

Ruijie Cloud On-Premises

User Guide



Document Version: V1.0 Date: November 17, 2023 Copyright © 2024 Ruijie Networks

Copyright

Copyright © 2024 Ruijie Networks

All rights are reserved in this document and this statement.

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



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

Disclaimer

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

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

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

Preface

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: <u>https://caseportal.ruijienetworks.com</u>
- Community: <u>https://community.ruijienetworks.com</u>
- Technical support email: <u>service_rj@ruijienetworks.com</u>

Conventions

1. GUI Symbols

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

2. Signs

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

Warning

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

A Caution

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

🚺 Note

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

Specification

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

3. Note

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

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

Contents

Preface I
1 Product Introduction
1.1 Ruijie Cloud On-Premises (OP) Service Overview1
1.2 Key Features1
2 Quick Start
2.1 How to Login Ruijie Cloud OP Service2
2.2 Adding a Project2
3 AI Networking
3.1 Smart Config
3.1.1 Configuration6
3.1.2 Optimization7
3.1.3 Delivery
4 Network Configuration9
4.1 Creating a Wired VLAN9
4.1.1 Overview
4.1.2 Configuration Steps9
4.1.3 FAQs
4.2 Creating a Wireless VLAN
4.2.1 Overview
4.2.2 Configuration Steps13
4.2.3 FAQs
4.3 Configuring the AP Management Service Network (AP Management VLAN)18
4.3.1 Demand18

4.3.2 Configuration Steps18	3
4.4 Multi-WAN22	2
4.4.1 Overview	2
4.4.2 Multi-WAN Bandwidth Superimposition23	3
4.4.3 Configuring Traffic of Different Users to Pass Through Different Lines	3
4.4.4 Configuring the Traffic for Accessing a Private Line Server to Go Through a Private	
Line	3
5 Optimization Configuration	
5.1 Wi-Fi Optimization	I
5.2 Loop Prevention	3
5.2.1 Overview	3
5.2.2 Configuration Steps	1
5.3 DHCP Snooping	5
5.3.1 Overview	5
5.3.2 Configuration Steps	3
5.4 Traffic Control	3
5.4.1 IP Traffic Control)
5.4.2 Application Traffic Control40)
5.4.3 Configuring the Policy Priority42	2
5.4.4 App/Website Control	3
6 Security Configuration	;
6.1 Network Access Control (simplified)46	3
6.1.1 Applicable Scenarios	3
6.1.2 Models of ACL-Supported Products	3
6.1.3 Configuration Steps46	3

6.2 Gateway Anti-ARP Spoofing Solution	
6.2.1 Overview	
6.2.2 Principles	
6.2.3 Models of Products Supporting the Feature and Topology	51
6.2.4 Configuration Steps	51
6.2.5 FAQs	
7 General Configuration	
7.1 Intranet Access	53
7.1.1 Overview	53
7.1.2 Configuration Steps	53
7.2 Project Password	55
7.3 ACL	
7.3.1 Creating ACL Rules	
7.4 CLI Config Task	
7.4.1 Add a CLI Command Set	
7.4.2 Batch CLI Configuration	
8 Gateway Configuration	61
8.1 Interface	61
8.2 Routing	62
8.2.1 Adding a Static Route	62
8.2.2 Adding PBR	63
8.3 NAT	65
8.3.1 Applicable Scenarios	65
8.3.2 Configuration Steps	65

8.4 Configuring VPN	68
8.5 Configuring Portal Authentication	
8.6 Configuring Dynamic DNS	111
8.7 Configuring IPTV	113
8.8 PPPoE Server	114
9 Switch Configuration	116
9.1 Interface	116
9.2 Configuring a VLAN for an Interface	117
9.3 Routing	118
9.3.1 Adding a Static Route	118
9.3.2 Adding PBR	119
9.4 Voice VLAN	121
9.4.1 Overview	121
9.4.2 Configuration Steps	121
10 Wireless Configuration	124
10.1 AP Mesh	124
10.2 SSID	126
10.2.1 SSID Basic Settings	126
10.2.2 Radio Settings	137
10.3 Radio	138
10.4 Rate Limit	140
10.4.1 Overview	140
10.4.2 User Rate Limit	140
10.4.3 Wireless Rate Limit	141

10.4.4 AP Rate Limit	
10.4.5 Packet Rate Limit	
10.5 Load Balancing	
10.6 Client Blocklist and Allowlist	147
10.7 AP VLAN	
11 Authentication Configuration	
11.1 Captive Portal	
11.2 User Management	
11.2.1 Account	
11.2.2 Voucher	
11.2.3 User Group	
11.3 PPSK	
11.4 Allowlist	
11.4.1 Pre-Authentication Access Server List	
11.4.2 Authentication-Free Client List	
12 Cloud Account and Project Management	
12.1 Adding a Sub Project	
12.2 Managing Cloud Login Accounts	
12.3 Managing Cloud Sub Accounts	
12.4 Switching Accounts	
13 Monitoring	175
13.1 Viewing all the Device	
13.2 Viewing all the Alarm	
13.3 Viewing Topology	176

13.4 Detecting Device	177
13.5 Wi-Fi Experience	178
13.6 Data insights	179
13.7 Edit Topology	179
13.7.1 Common Troubleshooting	
13.8 Upgrade	
13.8.1 Upgrade	
13.8.2 Firmware Version	
13.9 Configuring Alarms	
13.10 Managing Contacts	
13.11 Viewing the Number of Global Alarms Quickly	
13.12 Viewing Details About Global Alarms	
13.13 Viewing Alarms of a Project	
13.14 Layout	
14 Delivery Center	
14.1 Smart Detection	
14.2 Project Report	
14.2.1 Applicable Scenarios	
14.2.2 Configuration Steps	
14.3 Project Handover	
14.3.1 Applicable Scenarios	
14.3.2 Configuration Steps	
15 Appendix: Frequently-Used Controls	
15.1 Notification	

15.2 Add	
15.3 Delete	
15.4 Quickly locate the table entry you want to find by entering keywords	
15.5 Status	193
15.6 Change Project Name or Password	194

1 Product Introduction

1.1 Ruijie Cloud On-Premises (OP) Service Overview

Ruijie Cloud OP Service is Ruijie's easy and efficient cloud solutions for ISP and MSP to provide cloud management features on local. The solutions include device deployment, monitoring, network optimization, and operational life cycle management; providing customers with plug-and-play deployment and operation and maintenance (O&M). It satisfies needs of automatic cloud RF planning and user experience monitoring. Moreover, it supports flexible wireless Wi-Fi management, including secure Private Pre-Shared Key (PPSK) authentication (one person, one machine, and one password), and Portal service.

1.2 Key Features

- Unified device management
- Secure PPSK authentication for employees
- Captive portal for guests
- Cloud Monitoring & alert
- Tenant and Subaccount permission assignment

2 Quick Start

2.1 How to Login Ruijie Cloud OP Service

(1) Visit your customized domain for On-Premises service.



(2) Input the Admin account and Click Sign in to login directly.

2.2 Adding a Project

A project group includes many networks, and is usually used to represent the network of a province, a city, or a company.

1 Note

Adding devices to a project group is not supported. The project group is used to manage multiple projects.

Procedure

(1) Choose Home > Project > Add > Add Project

Ruíjie I Rcycc 🎢	Home	Project		
Project 7	•	Device 5	Alarm 3	φ.
Created (7)	Received(0)	Shared(0)		
Add v	Project Management	Unbind Device	Enter project name Q	
Add Project	Name		Scenario Alarms	Online Guests AP

(2) Set basic parameters of the project. Then click Next.

				Basic Informati	ion
asic				Network Alias	
* Network Alias:	Enter the project name			Time Zone	China (GMT+8:00)
* Management Password	Enter the management pas	sword		Location	
and agenter in a sword of	enter the management par	anora		SSID	
	Note: if the device has been should be configured the sar	configured before, the ma ne with the eWeb passwo	nagement password rd.		
Scenario:					
	Office	Hotel	Villa/Home		
	Factory/Warehouse	Restaurant	School		
		M			
	Retall/Shop	Residence	Customize		
Time Zone:	(GMT+8:00)China				
	Adva	inced 🔻			

Name: indicates the name of a project. The value is a string of up to 32 characters, including letters, numerals, or underscores (_).

Management Password: indicates the management password.

A Caution

If the device has been configured before, the management password should be configured the same with the Eweb password.

Scenario: indicates the scenario that suits the customer's actual scenario.

Time Zone: indicates the time zone where the current customer is located.

Type: indicates the type of the project. If there is an AC in the project, select AC + Fit AP.

Bind Location: indicates the location of the project.

(3) Select device type and set Wi-Fi parameters. Then click OK.

Add Device Select the de	evice model	Add Device	+ Finish	Х
Select device type(Select at least one device type.)	Basic			
AP Gateway Switch Home Router Wireless Bridge	Device type			
	Add to	Test		
Cancel Next				

Wireless Settings	Х
WiFi Settings More V	
* WiFi Name / SSID :	
Password:	No encryption (Open) Strong encryption (WPA2-PSK)
Collapse<< Hide SSID :	(Hidden from others, and can only be added manually)
Radio :	🗹 Radio1 🔽 Radio2
IP Assignment:	 Clients Obtain IP Addresses from AP The STA obtains an IP address from the AP. (The NAT mode is also called routing mode in which the IP address pool of STAs is on the AP.)
	 Clients Share Address Pool with AP The STA and the AP are on the same VLAN, and share the same IP address pool. (This mode is applicable when the AP's IP address is also assigned by the DHCP server.)
	 Bridge mode (or switching mode) The STA and the AP are on different VLANs, and the STA VLAN and IP address pool are part of the local network. (This mode is applicable when the local network has a separate VLAN and address pool for STAs.)
5G-Prior Access:	Open
Per-user rate limit :	Open
Rate Limit for SSID Users	Open
Add WiFi	

RF Configuration

Cancel OK

SSID: indicates the WLAN name of a project.

Password: indicates the SSID encryption method and password.

Hide SSID: indicates that the SSID is hidden or broadcast.

Radio: indicates the radio that needs to be enabled.

IP Assignment: indicates the mode in which clients obtain IP addresses.

5G-prior Access: indicates that clients are connected to the 5 GHz frequency band preferentially. Legacy clients are connected to 2.4 GHz frequency band.

Per-user rate limit: indicates channel width control for each user who connects to this Wi-Fi.

Rate Limit for SSID Users: indicates channel width control for the total traffic on this SSID.

- (4) Add devices manually or through batch import.
- Option 1: Add devices manually.

Enter the device SN and alias.

Add Device		-	Select the dev	ice model A	dd Device	+ Finish	Х
Switch				Basic			
You can add a switch in one of	f the following four modes (click to switcl	:h mode):		Device type	Switch		
				Add to	Test		
By entering device SN	By batch adding using an excel file						
				Added devices			
1 SN :	Alias:		+	Switch	0		
Back		Cancel	Finish				

Option 2: Add devices through batch import. In the template, up to 500 records can be imported each time.

Add Device	device model A	dd Device+ Finish	×
Switch	Basic		
You can add a switch in one of the following four modes (click to switch mode):	Device type	Switch	
By entering device SN By batch adding using an excel file	Add to	Test	
Download and fill in the device information in the template lin to 500 records can be imported each time	Added devices		
	Switch	0	
Select an us or us file Download Template			
Back Cancel Finish			

- a Click Batch Import.
- b Click Download Template to download the template
- c Fill in the device SN and alias in the template and save it.
- d Click Upload Template File to upload the edited template file.
- e Click the **Import** button.
- (5) After devices are added, click **Save & Next**.

The project is added successfully.

Finish		dd Project	+Add Device	+ Finish		×
			AF	Succeeded!		
AP	Switch	Unauthorized Gatew	vay Gateway ⊦	ome Router Wireless Bridge		
	No		SN	Alias	Action	
				No Data		
			First	Previous Page 0 of 0 Next Last		10 🔺 0 in total
						Close

3 Al Networking

3.1 Smart Config

3.1.1 Configuration

(1) Choose **Project > Smart Config**, click **Configuration**.

You can create wired and wireless VLANs, and perform ACL, AP VLAN, and WAN configurations on the page that is displayed.

Click **To configure** under the item that you want to configure. You will be redirected to the corresponding **configuration** page.

Ruijio IRcycc	Home Projec	d		Leco super_tenant
EG210G-E		01 Connect Clients to Network	02 Link and Network Device	03 Earess Path Configuration
Workspace				
Al Networking	Configuration	Add Wired VLANS Create wired VLAN	Management IP Address of AP Independent network segment and VLAN assig	Add Internet and private lines, and manage rout Oconfigured > e selection rules for clients, such as polici-base
Smart Config		Improve performance Strengthen security	Improve performance Strengthen security	d routing and load balancing
Configuration	Cetimization	create wireless VLANs		Improve Internet speed Increase egress route utilization
Network-Wide	Optimization	Add WI-FI, create wireless VLANs		
Devices Auth & Accounts		Improve performance Strengthen security		
Monitoring	Delivery	Network Access Control Restrict inter-client access		
옮 Network-Wide		Strengthen security		
Devices				
Clients				
🛱 Logs				
2 Delivery Center				

ACL configuration is used as an example to illustrate the configuration steps.

First, click **To configure**. The ACL page is displayed. On the page that is displayed, click **To configure** to start the configuration.

You can use this ACL feature to assign a service network to the **Interworking Zone** or the **Isolation Zone**, depending on the access control rights you want to assign to this service network. Service networks in the Interworking Zone can access each other, while those in the Isolation Zone cannot.

Service networks in the Interworking Zone cannot access those in the Isolation Zone, and vice versa.

You can restrict the access control rights of a service network by dragging it from the **Interworking Zone** to the **Isolation Zone**, and then clicking **Save**.

By clicking **No IP** under a service network in the **Isolation Zone**, you can set an IP address or an IP address range that is allowed to access this service network.

DemoProject2 V	Access Control List (ACL)			
硷 Workspace	① Drag a service network to	the 【Interworking Zone】 or 【Is	olation Zone】 as required, More	
🖏 Smart Config	Interworking Zone			Isolation Zone @
Configuration	Service networks in the Interworkin	g Zone can access each other		Service networks in the Isolation Zone cannot access each other. If necessary, a network segment or IP can be added for mutual access
Network-Wide >	VLAN 1 VLAN1	X VLAN3	1	between a certain service network in the Isolation Zone and the one in the Interworking Zone
🛱 Devices >	192.168.110.1/255.255.255.0	192.168.3.1/255.255.255.0		
⊘ Authentication ⇒	D VLAN5		\leftarrow Cannot access each other \rightarrow	
Monitoring	192.168.5.1/255.255.255.0			- day
ት Network-Wide >				No.
Devices				Service networks to which you want to grant access
Clients >				permissions Drag
E Logs				
😂 Delivery Center 🔅				

3.1.2 Optimization

On the **Optimization** page, you can configure features such as Wi-Fi optimization, loop prevention, DHCP snooping, and ARP spoofing guard.

Click **To configure** under the item that you want to configure. You will be redirected to the corresponding configuration page.

WIO configuration is used as an example to illustrate the configuration steps.

First, click **To configure**. The WIO page is displayed. On the page that is displayed, click **Enable Wi-Fi Optimization**, and then click **Optimize Now**.

The system will perform the network optimization. After the optimization is complete, you can check the results by scrolling down the page.

You can set the time for scheduled optimization by clicking **Optimization Schedule**, and then clicking **Save** to save the configuration.

DemoProject1	신	01 Connect Clients to Network	02 Link and Network Device	03 Foress route configuration
✿ Workspace				
Smart Config	Configuration	Wireless Intelligent Optimiza Improve Wi-FI performance and Wi- Fi experience	Loop Prevention Prevent network-wide breakdown d To configure ue to loops	
Configuration		Boost WI-Fi speed	Improve stability	
Ø Network-Wide				
幸 Devices	Optimization		DHCP Snooping	
Authentication	>		ected because the client obtains a f orged IP address	ÂÂ
Monitoring			Improve stability	Not Configured
& Network-Wide	Delivery		ARP Spoofing Guard	
Devices			Prevent a client from being disconn To configure	
Clients			there exists a set of the set	
E Logs			improve stability	
2 Delivery Center				

3.1.3 Delivery

You can perform a network-wide smart check, view reports and update devices by clicking **Delivery**. Click **To configure** under the item that you want to configure. You will be redirected to the corresponding configuration page.

Smart Check is used as an example to illustrate the configuration steps.

First, click To configure. Click Check Now.

The system will perform the smart check. After the check is complete, you can click **View Report** to view the project report.



4 Network Configuration

4.1 Creating a Wired VLAN

4.1.1 Overview

Different clients exist on a network, such as PCs and cameras. When a camera is running, broadcast or abnormal traffic often occurs, imposing negative effects on the service network. The administrator wants to isolate the broadcast and abnormal traffic of the camera from the running service network.

4.1.2 Configuration Steps

(1) Adding a wired VLAN: Choose Project > Configuration > Network-Wide > Client Access, click Add and select Add wired VLANs to add wired VLAN configuration for the current network, or select an existing wired VLAN and click Configuration.

DemoProject1 V	Client Access Device	e Management			
俭 Workspace	Planned: (1) Add	VLAN1			Configuration More ~
Smart Config	VLAN1 VLAN1 Add wired VL	ANs ID Gateway IP Address (SVI) 192.168.110.1	DHCP Server E EG310GH-E 1	DHCP Pool 192.168.110.1-192.168.110.254 Lease Time: 30Min	Used/Total IPs: 5/254
Configuration	Wired Add wireless	VLANS			
Network-Wide			C		
≇ Devices >			(1000)		
Monitoring				Order of Instance	
& Network-Wide ⇒				J.	
Devices				NetGL201-4432-anty Styling T1010000000	
🖬 Clients >					
E Logs					
	Service Configurations		National Sector	NEED YOU AREA MAN, MEED YOU AREA MAN, BUT NOC P Drawler COSTO COM	
📚 Delivery Center 🔌	Multi-WAN Config Access Control List (ACL)		and any		0 + -

(2) Setting service parameters: Set the VLAN for wired access and create a Dynamic Host Configuration Protocol (DHCP) address pool for devices in the VLAN to automatically obtain IP addresses. The gateway can serve as the address pool server to assign addresses to access clients. If a core switch supporting the address pool function is deployed on a network, you can configure the switch as the address pool server. After configuring service parameters, click **Next**.

etwork planning / Edit Wired VLANs	×
1 Network Param 2 Wired Access — 3 Confirm — 4 Apply Config	
Description: Dining Room	
VLAN ID: 3	
Default Gateway/Subnet Mask: 192.168.3.1 / 255.255.255.0	
DHCP Pool: ()	
IP Segment: 192.168.3.1 . 192.168.3.254	
Assign IP from:	
Next	

The following table lists the description of parameters.

Parameter	Description
Description	Enter the VLAN description, for example, Office PC.
VLAN ID	The VLAN ID can be set to any value from 2 to 232 and from 234 to 4060, except the used value.
Default Gateway/Subnet Mask	After the VLAN ID is configured, the value of the default gateway or the subnet mask will be updated automatically 1s later.
DHCP Pool	You are advised to keep the default configuration. If the DHCP pool is disabled, a camera or PC needs to be manually configured with a static IP address. The deployment location of the IP address pool can be selected as needed. Generally, the gateway used as the DHCP server is applicable to a Layer 2 network, and the core switch used as the DHCP server is applicable to a Layer 3 network.
IP Segment	The parameter is available only when the DHCP pool is enabled. When the VLAN ID is configured, the IP segment will be updated automatically 1s later.
Assign IP from	The parameter is available only when the DHCP pool is enabled. You are advised to keep the default configuration.

(3) Select the interface for connecting the camera in the topology on the left, and select the port to connect the camera from port icons on the right. The port icon will change from gray-black to blue. Click Next.

Network planning / Edit Wired VLANs	
✓ Network Param	Wired Access — (3) Confirm — (4) Apply Config
	VLAN3 (Dining Room) 192.168.3.1-255.255.05elected1device(s)4port(s)
The second secon	Ruije @ NATKO22HH0027 Natko22HH0027 Natko22H027 Natko22H027 Natko22H0027 Natko22H0027 Natko22H0027 Natko22H0027 Natko22H027 Natko22H027 Natko22H027 Natko22H027 Natko22H027 Natko22H027 Natko22H027 Natko22H027 Natko22H027 Natko2H027 Natko22H027

(4) Click Apply. The configuration will be delivered to the gateway and the switch, and takes effect.

✓ Network Param	Wired Access —	3 Confirm (4) Apply Config		
٩	To ensure that the work (Dining Room VLAN3 192.168.3.1~192.168.3.254) takes effect, configuration will be delivered to	6device
	EG310GH-E NAEK002BH0001	Add port VLAN3, IP 192.168.3.1, subnet mask 25: Add address pool VLAN3, start address 192.168. lease time 480 mins	5.255.255.0 8.1, end address 192.168.3.254, DNS 192.168	.3.1,
	NB53200-48GT4XS NAEK002BH0002	The port Gi9-12 is configured as the Access port Add VLAN 3[Auto Configuration]: The port Ag8,Gi3-6 is configured as the Trunk p 4094[Auto Configuration]:	, VLAN ID 3 ort, Native VLAN ID 1, Allowed VLAN ID 1-	
аланананананананананананананананананана	NBS3100-24GT4SFP-P NAEK002BH0003	Add VLAN 3[Auto Configuration]: The port Gi1-2,Gi24 is configured as the Trunk p 4094[Auto Configuration]:	ort, Native VLAN ID 1, Allowed VLAN ID 1-	
0		Add M AM 21Auto Configurations		

(5) The service network is added successfully when the message indicating delivery success is displayed.

