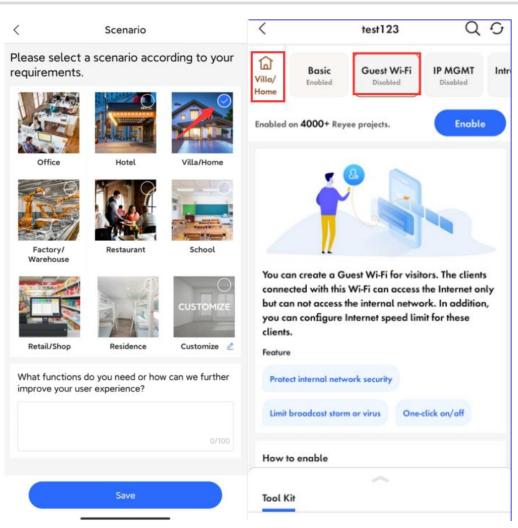
- The EG works as a DHCP server to assign IP addresses to users, Reyee AP, and Reyee switch.
- The Reyee AP and switch obtain IP addresses on the network segment of VLAN 1 for Internet access.
- Internal users obtain IP addresses on the network segment of VLAN 6 for Internet access and guests obtain IP addresses on the network segment of VLAN 7 for Internet access.

Configuration Steps

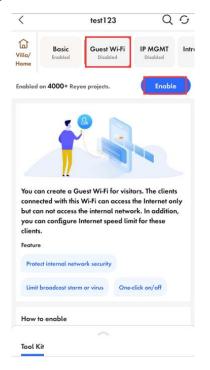
(1) Log in to your Ruijie Cloud App on the smartphone and access the project with Reyee router and RAP.



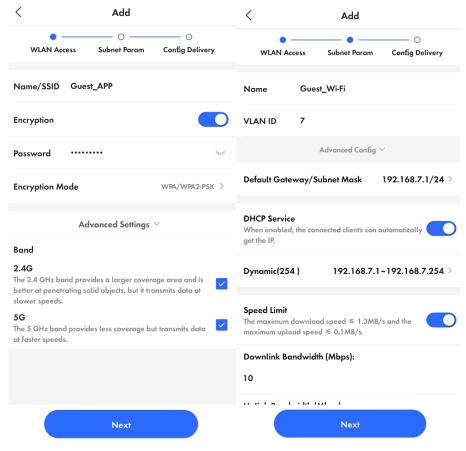
(2) Select Villa/Home under Scenario. You can see the Guest Wi-Fi button.



(3) Select Guest Wi-Fi and click Enable button.



(4) Modify gest Wi-Fi information, configure an Internal user SSID named Guest_APP and associate VLAN 6 with this SSID, and configure a guest Wi-Fi SSID named Guest_Wi-Fi and associate VLAN 7 with this SSID. Then Click Save to save your configuration.



- (5) Wait around 1 minute for the system to deliver the configuration to the device.
 - < Configuration Delivery



<	Configuration succeeded	<	test123	QG
		Villa/ Home	Guest Wi-Fi Enobled	IP MGMT Intro
	Delivery succeeded		Internet Resources	in an interest
		Configuration		
		Guest Wi-Fi		
		Configured :		
		Wi-Fi: Guest_APPVLAN: 7	 Internet spe Not allow t network 	eed limit o access interna!
		Tool Kit	\sim	

Configuration Verification

A guest at 192.168.7.97 cannot access the internal user at 192.168.6.147.

Ruijie	uest_APP 80W e:b9:70:73:a4:9		-16 dBm
	Channel:56	Link speed:390) Mbps
. IP	:192.168.7.97	MAC:bce2.659	a.8dbe
Gatewo	iy:192.168.7.1	DNS:192.168.	7.1
-20		~~	
-80			
	92.168.6.14	47	DONE
Hanor View	10 Par	ise ise	
13	0	100.00%	0 ms
Sent	Received	Loss rate	Avg Delay

5.4 Reyee Economic Hotel Network Solution

5.4.1 Application Scenario

Reyee economic hotel network solution provides an affordable 5-star Wi-Fi for clients. It can operate concurrently at 2.4 GHz and 5 GHz, providing high-speed wireless access of 574 Mbit/s at 2.4GHz, 1201 Mbit/s at 5 GHz,

and up to 1775 Mbit/s per AP. The wall AP provides a LAN port at the front to facilitate the expansion of IPTV terminals, IP phones, and other terminals.

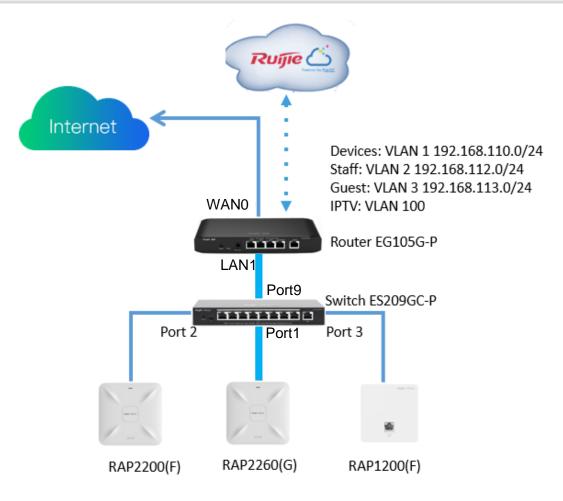


5.4.2 Configuration Example

Requirement

- A wireless network needs to be built for the hotel, and guests need to pass voucher authentication before accessing the Internet and are not allowed to access the internal network of the hotel.
- Wired connections are configured for IPTV.

Network Topology



Devices List

Туре	Model	Function
Router	EG105G-P	 Connects to the Internet and works as the DHCP server for downlink devices and clients. Manages the AP and switch locally. Supports voucher authentication with Ruijie Cloud.
Switch	ES209GC-P	Provides wired and PoE connections.
Wall AP	RAP1200(F)	Provides wireless connections for rooms. Provides a wired connection for IPTV.
Indoor AP	RAP2200(F)&RAP2260(G)	Provides wireless connections for the hall and corridor.

Configuration Steps

(1) Power on and connect the device according to the topology.

(2) By default, the IP address of the router is 192.168.110.1. Click **Start Setup** to perform basic network setting.

	Devices: 5. nake sure that the device count and topology are co	ment. The unmanaged switch will not a	innear in the list			Ø
	uare une une une devices (oune and oppology are co atus (Online Devices / Total)	ОНСР	Revent	Desta 1/1 Switches	(空) 1/1 APs	Refresh Q
	Network					
	Model	SN	IP	MAC	Software Ver	
Se Re	EG105G-P-V2 [Master]	EG3 '0019	192.168.110.1	00:DC 08:43	ReyeeOS 1.56.1325	
	P RAP1200(F)	G1QF 384A	192.168.110.205	C4:70: 3:6A	AP_3.0(1)B11P35,Release(08132700)	
	P RAP2260(E)	G1QH 0534	192.168.110.200	EC:89: 4:97	ReyeeOS 1.75.1318	
	P RAP2200(F)	G1QH 1978	192.168.110.39	C4:70:A :64	ReyeeOS 1.75.1320	
5	witch RG-ES209GC-P	CAQC 4240	192.168.110.44	EC:89:7(B5	ESW_1.0(1)B1P3,Release(07200415)	

a Set Network Name, Network Settings, SSID for staffs, and Management Password.

* Network Nan	e Reyee-Hotel
Network Settin	gs
	t OPPPOE ODHCP Static IP Current Settings: DHCP Hotel-Staff
WI-FI Passwo	d O Security O Open
	••••••
Management I	assword (Please remember the password.)
* Manageme Passwo	
Country/Regio	n/Time Zone
* Country/Regi	n China (CN) ~
	e (GMT+8:00)Asia/Shanohai v revious Create Network & Connect
	evious Create Network & Connect

b Click Create Network & Connect to active the configuration and add the devices to Ruijie Cloud.

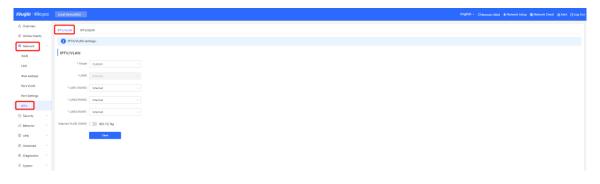
A abc 1.com V	Reyee-Hotel V Search Network Q	
位 DASHBOARD	Texture Advant	
윦 TOPOLOGY	Topology Advanced	
前 ALARM	Please select the device	
REPORT		
Network	(WAN)	
Voucher		
B DEVICE	EG105G-P	
AP	EG105G-P	
AC	(LAN1)	
Switch	(Uplink)	
Gateway Home Router	фина.	
Bridge	Unknown	
A CAMERA	Virtual device	
Cameras	(port2) (port3)	(port1)
NVR	(WAN) (WAN)	(WAN)
A CLIENT	φ φ	Ţ
	AP AP RAP1220(F) RAP2250(E)	AP RAP2200(F)

(3) Switch to the Local mode. Choose Network > LAN > LAN Settings to create VLAN 2 and VLAN 3 for staffs and guests.