	Network Param Vired Access - Confirm Apply Config
[DemoProject1] Delivery succ [Dining Room] VLAN 3 Default Gateway: 192.16	eeded. 8.3.1 255.255.0 IP Segment:192.168.3.1 192.168.3.254 DHCP Server:Gateway
bu can also Plan switch ports for connecting to APS. If there are non-connected APs in the project. you can plan switch ports for connecting to these APs in advance.	Access Control List (ACL) Block mutual access between this network segment and other network segments, or allow mutual access for some network segments for guest, finance, and server scenarios.
Device Config ON EG310GH-E	

Check Network Continue to add

4.1.3 FAQs

- 1. Why Do I Classify VLANs?
- (1) Reducing resource waste caused by broadcast traffic

In monitoring, door control, IPTV, and other scenarios, the heavy broadcast traffic of different services can easily affect each other, causing network jamming. Broadcast domains need to be isolated to reduce the bandwidth occupied by broadcast packets and avoid broadcast storms.

- There are broadcast packets of various network protocols, such as Address Resolution Protocol (ARP) requests for querying MAC addresses of identified devices, and DHCP requests for requesting IP addresses. When there are considerable clients on the network, broadcast packets will occupy numerous bandwidth resources, causing resource waste. VLANs can isolate broadcast domains and reduce bandwidth resource waste.
- In monitoring, door control, broadcast system, and other scenarios, broadcast or multicast packets (devices that do not support multicasting will process multicast packets as broadcast packets) are usually used. Therefore, separate VLANs need to be configured for monitoring and video (such as IPTV) devices to isolate such traffic from common service traffic.
- (2) Facilitating management

After VLANs are classified based on departments, policies can be conveniently configured for different departments and enterprise intranets can be better managed.

In hotel scenarios, there may be Internet access by guests, conference room and banquet network, reception office network, and monitoring network. The reception office network involves the check-in/refund handling. In enterprise office scenarios, different departments may have different intranet access permissions and different security requirements. It is necessary to classify VLANs by user category and configure access control lists (ACLs) and other policies to meet different service requirements.

- (3) Ensuring intranet security
- In a LAN, device information can be easily captured, and even data may be stolen, imposing security risks. After VLANs are configured, LANs can be divided into different VLANs to narrow down the broadcast scope of different packets, thereby enhancing information security.

For example, in the enterprise office scenario, configuring a guest VLAN can greatly reduce security threats imposed by visitors to the intranet.

 Some virus software identifies other devices in the same VLAN through scanning in broadcast mode, and spreads viruses to the other devices in the same VLAN. Classifying VLANs can restrict the spread within the same VLAN.

For example, in the primary and middle school scenarios, teachers' Internet access devices and teaching devices can be added to different VLANs to prevent the spread of viruses on a teacher's PC to the teaching devices.

In conclusion, on the enterprise network, hotel network, school network, multi-client network, and monitoring and IPTV service networks, classify VLANs to improve the network experience and security.

2. How Do I Set the Lease Time of DHCP Addresses?

Purpose of Lease Period

When clients are online, they renew the lease automatically when 1/2 or 7/8 of the lease period has elapsed. If the lease is not renewed because a client goes offline or other problems arise, the client can continue to use the original IP address after reconnection before the lease period expires. For example, if the lease period is 24 hours and a client goes offline, the client can still use the original IP address after re-login within one day. If the lease period expires, the IP address will be returned to the address pool. When the client connects to the network

again, it will obtain an address again. In general scenarios, keep the default value for the lease period. If the address pool has sufficient addresses, set the lease period to a smaller value; if the addresses are sufficient, set the lease period to a larger value.

Configuration Steps

 Choose Configuration > Network-Wide > Planned, select a VLAN, and then click Configuration at the upper right corner.

DemoProject1 V	Client Access Device	Management	
硷 Workspace	Planned: (3) Add v	Dining Room	Configuration More v
Smart Config	VLAN1 VLAN1	VLAN ID Gateway IP Address (SVI) DHCP Server DHCP Pool 3 192 168 3 1 FG310GHLF 192 168 3 1 192 168 3	254 Leace Time: Rhours Heed/Total IPs: 1/254
Configuration	Wired		ST Lease finer ondars oscariotarius (j.s.)
Network-Wide >	Dining Room VLAN3		9
In Devices	Wired	(www) (www) (www)	
$\tilde{\tilde{Authentication}}$ Authentication $\tilde{\tilde{Authentication}}$	GUEST VLAN33		J
Monitoring	Wireless		
🗞 Network-Wide 💚	1		
Devices		National Address Sectore interaction	
Clients >			
E Logs			
	Service Configurations	NESTIDO AGNEZ. NESTIDO AGNEZ. NESTIDO AGNEZ. NESTIDO AGNEZ. SETARENDO AGNEZO AGNEZIO AGNE	16 ESTING P
😂 Delivery Center 💚	Multi-WAN Config Access Control List (ACL)		• •

(2) Enter the lease period and click Save.

Network planning / Edit Wired VLANs					>
	Network	k Param Wired Access			
	Description:	Dining Room			
	VLAN ID:				
Default Gatew	way/Subnet Mask:	192.168.3.1 /	255.255.255.0		
	DHCP Pool:	0			
	IP Segment:	192.168.3.1	192.168.3.254		
	Assign IP from: 🤅	 Gateway (Router) Usually for L2 network. 			
	Lease Time:	0 days 8	hours 0 Min]	
		Save			

4.2 Creating a Wireless VLAN

4.2.1 Overview

To manage the Wi-Fi usage of different user groups (such as company employees and external guests) separately, the company wants to provide separate Wi-Fi access for guests, and isolate the IP segment used by the guests' terminals and the VLAN to which they belong from company employees.

4.2.2 Configuration Steps

(1) Adding a wireless VLAN: Click **Add** and select **Add wireless VLANs** to add wireless VLAN configuration for the current network.

DemoProject1 V	Client Access Device Management	
窗 Workspace	Planned: (2) Add Dining Room Configuration More ~	
Smart Config	VLANI VLANI Add wired VLANs ID Gateway IP Address (SVI) DHCP Server DHCP Pool 102 168 2 364 L Loss Times Bhaves L Used (Tabl IPs 106 4	
Configuration	Wired Add wireless VLANs	
Network-Wide	Dining Room VLAN3	
IT Devices	Wired and the second se	
Monitoring		
💑 Network-Wide 🔅		
Devices	¢	
🖬 Clients	M 3204 APPEND	
E Logs	6 6 6	
	Service Configurations	
2 Delivery Center	Multi-WAN Config	2
	Access Control List (ACL)	-

Alternatively, select an existing wired VLAN and click **More** and select **Wi-Fi Network** to add a Wi-Fi network based on the current wired VLAN.

DemoProject1 V	Client Access Devic	e Management	
硷 Workspace	Planned: (2) Add V	Dining Room	Configuration More -
🕏 Smart Config	VLAN1 VLAN1	VLAN ID Gateway IP Address (SVI) DHCP Server 3 192.168.3.1 EG310GH-E	DHCP Pool W-FI Network 192.168.3.1-192.168.3.254 Lease Time: 8hours Used/Total IP Delete VI AM
Configuration	Wired		Debte Weed Network
⊗ Network-Wide →	Dining Room VLAN3		Elete Wired NetWork
幸 Devices >	Wired		ani ani ani ani
\bigotimes Authentication $>$			
Monitoring			NUMBER OF THE OWNER OWNER OF THE OWNER OWNE
🕉 Network-Wide 🗧			
Devices			100 100 100 100 100 100 100 100 100 100
f Clients			
E Logs		1 Notice Advert	
	Service Configurations	949-0000	
🏖 Delivery Center 🔌	Multi-WAN Config		
	Access Control List (ACL)	a Daris Al Group	A Group And Participants III

(2) Setting Wi-Fi service parameters: Set Wi-Fi information first, such as the Wi-Fi name and password.

Network planning / Edit Wireless VLANs	×
1 WLAN Access — 2 Network Param 3 Confirm — 4 Apply Config	
* Wi-Fi Name: ren-testas-001@yopmail.com	
Encryption: Encryption Disabled	
• Wi-Fi password: Ruijie123 (1)	
Advanced 🔿	
Band: 💿 24G & 5G 💿 24G 💿 5G	
Next	

The following table lists the description of parameters.

Parameter	Description
SSID	Enter a string of less than 32 charters, including letters, numerals, spaces, and special characters (@&.). If spaces are contained, it cannot be longer than characters. For example, set SSID to Guest.
Encryption	You are advised to encrypt the network to prevent other clients from accessing the network. If an open network is required, click Disabled.
Password	Enter the password with a string of 8 to 16 characters, containing letters, numbers and special characters (<=>[]!@#\$*().). For example, set Password to Ruijie123.
Advanced Settings > Band	The value is 2.4G & 5G, 2.4G, or 5G. The default value is 2.4G & 5G.

(3) Configuring the VLAN for wired access: Create a DHCP address pool for devices in the VLAN to automatically obtain IP addresses. The gateway can serve as the address pool server to assign addresses to access clients. If a core switch supporting the address pool function is deployed on a network, you can configure the switch as the address pool server. After configuring service parameters, click **Next**.

Network planning / Edit Wireless VLANs	×
WLAN Access – 2 Network Param 3 Confirm — 4 Apply Config	
Description: GUEST	
VLAN ID: 33 Select	
Default Gateway/Subnet Maskc 192.168.33.1 / 255.255.255.0	
DHCP Pool: 🔵 🛈	
IP Segment 192.168.33.1 . 192.168.33.254	
Assign IP from: Gateway (Router) Usually for L2 network.	

The following table lists the description of parameters.

Parameter	Description
Description	Enter the description of the guest VLAN.

Parameter	Description		
	The VLAN ID can be set to any value from 2 to 232 and from 234 to 4060.		
	If the service network created is used for both wired and wireless client access,		
	and the corresponding wired service network (such as a wired network for guests) exists, click Select to select a VLAN ID from Existing VLANs , and		
	then click it to add a wireless network based on the wired service network.		
VLAN ID	Description: GUEST		
	VLAN ID: Please enter the VLA Select		
	Default Gateway/Subnet Mask: 192.168.1.1 Existing VLANs		
	DHCP Pool: (i) 23 (Meeting Room) 33 (guest)		
Default	When the VLAN ID is configured, the value of the default gateway or the		
Gateway/Subnet Mask	subnet mask will be updated automatically 1s later.		
	You are advised to keep the default configuration.		
	If the DHCP pool is disabled, a camera or PC needs to be manually configured with a static IP address.		
DHCP Pool	The deployment location of the IP address pool can be selected as needed.		
	Generally, the gateway used as the DHCP server is applicable to a Layer 2		
	network, and the core switch used as the DHCP server is applicable to a Layer 3 network.		
IP Segment	The parameter is available only when the DHCP pool is enabled. After the		
	VLAN ID is configured, the IP segment will be updated automatically 1s later.		
Assign IP from	The parameter is available only when the DHCP pool is enabled. You are advised to keep the default configuration.		

(4) Confirm the WLAN network configuration and click Apply. The configuration will be delivered to the gateway, switch, and AP, and takes effect.

Network planning / Edit Wireless VLANs			3
✓ WLAN Access –	Network Param	3 Confirm — (4) Apply Config	9
9	To ensure that the work (GUEST VLAN33) 192.168.33.1~192.168.33.254	takes effect, configuration will be delivered 11devices: to
	AP) SSID ren-testas-001@yopmail.com, password	1 rmp123
	EG310GH-E NAEK002BH0001	Add port VLAN33, IP 192.168.33.1, subnet mar Add address pool VLAN33, start address 192. 192.168.33.1, lease time 480 mins	sk 255.255.255.0 168.33.1, end address 192.168.33.254, DNS
	NBS3200-48GT4XS NAEK002BH0002	Add VLAN 33[Auto Configuration]:	
		Add VLAN 33[Auto Configuration]:	
	Back	pply	

(5) The service network is added successfully when the message indicating delivery success is displayed.

rk planning / Edit Wireless VLANs		
	🕜 WLAN Access – 🔗 Network Param 🔗 Confirm — 🕢 Apply Config	
CUEST] VLAN 33 Default Gateway: 192.168.3	cceeded. 13.1 255 255.255.0 IP Segment: 192.168.33.1 192.168.33.254 DHCP Server:Gateway	
Ou can also Plan switch ports for connecting to APs. If there are non-connected APs in th project, you can plan switch ports for connecting to these APs in advance. To configure	Access Control List (ACL) Block mutual access between this retwork segments, or allow mutual access for some network segments for access for some network segments for access for some network segments for access for the format of the network segments for access for the network segments for access for access for the network segments for access for access for the network segment segments for access for access for the network segment for access for access for the network segment for access for access for access for the network segment for access for access for the network segment for access for access for access for access for the network segment for access for access for access for access for access for the network segment for access for the network segment for access for	
Device Config Device Config Device Config Co		^

4.2.3 FAQs

1. How Do I Add the Names of Multiple Wi-Fi Networks to the Same VLAN?

When multiple Wi-Fi signals need to be added to the same VLAN, you can select the VLAN, to which Wi-Fi signals need to be added, in the service map in the middle, click **More** and select **Wi-Fi Network**, add Wi-Fi information, and deliver the configuration.

DemoProject1 V	Client Access Devic	te Management	
ᢙ Workspace	Planned: (3) Add 🗸	Dining Room Configur	ation More V
Smart Config	VLAN1 VLAN1	VLAN ID Gateway IP Address (SVI) DHCP Server DHCP Pool 3 102 168 3 1 E-310CH-F 102 168 3 1-102 168 3 254 Lace Time: 8houre Licet/Total IP	Wi-Fi Network
Configuration	Wired	S TSETOLST LOSTOTPE TSETOLST TSETOLSEST LEBSETTILE, OTOLIS OSEQ/TOBIL	Delete VLAN
Ø Network-Wide >	Dining Room VLAN3	📮 🍳 🍳 👘	Delete Wired Network
≇ Devices >	Wired		
	GUEST VLAN33		
Monitoring	Wireless	Design and the second s	
🗞 Network-Wide 🗧		¢	
Devices			
Clients			
E Logs	Service Configurations	L Service State St	
Selivery Center	Multi-WAN Config		<u> </u>
	Access Control List (ACL)	Million Ballion Ballion Million African Ballion Biological Ballion	-

2. How Do I Add the Names of Multiple Wi-Fi Networks to Different VLANs?

When multiple Wi-Fi networks need to be added to different VLANs, add wireless networks multiple times by referring to <u>4.2.2 Configuration Steps</u>.

DemoProject1	Client Access Devic	e Manageme	nt			
硷 Workspace	Planned: (3) Add V	Dining Ro	om			Configuration More ~
🛱 Smart Config	VLAN1 VLAN1	VLAN ID 3	Gateway IP Address (SVI) 192.168.3.1	DHCP Server EG310GH-E	DHCP Pool 192.168.3.1-192.168.3.254 Lease Time: 8hours U	lsed/Total IPs: 1/254
Configuration	Wired					
Onetwork-Wide	Dining Room VLAN3					Ruine 123
章 Devices	Wired Wireless				Canada Canada Canada Canada	a 1204guest
Authentication	GUEST VLAN33					Ruijie123
Monitoring	Wireless					
නී Network-Wide						
Devices						
Clients					All a set has a set had a set of set	
E Logs	Service Configurations					
2 Delivery Center	Multi-WAN Config Access Control List (ACL)				Alter Party Market	0 + -

4.3 Configuring the AP Management Service Network (AP Management VLAN)

4.3.1 Demand

Multiple access points (APs) are deployed on the network to transmit wireless network signals. One separate VLAN needs to be configured for management packets of the APs. Configuring a separate management service network can avoid AP go-offline due to the complex environment on the service network, thereby enhancing the stability.

Ruijie Cloud can automatically detect switch ports, to which APs are connected, and users do not need to record them in advance, simplifying the difficulty in modifying and managing VLANs.

4.3.2 Configuration Steps

1. Configuring an AP Management VLAN

(1) Choose Network-Wide > Network > VLAN > Device Management. Information about APs on the network is displayed, including the management VLAN, device models, SNs, management IP addresses, MAC addresses, and online status. Click Configuration to configure the AP management service network.

Network Configuration

DemoProject2 V	Client Access Devi	ice Management					
企 Workspace	VLAN1	AP Management				Configu	ration Reserved Port
🕏 Smart Config	VLAN 1	VLAN ID Gateway IP Ao 1 192.168.110.1	ddress (SVI) DHCP 9 EG3100	 0.1-192.168.110.254 Lea	Lease Time: 30Min Used/Total IPs: 5/254		
Configuration							
Network-Wide		Wireless AP(5)					
w Hetholik Hide		Device model	Comment	SN	MAC	Online Status	Management IP
≇ Devices >							
		RAP1260(G)		NAEK002FH0007	00d2.f800.2f71	🔮 Online	192.168.110.7
		RAP1260(G)		NAEK002FH0008	00d2.f800.2f81	Online	192.168.110.8
Monitoring		PAP2260(C)		NAEKOOZEHOOOO	0042 f800 2f01	Online	102 168 110 0
& Network-Wide ⇒		1041 2200(0)		NALKOOZITIO005	0002.1000.2191	• Online	192.100.110.9
🖴 Devices >		RAP2260(G)		NAEK002FH0010	00d2.f800.2f01	Online 🛛	192.168.110.10
🗈 Clients >		RAP2260(G)		NAEK002FH0011	00d2.f800.2f11	Online	192.168.110.11
🗄 Logs >						5 in tota	al < 1 > 10 / page >
😂 Delivery Center 🔅							

- (2) Enter the description, set VLAN ID to 23, and wait about 1 second. The default gateway/subnet mask and IP address segment will be automatically updated. You can select the deployment location of the IP address pool based on actual requirements: In general, the gateway serves as the DHCP server in Layer-2 network scenarios, and the core switch serves as the DHCP server in Layer-3 network scenarios. Click Save.
 - A Caution
 - You are advised to use default configurations for other parameters. Do not disable the DHCP address pool. Otherwise, IP addresses cannot be assigned to APs and you have to configure static IP addresses to the APs manually one by one.
 - In **Description**, enter the description of the current service network for differentiation from other service networks.
 - The VLAN ID can be set to any value in the range of 2 to 232 and 234 to 4060 except the numbers used by existing VLAN IDs.

etwork planning / Edit Wireless AP Management Services					
	Description:	GUEST VLAN			
	VLAN ID:	23			
	Default Gateway/Subnet Mask	192.168.23.1	/ 255.255.255.0		
	DHCP Pool:	0			
	IP Segment:	192.168.23.1	. 192.168.23.254		
	Assign IP from:	 Gateway (Router) Usually for L2 network 	í.		
	Lease Time:	0 days 8	hours 0	Min	
		Next			

(3) Click Apply. The configuration is delivered to the gateways and switches and takes effect. Wait till the prompt "Delivery succeeded" is displayed, indicating that the service network is added.

1 Note

After the configuration delivery is completed, PoE ports on the switches that are connected to the APs will be restarted to restart the APs. If there are configuration-free switches on the network, restart the APs manually.



(4) The AP management network configuration is delivered.

	Project2] Delivery succeeded. AN] VLAN23 Default Gateway: 192.168.23.1 255.255.50 IP Segment:192.168.23.1 192.168.23.254 DHCP Server.Gateway	
Device C		
ON EG3100 Gateway, SN	E K002FH0001	
2023-02-2023-02-	(S7) Update port VLAN config Module vlan_port of device NAEK002FH0001 changes. (S7) Update LAN config Device: NAEK002FH0001; Configuration: [('dhcpEnable':'rue','ip':'192.168.110.1','ipNum''.254,'ipStart':'192.168.110.1','leaseTime''.30, "mac'':'00:d0:#899.00:31', "mac'':'00:31', "mac'':'00:31', "mac''', "mac'', "mac''', "mac'', "mac'', "mac''', "mac'',	ask
ON NBS31 Switch, SN:N	4GT4SFP-P 302F10005	
0 [2023-02-	:57] Switch config Device: NAEK002FH0005;Port ID: [Gi1];Port status: true,Port description: "Port type: Trunk,Port VLAN: 23,Allowed VLAN: 1-4094,	
ON NBS31 Switch, SN:N	4GT45FP-P 002FH0003	

2. Configuring a Reserved Port for an AP (applicable to the scenario in which APs are not connected)

If an AP is not connected to the network, you can reserve a switch port for the AP.

(1) Choose Network-Wide > VLAN > Device Management > Reserved Port.

DemoProject2 V	Client Access	Device Manageme	nt				
窗 Workspace	VLAN23	AP Manage	ement			Configurat	ion Reserved Port
🕏 Smart Config	VLAN 23	VLAN ID 23	Gateway IP Address (S) 192.168.23.1	VI) DHCP Server EG310GH-E	DHCP Pool 192.168.23.1-192.168.23.254	Lease Time: 8hours Used/Tot	al IPs: 1/254
Configuration		Wireless AF	2(5)				
Network-Wide		Devic	e model Com	ment SN	MAC	Online Status	Management IP
The Devices		Den				ennite status	management n
		RAP	1260(G) -	- NAEK002FI	10007 00d2.f800.2f7	1 Online	192.168.110.7
Monitoring		RAP	1260(G) -	- NAEK002FI	10008 00d2.f800.2f8	1 Online	192.168.110.8
& Natural Mida		RAP	2260(G) -	- NAEK002FI	10009 00d2.f800.2f9	1 Ø Online	192.168.110.9
R Network-wide		RAP	2260(G) -	- NAEK002F	10010 00d2.f800.2f0	1 Online	192.168.110.10
Devices		RAP	2260(G) -	- NAEK002FI	10011 00d2.f800.2f1	1 Online	192.168.110.11
Clients >							
E Logs >						5 in total	< 1 > 10 / page <
😂 Delivery Center 💚							

(2) Click the switch for connecting to an AP (you can select multiple switches) in the topology on the left, and select the port reserved for AP wired connection on the switch on the port icon panel on the right. The port icon changes from dark gray to blue. Click **Next**.



(3) Click **Apply**. The configuration is delivered to the switch and takes effect. Wait till the prompt "Delivery succeeded" is displayed, indicating that the reserved port is configured successfully.