Rugie IRcycc	E Local Deviced	(02) w						English - 🛆 Remo	ne O&M 👋 Network Setup 🚳 Network C	Deck #Alert @Log (
A Overview	LAN Settings	DHCP Clients Static IP Addre	esses DHCP Option DNS Proxy							
Network	🚺 LAN S	() Lis serings								
WAN	LAN Sett	LAN Settings								
LAN	Up to 8 er	tries can be added.								
IPv6 Address			Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
Port VLAN		192.168.110.1	255.255.255.0	Default VLAN		Enabled	192.168.110.1	254	10	Edit Delete
Port Settings		192.168.11.3	255,255,255,0	11		Disabled				Edit Delete
IPTV		192.168.12.1	255.255.255.0	12		Disabled				Edit Delete
() Security ~ ~		192.168.116.1	255.255.255.0	13	11111	Disabled				Edit Delete
© v₽N ~										
Advenced										
Diagnostics ~ ~										
S System ~										

(4) Switch to the Local mode. Choose Network > IPTV to perform IPTV settings obtained from the ISP.

For example, the VLAN ID for IPTV is 100.



IPTV/VLAN IPTV/IC	SMP	
iPTV/VLAN set	tings.	
IPTV/VLAN		
* Mode	Custom \lor	
* LANO	Internet v	
* LAN1/WAN3	IPTV ~	
* LAN2/WAN2	Internet \lor	
* LAN3/WAN1	Internet V	
* IPTV VLAN ID	100	
Internet VLAN (WAN)	802.1Q Tag	
	Save	

(5) Choose Network > LAN Ports > Add and configure VLAN 100 for IPTV. If the default VLAN 1 is used, ignore this step.

Rujjie	Network			Navigation Q	English ~	△Remote O&M	A Network Setup	Network Check	<u>清</u> Alert	🕒 Log Ou
Q Navigation	LAN Port Settings									
Overview	The configuration takes effect only for the AP with Note: The configured LAN port settings prevail.	Add			×					
a Network	Default Settings	VLAN ID	100		0					
Network Planning	VLAN ID	* Applied to	Enter an AP name or SN.							
Wi-Fi	(Range: 2-232 and 234-4090.	Applied to	Enter an AP name or SN.							
WIO	WAN port.)			Cancel	ок					
Radio Frequency	Applied to AP device with no LAN port se	ttings 0								
Reyee Mesh	Save									
LAN Ports	LAN Port Settings							+ Add 🗊		
LED Alerts	Up to & VLAN IDs or 32. APs can be added (0. APs ha									
Alerts		ve been added).								
Gateway	VLAN ID ¢			Applied to				Action		

(6) Choose Network >Wi-Fi > Wi-Fi Settings, configure Wi-Fi for staffs and guests, and select VLAN 2 for staffs.

Ruijie #Rcycc	Network
Q Navigation	Wi-Fi Settings Guest Wi-Fi Wi-Fi List Healthy Mode Load Balancing
Overview	· · · · ·
😤 Network 🔷	Tip: Changing configuration requires a reboot and clients will be reconnected.
Network Planning	Wi-Fi Settings Device Group: Default
Wi-Fi	* SSID @Ruijie-m0868
WIO	Band 2.4G + 5G ~
Radio Frequency	Security Open \lor
Reyee Mesh	Collapse
LAN Ports	Wireless Schedule All Time \lor
LED	VLAN 2
Alerts	4
Devices	Hide SSID (The SSID is hidden and must be manually entered.)
🖹 Gateway	Client Isolation OPrevent wireless clients of this Wi-Fi from communicating with one another.
Ø Clients Management	Band Steering (The 5G-supported client will access 5G radio preferentially.)
📳 System 🗸 🗸	XPress (The client will experience faster speed.)
	Layer-3 Roaming (The client will keep his IP address unchanged in this Wi-Fi network.)
	Wi-Fi6 (802.11ax High-Speed Wireless Connectivity.) ⊘
	Save

(7) Enable the guest Wi-Fi and select VLAN 3 for it.

Switch to the Network mode. Choose Network > Wi-Fi > Guest Wi-Fi.

Ruíjie ARcycc	Network
Navigation Overview	Wi-Fi Settings Guest Wi-Fi List Healthy Mode Load Balancing
A Network	<i>i</i> Tip: Changing configuration requires a reboot and clients will be reconnected.
Network Planning	Guest Wi-Fi Device Group: Default V
Wi-Fi	Enable
RLDP	* SSID @Ruijie-guest-BCFA
DHCP Snooping	Band 2.4G + 5G \checkmark
WIO	Security Open 🗸
Radio Frequency	Collapse
Reyee Mesh LAN Ports	Effective Time Never Disable \vee
LED	VLAN 13 (11111)
Alerts	Hide SSID (The SSID is hidden and must be manually entered.)
Batch Config	Client Isolation OPrevent wireless clients of this Wi-Fi from communicating with one another.
Devices	Band Steering (The 5G-supported client will access 5G radio preferentially.)
🖶 Gateway	XPress (The client will experience faster speed.)
Firewall	Layer-3 Roaming (The client will keep his IP address unchanged in this Wi-Fi network.)
8 Clients Managemént System	Wi-Fi6 (802.11ax High-Speed Wireless Connectivity.) 🕐
	Save

(8) Switch to the Local mode. Choose Behavior > Access Control and configure an ACL to prevent guests from accessing the internal network.

Add two ACL rules to prevent hosts in VLAN 3 from accessing hosts in VLAN 1 and VLAN 2, and apply them to the LAN port.

Add Rule				×			
Based on	O MAC 💿	I IP					
Src IP Address: Port	192.168.113.	0/24 :	1-65535				
Dest IP Address: Port	192.168.110.	0/24 :	1-65535				
Protocol Type	All Protocols		~				
Control Type	Block (Rever	se flow mismatch	ies) 🗸				
Effective Time	All Time		~				
Interface	LAN		~				
Remark	Enter the AC	L purpose.					
ACL List			Cancel	ок		+ Add	Delete Selected
Up to 50 entries can be added.							
Rule	Control Type	Wireless Schedule	Interface	Effective State	Remark	Match Order	Action
Src IP Address 192.168.113.0/24 : All Ports Dest IP Address 192.168.112.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active		4	Edit Delete
Src IP Address 192.168.113.0/24 : All Ports Dest IP Address 192.168.110.0/24 : All Ports Bestened All Portscole	Block	All Time	LAN	Active		٢	Edit Delete

- (9) Log in to Ruijie Cloud to configure cloud voucher authentication for guests.
 - a Click the SN of the EG to access the page of device details.

	ALL \sim	Reyee-Hote	Search Network	Q					(GMT+8:00)A	sia/Shanghai Manage Project	Take over Ne	twork Unbin	d Device
DASHBOARD													
TOPOLOGY	Gatewa	ay List								Au	to Refresh: 🧲	00	:: • :
i ALARM	Add	Web CLI	eWeb More -	0 Selected							SN, Alia	s, Description	C
REPORT		Status	SN	Alias ()	MGMT IP	MAC	Egress IP	Network	Firmware Version	Offline Time	Model	Description	Actio
Network		Online	<u>H1Q' '54</u>	Rujie	172.26.5.46	ecb5	15 120	Revee-Hotel	ReyeeOS 1.56.1325	2022-04-19 21:36:07	EG105G-P	Emply	Ē
Voucher				-	First	Previous	Page 1 of 1	Next	Last			10 =	1 in tot
DEVICE													
AP													
AC													
Switch													
Gateway													
Home Router													
Bridge													
CAMERA													
Cameras													
NVR													

b Choose Config > Cloud Portal Auth.

Ruíjie		🗳 C @ C @•
A abcdefg@111.com V	Device Details ×	Take over Network Unbind Device
û DASHBOARD	Base	
옮 TOPOLOGY	VAN LAN Disconnected Disabled PPPeE Static IP DHCP Copper SFP Alas: Rulje	tefresh: 💽 😌 🖄 📰 = 🕄
述 ALARM	Lee Lee Lee Lee Harrier wed SN H11 54	SN, Alias, Description Q
REPORT	Modet: EG1050-P	Model Description Action
Network	Operation Mode: Route Egress IP 12 Actual Master Device: H1GHET T4 MGMT IP 172.26 5.46	EG105G-P Emply II
Voucher	Network Master Device: OHTG. 754 Firmware Version: ReyeoOS 1.56.1325	10 a 1 in total
E DEVICE	Overview Config	
AP	Device Config	¢
AC Switch	Device Comp	<u></u>
Gateway	Web CLI eVieb TELNET SSH Tunnel Reboot Cloud Portal Auth	
Home Router		
Bridge	IPTV	
🛱 CAMERA	IPTV/VLAN IPTV/IGMP	
Cameras		
NVR	WAN LAN Disconnected Disabled PPPoE Static IP DHCP Copper SFP	
A CLIENT		
	Dynamic DNS 🛛	

c Enable authentication and configure IP addresses of guests in the range from 192.168.113.2 to 192.168.113.254.