Image: Construction of the construc		
Image: Constraint of the port Gig-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 Image: Constraint of the port Gig-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 Image: Constraint of the port Gig-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 Image: Constraint of the port Gig-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 Image: Constraint of the port Gig-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 Image: Constraint of the port Gig-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 Image: Constraint of the port Gig-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 Image: Constraint of the port Gig-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 Image: Constraint of the port Gig-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 Image: Constraint of the port Gig-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 Image: Constraint of the port Gig-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 Image: Constraint of the port Gig-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 Image: Constraint of the port Gig-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36		To ensure that the network takes effect, configuration will be delivered to3devices:
The port Gi9-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 The port Gi9-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 The port Gi9-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 The port Gi9-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 The port Gi9-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 The port Gi9-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36 The port Gi9-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23, 35-36		The port Gi9-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23,35-36 NBS1100-240745FP-P NAEK002FH0005
The port Gi9-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23,35-36		The port Gi9-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23,35-36 NB53200-486TAXS NAEK002FH0002
		The port Gi9-12 is configured as the Trunk port, Native VLAN ID 23, Allowed VLAN ID 23,35-36 NBS1100-240745FP-P NAEK002FH0004
Hard Hard Hard Hard Hard Hard Hard Hard	How How How How	

(4) The port configuration is delivered successfully.

ork planning / Reserved Port	
ComoProject2] Delivery succeeded.	
Device Config	
ON NB53100-24GT45FP-P Switch, SNINAEK002FH0005	
[2023-02-01 16:04] Switch config Device: NAEK002FH0005;Port ID: [Gi9, Gi10, Gi11, Gi12];Whether the L3 interface is enabled: false;Port status: true;Port description: "Port type: Trunk;Port VLAN: 23,Allow	ed VL
ON NBS3200-48GT4XS Switch, SNINAEK002FH0002	
2023-02-01 16:04] Switch config Device: NAEK002FH0002;Port ID: [Gi9, Gi10, Gi11, Gi12];Whether the L3 interface is enabled: false,Port status: true,Port description: "Port type: Trunk,Port VLAN: 23,Allow	ed VL
ON NB53100-24GT45FP-P Switch, SktNAEK002H0004	

3. Verification

Check information about the configured AP management service network on the service map page. IP addresses obtained by APs belong to the 192.168.23.0/24 network segment.



4.4 Multi-WAN

4.4.1 Overview

1. Applicable Scenarios

When a gateway is connected to multiple extranet lines, the multi-WAN function can be configured to meet different requirements. This function mainly applies to the following three scenarios:



- Traffic from different users is transmitted through different egresses: IP traffic from some intranet users can be transmitted through a fixed extranet line.
- Bandwidth superimposition (load balancing): The gateway automatically distributes egress traffic to multiple extranet lines to achieve the bandwidth superimposition effect.
- Private line for access to the private line server: A private network refers to a network that cannot access
 the Internet, such as e-government private networks. The access traffic of a device on the intranet to private
 line resources needs to be transmitted through the private line egress, while the Internet access traffic
 needs to be transmitted through other egresses.

2. Configuration Page

Choose Network-Wide > Multi-WAN to go to the Smart WAN Selection page.



4.4.2 Multi-WAN Bandwidth Superimposition

1. Demand

A company's network connects to two broadband Internet access lines. The bandwidths need to be superimposed to meet the Internet access needs of multiple users.



2. Configuration Ideas

- (1) Configure WAN ports to access the Internet through dynamic IP addresses, static IP addresses (nonprivate line), or PPPoE.
- (2) Enable load balancing.
- 3. Configuration Steps
- (1) Click Add WAN Link to go to the Multi-WAN Config page of the gateway.

Smart WAN Selection					-WAN Link to Internet	
Target Network			Internet			
Egress WAN Link		ISP1 WAN • : 1000M Description: PPPoE DHCP	ISP2 WAN1 Image: Market interval Description: Dynamic IP 192.168.18.8	ISP3 WAN2 I Description: PPP0E 222,40,76.22 I	ISP4 WAN3 Image: Marcology Description: Static IP 192.168.66.8 Image: Marcology	+ Add WAN Link
	Load Balancing ()	Access Private				
Clients	VLAN 1 1 192.168.110.0/255.255.255.0	Network	Fixed Egress: ISP1 PBR Drag and drop networks here	PBR not supported for WAN link with dynamic IP address	Fixed Egress: ISP3 PBR Drag and drop networks here	Fixed Egress: ISP4 PBR Drag and drop networks here
	Guest 25 192.168.25.0/255.255.255.0		+Add Custom IP/IP Range		+Add Custom IP/IP Range	+Add Custom IP/IP Range

(2) Select a WAN port and configure the Internet access type for the WAN port based on the operator's requirements. It can be set to **Static IP**, **DHCP**, or **PPPoE (ADSL)**.Click **Save**.

1 Note

• If the configuration is inconsistent with the operator's requirements, for example, the account or password is incorrect, the network may be abnormal or disconnected.

		LAND	LAN1	LANZ	LAN3	LAN4	LANS	LAND/WANZ	WAN1	WAND	
Type:	PPPoE (ADSL)	~									
* IP:	Static IP				* Account:	admin			* Password:	admin	
Interface Alias:	DHCP										
	PPPoE (ADSL)										

(3) Click the back button on the right of Multi-WAN Config or click Network > Planning and Configuration > Egress Path Selection to return to the Smart WAN Selection page.

rens Route Config / Multi-WAN Config Multi-WAN Config Configu C											Configured	
		LANO	LAN1	LAN2	LANS	LAN4	LANS	LANG/WAN3		WAN1 WAND		
Type: * IP:	PPPoE (ADSL)				* Account:	admin				* Password: admin		
Interface Alias:	Please enter the a	lias.										
Tip: Egress path se egress path select	election settings suc ion settings after al	h as (load I WAN ports	balancing, pol s are configure	icy-based ro	outing, and sta	ntic routing)	" can be fo	und in <mark>Netwo</mark>	ork > Planning a	and Configuration > Egress Path Selection	', You are advised	to perform
							Save					

(4) Enable Load Balancing and click Weight to set the traffic weight.

Configure the load balancing weight based on the actual broadband proportion. The load is balanced based on the configured downlink bandwidth proportion by default. For example, the bandwidth is set to 200 Mbps for WAN1 port and 100 Mbps for other WAN ports. You can set the weight of the WAN1 port to 2 and the weight of other ports to 1. Click **Save**.

Smart WAN Selection										-Inactive WAN Link
Target Network					Internet					
			Weight Settings [®]			×				
		ISP1	WAN3:	1				ISP4 WAN3 * I		
Egress WAN Link		1000M PPPoE	WAN2:	1				Description: Static IP 192.168.66.8	Add WAN Link	
			WAN1:	2						
Clients	Default Weight>		WAN :	1			PBR	Fixed Egress: ISP3 PBR	Fixed Egress: ISP4 PBR	
	VLAN 1 1 192.168.110.0/255.255.255.0	Finan 192.1						Drag and drop networks here	Drag and drop networks here	
	Guest 25 192.168.25.0/255.255.255.0				Cancel	iave		+Add Custom IP/IP Range	+Add Custom IP/IP Range	
4.4.3 Configuring Traffic of Different Users to Pass Through Different Lines

1. Demand

A company's network connects to two broadband lines, and traffic from wired office users needs to be transmitted by the WAN2 port and the traffic from the wireless network needs to be transmitted by the WAN1 port. Bandwidth is automatically assigned to other users. The WAN1 port of the gateway is connected to an optical modem of China Telecom and the WAN2 port is connected to an optical modem of China Unicom.

2. Configuration Ideas

- (1) Configure WAN ports to access the Internet through static IP addresses PPPoE.
- (2) Configure traffic of different users to pass through different lines.
- (3) Bandwidth is automatically assigned to other users.

3. Configuration Steps

(1) Click Add WAN Link to go to the Multi-WAN Config page of the gateway.

Smart WAN Selection					-WAN Link to Internet	-WAN Link to Private Network -Inactive WAN Link
Target Network						
Egress WAN Link		INDOM Description: PPPoE DHCP	ISP2 WAN1 I Description: Dynamic IP 192.168.18.88	ISP3 WAN2 Image: Space state stat	Description: Static IP 192.168.66.8	+ Add WAN Link
ell su te	Default Load Balancing ⑦	Access Private	Eived Egrass: ISD1 PRR	Eived Farase: ISD2 PRR	Eived Egrass: ISD3 PRR	Eived Forese: ISDA PRR
Clients	VLAN 1 1 192.168.110.0/255.255.255.0	Network	Drag and drop networks here	PBR not supported for WAN link with dynamic IP address	Drag and drop networks here	Drag and drop networks here
	Guest 25 192.168.25.0/255.255.255.0		+Add Custom IP/IP Range		+Add Custom IP/IP Range	+Add Custom IP/IP Range

(2) Select a WAN port and configure the Internet access type for the WAN port based on the operator's requirements. It can be set to **Static IP**, **DHCP**, or **PPPoE (ADSL)**.Click **Save**.



If the configuration is inconsistent with the operator's requirements, for example, the account or password is incorrect, the network may be abnormal or disconnected.

		LAND	LANI	LAN2	LAN3	LAN4	LANS	LAN6/WAN3	LANT/WAN2			WAND		
Type:	PPPoE (ADSL)	^												
* IP:	Static IP				* Account:	admin				* Passwo	rd: ad	min		
Interface Alias	DHCP													
Interface Allas.	PPPoE (ADSL)													

(3) Click the back button on the right of Multi-WAN Config or click Network > Planning and Configuration > Egress Path Selection to return to the Smart WAN Selection page.

	LANO LAN	LAN2 LAN3	LAN4 LAN5	LANG/WAN3 LAND/WAN2		
Type: PPPoE (Al * IP: 222.40.76. erface Alias: Please ent	DSL) V 22 ter the alias.	+ Accou	nt: admin		* Password: admin	
gress path selection sett ss path selection settings	ings such as (load balanci after all WAN ports are co	ng, policy-based routing, and	static routing) " can be	e found in <u>Network > Planning</u>	and Configuration > Egress Path Selection,	, You are advised to p

(4) Configure a routing policy.

🛕 Caution

• Only static IP addresses or PPPoE (ADSL) support the policy-based route (PBR) configuration.

If you need to add a created service network to a fixed line, for example, configure all users in VLAN 23 to access the Internet through the egress of ISP1, select VLAN 23 and drag it to the corresponding service network area, such as **Fixed Egress: ISP1**.

Smart WAN Selection					-WAN Link to Internet	-WAN Link to Private Network -Inactive WAN Link
Target Network			Internet	+ 1 +		
		ISP1 WAN	ISP2 WAN1 •	ISP3 WAN2 ·	ISP4 WANS .	
Egress WAN Link		1000M Description: PPPoE DHCP	Description: Dynamic IP 192.168.18.88	Description: PPPoE 222.40.76.22	Description: Static IP 192.168.66.8	+ Add WAN Link
Clients	Default Weight>	Network	Fixed Egress: ISP1 PBR	Fixed Egress: ISP2 PBR	Fixed Egress: ISP3 PBR	Fixed Egress: ISP4 PBR
	VLAN 1 1 192.168.110.0/255.255.255.0	Guest 25 192.168.25.0/255.255.255.0	Finance 23	PBR not supported for WAN link with dynamic IP address	Drag and drop networks here	Drag and drop networks here
			+Add Custom IP/IP Range		+Add Custom IP/IP Range	+Add Custom IP/IP Range

You can also click Add Custom IP/IP Range, for example, add an IP address or IP address range for Fixed Egress: ISP3.

Smart WAN Selection				WAN Link to Internet	-WAN Link to Private NetworkInactive WAN Link
Target Network	Add or Edit PBR	۲	×	1	
Egress WAN Link	ISP1 ISP2 Please	e enter the IP address or IP range wan2 specified with : cy-base6Route 16.11.12 or 17.16.2.0/355.355.255.0 + Add User IP/IP Range] 0	ISP2 WAN3 * :] Description: Static IP.] 192.168.66.8	+ Add WAN Link
Clients Default Coad Bo VLAN 1 1 192.166.110.0/25	lan User1 User2 =			Fixed Egress: ISP3 PBR Drag and drop networks here	Fixed Egress: ISP4 PBR Drag and drop networks here
		Cancel	ОК	+ Add Custom IP/IP Range	+Add Custom IP/IP Range

4.4.4 Configuring the Traffic for Accessing a Private Line Server to Go Through a Private Line

1. Demand

A company's network connects to three Internet broadband lines: ISP1, ISP2, and ISP3 lines, and the company has a financial private line. The financial software on the intranet can normally access the financial server through the financial private line and all devices can access the Internet through the ISP lines.

2. Configuration Ideas

- (1) Configure a static IP address for the WAN3 port and select the private line.
- (2) There are two policies available for private networks:

 Specifying the destination network: When all users access the Internet, the traffic for accessing the specified destination network (such as the server IP address) is transmitted through the private line and other traffic is not transmitted through the private line.

• Specifying Intranet users: When specified Intranet users access the Internet, the traffic of the users is transmitted through the private line and the traffic of other users is not transmitted through the private line.

3. Configuration Steps

- (1) Click Add WAN Link to go to the Multi-WAN Config page.

(2) Configure Internet access type for the WAN port based on the operator's requirements. Type can be set to Static IP for private lines. Set Private Line to Yes, click Save, and then click the back arrow on the right of Multi-WAN Config at the upper right corner.

Egress Route Config / I	Multi-WAN Config Config							n noff
		LAND	LANT	LAN2 LAN3	LANA LANS	LANG/MINIS	VIANT NAAM	
Type:	Static IP V							
• IP :	192.168.1.10			 Subnet Mask: 	255.255.255.0		• Egress Gateway: 192.168.1.2	
Interface Alias:	Please enter the allas.							
Private Line :	Yes 🗸 🗸	A private netw	vork refers to a	network that cannot a	ccess the internet, such as e	-government private network	Ŝ.	
Tip: Egress path sel settings after all W	ection settings such as (loar IAN ports are configured.	d balancing, po	licy-based rou	ting, and static routin	g) " can be found in <u>Netw</u> Save	rork > Planning and Configur	ation > Egress Path Selection, " , You are advised to	perform egress path selection

1 Note

- Private lines can be selected only for static IP addresses. After the private line is enabled, the device will forward traffic according to the policy (specifying users or specifying private line resources) specified for the private line.
- (3) Policy 1: Allow some users to only access the private line. You can drag a created VLAN to the Fixed Egress: Private Line module.

Smart WAN Selection			-WAN Link to Internet -WAN Link to Private Network -Inactive WAN Link
Target Network	Internat	Private (Cannot access Network the internet) +Add Private Static Network Addres Route	
Egress WAN Link	(57) WAN • (52) WAN1 • : 1000MI (Decryption - -) Decryption - - Decryption - - 9996 [Decryption - - 102.168.13,88 - - Decryption - -	Image: Second	+ Add VIAN Link
Clients Defaul VLAN 19216	Laad Bilancing O: Access Private Fixed Egress: It Wetwork Petrovic Constraints (Constraints) 111 11200/2552552550 Intel 101 1192166.1010/255255250 Intel	PBR Fixed Egress: ISP2 PBR Fixed Egress: ISP3 etworks PBR not supported for WAN link with dynamic IP address Dag and drop network Notes engre - Add Custum (P)/P Rail	PBR Fixed Egress: PBR Private Line Fixed 102 1921101 1020052552550 rgf +Add Custom IP/IP Range

You can also click Add Custom IP/IP Range to add an IP address or IP address segment.

Smart WAN Selection					-WAN	Unk to Internet
Target Network			Contrast.	Private (Cannot acces Network the internet) +Add Private Network Address	55 10	
Egress WAN Link		Add or Edit PBR	Please enter the IP address or IP range want Paring banefloate 1722.16.11.12 or 17.16.2.0/255.255.255.0 + Add User IP/IP Range	A specified with :	WAN3 * 5 Inform - Add 192.168.130	** **********
Clients	Default Coad Balancin Weight- VLAN 1 [1 192.106.110.0/255.255.2	User1 User2			xed Egress: ISP3 PBR rag and drop networks ere Add Custom IB/IP Range	Fixed Egress Per Private Line Per Rinance 102 143. Host Not 2015 2535555
				Cancel		

(4) Policy 2: Allow the default service network to access the private line.

Click Add Private Network Address or set Access Private Network to On to go to the Add or Edit Private Network Address page.

Smart WAN Selection				WA	IN Link to Internet HWAN Link to Private Network Hinactive WAN Link
Target Network			Private (Cannot acc Network the Interne «Add Private Network Address Ro	ess 10 affic ute	
Egress WAN Link	1000 WAN + 1 10 1000/ Description PPWL DICP 11	10escription	WAN2 • I Internet Int	WAN3 • 1 scription A	+ ed WAAN Link
Clients	Default Load Balancing & Access Private Weights VLAN 1 1 192.168.110.6/255.255.25 Gweet 50 192.148.101.6/255.255.255.0	Fixed Egress: ISP1 PBR: Drag and drop networks here + Add Custom IP/IP Range	Fixed Egress: ISP2 PBR PBR not supported for WAN link with dynamic IP address	Fixed Egress: ISP3 PBR Drag and drop networks here +Add Custom IP/IP Range	E Fixed Egress: PER Private Line 192 108 102 0035355350 +Add Curtom IN/P Range



Edit the destination network specified for the private line (you need to specify the address or address segment of the private line you want to access, such as the tax network or medical network; you can set multiple addresses).



• The address should be as accurate as possible to avoid selecting the private network for the normal Internet access and affecting the normal Internet access service.

Smart WAN Selection				WAN Link to InternetWAN Link to Private NetworkInactive WAN Link
Target Network		(thermat	Private (Cannot access Network the Internet) « Add Private State Network Address State	
	A	dd or Edit Private Network Address	x	
Egress WAN Link		Image: Spring state Please enter Private N Spring state 172.16.11.12 or 17 + add + add	Network Address : Sanickover (16.20/255.255.55.0 0	Add MANY Link
Clients	Default Load Balancin Weight> VLAN 1 1 192168.110.0/255.255.21		wed Egress. IS yeap and drop n	593 min B Fixed Egness: min Private Line Minance 102 102.105.0255255255
		-	Add Custom IP/	AP Renge +Add Custom IP/IP Range
			Cancel	

5 Optimization Configuration

5.1 Wi-Fi Optimization

Overview

Wi-Fi optimization is an intelligent and automatic RF optimization scheme tailored for complex scenarios with multiple APs. This function is supported by enterprise APs, most Reyee APs, and EGs. After the device enabled with Wi-Fi optimization collects spatial information, including the SSID, channel, signal strength, and client status (for example, transfer rate, delay, packet loss rate), it analyses information through the intelligent algorithm to provide the optimal network solution (channel and power planning for each AP), and automatically adjusts the configuration of APs on the network.

Wi-Fi optimization is applicable to the following scenarios:

- In the scenario where over 100 APs need to be optimized, auto channel optimization does not achieve good roaming effect, and it takes too much time to manually adjust the channel and power.
- In an office with dozens of APs where network connections are unstable for some PCs or phones, clients may experience web buffering and low speed. Wireless network optimization is time- and labor-consuming.

Procedure

- Log in to Ruijie Cloud, choose Project > Configuration > Network-Wide > Optimization > Wi-Fi
 Optimization and select a network in this account.
- (2) Click Enable Wi-Fi optimization.

	Wi-Fi Optimization
2.4G	Optimize the channel and the power of APs in the project with one click, so as to reduce the interference of wireless channels and improve the user experience.
	Note: Please enable Wi-Fi optimization during non-peak hours.
36 36 36 5G 36 60 135	Enable Wi-Fi Optimization

(3) Click Optimize Now to start optimization.

Wi-Fi Optimization Settings



Online Clients: indicates the number of all online wireless clients.

Estimated Time: indicates the estimated time to complete optimization.

Optimization Schedule: enables or disables scheduled optimization. You are advised to optimize Wi-Fi during non-peak hours.

If you want set scheduled optimization, enable **Optimization Schedule**, set the optimization time and action, and click **Save**.

Optimization	Schedule
Enabled	
Start Time	· · · · · · · · · · · · · · · · · · ·
Repeat on	 Monday Tuesday Wednesday Thursday Friday Saturday Sunday
Action	 Synchronize recommended channel and power Synchronize recommended channel
	save

(4) After the optimization is complete, the browser displays the optimization details.

Last Optimization 2022-03-07 10:00	0:37 Improved by	60%	Optimized APs Total APs: 5	3						
Wi-Fi Optimization	Record									
AP SN ©	Alias	Optimized	Band ©		Channel Before Optimization	Channel After Optimization	Power Before Optimization	Power After Optimization	Other	
1234942512345	AP710		2.4G		6	6	100	100		-
1234942512345	AP710	Yes	5G		149	149	100	99		P C
G1L9199001308	AP720-L	Yes	2.4G		9	1	99	99		0
G1L9199001308	AP720-L		5G		60	60	99	99		
G1MQ3U600181A	A720	Yes	2.4G		6	11	99	99		
G1MQ3U600181A	A720		5G		157	157	99	99		
CANLC2R001191	ReyeeAP1		2.4G	Other para	ameters: channel width before	80, channel width after: 80; ro	aming sensitivity before: 0, roan	ning sensitivity after: 0; interfer	ence before: 0, interference at	her: 0.
CANLC2R001191	ReyeeAP1		5G		36	36	100	100	Other parameters. c	

Last Optimization: indicates the time of last optimization.

Improved by: indicates the improved device percentage.

Optimized APs: indicates the number of optimized devices.

AP SN: indicates the serial number of an AP.

Alias: indicates the description of an AP.

Optimized: indicates the optimized result.

Band: indicates the optimized wireless band.

Channel Before Optimization: indicates the wireless channel before optimization.

Channel After Optimization: indicates the wireless channel after optimization.

Power Before Optimization: indicates the local power before optimization.

Power after Optimization: indicates the local power after optimization.

Other: indicates other parameters for Reyee devices. The parameters are as follows:

- O Channel width before: indicates the channel width before optimization.
- O Channel width after: indicates the channel width after optimization.
- O Roaming sensitivity before: indicates the roaming sensitivity before optimization.
- O Roaming sensitivity after: indicates the roaming sensitivity after optimization.
- O Interference before: indicates the interference before optimization.
- O Interference after: indicates the interference after optimization.