Ruíjie	MC Auth Auth Atter you enable Cloud Portal Auth, it will be synced to the Reyee EG automatically.	e @ a e @
A abcdefg@111.com V	AL Portal Escape 🛛 🔍	Take over Network Unbind Device
C DASHBOARD	Auth IP/Range 192.168.113.2.192.168.113.254 +	
ஃ TOPOLOGY		tefresh: 💽 😌 🖄 🗰 = 🔀
逝 ALARM	Seamless Online @	SN, Alias, Description Q
REPORT	User Offine Detection	Model Description Action
Network	Please select a portal or add a new portal.	EG105G-P Emply
Voucher	test	10 a 1 in total
E DEVICE		
AP	Rups	
AC		
Switch Gateway	🔘 Voucher Login	
	Access Code	
Bridge		
& CAMERA		
Cameras		
NVR		
A CLIENT		
	Sive	

d Add the voucher package for guests.

Choose Voucher > Manage Package > Add Package and add a voucher package for guests.

Ruíjie 🛆	MONITORING CONFIGURATION MAINTENANCE	🗳 o o 😌 e
A abcdefg@111.com ~	Revee-Hotel V Search Network Q (GMT+8:00)/starS	ihanghal Manage Project Take over Network Unbind Device
PROJECT		
♥ WIRELESS	Note: Reyee AP requires authentication on Reyee gateway. Please enable Cloud Auth on EG for Reyee devices. How to enable Cloud Auth on Reyee EG?	
Basic	Voucher	
Layout Radio	Print Vouchers Manage Paccage More -	Voucher Code, Alias, Packi Q Advanced Search
Wi-Fi Optimization	Voucher Code Alias Package Name Price Period Created at Activated at Expired at Devices Bind MAC	Download Speed Upload Speed Status
Roaming	No Data	
Bluetooth	First Previous Page 0 of 0 Next Last	10 • 0 in tota
Load Balancing		
AUTHENTICATION		
Captive Portal		
PPSK		
Voucher		
Account Easy Sharing		
ADVANCED		
Batch CLI Config		
Customize CLI Set		

Example: Set Concurrent Devices to 2, Period to 1 Day, and Upload Speed and Download Speed to 2 Mbit/s.

0						
Ruíjie 🛆	MONITORING CON	FIGURATION				
A abcdefg@111.com ∨ PROJECT	Reyee-Hotel V Search	Network Q	Add Package Package Name	Guest	×	T+8:00)Asia/S
WIRELESS Basic	Note: Reyee AP requires a Voucher > Manage Pa					
Layout Radio	Add Package	ckayo	Price Concurrent Devices	2 ~		
Wi-Fi Optimization Sets	Package Name	Descript	ti Bind MAC			Jownload Speed
Roaming Bluetooth Load Balancing	test		Period Download Speed Upload Speed	1 Day ✓ 2 Mbps ✓ 2 Mbps ✓		1.00 Mbps
Captive Portal PPSK Voucher				OK Cancel]	
Account Easy Sharing						
ADVANCED Batch CLI Config Customize CLI Set AP VLAN						

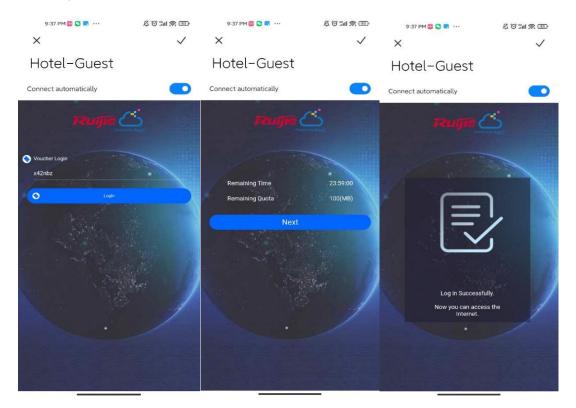
e Click **Print Voucher** to obtain the code for guests.

Ruíjie	MONITORING CONFIGURATION MAINTENANCE	🔒 0 0 🖓
A abcdefg@111.com ∨	Reyee-Hotel > Search Hetwork Q (GMT+8:00)/coa/Shanghai	Manage Project Take over Network Unbind Device
 PROJECT WIRELESS Basic Layout 	Note: Reyoe AP requires authentication on Reyoe gateway. Please enable Cloud Auth on EQ for Reyoe devices. How to enable Cloud Auth on Bryse EQ? Voucher	년 第 ~ 55 Voucher Code, Alias, Packa Q Advanced Search ~
Radio		
Wi-Fi Optimization	Voucher Code Alias Package Name Price Period Created at Activated at Expired at Devices Bind MAC Dow No Data No Data	nload Speed Upload Speed Status
Bluetooth Load Balancing	First Previous Plags 6 and Last	0 in total
③ AUTHENTICATION		Q
Captive Portal PPSK		
PPSK Voucher		
Account		
Easy Sharing		
ADVANCED		
Batch CLI Config Customize CLI Set		
AP VLAN		
Ruffe C	MONITORING CONFIGURATION MAINTENANCE*	Manage Project
PROJECT	References of the second	Manage Project
* WIRELESS Basic Layout	Note: Reyee AP requires authentication on Reyee gateway: Please enable Cloud Auth on EG for Reyee devices. How to enable: Cloud Auth on Bryee EG? Voucher) Print Voucher	
Radio	Print Configuration Profile Information on Voucher	
Wi-Fi Optimization	[•] Quantity	
Roaming Bluetooth		Bind MAC No
Load Balancing		Period 1 Day
O AUTHENTICATION	020 Preview	Q
Captive Portal	*Package 2, Manago Packago Voucher Code	
PPSK Voucher	Cuest	XX
Account		
Easy Sharing	Logo I Clear	
ADVANCED		
Batch CLI Config	Text	
Customize CLI Set AP VLAN	0.43	
	Print Method	
	Print in 2 Columns (A4)	

x42nbz	Print	1 sheet of p	paper
	Destination	Microsoft Print to PDF	•
	Pages	All	•
	Layout	Landscape	•
	Color	Black and white	*
	More settings		~
		Print Car	ncel

5.4.3 Configuration Verification

Connect guest Wi-Fi. You can see that the internal IP address 192.168.110.1 cannot be accessed.



6 FAQ

- 6.1 Reyee Password FAQ (Collection)
- 6.2 Ruijie Cloud Reyee EG authentication FAQ (Collection)
- 6.3 Reyee Mesh FAQ (Collection)
- 6.4 Reyee IPTV FAQ (Collection)
- 6.5 Reyee Authentication FAQ (Collection)
- 6.6 Reyee Behavior Strategy FAQ (Collection)
- 6.7 Reyee DDNS FAQ (Collection)
- 6.8 Reyee VPN FAQ ((collection))
- 6.9 Reyee Flow Control FAQ (Collection)
- 6.10 Reyee Guest Wi-Fi FAQ (Collection)
- 6.11 <u>Reyee Wireless Configuration FAQ (Collection)</u>
- 6.12 Reyee Self-Organizing Network (SON) FAQ (Collection)
- 6.13 <u>Reyee series Devices Parameters Tables</u>
- 6.14 Reyee Parameter Consultation FAQ (Collection)

7 Appendix: Surveillance

The overview page displays Device Info, Wi-Fi, Network Status, and Real-Time Flow.

Ruijie Rcycc	Ruijie-Hotel > Ruijie Manter	English ∽Ruijie Cloud MDownload App & Network Setup @ Network Check ∦Warn ☐ Log Out
& Overview	Device Info Setup> WI-FI	Setup>
Online Clients	Hostname: Ruijie SN: 1	
Router	IP: 172.26.6.124 Primary Wi-Fi: @Ruijie-m3935 • EG105G-P MAC: EC69.7017/39:35 Security: No	Guest Wi-Fi: Security: No
	Software Ver: ReyeeOS 1.56.1306	
🖻 Switches		
Network V	Net Status (Online Devices / Total)	Refresh ©
		○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○
	Internet Router Switches	APs Online Clients
	Real-Time Flow (Kbps)	Kbps \checkmark WANT \checkmark
	250	k Flow
	200-	
	150-	
	100-	
	50	
	11:55:56 11:56:08 11:56:20 11:56:32 11:56:44 11:56:56 11:57:08 11:57:20 11:	isžiai 11.sžv.42 11.sžv.53 11.sš8.04 11.sš8.16 11.sš8.27 11.sš8.37
«Collapse		

7.1 Device Info

Choose **Overview > Overview**. One the **Device Info** page, the model, host name, IP address, MAC address, software version, and SN of the router are displayed.