5.2 Loop Prevention

5.2.1 Overview

Enabling loop prevention can avoid network congestion and disconnection caused by loops. Ports connected to the switch will be automatically disabled after a loop occurs.

5.2.2 Configuration Steps

Choose Configuration > Network-Wide > Optimization > Loop Prevention.

moProject3					
Workspace					
Smart Config					
figuration					
Network-Wide	>	Network	Optimization	Security	Loop Prevention (RLDP)
Devices	>	VLAN	Wi-Fi Optimization	ACL	Enabling loop protection can avoid network congestion and disconnection caused by loops. Ports
Authentication	>	Multi-WAN	Loop Prevention	ARP Spoofing Guard	connected to the switch will be automatically disabled after a loop occurs.
nitoring			DHCP Snooping		
Network-Wide	>				Optimize Now
Devices	>				
Clients	>				
Logs	>				

DemoProject3	\mathbf{v}		
俭 Workspace			
🖏 Smart Config			
Configuration			
Network-Wide	×	Switch continues to work Will be sent for will be sent for	Loop Prevention (RLDP)
击 Devices	>		Enabling loop protection can avoid network
⊘ Authentication	>	Aresed log	congestion and disconnection caused by loops. Ports connected to the switch will be automatically disabled after a loop occurs.
Monitoring			
品 Network-Wide	>		Optimize Now
P Devices	>		
🔝 Clients	>		
E Logs	>		
Selivery Cente	r>	_	

Click **Optimize Now**. You are advised to use the default value. Click **Deliver Config**.

DemoProject3 V	Loop Prevention / Loop Prevention Config						
ⓐ Workspace ← Loop Prevention Config							
你 Smart Config	Please click switches on which you want to enable the Loop Protection feature: Recommendation Custom Custom Custom						
Configuration	Enable on all identified access Manually select access switches switches in the project						
Ø Network-Wide >	(a) Distated						
🗄 Devices >	NSS200-4907AS						
\bigotimes Authentication $>$							
Monitoring	(G24) (nutred (G24) (nutred (G24) (nutred (G24)						
용 Network-Wide >	+ N851100-2407467						
Pevices >	SHARE0036H0003 (G1-2) (G1) (G1)						
Clients >	φ φ φ						
Logs >	Selected: 3 device(s) Deliver Config						
😓 Delivery Center							



5.3 DHCP Snooping

5.3.1 Overview

If a private router is connected to the network, some clients may obtain incorrect IP addresses and fail to access the Internet.

After the DHCP Snooping feature is enabled, a client on the original network will not be able to obtain an IP address assigned by the private router, thus ensuring network stability.



5.3.2 Configuration Steps

Choose Configuration > Network-Wide > Optimization > DHCP Snooping.

DemoProject3					
硷 Workspace					
協 Smart Config					
Configuration			Ensure IP address obta from this server	ining	DHCP Snooping (Block Illegal DHCP
Network-Wide	Network	Optimization	Security	1	
⊞ Devices	VLAN	Wi-Fi Optimization	ACL		After the DHUP Shooping feature is enabled, a client on the original network will not be able to obtain an IP
	> Multi-WAN	Loop Prevention	ARP Spoofing Guard		address assigned by the private router, thus ensuring network stability.
Monitoring		DHCP Snooping			Optimize Now
路 Network-Wide	×				
Devices	×				
f. Clients	×				
E Logs	Σ				



Click Optimize Now. You are advised to use the default value. Click Deliver Config.

DHCP Snooping / DHCP Snooping Config		
\leftarrow DHCP Snooping Config		
Please click switches on which you v	vant to enable the DHCP Snooping feature:	
Recommend Enable on all switches	Customed Manually select access switches	
Selected: 5 device(s)	Deliver Config	

DemoProject3		DHCP Snooping / DHCP Snooping Config
l Workspace		← DHCP Snooping Config Configuration successfully delivered.
弥 Smart Config		Please click switches on which you want to enable the DHCP prooping reasure. Recommend Customed Enable on all switches Manually select access switches
Configuration		
Network-Wide		٩
⊒ Devices		
		4
Monitoring		
🖧 Network-Wide		
Devices		
🗋 Clients		
딸 Logs	>	Selected: 5 device(s) Deliver Config

DemoProject3	DHCP Snooping
硷 Workspace	After the DHCP Snooping feature is enabled, a client on the original network will not be able to obtain an IP address assigned by the private router, thus ensuring network stability.
🖧 Smart Config	DHCP Snooping 💽
Configuration	Configure
Ø Network-Wide	
🗄 Devices	
\oslash Authentication	
Monitoring	
🖧 Network-Wide	
Devices	+ \$\frac{1}{2}\begin{tabular}{c} & & & & & & & & & & & & & & & & & & &
f. Clients	a <u>a</u> a
딸 Logs	

5.4 Traffic Control

Set real-time traffic rate for a user or an application.

When the bandwidth of the project is insufficient, guarantee the real-time rate for key users or applications, while high-rate and non-key users and applications are rate limited.

You can use the traffic control template to manage the real-time traffic rate for a user or application.

When the bandwidth of the project is insufficient, guarantee the real-time rate for key users or applications, while high-rate and non-key users and applications are rate limited.

I. Click		Interface		Bandwidth			etting
DemoProject3		Flow Control	Application Control				i.
☆ Workspace							
🖏 Smart Config		You can use the traffic control temp When the bandwidth of the project	plate to manage the real-time traffic rat is insufficient, guarantee the real-time	e for a user or application rate for key users or app	n. Ilications, while high-rate and non-key users a	nd applications are rate limited.	
Configuration		Select Template					- 11
Network-Wide	>	Traffic control can be configured	later if you want to test the actual s	peed of the extranet.			
H Devices	>	Configure later Not configured because a traffic template is not selected	Office Template Guarantee the use exp office applications	perience of common	Entertainment Template Guarantee the use experience of entertainment applications and daily life	Manual Template Control the traffic of custom applications	
Authentication	>	tomplate to net concered.	onios apprioratorio.		applications.		
Monitoring		Interface Bandwidth Set	ttings				11
& Network-Wide	>	Traffic control policy only takes effe	ect on selected interfaces.				
Devices	>	WAN(br-wan) WAN	ter if you want to test the actual speed of 1 1(br-wan1)	WAN3(br-wan3)			
Clients	>						
🗑 Logs	>	WAN: Uplink	Mbps Downlin	nk	Mbps		
😓 Delivery Center	>						11
				s	ave		

2. Select a template.

Configure later: indicates that traffic control is disabled.

Office Template: indicates that the embedded smart traffic control policy guarantees the traffic of common office and work applications, and user-defined policies can be added.

Entertainment Template: indicates that the embedded smart traffic control policy guarantees the traffic of entertainment and common daily life applications, and user-defined policies can be added.

Manual Template: indicates that traffic control settings are customized and a traffic control policy is manually added.

3. Add a custom traffic control policy.

NER 20220214	V					
NDR_20230214		Flow Control	App/Website Control			
Horkspace						
🖏 Smart Config		Smart Flow Control	ustom traffic control policy			
Configuration		LAN3/WAN1(GI0/3)				
Network-Wide		Add V Delete Selecte	ed			0
	>	IP Traffic Control	y Alias	Control Mode	IP/Clients	Action
	ı >	Application traffic Control	Rate limit		192.168.101.2-	
Monitoring		1 1	55 Overall 🕇 0.001Mb	ops ~ 656.000Mbps 🕴 0.001Mbps ~ 66.000M	192.168.101.254	Edit Delete
융 Network-Wide						1 in total < 1 > 10 / page >
Devices	>					
Clients	>					
E Logs	>					
📚 Delivery Cen	ter⇒					

4. Configure a traffic control policy: When the bandwidth reaches 3 Mbps, a user can watch high-definition videos smoothly; when the bandwidth reaches 1 Mbps, a user can watch standard-definition videos smoothly; when the bandwidth reaches 0.1 Mbps, a user can browse Web pages smoothly.

Browsing we	b pages		Standard-d	efinition video	ŀ	High-definition video
0.1 Mb	ps		11	Mbps		3 Mbps
NBR_20230214 V	Flow Control	App/Website Control				
Smart Config	Smart Flow Control	Custom traffic control policy				
Configuration	LAN3/WAN1(GI0/3)					
Network-Wide >	Add V Delete S	Selected				0
III Devices	IP Traffic Control Application Traffic Control	olicy Alias	Control Mode	IP/Clients	Application	Action
Authentication >	1	55		192.168.101.2-		Edit Delete
Monitoring		Overall 🕇 0.00	1Mbps ~ 656.000Mbps	00Mbps 192.168.101.254		
& Network-Wide ⇒						1 in total < 1 > 10 / page V
Devices						
Clients >						
₽ Logs >						
Delivery Center						

5.4.1 IP Traffic Control

Select IP: Select the IP address range, in which the traffic control policy takes effect.

Select Traffic Control Mode: Select Rate limit or No rate limit.

Rate Limit Settings: Overall rate limit indicates the overall maximum rate and Per IP rate limit indicates the maximum rate for each IP address.

Overall maximum/Per IP maximum: indicates the uplink and downlink maximum rates, in Mbps.

Overall minimum in the **Advanced** area: indicates the guaranteed rate for users when the bandwidth is insufficient.

Apply to interface: indicates the port, in which the policy takes effect. You are advised to select All Ports.

Policy Name: Configure a name for the policy to facilitate maintenance.

Custom traffic control policy ③	2
1 Select IP	
Select	\vee
2 Select Traffic Control Mode	
Rate limit Limit the IP addresses of non-key users or from which traffic is transmitted at a high rate.	
 No rate limit Do not limit Internet speed of selected users. 	
3 Rate Limit Settings	
Rate limit mode: Overall rate limit V	
Overall maximum:Uplink Mbps Downlink Mbps	
Advanced: A	
Overall minimum:Uplink Mbps Downlink Mbps	
4 Apply to interface	
All Ports LAN3/WAN1(Gi0/3)	
5 Status	
6 Policy Name	
Enter a name for the policy.	

OK

5.4.2 Application Traffic Control

Select IP: Select the IP address range, in which the traffic control policy takes effect.

Select Application: Select the application whose traffic needs to be controlled. You can enter keywords for search.

2	Soloct A	oplication
- 2	Select A	pplication

All applications	۲	Custom applications	0
Enter a search term			
▼ HTTP			
▶ WebApplication	on		
Fast			
BaiDuWenKu			
▶ WebApplication	on_A	pp	

Select Traffic Control Mode: Select Rate limit or No rate limit.

Rate Limit Settings: Overall rate limit indicates the overall maximum rate and Per IP rate limit indicates the maximum rate for each IP address.

Overall maximum/Per IP maximum: indicates the uplink and downlink maximum rates, in Mbps.

Overall minimum in the **Advanced** area: indicates the guaranteed rate for users when the bandwidth is insufficient.

Apply to interface: indicates the port, in which the policy takes effect. You are advised to select All Ports.

Policy Name: Configure a name for the policy to facilitate maintenance.

Custom traffic control policy ③	×
1 Select IP	
Select	~
2 Select Application • All applications • Custom applications • ① • ① • ①	
3 Select Traffic Control Mode	
Rate limit Limit the IP addresses of non-key users or from which traffic is transmitted at a high rate.	
 No rate limit Do not limit Internet speed of selected users. 	
4 Rate Limit Settings	
Rate limit mode: Overall rate limit <	
Overall maximum:Uplink Mbps Downlink Mbps	
Advanced: 🔨	
Overall minimum:Uplink Mbps Downlink Mbps	
5 Apply to interface	
All Ports LAN3/WAN1(Gi0/3)	
6 Status	
7 Policy Name	
Enter a name for the policy.	

ОК

5.4.3 Configuring the Policy Priority

Click the number of a policy to adjust the policy sequence. A smaller number indicates a higher priority.

Flow Control	App/	App/Website Control		
Smart Flow Control	Custom traffic c	ontrol policy		
Adjust order				
Exchange the order of this rule and rule {n}.				
(A smaller number indicates a higher	priority.) ias		C	
	23223	Rate limit	~ 23.00	

5.4.4 App/Website Control

Here you can add blocked applications and websites. Access to a blocked app or website will be restricted.

NBR_20230214	Flow	v Control	App/Website Control			
ඛ Workspace	App/Website	Control				
Smart Config	Here you can add	blocked applications and	sobsiles. Access to a blocked app or website will be restricted y cannot access the internet.			
Configuration	Add 🖸	Delete Selected				0
Network-Wide		Policy Alias	IPiClients	App/Website Control	Action	
Devices		xmtest0216_003	192.168.100 10-192.168.100.222	HTTP Social_applications ProtocalClass FileTransfer Vpn-app REMOTE-PROTOCOL SoftwareUpdate ForumBlog OnlinePaymentConlineBank Voip OnlineStorage DownloadTools_MOBILE News[Reader]Life	Edit Delete	
Monitoring		test1	192.168.30.1-192.168.30.254	Information Business-Economic Bad Hot-Websites xlaomeitest01 xlaomeitest02	Edit Delete	
Devices		test2	192.168.30.1-192.168.30.254	Information Business-Economic Bad Hot-Websites xisomeitest01 xisomeitest02	Edit Delete	
Clients)		xmtest0216_001	192.168.201.2-192.168.201.254	Information Business-Economic Bad Hot-Websites	Edit Delete	
E Logs					4 in total < 1 > 10 / pa	xage √]

1. Choose **Project > Network-Wide > Traffic Control > App/Website Control** and click **Add**.

2. Configure a policy.

OK

App/Website Control	×
1 Select IP	
Select	
2 Select Application or Website Custom Websites	
Enter a search term SoftwareUpdate Forum Blog OnlinePayment OnlineBank Voip Voip OnlineStorage DownloadTools_MOBILE News Reader Life ICMP-DETAIL IP-RAW 	 Vpn-app REMOTE-PROTOCOL NetworkDisk OnlineStorage Voip
 VetworkDisk 	
3 Effective time	
Nightime	~
4 Status 5 Application Control Policy Alias	
Enter a name for the policy.	

Select IP: Select the IP address range, in which the policy does not take effect.

Select Application or Website: Select an application or website to be blocked. You can click **Custom Websites** to add the website domain name to be blocked.

NBR_20230214 V	Flow Control	App/Website Control	App/Website Control	×
☑ Workspace			1 Select IP	
👫 Smart Config	App/Website Control Here you can add blocked applications and		Select	
Configuration	Add Delete Selected		2 Select Application or Website	
Network-Wide >	Policy Alias	IP/Clients	Custom Websites	
E Devices → Authentication →			edat_applications ProtocolClass ColorPayment OntimeBank ColorPayment OntimeBank ColorPayment OntimeBank ColorPayment OntimeBank	Vpn-app REMOTE-PROTOCOL NetworkDisk
Monitoring		Custom Websites	× ¢OnlineBank	ConfineStorage
Devices >		192 Website Class Name Description URL	Action	
☐ Clients →		192 xiaomeitest01 xiaomeitest 163.com/app	o/123.aspx Edit DeleteMOBILE	
🗄 Logs >			1 in total < 1 > 10 / page >	
念 Delivery Center ⇒			Cencel Add	
			3 Effective time	
			The form	
			4 Status	
			5 Application Control Policy Alias	
			Enter a name for the policy.	
				ОК
				_

1 Note

 URLs support two levels of directories at most, for example, www.ruijie.com.cn/about/summary.aspx.URLs must be separated by either a carriage return character or a comma. URL prefixes such as http:// or https:// are not required.

Effective time: Select the time when the policy takes effect.

Application Control Policy Alias: Enter the policy comment to facilitate maintenance.

6 Security Configuration

6.1 Network Access Control (simplified)

6.1.1 Applicable Scenarios

There are various types of users on the network. To ensure security, some users are banned from accessing each other, such as visitors, finance department, servers, and monitoring devices. Service access control can prohibit mutual access between different network segments.

6.1.2 Models of ACL-Supported Products

Product Type	Device Name	Version
Gateway	EG series EG-E series	
Reyee Switch	NBS5100 series NBS5200 series NBS6002 series NBS7003 series NBS7006 series	ReyeeOS 1.86 or later

6.1.3 Configuration Steps

1. Creating a Service Network

For details, see <u>4.1 Creating a Wired VLAN</u>

2. Configuring Service Access Control

Choose Configuration > Network-Wide > Security > Network Access Control.

Security Configuration

Cookbook

Ruffie IRcycc 2	Home	Project				1000 L;	w_testas@ch∨ ⊙ © Ω Ω 💬 ⊚
DemoProject1 V	Al Roar	ming					
Workspace	Al Roam	ing L2 L3 Roaming	9				
AI Networking							
Smart Config	802.1 To ensu	I1K/V Roaming 💽 In are smart roaming, when the to	process pology changes, please tap here scan	the wireless network again.			
Al Diagnostics	(The fo	llowing is the latest three-day s	statistics, in which the signal strength	and uplink and downlink rates are avera	jed.)		Total Client List O
Configuration				aming Steering Counts	RSSI Before Roaming dBm	Rx Negotiated Rate Mbps	Tx Negotiated Rate Mbps
Network-Wide	Network	Optimization	Security		-	(Betore/After Roaming)	(Before/After Koaming)
華 Devices >	Network	Wi-Fi Optimization	Network Access Control				
Auth & Accounts >	Multi-WAN	AI Roaming	ARP Spoofing Guard				
Monitoring		Loop Prevention			No Data		
융 Network-Wide >		DHCP Snooping					
Devices		Traffic Control					
☐ Clients →							
E Logs							
Delivery Center >							

(1) Click To configure to go to the Network Access Control page.

On this page, service networks are divided into two zones based on the access permission of the service networks.

Interworking Zone

Service networks in the interworking zone can access each other.

Isolation Zone

Service network segments in the isolation zone cannot access those in the interworking zone and vice versa.

Service network segments in the isolation zone are isolated from each other.

The ban is bidirectional. For example, if both network segments A and B are banned, A cannot access B, and B cannot access A, either.



Cookbook

	Home Project	
DemoProject1 V	Network Access Control	
	Drag a service network to the [Interworking Zone] or [Isolation Zone] as required, More	
AI Networking	Interworking Zone	Isolation Zone 🔿
Smart Config	Service networks in the Interworking Zone can access each other	Service networks in the Isolation Zone cannot access each other. If necessary, a network segment or IP can be added for mutual access between a certain service network in the Isolation Zone and the one in the Interworking Zone
Al Diagnostics	VLAN 1 I VLAN1	
Configuration	192.168.110.1/255.255.255.0	
⊗ Network-Wide →		Dining Room I VLAN23
Devices		192.168.287/255.255.25
Manifesian		
A Network-Wide		Cannot access each other
Devices		Ch.
🖬 Clients >		v
E Logs		Service networks to which you want to grant access permissions Drag
Delivery Center >		

(2) Drag a service network whose access permission needs to be restricted from the interworking zone to the isolation zone and click **Save**.

	Home	e Project		🔤 🖾 C. D. 🖾 🛞 🛞
DemoProject1 V		Network Access Control		
Workspace		Drag a service network to the [Interworking Zone] or [Isolation Zone] as required, More		
AI Networking		Interworking Zone		Isolation Zong
Smart Config		Service networks in the Interworking Zone can access each other		Service networks in the Isolation Zone cannot access each other. If necessary, a network segment or IP can be added for mutual access between a certain service network in the Isolation Zone and the one in the Intervention Zone
Al Diagnostics		VLAN 1 VLAN1		
Configuration		192.168.110.1/255.255.2		After the service network is saved, you can add IP or IP range to the service network X
Network-Wide				Dining Room VLAN23 192.168.23.1/255.255.255.0
Auth & Accounts >			Þ	IP No IP
Monitoring				
å Network-Wide ⇒			Cannot access each other	
Devices				
f∐ Clients →				
E Logs				
a Delivery Center				
			Cancel	

(3) (Optional) In Isolation Zone, click No IP.

No IP:

- o Exceptional exemption rules have a higher priority than banning rules.
- It is used to exempt a specific IP or network segment, for example, after adding a monitoring network to the isolation zone, you can exempt the administrator IP address and allow it to access other service networks.
- Banning exemption is also bidirectional. For example, if network segment A allows access from IP X, the access from network segment A to IP X and the access from IP X to network segment A are both reachable.

In Isolation Zone, select a service network and click No IP to go to the Add Accessible IP page. Configure the accessible IP address or IP address range and click Save.

Ruijie IRcycc 🏠 H	lome Project		🔤 line_testas@ch 🗸 💿 🛞 🛞
DemoProject1 V	Network Access Control		
Workspace	Drag a service network to the [Interworking Zone] or [Isolation Zone] as required, More	
AI Networking	latamatika 7an		
Smart Config	Service networks in the Interworking Zone can access each of	Add Accessible IP X	isolation Zone cannot access each other. If necessary, a network segment or IP can be added
Al Diagnostics	VI AN 1 I VI AN1		ween a bertain service network in the isolation zone and the one in the interworking zone
Configuration	192.168.110.1/255.255.255.0	Enter or select VLAR23/Ulling koom (192, 10623-1/253-253-253-2) IP or IP range for mutual access Existing service networks Custom IP range Single IP 52	N23
Network-Wide >		102 168 22 23	
Devices		126-1006-0-04	
✓ Auth & Accounts >			
Monitoring		I	
Devices			
Clients >			
E Logs >			
🍣 Delivery Center 🗇		Cancel	

Ruffe IRcycc 2	lome Project			🚥 isw_testas@ich 🗸 🕤 🕲 🔕
DemoProject1 V	Natural Access Control			
Workspace	O Drag a service network to the [Interworking Zone] or [Isolation Zone] as required. More	e succeeded!		
AI Networking	Interworking Tops		kalatian Zana 🔕	
Smart Config	Service networks in the Interworking Zone can access each other		Service networks in the Isolation Zone cannot acc for mutual access between a certain service net	cess each other. If necessary, a network segment or IP can be added etwork in the Isolation Zone and the one in the Interworking Zone
 Al Diagnostics 	VLAN 1 VLAN1			
© Network-Wide >	192.168.110.1/255.255.255.0		Dining Room VLAN23 192.168.23.1/255.255.255.0 IP 192.168.23.32	
Devices >			Continue to add	
		~		
Monitoring		hở -		
& Network-Wide ⇒		Cannot access each other		
ie Devices →				
🗟 Logs >				
🍣 Delivery Center 🔅				

6.2 Gateway Anti-ARP Spoofing Solution

6.2.1 Overview

A user may connect a small wireless router to a network without authorization and its IP address is the same as the IP address of the gateway, or malicious users impersonate the gateway. As a result, users cannot access the Internet.