In the Overview pane, the memory usage, online client count, status, uptime, and system time are displayed.

Rujje		English ~	🛆 Ruijie Cloud 🞇	Download App	A Network Setup	Q Network Check	<u>満</u> Alert	⊖Log Out
🖧 Overview	Overview Real Time Flow Flow History							
Online Clients	1							
Network	Overview							
⊘ Security ~	Memory Usage	Online Clients	Status: Onli Uptime: 5 d		minutes 12 second			
🔟 Behavior	40 %	1		022-09-06 17:21:4				
₩ VPN ×	Device Details							
🗄 Advanced	Model: EG105G-E	Hostname: EG105G-E &			SN: MACC105GE	3826		
	MAC: 80:D0:F8:15:08:68	Work Mode: Router 🖉		1	Role: Master AC 🛛			
🗄 System 🗸	Hardware Ver: 1.00	Software Ver: ReyeeOS 1.202.2031						
	Ethernet status							
	Connected							
			h 💼					e
		LAN0 LAN1/WAN3 LAN2/WAN2 LAN3/	/WAN1 WAN0					4

- The **Online** status indicates the SON status of the Reyee devices but not Ruijie Cloud.
- You can click **Hostname** to modify the device name.

Edit Hostname	
EG105G-E	
Cancel	
Hostname: EG105G-E 🖉	
Work Mode: Router 🖉	
Software Ver: ReyeeOS 1.202.2031	

 Click Work Mode to switch the device mode. Two modes are available: Router and AC modes. The default mode is Router.

Description:
 The device IP address may change upon mode change.
 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.
 The system menu varies with different work modes.
5. The device will be restored and rebooted upon mode change.
Work Mode Router \checkmark ②
Self-Organizing 🔵 🕐 🚺 Tip
Network
AC 🔵 🕐
Save

- Router Mode: indicates NAT forwarding.
- o **AC Mode:** indicates bridge forwarding.
- o SON:
 - o -If SON is enabled, the device role is displayed.
 - o -If SON is disabled, the device works in standalone mode.
 - o SON is enabled by default in AC mode.
- o AC:
 - o -It is enabled by default. The device works as a virtual AC to manage downlink devices.
 - o -When it is disabled, the device must be elected as the AC before managing downlink devices.

7.2 Wi-Fi Information

You can name the Wi-Fi of the network and enable guest Wi-Fi.

Wi-Fi		Setup>
Primary Wi-Fi: @Ruijie-m3935 Security: No	Guest Wi-Fi: Security: No	

Setup: Go to the Wi-Fi setting page.

7.3 Network Status

The Network Status page displays the topology and connected status of the network.

Net Status (Online Devices / Total)					Refresh O
(S) 1	15.12Kbps 8.11Kbp	ps 5viich		<u>2</u>	
	1	0/0	1/1	1	
Internet	Router	Switches	APs	Online Clients	

7.4 Real-Time Flow

Choose Gateway > Overview > Real Time Flow. The Real-Time Flow page appears.

Check real-time traffic flows based on ports, users, and apps, including uplink and downlink flows. The default unit is kbit/s. You can change it to be bit/s and Mbit/s.

Port Real-Time Flow User Real-Ti	ne Flow App Real-Time Flow	
Choose Outbound Interface: ALL-W/	N	
Outbound Interface	Flow Rate Down Up	
ALL-WAN		8.45Kt 19.63Kt
WAN		8.45K 19.63K
hoose Outbound Interface: ALL-WA	N V	
ow in the Last Hour		Kbps
1,800 -	Uplink Flow Downlink Flow	
1,000 -		
1,500		

7.5 Flow History

Note

This feature is supported by R202 and later versions.

Choose Overview > Flow History. The Flow History page appears.

Check historical traffic flow based on ports, users, and apps, including uplink and downlink flows.

Overview Real Ti	ime Flow Flow Histo	ry										
Port Flow History	User Flow History	App Flow History										
Choose Outbound	Interface: ALL-WAN	V Time Spar	n: 24h 48h									
Flow History												Kbps \lor
1,400 -				- - - Up	link Flow –	Downlink Flow						
1,200 -												
1,000												
800 -												
600 -												
400 -												
200 -												
0	50 20:17:50 21:27:50 2	2:37:50 23:47:50 00:5	7:50 02:07:50	03:17:50 04:27	-50 05-37-50	06:47:50 07:57:	0 09:07:50 1	D:17:50 11:2	7.50 12.37.50	13:47:50 14:4	57:50 16:07:50	17:17:50

7.6 URL Logs

URL logs are URL access records of devices on the internal network, including the URL, access count, and audit result.

1 Note

This feature is supported by only EG3 series routers such as EG310G-E.

- (1) Choose **Overview** > **URL Log**.
- (2) Enable URL logging.

Toggle the switch to **Enable** and click **OK** in the dialog box.

Overview Real Time Flow Flow H	listory URL Log Online Client			
Enable	rationy one cog on any client			
Overview Real Time Nov Flow History	URLLog Online Clent			
Enable 💽		record IP Example:	53.1.5 Save 3	C Enter IP or URL for search C Refresh
Time	P	Access Count	URL	Access Centrol
		No D	•	
(f) 1 (10page -)				
		Tip Are you over you want to Enable URL Cancel	* *	

(3) (Optional) Configure an IP address to view its URL access records.

The system logs URL access records of all devices on the internal network by default. To view URL access records of a specific device, configure an IP address in the **record IP** text box and click **Save**.

Enable 💶		record IP	Deample: 1.1.1.1 Serve 🕐	C Enter IP or URL for search
Time	P	Access Count	URL	Access Centrol
2022-08-15 09:26	192.168.33.3	1	http://doudloge.j.link:6222	Allow
2022-08-15 09:26	192.168.33.4	15	http://wx.qloga.on	Allow
2022-08-15 09:26	192.168.33.3	1	http://www.baidu.com	Allow
022-08-15 09:25	192.168.33.4	3	http://120.241.131.85	Allow
2022-08-15 09:25	192.168.33.4	1	http://112.60.8.27	Allow
2022-08-15 09:25	192.168.33.4	5	http://sawtshort.webin.qq.com	Allow
2022-08-15 09:25	192.168.33.4	16	http://wx.qloga.on	Allow
2022-08-15 09:25	192.168.33.4	1	https://wework.gpic.cn	Allow
2022-08-15 09:25	192.168.33.4	1	http://182.254.118.119	Allow
2022-08-15 09:25	192.168.33.4	3	https://essets.man.cn	Allow

1 Note

To restore URL access records of all devices on the internal network, clear the **record IP** text box and click **Save**.

(4) Check URL log details.

A log includes the access time, IP address, and access count.

You can search logs by IP address or URL.

verview Real Time Flow Flow History UR	Llog Online Client			
inabla 💽		record IP Example: 1.1.1.1	Save 🕐	C 192.168.33.3
lime	P	Access Count	URL	Access Control
222-08-15 09:26	192.168.33.3	1	http://cloudloga.j.link:6222	Allow
22-08-15 09:26	192.168.33.3	1	http://www.baidu.com	Allow
22-08-15 09:25	192.168.33.3	1	http://www.baidu.com	Allow
22-08-15 09:24	192.168.33.3	1	http://47.104.204.63	Allow
< 1 > 10/page ~				Total
10/page -	Llog Online Client			100
rview Real Time Flow Flow History UR	Llog Ordina Clant	recod P Example 1.1.1	•	
rview Real Time Flow Flow History UR	Ling Online Davit	Access Careet	0 01	
nview Real Time Riow Pilow Mistory UR uble 🌑				C table C faite
		Access Count	URL	C hala

7.7 Online Clients

Choose Gateway > Overview > Online Clients. The Online Clients page appears.

Select a client from the client list and click **View Details**. You can find the client's username, type (wired/wireless), IP address, MAC address, current rate, connected Wi-Fi name, and access control status.

Edit Client				×
IP:	192.168.111.20	Access Name:	Ruijie	
MAC:	EC:B9:70:13:73:16	Access Location:	MACCMR1250X01/LAN0	
Online Time:	2022-08-31 20:22:25	Manufacturer:	Ruijie Networks Co.,LTD	
Offline Time:	-	Product:	Ruijie Network Device	
Wireless Access:	No			
Client Name:	EW3200GX-137316	Client Type:	Network Device \sim	
Auto Grouping:	No \vee	Client Group:	Select \vee	

Cancel