Gateway anti-ARP spoofing can block ARP packets from non-trusted interfaces and ensure that the real gateway is not forged, and users can access the Internet normally.

Typical Topology of Gateway Anti-ARP Spoofing



6.2.2 Principles

1. ARP

Address Resolution Protocol (ARP) can resolve MAC addresses based on IP addresses. The MAC addresses can be used for data forwarding in a LAN. When a MAC address is needed, host A broadcasts an ARP request to all hosts on the network. The ARP request contains IP information. Host B with the IP address same as that in the request responds to host A with its MAC address. After receiving the MAC address of host B, host A records it in its ARP table. Then, host A will forward data to host B according to the ARP table.

2. Gateway ARP Spoofing

If there are more than one IP address on the network, there is a probability that a wrong MAC address is obtained, resulting in message transmission errors and bringing great security risks.

Gateway ARP spoofing is that the IP address of the gateway is impersonated, causing disconnection of normal network services and malicious interception of user communication.

3. Anti-ARP Spoofing

Switch interfaces block ARP packets that contain the gateway IP address from untrusted interfaces and only the ARP packets from trusted interfaces are forwarded to prevent users from receiving the wrong gateway MAC address.

Enable gateway anti-ARP spoofing on the ports (Gi 0/3 and Gi 0/4 in this example) of the access switch (switch A) that are directly connected to PCs. The gateway address is the intranet gateway address and the intranet server address.

6.2.3 Models of Products Supporting the Feature and Topology

Product Type	Device Name	Version
Switch	NBS series	The version is unlimited. You are advised to upgrade the device to the latest version.

6.2.4 Configuration Steps

Choose Configuration > Network-Wide > ARP Spoofing Guard > Enable.

DemoProject2 V						
窗 Workspace						
発 Smart Config						
Configuration						
Network-Wide	Network	Optimization	Security		ARP Spoofing Guard	
幸 Devices >	VLAN	Wi-Fi Optimization	ACL	ed ARP packets	If a PC or mobile phone on a LAN is spoofed by a malicious host, the malicious host will	
Authentication >	Multi-WAN	Loop Prevention	ARP Spoofing Guard	Ider Host A Other hosts on	disguise itself as the gateway and block Internet access of other hosts on the LAN. By	
Monitoring		DHCP Snooping		ewayby mistake the LAN access the Internet	enabling ARP Spoofing Guard, you can protect the endpoints on the LAN from ARP	
& Network-Wide			With ARP guar	d enabled, spoofing attacks	spoofing attacks.	
Devices			can con	nnect to the Internet.	Enable	
🖞 Clients >						
🗄 Logs >						
😂 Delivery Center 🔅						

Select the gateway IP address and switch, for which anti-ARP spoofing needs to be configured. The system automatically lists the gateway IP addresses of the service networks. By default (recommended), all access switches of the current network are selected.

DemoProject2 V	ARP Spoofing Guard / ARP Guard Confi	g
硷 Workspace	← ARP Guard Config	
🕏 Smart Config	Networks ② 2/4	Select switches and enable them with ARP Spoofing Guard: Recommended Custom
Configuration	☑ 192.168.35.1 (VLAN 35)	Auto identify access switches Manually select access switches
Ø Network-Wide >	192.168.36.1 (VLAN 36)	٥
🗄 Devices >	192.168.23.1 (VLAN 23)	
Monitoring		\$
🖧 Network-Wide 💚		
Devices		
Clients >		
E Logs		
📚 Delivery Center 💚		and a star and a
	Switches Selected:3	Deliver Config

If anti-ARP spoofing does not need to be configured for all access switches, click **Custom**, select the required switches in the topology, and then click **Deliver Config**.

Cookbook

DemoProject2 V	ARP Spoofing Guard / ARP Guard Co	nfig
硷 Workspace	← ARP Guard Config	
务 Smart Config	Networks ⑦ 2/4	Select switches and enable them with ARP Spoofing Guard:
	2 192.168.110.1 (VLAN 1)	Recommended Custom Auto identify access switches Manually select access switches
Configuration	2 192.168.35.1 (VLAN 35)	
Network-Wide >	192.168.36.1 (VLAN 36)	a
≇ Devices >	192.168.23.1 (VLAN 23)	Ť
\oslash Authentication \rightarrow		
Monitoring		
Devices		
🖸 Clients >		BETTE - BETTE
🛱 Logs >		
📚 Delivery Center 🔅		Real Real Contraction
	Switches Selected:2	Deliver Config

After configuration, IP addresses and switches, for which anti-ARP spoofing is configured, are displayed. If you need to modify the configuration, click **Edit**. If you need to disable anti-ARP spoofing, click **Disable**.

DemoProject2	ARP Spoofing Guard ③	
@ Workspace	Edit Disable	
Smart Config	Networks 2/4	Device 2/4
Configuration	Networks Enabled with ARP Spoofing Guard	9
Ø Network-Wide	192.168.35.1 (VLAN 35)	I
輩 Devices	> Networks Disabled with ARP Spoofing	
	Guard 192.168.36.1 (VLAN 36)	E DE BART AN IN LOCATION FRANCISCO FRANCISCO FRANCISCO FRANCISCO FRANCISCO FRANCISCO FRANCISCO FRANCISCO FRANCISCO FRANCISCO LA COLORIZACIÓN FRANCISCO FRANC
Monitoring	192.168.23.1 (VLAN 23)	(P) THE
δ ⁸ Network-Wide		MIX.000 MIX.001 To A A VALUE - MIX
Devices		
Clients		INTERNAL VECTOR AND
E Logs		a a a
Delivery Center		Object Object + International International -

6.2.5 FAQs

1. If a switch is selected for enabling anti-ARP spoofing but the network topology changes, can Ruijie Cloud automatically identify the change and revise the configuration?

No. After the topology changes, you need to go to the anti-ARP spoofing configuration page and deliver the configuration again.

2. All ports except uplink ports on a switch with anti-ARP spoofing enabled will block the forwarding of ARP packets that carry the gateway IP address. When the uplink ports of the switch change, can Ruijie Cloud automatically identify the change and deliver the configuration?

No. After the uplink ports change, you need to go to the anti-ARP spoofing page and deliver the configuration again. If the configuration is not re-delivered, some devices fail to obtain gateway information, resulting in network disconnection.

7 General Configuration

7.1 Intranet Access

7.1.1 Overview

Through intranet access, you can add a remote management tunnel to manage devices on the intranet using the eWeb management system.

7.1.2 Configuration Steps

Ruijie-test_Auto 🗸	Custom	Device			
AI Networking					
Smart Config		+Add Tunnel			
Configuration					
⊗ Network-Wide >					
🗄 Devices >	General	Gateway	Switch	Wireless	
	Intranet Access	Interface	Interface	SSID	
Monitoring	ACL	Routing	VLAN	Radio	
备 Network-Wide >	IP-MAC Binding	NAT	Routing	Radio Planning	
Devices	SNMP	VPN	Loop Prevention	Rate Limit	
	Project Password	Portal Auth	DHCP Snooping	AP Mesh	
. Clients	CLI Config Task	Dynamic DNS	Interface Rate Limit	Load Balancing	
E Logs	Batch CLI Config	Session Limit	Voice VLAN	Wireless Block/Allow	
- Delivery Center		IPTV	Hot Standby	AP VLAN	
w		PPPoE Server	IP Source Guard		
			Interface Protection		

Choose Configuration > Devices > General > Intranet Access.

Click Add Tunnel on the Intranet Access page. You can create a remote tunnel to access the intranet devices.

DemoProject3 V	
Q Workspace	() Through intranet access, you can add a remote management tunnel to manage devices on the intranet using the eWeb management system.
L Workspace	Custom Device
🖏 Smart Config	
Configuration	
Ø Network-Wide >	
국 Devices >	+Add Tunnel
⊘ Authentication ⇒	
Monitoring	
윦 Network-Wide >	
Devices	
1. Clients >	
🛱 Logs >	
🛎 Delivery Center 🔌	

DemoProject1 V	
ඛ Workspace	Through intranet access, you Add Tunnel X Custom Device
🖏 Smart Config	* Ann Name' HTTP
Configuration	
Ø Network-Wide	App Icon: 😑 😑 🔕 🥝
🛱 Devices >	
$igodoldsymbol{igodoldsymbol{\Theta}}$ Authentication \rightarrow	App type: • HTTP _ HTTPs
Monitoring	* Inside Host: 192.168.20.36 80
& Network-Wide ⊃	
Devices	
🚹 Clients >	Cancel OK
Logs >	
Delivery Center >	

DemoProject1				
企 Workspace		 Through intr 	anet access, you can add a remote	e manac Apply successfully.
		Custom	Device	
🗞 Smart Config				
Configuration				НТТР
Ø Network-Wide				Inside Host & port 192.168.20.36:80
국 Devices			+Add Tunnel	, and a defined and
⊘ Authentication	>			
Monitoring				Э To configure
A Network-Wide	>			
P Devices	>			
Clients	>			
🛱 Logs	>			
Delivery Center	>			

DemoProject1 V	
A Wedenage	() Through intranet access, you can add a remote management tunnel to manage devices on the intranet using the eWeb management system.
La Workspace	Custom Device
🐝 Smart Config	
Configuration	пара нттр
Ø Network-Wide	x in 2023-02-03 11:44
🗮 Devices >	+ Add Tun The tunnel has been created successfully. You can click the button to open.
⊘ Authentication >	Close Open
Monitoring	
🖧 Network-Wide >	
Devices	
🖬 Clients >	
Logs >	
😂 Delivery Center >	

123 Outside Host & p 34.143.190.78:64 Inside Host & por 192.168.30.50:80	ort 802 Expired on 20 t	22-12-13 18:00		
€ To configure	<u>∕</u> ∠Edit	🖞 Delete		
← → C ⊗ 34.143.190.	78 :64802			
	R	HI, NE	Rcy	CC
	Pa	ssword	lo	7775
	Forgot	Password?	English	*

7.2 Project Password

Choose Configuration > Devices > General > Project Password.

Enter a new device password and click Save.

D	emoProject3	Device Password	U.		
奋	Workspace	Device Password :	Enter the device pa	nssword. Ø	
₿.	Smart Config	Save			
Co	figuration	_			
0	Network-Wide				
*	Devices	General	Gateway	Switch	Wireless
\heartsuit	Authentication	Intranet Access	Interface	Interface	AP Mesh
Mo	nitoring	Project Password	Routing	Port Settings	SSID
ጽ	Network-Wide	ACL	NAT	VLAN	Radio
	Devices	CLI Config Task	Dynamic DNS	Routing	Roaming
வ	Clients	Batch CLI Config	IPTV Portal Auth	Voice VLAN	Rate Limit
th the	Logs		VPN		无线黑白名单
0.	Delivery Center				AP VLAN
	2 control y control				

Device Password							
Device Password :	Enter the device password.	Ø					
Save							

7.3 ACL

An access control list (ACL) is commonly referred to as packet filter in some documents. An ACL defines a series of permit or deny rules and applies these rules to device interfaces to control packets sent to and from the interfaces, so as to enhance security of the network device.

You can add ACLs based on MAC addresses or IP addresses and bind ACLs to ports.

7.3.1 Creating ACL Rules

Choose Project > Configuration > Devices > General > ACL.

(1) Click Add to set the ACL control type, enter an ACL name, select ports and rules.

Based on MAC address: To control the L2 packets entering/leaving the port, and deny or permit specific L2 packets destined to a network.

Based on IP address: To control the Ipv4 packets entering/leaving a port, and deny or permit specific Ipv4 packets destined to a network.

DemoProject1	Please select the de	evice: NAEK0074H0001(-)								
⑥ Workspace										
Smart Config	Note: If no rule is added, the system will block all traffic.									
Pr omar comy	+ A43 D Batch Delete									
Configuration										
Network-Wide		ACL Name	ACL Type	Rules	Apply to	Action				
# Devices		macc_network_acl	IP-based	Deny Source IP:192.168.110.0/255.255.255.0 Destinat	All LAN ports	Edit Delete				
Authentication		macc_network_acl	IP-based	Deny Source IP:192.168.3.0/255.255.255.0 Destinatio	All LAN ports	Edit Delete				
Monitoring						2 in total < 1 > 10 / page >				
& Network-Wide										
Pevices										
Clients										
E Logs										
2 Delivery Center										

Cookbook

Cancel

OK

Edit /	ACL			×
1	Select ACL type MAC address-based	IP-based		
2	ACL Name			
	test			
3	Apply to			
	All LAN ports		×	
4	Rules			
	Rule type:	● Permit ◯ Deny		
	Protocol Type:	All V		
	Source IP Address:	All v		
	Origin Port:	All 🗸		
	Destination IP Address:	All v		
	Destination port:	All v		
	Time Period:	weekend	×]	

Rules: The rules include two actions of **Permit** or **Deny**, and the matching rules of packets.

Parameter	Description				
	Configuring ACL Rules Action				
ACL	Block: If packets match this rule, the packets are denied.				
	Allow: If packets match this rule, the packets are permitted.				
IP Protocol Number	Match IP protocol number The value ranges from 0 to 255. Check All to match all IP protocols.				
Src IB Addross	Match the source IP address of the packet. Check All to match all source IP				
Sit IF Address	addresses.				
Dest IP Address	Match the destination IP address of the packet. Check All to match all				

Table 9-1 Description of ACL Rule Configuration Parameters

Parameter	Description				
	destination IP addresses				
EtherType Value	Match Ethernet protocol type. The value range is 0x600~0xFFFF. Check All to match all protocol type numbers.				
Src Mac	Match the MAC address of the source host. Check All to match all source MAC addresses				
Dest MAC	Match the MAC address of the destination host. Check All to match all destination MAC addresses				

1 Note

- If no rule is added, the system will block all traffic.
- An ACL applied by a port cannot be edited or deleted. To edit, unbind the ACL from the port first.

7.4 CLI Config Task

7.4.1 Add a CLI Command Set

Limitations

The function is only supported on RGOS devices.

Procedure

- (1) Choose **Project > Configuration > Devices > CLI Config Task**.
- (2) Click Add a CLI Command Set to customize a CLI Task.

Rujjie I Rayac 2 Home Project	🔤 bar, testar@dh V 💮 🔍 🖵 🛞 🛞
20230213_test V	
Workspace	Test the interfere
+Add a C	Add a CU Command Set X
Smart Config	
Al Diagnostics	Enter the name of the CLI command set here if you want to save it as a new command set.
Configuration	Enter CLI commands here separated with fine breaks.
Network-Wide	
Monitoring	
& Network-Wide >	
Devices	The description can help you remember the purpose of this command set. Optional You can copy a command set from other sources.
☐ Clients →	You can copy a command set from other sources:
E Logs	Test
😂 Delivery Center >	Copy it to the command input box
	Swe Clear

(3) Enter the set name and commands and click Save.

Add	×
sho_interface	
sho ip in b	
	_//
sho interface	
Copy CLI Set	
Сору	
Save	∋ar

If the CLI command is the same as another one, you can select the CLI set and click Copy.

7.4.2 Batch CLI Configuration

Limitations

The function is only supported on RGOS devices.

Procedure

- (1) Choose Project > Configuration > Device > Batch CLI Config.
- (2) Click Add Configuration Tasks.

Ruffe IRcycc A	ome Project				1000 lsw_testas@ch V	⊙ ⊂ ↓ ⊡ ⊚ ⊗
20230213_test V						
	Add Configuration Tasks					
AI Networking	Delivery Time	Total Devices	Success	Failure	Configuration Command	Operation
Smart Config	Ha"					
Al Diagnostics						
Configuration						
Network-Wide						
\oplus Devices \rightarrow						
Auth & Accounts >						
Monitoring						
💑 Network-Wide >						
Devices						
Clients >						
E Logs >						
😂 Delivery Center 🚿						

(3) Select one or more devices, and click Apply.

General Configuration

	Home Projec	:t				1000 lsw_testas@ch V	● < C < ⊂ < < < < < < < < < < < < < < < <
DemoProject1 V							
Workspace	GATEWAY	✓ Project Name	Firmware Ve	rsion Model	Search		8
AI Networking		Online Status	Project	Comment	SN	Firmware Version	Device model
 Smart Config 		Online	DemoProject1		NAEK1EFCH0001	ReyeeOS 1.206.2023	EG310GH-E
Al Diagnostics						1	in total < 1 > 10 / page >
Configuration	Back					Batch apply to designated dev	ices Apply Apply All
Network-Wide							
Auth & Accounts >							

(4) Set parameters and click Apply.

The command will be delivered immediately if you do not set the scheduled command delivery time.

Batch Customize CLI Commands	X
Select Date 📋 (Tip:The command will be delivered immediately if you do not set the scheduled command delivery	time.)
Enter the name of the CLI command set here if you want to save it as a new command set.	
Enter CLI commands here separated with line breaks.	li
The description can help you remember the purpose of this command set. Optional You can copy a command set from other sources.	
You can copy a command set from other sources:	
Test Copy it to the command input box	
Save Deliver C	lear

(5) Click **Back** to return to the **Batch CLI Config Status** page.

Ruffe IRcycc 2 Hor	me Project				Isse_testas@ch V	● ♀ ♀ ⋿ ⊜ 용
DemoProject1 V						
	Add Configuration Tasks					88
AI Networking	Delivery Time	Total Devices	Success	Failure	Configuration Command	Operation
Smart Config						
AI Diagnostics	R					
Configuration				No Data		
Network-Wide						

8 Gateway Configuration

8.1 Interface

Choose **Project** > **Configuration** > **Devices** > **Gateway** > **Interface**. The gateway port page is displayed.

Ruijie-test_Auto ∨				
ᢙ Workspace				
AI Networking				
Smart Config				
Configuration				
Ø Network-Wide >				
표 Devices →	General	Gateway	Switch	Wireless
	Intranet Access	Interface	Interface	SSID
Monitoring	ACL	Routing	VLAN	Radio
备 Network-Wide >	IP-MAC Binding	NAT	Routing	Radio Planning
Devices	SNMP	VPN	Loop Prevention	Rate Limit
f.] Clients >	Project Password	Portal Auth	DHCP Snooping	AP Mesh
	CLI Config Task	Dynamic DNS	Interface Rate Limit	Load Balancing
🖬 LOGS 💦 👌	Batch CLI Config	Session Limit	Voice VLAN	Wireless Block/Allow
😂 Delivery Center 💛		IPTV	Hot Standby	AP VLAN
		PPPoE Server	IP Source Guard	
			Interface Protection	

Click a WAN port on the gateway and set the networking mode. Click Save.

DemoProject2 V	Please select the device: N	AEK002FH0001(-)	~									
硷 Workspace	, ion										o 💼 o	
🖏 Smart Config									LAN	WAN Statio	IP Dynamic IP	PPPOE
Configuration		LANO LANI	LAN2	LANS	LANH			LAN7/WAN2	WANT .			
Network-Wide >	WAN2											
≇ Devices >	* Type :	PPoE (ADSL)					~					
		Static IP										
Monitoring	* Account :	DHCP										
& Network-Wide >	* Password :	PPoE (ADSL)										
Devices	* IP :	Auto										
Clients	Interface Alias:											
🛱 Logs >	Uplink Bandwidth :							Mbps				
Delivery Center	Downlink bandwidth:							Mbps				
					1	Save						

Click a LAN port on the gateway, and set **Interface Type**, **Native ID**, and **Allowed VLAN** for the LAN port, and then click **Save**.
DemoProject2 V	Please select the device: NA	AEK002FH0001(-)	~							
硷 Workspace	Port									
🕏 Smart Config							LAN	WAN Static IF	Dynamic IP	PPPOE
Configuration		LAND LAN1	LAN2 LAN3	LAN4	LANS LANG/M	WANS LANZ/WANZ	WANT	WAND		
Network-Wide			•			k 💼	.	.		
幸 Devices >	Ag1									
\oslash Authentication \rightarrow	* Interface Type :	Trunk ^								
Monitoring	* Native ID:	Trunk								
🗞 Network-Wide >	* Allowed VLAN :	Access 23,35-36,233								
Devices										Save
🖬 Clients >										
E Logs >										
📚 Delivery Center 💚										

8.2 Routing

8.2.1 Adding a Static Route

1. Introduction

Static routes are manually configured. When a data packet matches a static route, the packet will be forwarded based on the specified forwarding mode.

A Caution

Static routes cannot automatically adapt to changes of the network topology. When the network topology changes, you need to reconfigure the static routes.

2. Configuration Steps

(1) Choose **Project > Configuration > Device > Getaway > Routing** to go to the route configuration page.

Ruijie-test_Auto					
企 Workspace					
AI Networking					
Smart Config					
Configuration					
Network-Wide	>				
≇ Devices	>	General	Gateway	Switch	Wireless
	>	Intranet Access	Interface	Interface	SSID
Monitoring		ACL	Routing	VLAN	Radio
& Network-Wide	>	IP-MAC Binding	NAT	Routing	Radio Planning
Devices	>	SNMP	VPN	Loop Prevention	Rate Limit
1. Clients	>	Project Password	Portal Auth	DHCP Snooping	AP Mesh
E Logs	>	Batch CLI Config	Session Limit	Voice VLAN	Wireless Block/Allow
⁰ » Delivery Centor		2	IPTV	Hot Standby	AP VLAN
log Denvery Center	,		PPPoE Server	IP Source Guard	
				Interface Protection	

(2) Click
 Static Routing to add a static route. Click Save.

DemoProject2 V	Please select the device: NAEK003AH00	001(-) 🗸			
窗 Workspace	Routing				
🕏 Smart Config	Static Routing				
Configuration	Destination Address*	Subnet Mask*	Next-hop (except dialing)*	Egress Interface	
Ø Network-Wide >	192.168.0.0	255.255.0.0	172.20.72.1	WAN	v] 1
\mp Devices \rightarrow					
\bigotimes Authentication $>$	172.16.0.0	255.255.0.0	172.20.72.1	WAN	~
Monitoring			Save		
🗞 Network-Wide 💚	Policy-based Routing				
Devices					
Clients >					
E Logs					
😂 Delivery Center 🔌			No Data		

The following table lists the description of parameters.

Parameter	Description
Destination Address	Specify the destination network to which data packets are to be sent. The device matches the data packet based on the destination address and subnet mask.
Subnet Mask	Specify the subnet mask of the destination network. The device matches the data packet based on the destination address and subnet mask.
Next-hop Address	Specify the IP address of the next hop in the route for data packets. If the outbound interface accesses the Internet through PPPoE dialing, you do not need to configure the next-hop address.
Egress	Specify the interface that forwards data packets.

8.2.2 Adding PBR

1. Introduction

Policy-based routing (PBR) is a mechanism for routing and forwarding based on user-specified policies. When a router forwards data packets, it filters the packets based on configured rules, and then forwards the matched packets according to the specified forwarding policy. PBR enables the device to define rules according to specific fields (source or destination IP address and protocol type) in the data packets, and forward the data packets from a specific interface.

In a multi-line scenario, if the device is connected to the Internet and the internal network through different lines, traffic will be evenly routed over the lines if no routing settings are available. In this case, access data to the internal network may be sent to the external network, or access data to the external network may be sent to the internal network, resulting in network exceptions. To prevent these exceptions, you need to configure PBR to control data isolation and forwarding on the internal and external networks.

The device can forward data packets using either of the following three policies: PBR, address-based routing, and static routing. When all the policies exist, PBR, static routing, and address-based routing are in descending order of priority.

2. Configuration Steps

(1) Choose **Project** > **Configuration** > **Device** > **Getaway** > **Routing** to go to the route configuration page.

Ruijie-test_Auto 🗸				
硷 Workspace				
AI Networking				
Smart Config				
Configuration				
Ø Network-Wide >				
≇ Devices >	General	Gateway	Switch	Wireless
	Intranet Access	Interface	Interface	SSID
Monitoring	ACL	Routing	VLAN	Radio
용 Network-Wide >	IP-MAC Binding	NAT	Routing	Radio Planning
Devices	SNMP	VPN	Loop Prevention	Rate Limit
f] Clients	Project Password	Portal Auth	DHCP Snooping	AP Mesh
	CLI Config Task	Dynamic DNS	Interface Rate Limit	Load Balancing
🗄 Logs >	Batch CLI Config	Session Limit	Voice VLAN	Wireless Block/Allow
A Delivery Center		IPTV	Hot Standby	AP VLAN
a contrary server		PPPoE Server	IP Source Guard	
			Interface Protection	

(2) Click \oplus Add PBR rules to add a PBR rule. Set parameters and then click Save.

DemoProject2 V	Please select the device: NAEK003AH0001(-) ~			
窗 Workspace	Routing				
🕏 Smart Config	Static Routing				
Configuration	Destination Address*	Subnet Mask*	Next-hop (except dialing)*	Egress Interface	
⊗ Network-Wide >	192.168.0.0	255.255.0.0	172.20.72.1	WAN	
$ \boxplus $ Devices \rightarrow					
	172.16.0.0	255.255.0.0	172.20.72.1	WAN	Ū
Monitoring			Save		
് Network-Wide >	Policy-based Routing				
Devices	Add PBR rules				
Clients	Rule Name Statu	IP Custom	Destination IP addr	wani v n	
🗄 Logs >	TETTOR		custom		
😂 Delivery Center 🔅		Custom *	Custom *		
		(Save		

The following table lists the description of parameters.

Parameter	Description
Rule Name	Specify the name of a PBR rule, which uniquely identifies a PBR rule. The name must be unique for each rule.
Status	Indicate whether to enable the PBR rule. If the value is disabled, this rule does not take effect.

Parameter	Description
Protocol Type	Specify the protocol for which the PBR rule is effective. You can set this parameter to IP , ICMP , UDP , TCP , or Custom .
Source IP address/range	Configure the source IP address or IP address range for matching PBR entries. The default value is All IP Addresses . All IP Addresses : Match all the source IP addresses. Custom : Match the source IP addresses in the specified IP address range.
Custom Source IP address/range	When Source IP address/range is set to Custom , you need to enter a single source IP address or a source IP address range.
Destination IP address/range	Configure the destination IP address or IP address range for matching PBR entries. The default value is AII IP Addresses . AII IP Addresses : Match all the destination IP addresses. Custom : Match the destination IP addresses in the specified IP address range.
Custom Destination address/range	When Destination IP address/range is set to Custom , you need to enter a destination IP address or a destination IP address range.
Port	Specify the interface that forwards data packets based on the hit PBR rule.

8.3 NAT

8.3.1 Applicable Scenarios

The port mapping function can establish the mapping relationship between the IP address and port number of a WAN port and the IP address and port number of a server on a LAN, so that all access traffic destined for a service port of the WAN port will be redirected to the corresponding port of the specified LAN server. This function enables external users to 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 network when they are in the enterprise or on a business trip.

8.3.2 Configuration Steps

(1) Choose Project > Configuration > Device > Gateway > NAT to go to the Port Mapping page.

Ruijie-test_Auto 🗸	Ruijie-tes	t_Auto - Customize	Up time: 77 day(s) 4 hour(s),	Time Zone: Asia/Shanghai
Workspace	-	-		
AI Networking	Topology			
Smart Config	@ Device			
Configuration	1			
Network-Wide	. Online Client			
∄ Devices →	General	Gateway	Switch	Wireless
	Intranet Access	Interface	Interface	SSID
Monitoring	ACL	Routing	VLAN	Radio
윪 Network-Wide >	IP-MAC Binding	NAT	Routing	Radio Planning
Devices	SNMP	VPN	Loop Prevention	Rate Limit
_	Project Password	Portal Auth	DHCP Snooping	AP Mesh
Clients >	CLI Config Task	Dynamic DNS	Interface Rate Limit	Load Balancing
Logs >	Batch CLI Config	Session Limit	Voice VLAN	Wireless Block/Allow
^o z Delivery Center		IPTV	Hot Standby	AP VLAN
Source Center		PPPoE Server	IP Source Guard	
			Interface Protection	

(2) Click \oplus Add Port Mapping, set parameters, and then click Save.

EGW_20230111 V	Please select the device: MACC336	570021(-) V			
	Port Mapping				
🕏 Smart Config	Note: By mapping intranet host to a	a network server, network users on the extranet can access th	e server, and obtain corresponding services.		
Configuration	Add Port Mapping				
Network-Wide >	Name	Intranet host service type Protocol	IP address/port of intranet host	IP address/port accessible by en	xtranet users after mapping
	Name	V TCP V		Examp Port V All WAN ports	V Examp
\bigtriangledown Authentication \rightarrow					
Monitoring			Save		
🖧 Network-Wide >					
Devices					
Ē Clients →					
🗟 Logs >					
😂 Delivery Center 🔿					

The following table lists the description of parameters.

Parameter	Description
Name	Enter the description of a port mapping rule, which is used to identify the rule.
Intranet host service type	Select the transport layer protocol type used by the service, such as TCP or UDP. The value ALL indicates that the rule applies to all protocols. The value must comply with the terminal configuration of a service.
Protocol	Select the transport layer protocol type used by the service, such as TCP or UDP. The value ALL indicates that the rule applies to all protocols. The value must comply with the terminal configuration of a service.

Parameter	Description
Internal Server IP	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	Specify the service port number of the internal server to be mapped to a 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 .
External Server IP	Specify the host address used for Internet access. The default value is the IP address of a WAN port.
External Port	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. IP address/port accessible by extranet users after mapping

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

1 Note

Solution to test failures:

- Modify the value of **External Server IP** and use the new external port number to perform the test again. The possible cause is that the port is blocked by the firewall.
- Enable the remote access permission on the server. The possible cause is that remote access is displayed on the server, resulting in normal internal access but abnormal access across network segments.

8.4 Configuring VPN

1. Overview

Virtual private network (VPN) is used to build a virtual private network on the public network, and transmit private network traffic on this virtual network.

There are two VPN application scenarios:

• Site-to-Site VPN

A connection is established between two LANs through a VPN tunnel. Figure 8-1 shows the typical network topology. An enterprise's HQ and branch are connected to the Internet through gateway 1 and gateway 2 respectively. The HQ and branch often send internal confidential data to each other because of business needs. To secure data transmission on the Internet, a VPN tunnel is established between gateway 1 and gateway 2.



Figure 8-1 Typical Network Topology of Site-to-Site VPN

In this scenario, the networks of the HQ and branch are connected to the Internet through fixed gateways, and the networking is relatively fixed. The access is bidirectional, that is, both the branch and HQ may initiate access to the peer end. It is often used for business communication of chain supermarkets, government departments, and banks.

Site-to-site VPN can be implemented in the following ways: PPTP, L2TP, IPSec, and L2TP over IPsec. Ruijie Cloud supports only the IPsec VPN mode.

Client-to-Site VPN

A connection is established between clients and the enterprise intranet through VPN tunnels. Figure 8-2 shows the typical network topology. Employees on business trips (clients) access the Intranet of the HQ through Internet to transmit data to the HQ and access internal servers. To secure data transmission, a VPN tunnel can be established between a client and the enterprise gateway.

In this scenario, the client address is not fixed and the access is one-way, that is, only the client initiates access to Intranet servers. It is suitable for employees on business trips or employees in temporary offices to remotely access the HQ intranet through mobile phones or PCs.





Client-to-site VPN can be implemented in the following ways: PPTP, L2TP, L2TP over VPN, and open VPN.

2. Configuring Site-to-Site VPN (Based on IPsec VPN)

- (1) Configure VPN for the HQ gateway.
 - a Log in to Ruijie Cloud and click the project, to which the HQ access gateway belongs, to go to the configuration page.
 - b Choose Configuration > Devices > Gateway > VPN.

EGW_20230111 V	VPN	'PN Account VF	PN Online User						VPN Guide
Workspace Smart Config	Add VPN Policy	1							
Configuration	Connection Status		Na	ne	Purpose	Config Status	VPN Mode	Action	0
E Devices					The to-Site	 Disabled 	Auto IPsec	2 6 🖻	
Authentication >	General	Gateway	Switch	Wireless	ient-to-Site	- Disabled	PPTP		
Monitoring	Intranet Access Project Password	Interface	Interface Port Settings	AP Mesh SSID	ient-to-Site	Enable	OpenVPN	上區前	
& Network-Wide	ACL	NAT	VLAN	Radio	ent-to-Site	- Disabled	L2TP Sec	260	
Devices	SNMP配置	Dynamic DNS	Routing	着封锁规划					
Clients >	CLI Config Task Batch CLI Config	IPTV Portal Auth	Hot Standby Security	Roaming Rate Limit					
E Logs		VPN	Voice VLAN	Load Balancing					
🈂 Delivery Center		—		无线黑白名单					
				AP VLAN					
VPN VPN Acc	count VPN On	line User							VPN Guide
Add VPN Policy									
									0
Connection Status		Name		Purpose		Config Status	VPN Mode	Action	
 Disconnected 		9999		Site-to-Site		 Disabled 	Auto IPsec	261	
		pptp22		Client-to-Site		 Disabled 	рртр	251	
		12321		Client-to-Site		Enable	OpenVPN	261	

c Click Add VPN Policy.

Add VPN Policy		>
Status	Disabled	
Remark	eg: reyee-test-vpn	
Purpose	VPN Site-to-Site	VPN Client-to-Site
Role	 Headquarters A dynamic or static public IP address is required. 	O Branch Subnet
VPN Mode 🕐	● Auto IPsec ○ Manual IPsec	:
WAN Interface	• WAN (192.168.200.78)	
Headquarters	EGW_20230111	
Headquarters Subnet (0	\vee
Branch Project	Select Project	

Cancel Add

d Set configuration items related to the HQ VPN.

Table 8-1 Configuration Items Related to the HQ VPN

Parameter	Description
Status	Specify whether to enable the VPN policy. Ensure that the VPN policies of both the HQ and branch are enabled so that the VPN between the HQ and branch can be established successfully.
Remark	Provide the description of the VPN policy.

Parameter	Description
Purpose	Specify the VPN usage scenario. Select Site-to-Site.
Role	Specify the role of the current gateway. Select Headquarter if the HQ gateway needs to be connected.
VPN Mode	Specify the IPSec VPN implementation mode. It can be set to the following: Auto IPsec : When the HQ gateway and branch gateway are managed by the same Cloud account, click Auto IPsec . When this mode is selected, a VPN tunnel can be automatically established by selecting the HQ gateway and the branch gateway. Manual IPsec : When this mode is selected, VPN needs to be manually configured on the HQ gateway or branch gateway so that a connection is established between the branch gateway and HQ gateway.
WAN Interface	
Headquarters	Specify the name of the HQ gateway.
Headquarters Subnet	
Branch Project	Project, to which the branch gateway belongs. Set this parameter when VPN Mode is set to Manual IPsec .

e Click Add.

(2) (Optional) Configure VPN for the branch gateway.

When VPN is configured for the HQ gateway, if **VPN Mode** is set to **Manual IPSec**, perform the following operations. If **VPN Mode** is not set to **Auto IPsec**, the following operations are not required.

- a Log in to Ruijie Cloud and click the project, to which the branch gateway belongs, to go to the configuration page.
- b Choose Project > Configuration > Devices > Gateway > VPN.

	EGW_20230111									
6	Workspace	VPN V	PN Account VF	PN Online User						VPN Guide
9	Smart Config	Add VPN Policy								0
Co	onfiguration	Connection Status		Nam		Purpose	Config Status	VPN Mode	Action	0
6	Network-Wide					Te-to-Site	 Disabled 	Auto IPsec	∠ 6 前	
9	Authentication	General	Gateway	Switch	Wireless	ent-to-Site	Disabled	рртр	268	
м	onitoring	Intranet Access Project Password	Interface Routing	Interface Port Settings	AP Mesh SSID	ent-to-Site	Enable	OpenVPN	∠ 6 ⊞	
å	Network-Wide	ACL	NAT	VLAN	Radio	ient-to-Site	 Disabled 	L2TP Sec	268	
<u>8</u>	Devices	SNMP配置 CLI Config Task	Dynamic DNS	Routing Hot Standby	射版规划 Reaming					
Ű.] Clients	Batch CLI Config	Portal Auth	Security	Rate Limit					
R	3 Logs		VPN	Voice VLAN	Load Balancing					
68	Delivery Center				AP VLAN					

c Click Add VPN Policy.

Add VPN Policy		X
Status	Disabled	
Remark	eg: reyee-test-vpn	
Purpose	VPN Site-to-Site	VPN Client-to-Site
Role	 Headquarters A dynamic or static public IP addresis required. 	Branch Subnet ss
VPN Mode	● Auto IPsec ○ Manual IF	Psec
WAN Interface	• WAN (192.168.200.78)	
Branch Subnet		V
Headquarters Project		V

Cancel Add

d Set configuration items related to the branch VPN.

Table 8-2 Configuration Items Related to the Branch VPN

Parameter	Description
Status	Specify whether to enable the VPN policy. Ensure that the VPN policies of both the HQ and branch are enabled so that the VPN between the HQ and branch can be established successfully.
Remark	Provide the description of the VPN policy.
Purpose	Specify the VPN usage scenario. Select Site-to-Site.

Parameter	Description
Role	Specify the role of the current gateway. Select Branch Subnet if the branch gateway needs to be connected.
VPN Mode	Auto or Manual
WAN Interface	Select the WAN Interface
Headquarters Subnet	Specify the subnet mask of the HQ gateway. Set this parameter when VPN Mode is set to Manual IPsec .
Headquarters IP/Domain	Specify the IP address or domain name of the HQ gateway. Set this parameter when VPN Mode is set to Manual IPsec .
Headquarters	Specify the name of the HQ gateway.
Branch Subnet	Specify the subnet mask of the branch gateway.
Pre-Shared Key	The pre-shared key required for IPsec encryption. Set this parameter when VPN Mode is set to Manual IPsec .

e (Optional) When **VPN Mode** is set to **Manual IPsec**, click **Advanced Settings** to set items related to Phase1 and Phase2.



Phase2 Setting		
Transform Set 1	AUTO	~
Transform Set 2	AUTO	\vee
PFS	● None ◯ d1 ◯ d2 ◯ d5	
SA Lifetime	3600 Seconds	

f Click Add.

3. Configuring Client-to-Site VPN (Based on PPTP VPN)

Client-to-site VPN needs to be configured on both the HQ gateway and a client so that a VPN connection can be established between the HQ and the client.

- (1) Configure VPN for the HQ gateway.
 - a Log in to Ruijie Cloud and click the project, to which the HQ access gateway belongs, to go to the configuration page.

b	Choose Configuration > Devices > Gateway > VPN	> VPN.
---	--	--------

EGW_20230111 V									
@ Workspace	VPN	/PN Account V	PN Online User						VPN Guide
🛱 Smart Config	Add VPN Policy								0
Configuration									0
	Connection Status		N	ime	Purpose	Config Status	VPN Mode	Action	
I Devices	General	Gateway	Switch	Wireless	Tte-to-Site	 Disabled 	Auto IPsec	260	
$\label{eq:authentication} \qquad \qquad$	Intranet Access	Interface	Interface	AP Mesh	ient-to-Site	 Disabled 	PPTP	260	
Monitoring	Project Password	Routing	Port Settings	SSID	ient-to-Site	Enable	OpenVPN	260	
🖧 Network-Wide >	ACL	NAT	VLAN	Radio	ent-to-Site	 Disabled 	L2TP Sec	2 6 0	
Devices	SNMP配置	Dynamic DNS	Routing	射级规划					
Clients >	CLI Config Task	IPTV Portal Auth	Hot Standby	Roaming Rate Limit					
E Logs >	batch coning	VPN	Voice VLAN	Load Balancing					
Se Delivery Center		_		无线黑白名单					
				AP VLAN					
VPN VPN Ac	count VPN On	line User							Ø VPN Guide
Add VPN Policy									
									0
									Č
Connection Status		Name		Purpose		Config Status	VPN Mode	Action	
 Disconnected 		qqqq		Site-to-Site		 Disabled 	Auto IPsec	2 6 1	
		pptp2	2	Client-to-Site		 Disabled 	PPTP	2 6 1	
		12321		Client-to-Site		Enable	OpenVPN	2 6 1	
		-		Client-to-Site		 Disabled 	L2TP Sec	2 🛯 🖻	

c Click Add VPN Policy.

Add VPN Policy		Х
Status	Disabled	
Remark	eg: reyee-test-vpn	
Purpose	VPN Site-to-Site	
VPN Mode 🕐	◯ L2TP over IPsec ◯ L2TP ◯ OpenVPN 🧿 PPTP	
Server IP/Domain	◯ IP ② ● Reyee DDNS ③	
	45.127.187.248 ruijieddns.vip ∨	
Local Tunnel IP		
IP Pool 🕐	Start IP 10.70.17.2 End IP 10.70.17.254	
MPPE	Disabled	
PPP Hello Interval	10	
O Advanced Settin	gs	
	Cancel	ł

d Configure the VPN policy for the HQ gateway.

Table 8-3 VPN Configuration Items for the HQ Gateway

Parameter	Description
Status	Specify whether to enable the VPN policy.
Remark	Provide the description of the VPN policy.
Purpose	Specify the VPN usage scenario. Select Client-to-Site.
VPN Mode	Select the mode for implementing client-to-site VPN. Select PPTP .

Parameter	Description
Server IP/Domain	Specify the IP address or domain name of the PPTP server.
Local Tunnel IP	Specify the local virtual IP address of the server of the VPN tunnel. After the client dials into the VPN, the client can access the server through this IP address.
IP Pool	Specify the address pool used by the PPTP server to allocate IP addresses to clients. Enter the start IP address and end IP address.
MPPE	Specify whether to use MPPE to encrypt the PPTP tunnel. After MPPE is enabled on the server: If Data encryption is set to Optional encryption on the client, the server and client can be connected but the server does not encrypt packets. If Data encryption is set to Require encryption on the client, the server and client can be connected and the server encrypts packets. If Data encryption is set to No encryption allowed on the client, the server and client cannot be connected. If MPPE is disabled on the server but the client requires encryption, the server and client connection fails. By default, MPPE is disabled on the server. After you enable MPPE, the bandwidth performance of the device degrades. You are advised to keep MPPE disabled if there are no special security requirements.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after PPTP VPN is deployed.
DNS	Specify the DNS server address pushed by the PPTP server to clients.

- e Click Add.
- (2) Configure the client.

The following uses a Windows 10 client as an example for description. For the configuration of other clients, click **VPN Guide** at the upper right corner of the configuration page.

a Log in to the Windows client and choose Control Panel > Network and Internet > Network and Sharing Center.





b Configure a VPN connection.

		-	
←	💇 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
		INEXT	Cancer
		_	• ×
÷	Connect to a Workplace	_	• ×
÷	Connect to a Workplace Do you want to use a connection that you already have?	-	□ ×
¢	Connect to a Workplace Do you want to use a connection that you already have? No, create a new connection	-	
÷	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	-	- ×
÷	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 Kuijie MY WAN Miniport (PPTP)	-	
¢	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 Yes, I'll choose an existing connection Ruijie MY WAN Miniport (PPTP) Ruijie Demo WAN Miniport (PPTP)	-	
¢	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 Yes, I'll choose an existing connection	-	
¢	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 Yes, I'll choose an existing connection	-	

 ← 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 Internet. 		1
How do you want to connect? → Use my Internet connection (VPN) Connect using a virtual private network (VPN) connection through the Internet.		1
→ Use my Internet connection (VPN) Connect using a virtual private network (VPN) connection through the Internet.		
i 🧶 — 🧶 — 💵		
→ Dial directly Connect directly to a phone number without going through the Internet.		-
ing ing ing		
	Canc	el
		~
← 🔄 Connect to a Workplace		^
Type the Internet address 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 credentials		
Allow other people to use this connection This option allows anyone with access to this computer to use this connection.		
Create	Cance	1

c Change settings of the adapter.



	Networking	Sharing	
Type of VPN:			
Point to Point Tunneling Pro	otocol (PPTP)		~
- 1000 - 1000		Advanced s	ettings
Data encryption:			
Optional encryption (connection)	ct even if no e	ncryption)	~
Authentication			
O Use Extensible Authent	ication Protoco	ol (EAP)	
			~
		Propert	ies
0			
Allow these protocols			
	and (DAD)		
		D. L. LICILIA	-
	ke Authenticat	ION Protocol (CHA	(P)
		AP v2)	
Microsoft CHAP Ver	sion 2 (MS-CH		
Challenge Handshar Microsoft CHAP Ven Automatically us password (and d	sion 2 (MS-CH e my Windows Iomain, if any)	logon name and	

d Check the VPN connection status.

Contraction of the second seco		
		Retrock Corrected
		age VHxConnection
		Network & Intervet setting Change undrugt with an analysis connection entered
# / B 😌 🗃 🇰 🏛		과 사망해 800m 미 800m 미
Windows Security	×	
Sign in		
User name		
Password		
ОК	Cancel	
		1



If your PC cannot access the internal devices of the HQ after the VPN connection is set up, run the **route** add command and add the static route on your PC. The following figure shows a command example.
 The IP address in this command is the virtual IP address obtained by the PC from the HQ. Then, the PC can access the internal devices of the HQ.

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

4. Configuring Client-to-Site VPN (Based on L2TP VPN)

Client-to-site VPN needs to be configured on both the HQ gateway and a client so that a VPN connection can be established between the HQ and the client.

- (1) Configure VPN for the HQ gateway.
 - a Log in to Ruijie Cloud and click the project, to which the HQ access gateway belongs, to go to the configuration page.
 - b Choose Project > Configuration > Devices > Gateway > VPN.

Ruijie-test_Auto		Select the device	e:	~			
AI Networking							
Smart Config							
Configuration							
Network-Wide	>						
፰ Devices	>	General	Gateway	Switch	Wireless		
	s >	Intranet Access	Interface	Interface	SSID		
Monitoring		ACL	Routing	VLAN	Radio		
윦 Network-Wide	>	IP-MAC Binding	NAT	Routing	Radio Planning		
Devices	>	SNMP	VPN	Loop Prevention	Rate Limit		
		Project Password	Portal Auth	DHCP Snooping	AP Mesh		
L Clients	>	CLI Config Task	Dynamic DNS	Interface Rate Limit	Load Balancing		
🕼 Logs	>	Batch CLI Config	Session Limit	Voice VLAN	Wireless Block/Allow		
and the second s	>		IPTV	Hot Standby	AP VLAN		
~,			PPPoE Server	IP Source Guard			
				Interface Protection			
VPN VPN Account	VPN Online	User					VPN Guide
Add VPN Policy							
							0
Connection Status		Name	Purpose	Config Status	VPN Mode	Action	
 Disconnected 		9999	Site-to-Site	- Disabled	Auto IPsec	261	
		pptp22	Client-to-Site	Disabled	PPTP		
		12321	Client-to-Site	Enable	OpenVPN	260	
			Client-to-Site	 Disabled 	L2TP Sec	2 6 8	

c Click Add VPN Policy.

Add VPN Policy				×
Status	Disabled			
Remark	eg: reyee-test-vpn			
Purpose	VPN Site-to-Site	CI	VPN VPN ient-to-Site	
VPN Mode	○ L2TP over IPsec	P () (DpenVPN O PPTP	
Server IP/Domain	🔿 IP 🕐 💿 Reyee DDNS 🤅)		
	45.127.187.248		ruijieddns.vip 🗸	
Local Tunnel IP				
IP Pool 🕐	Start IP 10.70.17.2	End IP	10.70.17.254	
Advanced Settings	5			
DNS	8.8.8.8			
Tunnel Authentication	Disabled			
PPP Hello Interval	10			

Cancel Add

d Configure the VPN policy for the HQ gateway.

Parameter	Description
Status	Specify whether to enable the VPN policy.
Remark	Provide the description of the VPN policy.
Purpose	Specify the VPN usage scenario. Select Client-to-Site.
VPN Mode	Select the mode for implementing client-to-site VPN. Select L2TP.
Server IP/Domain	Specify the IP address or domain name of the L2TP server.

Parameter	Description
Local Tunnel IP	Specify the local virtual IP address of the server of the VPN tunnel. After the client dials into the VPN, the client can access the server through this IP address.
IP Pool	Specify the address pool used by the L2TP server to allocate IP addresses to clients.
DNS	Specify the DNS server address pushed by the L2TP server to clients.
Tunnel Authentication	Specify whether to enable L2TP tunnel authentication. If you enable this function, you need to configure a tunnel authentication key. By default, tunnel authentication is disabled. The tunnel authentication request can be initiated by clients. If tunnel authentication is enabled on one end, a tunnel to the peer can be established only when tunnel authentication is also enabled on the peer and consistent keys are configured on the two ends. Otherwise, the local end will automatically shut down the tunnel connection. If tunnel authentication is disabled on both ends, no authentication key is required for tunnel establishment. When a PC functions as the client to access the L2TP server, you are advised not to enable tunnel authentication on the L2TP server.
PPP Hello Interval	Specify the interval for sending PPP Hello packets after PPTP VPN is deployed.
DNS	Specify the DNS server address pushed by the PPTP server to clients.

(2) Set a VPN account.

Only user accounts added to the VPN client list are allowed to dial up to connect to the L2TP server. Therefore, you need to manually configure user accounts for clients to access the L2TP server.

- a Choose Project > Configuration > Devices > Gateway > VPN > VPN Account.
- b Click Add VPN Account.

Add VPN Account

 		-
- 1	,	
	c	
 e		۰.
		•

Username	eg: Henry
Password	At least 8 characters
	Cancel Add

c Configure items related to a VPN account.

Table 8-4 VPN Account Configuration Items

Parameter	Description
Username	Specify the VPN username.
Password	Specify the password for the client to log in to the VPN.

d Click Add.

(3) Configure the client.

The following uses a Windows 10 client as an example for description. For the configuration of other clients, click **VPN Guide** at the upper right corner of the configuration page.

a Choose Control Pane > Network and Internet > Network and Sharing Center.



b Configure a VPN connection.



	-		×
←	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) WAN Miniport (PPTP) WAN Miniport (PPTP) WAN Miniport (PPTP)		
	Next	Canc	el
÷	Connect to a Workplace		×
	How do you want to connect?		
	How do you want to connect? \rightarrow Use my Internet connection (VPN) Connect using a virtual private network (VPN) connection through the Internet. \swarrow		
	How do you want to connect? → Use my Internet connection (VPN) Connect using a virtual private network (VPN) connection through the Internet. → Dial directly Connect directly to a phone number without going through the Internet.		
	How do you want to connect? -> Use my Internet connection (VPN) connect using a virtual private network (VPN) connection through the Internet. i i i i i i i i i i		

			-		\times
←	🌆 Connect to a Workplac	e			
	Type the Internet ad	dress to connect to			
	Your network administrate	or can give you this address.			
	Internet address:	172.26.6.190 The WAN IP of HQ			
1	Destination name:	VPN Connection			
	Use a smart card				
	🗹 Remember my cre	dentials			
	🌍 🗌 Allow other people	to use this connection			
	This option allows	anyone with access to this computer to use this connect	ion.		
			reate	Can	cel

c Change adapter's settings.

Network and Sharing Center			- 🗆 X
← → · ↑ 💆 > Control P	anel > All Control Panel Items > Network and Sha	aring Center	✓ ひ Search Control Panel ク
Control Panel Home	View your basic network information	n and set up connections	
Change adapter settings	View your active networks		
Change advanced sharing settings	Big4 Public network	Access type: Internet Connections: J Wi-Fi (Big4)	
Media streaming options			
	Local Area Connection Public network	Access type: No Internet access Connections: U Local Area Connection	
	Change your networking settings		
	Set up a new connection or network Set up a broadband, dial-up, or VPN of	connection; or set up a router or access point.	
	Troubleshoot problems Diagnose and repair network problem	ns, or get troubleshooting information.	
See also			
Internet Options Windows Defender Firewall			



d Check the VPN connection status.



If your PC cannot access internal devices of the HQ after the VPN connection is set up, run the route add command and add the static route on your PC. The following figure shows a command example. The IP address in this command is the virtual IP address obtained by the PC from the HQ. Then, the PC can access the internal devices of the HQ.

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

5. Configuring Client-to-Site VPN (Based on L2TP over IPSec VPN)

Client-to-site VPN needs to be configured on both the HQ gateway and a client so that a VPN connection can be established between the HQ and the client.

- (1) Configure VPN for the HQ gateway.
 - a Log in to Ruijie Cloud and click the project, to which the HQ access gateway belongs, to go to the configuration page.
 - b Choose Project > Configuration > Devices > Gateway > VPN > VPN.

VPN VPN Account VPN Online User						VPN Guide
Add VPN Policy						
						0
Connection Status	Name	Purpose	Config Status	VPN Mode	Action	
Disconnected	qqqq	Site-to-Site	 Disabled 	Auto IPsec		
	pptp22	Client-to-Site	 Disabled 	РРТР	261	
	12321	Client-to-Site	• Enable	OpenVPN	261	
		Client-to-Site	 Disabled 	L2TP Sec	2 6 1	

c Click Add VPN Policy.

Add VPN Policy	×
Status	Disabled
Remark	eg: reyee-test-vpn
Purpose	Site-to-Site
VPN Mode 🕐	L2TP over IPsec L2TP OpenVPN PPTP
Server IP/Domain	◯ IP ② ● Reyee DDNS ③
	45.127.187.248 ruijieddns.vip ∨
Pre-Shared Key	
Local Tunnel IP	
IP Pool 🕐	Start IP 10.70.17.2 End IP 10.70.17.254
O Advanced Settin	gs
	Cancel

d Configure the VPN policy for the HQ gateway.

Parameter	Description
Status	Specify whether to enable the VPN policy.
Remark	Provide the description of the VPN policy.
Purpose	Specify the VPN usage scenario. Select Client-to-Site.
VPN Mode	Select the mode for implementing client-to-site VPN. Select L2TP over IPsec.
Server IP/Domain	Specify the IP address or domain name of the L2TP server.
Pre-Shared Key	Specify the same unique pre-shared key as the credential for mutual authentication between the server and client.

Parameter	Description
Local Tunnel IP	
IP Pool	Specify the address pool used by the server to allocate IP addresses to clients.
DNS	
Tunnel Authentication	
PPP Hello Interval	Specify the interval for sending PPP Hello packets after L2TP over IPsec VPN is deployed.

(2) Set a VPN account.

Only user accounts added to the VPN client list are allowed to dial up to connect to the L2TP server. Therefore, you need to manually configure user accounts for clients to access the L2TP server.

- a Choose Configuration > Devices > Gateway > VPN > VPN Account.
- b Click Add VPN Account.

Add VPN Account		Х
Username	eg: Henry	
Password	At least 8 characters	
	Cancel	dd

c Configure items related to a VPN account.

Table 8-5 VPN Account Configuration Items

Parameter	Description
Username	Specify the VPN username.
Password	Specify the password for the client to log in to the VPN.

- d Click Add.
- (3) Configure the client.
 - a Choose Control Panel > Network and Internet > Network and Sharing Center.




b Configure a VPN connection.

content of the second second							
→ → ↑ E > Control	Panel > All Control Panel Items > Network and	I Sharing Center	~	Ğ	Search Cor	ntrol Pane	2I
ntrol Panel Home	View your basic network informa	tion and set up connections					
inge adapter settings	View your active networks						
nge advanced sharing	Big4	Access type: Internet					
dia streaming options	Public network	Connections: 📲 Wi-Fi (Big4)					
	Local Area Connection	Access type: No Internet access					
	Public network	Connections: 🏺 Local Area Connection					
	Set up a broadband, dial-up, or Vi	ork PN connection; or set up a router or access point.					
	Set up a broadband, dial-up, or VI	on PN connection; or set up a router or access point.					
	Set up a hew connection of network Set up a broadband, dial-up, or VI	on PN connection; or set up a router or access point. blems, or get troubleshooting information.					
	Set up a here connection of network Set up a broadband, dial-up, or VI	on PN connection; or set up a router or access point. blems, or get troubleshooting information.					
	Set up a horadband, dial-up, or VI	or. PN connection; or set up a router or access point. blems, or get troubleshooting information.					
	Set up a broadband, dial-up, or VI	on PN connection; or set up a router or access point. blems, or get troubleshooting information.					
	Set up a broadband, dial-up, or Vi Troubleshoot problems Diagnose and repair network prob	on PN connection; or set up a router or access point. blems, or get troubleshooting information.					
also rnet Ontions	Set up a broadband, dial-up, or VI	on PN connection; or set up a router or access point. blems, or get troubleshooting information.					

 \times 🔮 Set Up a Connection or Network \leftarrow 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) Cancel Next

				_		\times
←	🌆 Connect to a Workplace					
	How do you want to	connect?				_
	→ Use my Internet Connect using a virtu	connection (VPN al private network (VP) N) connection through the	Internet.		
	A —	- 🧼				
	→ Dial directly Connect directly to a	phone number withou	ut going through the Intern	et.		
	I	-				
					Canc	el
~	Connect to a Workplace			_		×
	Type the Internet add	ress to connect to)			
	Your network administrator	can give you this addr	ess.			
	Internet address:	172.26.6.190 The	e WAN IP of HQ			
	Destination name:	VPN Connection				
	Use a smart card					
	Remember my cred	entials				
	Illow other people t	o use this connection wone with access to the	his computer to use this co	nnection.		
	This option allows a		•			
	This option allows a					
	This option allows a		·		-	

c Change adapter's settings.



	Options	Security	Networking	Sharing	
ype of	VPN:				
layer 2	2 Tunnelin	g Protocol	with IPsec (L2	TP/IPsec)	~
				Advance	ed settings
lata en	cryption:			P. 3	
Optiona	al encrypti	on (connec	t even if no e	ncryption)	~
Authe	ntication				
OUs	e Extensib	le Authenti	ication Protoco	ol (EAP)	
					\sim
				Per	mention
				FIG	penies
	ow these p	protocols			
		ted passwo	ord (PAP)		
\square	Unencryp	tea pacent			
$\mathbf{\Sigma}$	Unencryp Challenge	Handshal	ke Authenticat	ion Protocol (CHAP)
	Unencryp Challenge Microsoft	Handshak CHAP Ven	ke Authenticat sion 2 (MS-CH	ion Protocol (AP v2)	CHAP)
	Unencryp Challenge Microsoft	Handshal CHAP Ven natically use	ke Authenticat sion 2 (MS-CH e my Windows omain, if any)	ion Protocol (AP v2) logon name a	CHAP) and

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

eneral	Options	Security	Networking	Sharing	
Type of	VPN:				
Layer 2	Tunnelin	g Protocol	with IPsec (L2	TP/IPsec)	~
Data en	cryption:			Advanced	l settings
Optiona	encrypti	on (conne	ct even if no e	ncryption)	~
Auther	ntication				
OUse	e Extensib	le Authent	ication Protoc	ol (EAP)	
				Prope	erties
Allo	w these p	protocols			
\checkmark	Unencryp	ted passw	ord (PAP)		
	Challenge	Handshal	ke Authenticat	ion Protocol (CH	HAP)
\checkmark	Microsoft	CHAP Ven	sion 2 (MS-CH	IAP v2)	
	Autom	natically us	e my Windows Iomain, if any)	logon name an	d



e Set Network Mode to PC to Router.

² o Overview							
Online Clients	Rotter Hostname EG105G-P MAG	Add User		×	3		(1) Reboot
A Router	Overview Basics Y Security	Service Type	ALL				
♥Wireless	1 VPN Clients	* Username	PC				0
Switches	VPN Client List	* Password		0		+ Add	Delete Selected
tet Network	Up to 32 entries can be added.	Network Mode	PC to Pouter	ו			
	Username	Hethork mode	PC to Router		eer Subnet	Status	Action
		Status					
			Cancel	OK			e
(Collapse							Ai

6. Configuring Client-to-Site VPN (Based on Open VPN)

Client-to-site VPN needs to be configured on both the HQ gateway and a client so that a VPN connection can be established between the HQ and the client.

- (1) Configure VPN for the HQ gateway.
 - a Log in to Ruijie Cloud and click the project, to which the HQ access gateway belongs, to go to the configuration page.
 - b Choose Configuration > Devices > Gateway > VPN > VPN.

VPN VPN Account VPN Online User					Vi	™ Guide
Add VPN Policy						
						0
Connection Status	Name	Purpose	Config Status	VPN Mode	Action	
Disconnected	9999	Site-to-Site	- Disabled	Auto IPsec	2 6 1	
	pptp22	Client-to-Site	 Disabled 	рртр	260	
	12321	Client-to-Site	Enable	OpenVPN	261	
		Client-to-Site	 Disabled 	L2TP Sec	261	

c Click Add VPN Policy.

Add VPN Policy		2
Status	Enable	
Remark	EG210G-E_OpenVPN	
Purpose	VPN Site-to-Site VPN Client-to-Site VPN	
VPN Mode	L2TP over IPsec L2TP OpenVPN PPTP	
Server IP/Domain 🕐	IP ①	
	192.168.1.18	
Server Mode 🕐	Account Certificate Account & Certificate	
Protocol	• UDP C TCP	
IP Pool		
Server Subnet 🕐	Please select	
Flow Control	VLAN 1 VLAN 233 (192.168.110.0)	
	66 (192.168.66.0)	
All Traffic over VPN 🕐	VLAN234 (192.168.130.0)	
Advanced	VLAN 235 (192.168.150.0)	

d Configure the VPN policy for the HQ gateway.

Parameter	Description
Status	Specify whether to enable the VPN policy.
Remark	Provide the description of the VPN policy.
Purpose	Specify the VPN usage scenario. Select Client-to-Site.
VPN Mode	Select the mode for implementing client-to-site VPN. Select Open VPN .
Server IP/Domain	Specify the IP address or domain name of the L2TP server.

Parameter	Description
Server Mode	 Select a server authentication mode. The options are Account and Certificate, Account: Enter the correct username and password and upload the CA certificate on the client to connect to the server. The configuration is simple. Certificate: Upload the CA certificate and client certificate and enter the correct private key on the client to connect to the server.
Protocol	Select a protocol for all OpenVPN communications based on a single IP port. The options are UDP and TCP . The default value is UDP , which is recommended. When you select a protocol, pay attention to the network status between two encrypted tunnel ends. If high latency or heavy packet loss occurs, select TCP as the underlying protocol.
IP Pool	Specify the address pool used by the server to allocate IP addresses to clients.
Server Subnet	
All Traffic over VPN	Specify whether to route all traffic over VPN. After this function is enabled, all the traffic is routed over the VPN tunnel. This means that the VPN tunnel is the default route.
Port ID	
TLS Authentication	
Data Compression	Specify whether to enable data compression. If this function is enabled, transmitted data is compressed using the LZO algorithm. Data compression saves bandwidth but consumes certain CPU resources. The setting on the client must be the same as that on the server. Otherwise, the connection fails.
Cipher	Select the data encryption mode before data transmission to ensure that even data packets are intercepted during transmission, the leaked data cannot be interpreted. If this parameter is set to Auto on the server, you can set this parameter to any option on the client. If a specific encryption algorithm is configured on the server, you must select the same encryption algorithm on the client. Otherwise, the connection fails.

(2) Create an OpenVPN user.

Only user accounts added to the VPN client list are allowed to dial up to connect to the OpenVPN server. Therefore, you need to manually configure user accounts for clients to access the OpenVPN server.

a Choose Configuration > Devices > Gateway > VPN > VPN Account.

Add

Cancel

b Click Add VPN Account.

Add VPN Account		×
Username	eg: Henry	
Password	At least 8 characters	

c Configure items related to a VPN account.

Table 8-6 VPN Account Configuration Items

Parameter	Description
Username	Specify the VPN username.
Password	Specify the password for the client to log in to the VPN.

- d Click Add.
- (3) Configure the client.

The following uses a Windows 10 client as an example for description. For the configuration of other clients, click **VPN Guide** at the upper right corner of the configuration page.

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.
- Export the client configuration on the web page.
- Right-click **OpenVPN** and choose **Import** > **Import file...** to import the client configuration on the client.

Disconnect		
Reconnect		
Show Status		
View Log		
Edit Config		
Clear Saved Passw	ords	
Import	>	Import file
Settings		Import from Access Server
Exit		Import from URL
		<i>\$</i>

N	ew f	fold	ler			
ents	*	^	Name	Date modified	Туре	Size
s	*		o client.ovpn	3/10/2022 11:20 PM	OpenVPN Config	2 KB
e - Pe	rsor					



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 the OpenVPN account.

Cookbook

😳 OpenVPN Connection	(client)			_		\times
Current State: Connecting						
Thu Mar 10 23:38:20 Thu Mar 10 23:38:20	client	×	ed. Compression -128-CBC' but r	n has beer nissing in -	used in t	the p hers
Thu Mar 10 23:38:20 Thu Mar 10 23:38:20 Thu Mar 10 23:38:20	emame: u11		er) 64bit 1, LZO 2.10	24] [PKC5	I I I (AEA	D]Di
Thu Mar 10 23:38:20 Pas Thu Mar 10 23:38:20 Thu Mar 10 23:38:21	ssword:		e, waiting INET]127.0.0.1).1:25340 :25340		
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 Thu Mar 10 23:38:21	nnecting automatically in 2 seconds					
<	_					>
,						
			OpenVPN	GUI 11.2	6.0.0/2.5	.5
Disconnect	Reconnect				Hide	

OpenVPN Connection (client) -							
Current State: Connected	l,						
Thu Mar 10 23:38:28 20 Thu Mar 10 23:38:20 20 Thu Mar 10 23:38:30 20	22 interactive service msg_chann 22 open_tun 22 tap-windows6 device [OpenVP 22 TAP-Windows Driver Version 9 22 Set TAP-Windows TUN subne 22 Notified TAP-Windows driver to 22 Successful ARP Flush on interf 22 MANAGEMENT: >STATE:164 22 IPv4 MTU set to 1500 on interf 22 TEST ROUTES: 1/1 succeede 22 MANAGEMENT: >STATE:164 22 C:\WINDOWS\system32\route 22 Route addition via service succ 22 Initialization Sequence Complet 22 MANAGEMENT: >STATE:164	el=808 'N TAP-Windows6] opened).24 t mode network/local/netmask = o set a DHCP IP/netmask of 10.8/ face [45] {C6800A22-9C51-4078-{ 6930308,ASSIGN_IP,,10.80.12.2 face 45 using service ed len=1 ret=1 a=0 u/d=up 16930310,ADD_ROUTES e.exe ADD 192.168.100.0 MASK ceeded ted 16930310,CONNECTED,SUCCES	10.80.12.0/10.8 0.12.2/255.255. 844C-40D24535 255.255.255.0 55,10.80.12.2,12				
<			>				
Assigned IP: 10.80.12.2							
Bytes in: 6930 (6.8 KiB) o	out: 4448 (4.3 KiB)	OpenVPN GU	11.26.0.0/2.5.5				
Discourset	Deserves						

8.5 Configuring Portal Authentication

1. Overview

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

After completing the configuration on Ruijie Cloud, the configuration is synchronized Reyee EG devices.

2. Getting Started

- Before configuring portal authentication, choose **Configuration** > **Network-Wide** > **Network** to configure service networks, that is, configure the VLANs, to which the IP addresses of the authenticated clients belong.
- Choose **Configuration** > **Auth & Accounts** > **Authentication** > **Captive Portal** to configure the portal authentication page.

3. Configuration Steps

Choose Configuration > Devices > Gateway > Portal Auth.

Ruijie-test_Auto 🗸				
俭 Workspace				
AI Networking				
Smart Config				
Configuration				
Network-Wide >				
≇ Devices >	General	Gateway	Switch	Wireless
	Intranet Access	Interface	Interface	SSID
Monitoring	ACL	Routing	VLAN	Radio
路 Network-Wide >	IP-MAC Binding	NAT	Routing	Radio Planning
Devices	SNMP	VPN	Loop Prevention	Rate Limit
ரி Clients	Project Password	Portal Auth	DHCP Snooping	AP Mesh
	CLI Config Task	Dynamic DNS	Interface Rate Limit	Load Balancing
🗄 Logs >	Batch CLI Config	Session Limit	Voice VLAN	Wireless Block/Allow
😂 Delivery Center >		IPTV	Hot Standby	AP VLAN
·····, ·····		PPPoE Server	IP Source Guard	
			Interface Protection	

- (1) Enable the portal authentication function.
- (2) In the Authenticated IP segment area, click Add and set parameters related to authenticated IP addresses.

Save

Cloud Portal Auth			×
Network			
Seamless Online 🛛 🤍	1 Day 🗸		
Select or add a new portal.			
333 Voucher Login Access Code Login One-dick Login Account Login Account Login SMS Login	33 1 1 1 Vesuchar Login Access Code Vajeree to the Terms of Steruce and Accessibilite Use Policy Login One-cick Login	22 Pacific Color Q Voucher Login Access Code Dagin One click Login One click Login	>

Table 8-7 Configuration Items Related to Authenticated IP Addresses

Parameter	Description
Network	Select the network segment, to which the IP address of an authenticated client belongs.
Seamless Online	After the function is enabled, clients in the authenticated IP address segment need to be authenticated only once if they log in within the specified time. After the function is enabled, you need to set the time range.
Select or add a new portal	Select the portal page to be displayed during authentication. The portal page can be customized as required. For details, see <u>11.1</u> <u>Captive Portal</u> .

(3) Click Save.

4. Verification

Log in to the Web management page of the gateway. In local device mode, choose **Advanced** > **Authentication** > **Cloud Auth**. The configurations on the cloud have been synchronized to the device.

Cloud Auth	Local A	Account Auth	Authorized Auth	QR Code Auth	Allowlist	Online Clients	Customized Portal
Ruijie C in a lay In a lay	loud supp rer-2 netw rer-3 netw	orts voucher auth ork, if the IP add ork, if the IP add	entication, local account ress of the EAP device i ress of the EAP device i	authentication, SMS is in the authenticati is in the authenticati	authentication a on IP range, ple on IP range, ple	nd one-click authentionse add its MAC add	cation. Please log into Ruijie Cloud to enable authentication. View ress to the MAC address whitelist of Allowiist. s to the IP address whitelist of Allowiist.
Authen	tication						
* Netwo	ork Type	Layer-2 Netwo	ork	~			
* Serv	er Type	Connect Wi-Fi	via WeChat	~			
* Auth Ser	ver URL	maccauth.ruiji	e.com.cn				
Rec	direct IP	47.104.189.18	D:81				
Client	Escape	Enable					
	l	Save					

8.6 Configuring Dynamic DNS

1. Overview

After the dynamic domain name server (DDNS) service is enabled, external users can use a fixed domain name to access service resources on the device over the Internet at any time, without the need to search for the WAN port IP address. The device supports two DDNS protocols: No-IP DNS and DynDNS.

2. Getting Started

Before you use the DDNS service, you need to register an account and a domain name on the third-party DDNS service provider for this service.

3. Configuration Steps

• Configuring the No-IP

Select the DDNS server with the domain name of www.noip.com.

Choose Configuration > Devices > Gateway > Dynamic DNS > No-IP.

Please select the device :	NAEK0037H0001(-)	V				
Ruijie DDNS	No-IP DynDNS					
() A	utomatically update your DNS hos	st each time when its public IP address	changes. To use No-IP or DynDN, please register	an ake account of the corresponding DNS pr	oviders: Noip (www.noip.com) and Dyndns (account.dyn.com).	
Service	Interface*	🔿 wan 🔿 wan1 🔿 wan2	🔾 wan3	O construction Obstants		
Userna	me *			Domain		
Passwo	rd *	ø				
Domair	ń *					
		Save Reset				

(1) Set configuration items on the **No-IP** tab.

Table 8-8	DDNS I	ogin	information

Parameter	Description
Service Interface	One domain name can be parsed to only one IP address. Therefore, you need to specify the WAN port bound to the domain name when multiple WAN ports are available. By default, the service interface is a WAN port.
Username & Password	Enter the username and password of the account registered at the official website of the DDNS service provider. Register at the official website of the DDNS service provider in advance.
Domain	Specify the domain name bound to the service interface IP address. One account can be bound to multiple domain names. You can choose to bind only one domain name to the IP address of the current service interface. Only the selected domain name is parsed to the WAN port IP address.

(2) Click Save.

• Configuring the DynDNS

Select the DDNS server with the domain name of www.dyndns.org.

Choose Configuration > Devices > Gateway > Dynamic DNS > DynDNS.

Please select the	device:	NAEK0037H000	1(-)	×							
Ruijie DDNS	S	No-IP	DynDNS								
	 Auto 	omatically updat	e your DNS hos	t each time when its	public IP addres	s changes. To use No-IP or	DynDN, please register	an account of the corresponding DNS pro	oviders: Noip (www.noip.com)	and Dyndns (account.dyn.com).	
	Service In	iterface*		🔿 wan 🔿 wa	n1 🔿 wan2	e 🔾 wan3					
	Username	e *						Connection Status Domain	-		
	Password	*			Ø						
	Domain *										
				Save	et						

(3) Set configuration items on the **DynDNS** tab.

Table 8-9 DDNS login information

Parameter	Description
Service Interface	One domain name can be parsed to only one IP address. Therefore, you need to specify the WAN port bound to the domain name when multiple WAN ports are available. By default, the service interface is a WAN port.

Parameter	Description
Username & Password	Enter the username and password of the account registered at the official website of the DNS service provider. Register at the official website of the DDNS service provider in advance.
Domain	Specify the domain name bound to the service interface IP address. One account can be bound to multiple domain names. You can choose to bind only one domain name to the IP address of the current service interface. Only the selected domain name is parsed to the WAN port IP address.

(4) Click Save.

4. Verifying Configuration

If **Connection Status** is displayed as **Connected**, the server connection is established successfully. After the configuration is completed, ping the domain name from the Internet. The ping succeeds and the domain name is parsed to the WAN port IP address.

8.7 Configuring IPTV

1. Overview

Internet Protocol television (IPTV) is a new technology that uses broadband cable television network and integrates Internet, multimedia, communication, and other technologies to provide home users with a variety of interactive services including digital television. It allows users to enjoy the IPTV service at home.

2. Limitations

IPTV is only supported on Reyee devices.

3. Getting Started

- Confirm that the IPTV service is activated.
- Check the local IPTV type: VLAN or IGMP. If the type is VLAN, confirm the VLAN ID. If you cannot confirm the type or VLAN ID, contact the local ISP.

4. Configuration Steps

• Configuring the IPTV Service of the VLAN Type

Choose Configuration > Devices > Gateway > IPTV > IPTV/VLAN.

Please select the device :	NAEK0037H0001(-)	\vee						
IPTV								
IPTV/VLAN	IPTV/IGMP					LAN WAN	Static IP Dynamic IP	PPPOE
			LANS LANA	LANS LANG/WANG	HAN1 WAND			
LAN2								
VLAN Type:	IPTV V							
VLAN ID :	Range:1-4094							

(1) Select the port for carrying the IPTV service on the device.

- (2) Set VLAN Type to IPTV.
- (3) Enter the VLAN ID provided by the ISP.
- (4) Click Save.

Save

For example, when you want to connect the IPTV set top box to LAN 3 port of the device and the VLAN ID is 20, the configuration UI is as follows.

After the configuration is completed, confirm that the IPTV set top box is connected to the correct port, for example, LAN 3 in the example.

A Caution

Enabling this function may lead to network disconnection. Exercise caution when performing this operation.

• Configuring the IPTV Service of the IGMP Type

Choose Configuration > Devices > Gateway > IPTV > IPTV/IGMP.

The IGMP type is applicable to the ISP FPT. After you enable IPTV connection, connect the IPTV set top box to any LAN port on the router.

Please select the device :	NAEK0037H000	1(-) ~	
IPTV			
IPTV/VLAN	IPTV/IGMP		
IGMP Enable :			

8.8 PPPoE Server

After enabling the PPPoE server, clients connected to the router's downstream need to enter their PPPoE account and password. Once authenticated, they will receive an IP address issued by the router in order to access the internet.

1. MAC binding and MAC filtering are invalid for a PPPoE client.

2. The IP addresses assigned by the PPPoE server cannot overlap with the address range of any interface on the device.

3. Authentication is invalid for a PPPoE client.

Ruffe IRcycc A	ome Project	Isw_testas@ch V	⊕ Q	D E) @	8
DemoProject1 V	Select the device: NAEKTEFCH0001(-) V					
☆ Workspace	Clobal Sattloor Evolute ID Pannar					
AI Networking	Uniour acturings Excluded in nariges					
Smart Config	1. MAC binding and MAC filtering are invalid for a PPPoE client.					
Al Diagnostics	The IP addresses assigned by the PPPoE server cannot overlap with the address range of any interface on the device. Authomatication is involted for a DDDst etilant					
• • • • • • • • • • • • • • • • • • • •						
Configuration	PPPoE Server:					
Network-Wide >	Mandatory DPPnF Dialum					
⊕ Devices →						
	Local Tunnel IP Address: 10.44.66.99					
Monitoring	Range of IP Address Pool: 10.44.66.100 - 10.44.66.200					
윪 Network-Wide >						
Devices	VLAN: Default VLAN V					
fi Clients >	Drimary DNC*					
🗟 Logs >						
Delivery Center >	Secondary DNS: Format: 1.1.1.1					
	Save					

Set exception IP addresses, which will be able to access the internet without having to dial through PPPoE.

A maximum of 5 excluded IP address ranges are supported.

	Home Project	in hw_testas@ch 🗸 🕤 🖓 🛞
DemoProject1 V	Select the device: NAEK1EFCH0001(·) V	
ᢙ Workspace	Global Settings Excluded IP Ranges	
AI Networking		
Smart Config	A maximum of 5 excluded IP address ranges are supported.	
Al Diagnostics	Add Batch Delete	
Configuration	Add ×	
Network-Wide	Start IP mark	Status Action
	Start IP: Format: 1.1.1.1 Enter the start IP	
# Devices >	x Fed ID: Committee 1111	
Auth & Accounts >		
Monitoring	Remark:	
on Network-Wide →		
Devices	Status:	
Clients >		
🗄 Logs >	Cancel	
😂 Delivery Center >		

9 Switch Configuration

9.1 Interface

Choose **Configuration > Devices > Switch > Interface** to go to the device network port page.

Ruijie-test_Auto V	Select the device	: CAQL71D016984(Floor2_CCTV_Switch) V	
 	Port			
AI Networking	1 2 3 4	5 6		
Smart Config		μi ά		
Configuration				
Network-Wide	,			Select
幸 Devices >>	General	Gateway	Switch	Wireless
	Intranet Access	Interface	Interface	SSID
Monitoring	ACL	Routing	VLAN	Radio
윪 Network-Wide	IP-MAC Binding	NAT	Routing	Radio Planning
Devices	SNMP	VPN	Loop Prevention	Rate Limit
பி Clients	Project Password	Portal Auth	DHCP Snooping	AP Mesh
	CLI Config Task	Dynamic DNS	Interface Rate Limit	Load Balancing
🖺 Logs 🔅	Batch CLI Config	Session Limit	Voice VLAN	Wireless Block/Allow
🍣 Delivery Center 🔅	>	IPTV	Hot Standby	AP VLAN
		PPPoE Server	IP Source Guard	
			Interface Protection	

Select a device, click the port to be configured, configure **Duplex**, **Speed**, **Port Type**, and **PoE-capable** for the port, and then click **Save**.

易网络体验5 🛛 🗸	Please select the device: NAEK0048H0003(-)	
硷 Workspace	Port	
🕏 Smart Config	1 8 5 7 9 11 13 15 17 19 21 28	
Configuration		
Ø Network-Wide >	2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28	
· 프 Devices >	Selected Ports: Gi2	
\bigtriangledown Authentication \rightarrow	* Enabled: Open	v router port switch: Unsupported
Monitoring		
& Network-Wide ⇒	Duplex: Auto-negotiation	V Port Type: Trunk V
Pevices >	Speed: Auto-negotiation	* Native ID: 1
Clients >		
E Logs >	Description: Wireless AP port	* Allowed VLAN: 1-4094
📚 Delivery Center 🔅	PoE-capable: Open	v
	Port Media: Unsupported	
		Save

Save

9.2 Configuring a VLAN for an Interface

(1) Creating a VLAN

Choose Configuration > Devices > Switch > VLAN.

Click Add, set VLAN ID, and click Save to add a VLAN.

Ruijie-test_Auto 🗸	Select the device:	Select the device: CAQL71D016984(Floor2_CCTV_Switch) V						
硷 Workspace	VLAN Mode	VLAN Mode						
AI Networking	Managed \vee	Managed V Set						
Smart Config	VLAN Configuration							
Configuration	⊙ Add ⊙	O Add O Batch Add VLAN						
⊗ Network-Wide >	VLAN ID	VLAN ID Remark						
≇ Devices >	General	Gateway	Switch	Wireless				
	Intranet Access	Interface	Interface	SSID				
Monitoring	ACL	Routing	VLAN	Radio				
备 Network-Wide >	IP-MAC Binding	NAT	Routing	Radio Planning				
Devices >	SNMP	VPN	Loop Prevention	Rate Limit				
句 Cliante	Project Password	Portal Auth	DHCP Snooping	AP Mesh				
	CLI Config Task	Dynamic DNS	Interface Rate Limit	Load Balancing				
E Logs >	Batch CLI Config	Session Limit	Voice VLAN	Wireless Block/Allow				
😂 Delivery Center >		IPTV	Hot Standby	AP VLAN				
		PPPoE Server	IP Source Guard					
			Interface Protection					

Select the device:	CAQL71D016984(Floor2_CCTV_Switch) \vee						
VLAN Mode							
Managed V							
	atch Add VLAN	o					
VLAN ID	Remark	0					
VLAN ID	Remark						

(2) Adding an interface to the VLAN

Choose **Configuration** > **Devices** > **Switch** > **Interface** to go to the device network port page.

Rujje IRcycc	Home Proj	ect			
Ruijie-test_Auto ∨	Select the devic	e: CAQL71D016984(Floor2_CCTV_Switch) ∨		
硷 Workspace	Port				
AI Networking	1.2.8.4	5 6			
Smart Config					
Configuration					
Ø Network-Wide >					Select the port t
≇ Devices >	General	Gateway	Switch	Wireless	
	Intranet Access	Interface	Interface	SSID	
Monitoring	ACL	Routing	VLAN	Radio	
윪 Network-Wide >	IP-MAC Binding	NAT	Routing	Radio Planning	
Devices	SNMP	VPN	Loop Prevention	Rate Limit	
	Project Password	Portal Auth	DHCP Snooping	AP Mesh	
. Clients	CLI Config Task	Dynamic DNS	Interface Rate Limit	Load Balancing	
🕼 Logs >	Batch CLI Config	Session Limit	Voice VLAN	Wireless Block/Allow	
on Delivery Center		IPTV	Hot Standby	AP VLAN	
~		PPPoE Server	IP Source Guard		
			Interface Protection		

Select a device, click the port to be configured, set **VLAN ID** to the ID of the created VLAN, and then click **Save**.

Port		
Selected Ports: Port 1		
Status:	Enable V	router port switch: Unsupported
Duplex:	Auto-negotiation V	Port Type: Access
Speed:	Auto-negotiation \lor	* VLAN ID: 4
Description :		
PoE-capable :	Open v	
Port Media:	Unsupported	
		Save

9.3 Routing

9.3.1 Adding a Static Route

Static routes are manually configured. When a data packet matches a static route, the packet will be forwarded based on the specified forwarding mode.

🛕 Caution

Static routes cannot automatically adapt to changes of the network topology. When the network topology changes, you need to reconfigure the static routes.

Procedure

Choose Project > Device > Switch > Routing, click Static Routing, click Save.

DemoProject6		Please select the device: NAEK002AH000	1(-)							
硷 Workspace		Routing								
👫 Smart Config		⊙ Static Routing								
Configuration		Destination Address*	Su	bnet Mask*	Next-hop (exce	ept dialing)*	Egr	ess Interface		
Network-Wide		Please enter the destination address	Please enter the s	ubnet mask.	Please enter the next-ho	p address				0
章 Devices										
Authentication					Save					
Monitoring		Policy-based Routing O Add PBR rules								
Network-Wide		Rule Name S	Status Protocol Type	Source IF	address/range	Destination IP address/range		Interface		
P Devices			IP	V All		All		WAN	× C	
Clients					Save					
E Logs	20									
Delivery Center										

The following table lists the description of parameters.

Parameter	Description
Destination Address	Specify the destination network to which data packets are to be sent. The device matches the data packet based on the destination address and subnet mask.
Subnet Mask	Specify the subnet mask of the destination network. The device matches the data packet based on the destination address and subnet mask.
Next-hop Address	Specify the IP address of the next hop in the route for data packets. If the outbound interface accesses the Internet through PPPoE dialing, you do not need to configure the next-hop address.
Egress	Specify the interface that forwards data packets.

9.3.2 Adding PBR

Policy-based routing (PBR) is a mechanism for routing and forwarding based on user-specified policies. When a router forwards data packets, it filters the packets based on configured rules, and then forwards the matched packets according to the specified forwarding policy. PBR enables the device to define rules according to specific fields (source or destination IP address and protocol type) in the data packets, and forward the data packets from a specific interface.

In a multi-line scenario, if the device is connected to the Internet and the internal network through different lines, traffic will be evenly routed over the lines if no routing settings are available. In this case, access data to the internal network may be sent to the external network, or access data to the external network may be sent to the

internal network, resulting in network exceptions. To prevent these exceptions, you need to configure PBR to control data isolation and forwarding on the internal and external networks.

The device can forward data packets using either of the following three policies: PBR, address-based routing, and static routing. When all the policies exist, PBR, static routing, and address-based routing are in descending order of priority.

Procedure

Choose Project > Device > Switch > Routing, choose Add PBR rules, set parameters, and click Save.



The following table lists the description of parameters.

Parameter	Description
Rule Name	Specify the name of a PBR rule, which uniquely identifies a PBR rule. The
	name must be unique for each rule.
Status	Indicate whether to enable the PBR rule. If the value is disabled, this rule does
	not take effect.
Protocol Type	Specify the protocol for which the PBR rule is effective. You can set this
	parameter to IP, ICMP, UDP, TCP, or Custom.
	Configure the source IP address or IP address range for matching PBR entries.
Source IP/IP Pange	The default value is All IP Addresses.
	All IP Addresses: Match all the source IP addresses.
	Custom: Match the source IP addresses in the specified IP address range.
	Configure the destination IP address or IP address range for matching PBR
Destination IP/IP	entries. The default value is All IP Addresses.
Range	All IP Addresses: Match all the destination IP addresses.
	Custom: Match the destination IP addresses in the specified IP address range.
Interface	Specify the interface that forwards data packets based on the hit PBR rule.

9.4 Voice VLAN

9.4.1 Overview

Voice VLAN is a VLAN specially classified for users' voice data streams. Voice VLAN limits data streams and voice streams to the data VLAN and voice VLAN respectively. When the voice VLAN feature is enabled, the CoS priority of voice data should be higher than that of service data, so as to reduce delay and packet loss during the transmission, thereby improving the voice quality.

9.4.2 Configuration Steps

Choose Configuration > Devices > Switch > Voice VLAN.

Ruijie-test_Auto ∨	Select the device:	CAQL71D016984(Flo	or2_CCTV_Switch) V	
☆ Workspace				
AI Networking				
Smart Config				
Configuration				
Network-Wide >				
፰ Devices >	General	Gateway	Switch	Wireless
	Intranet Access	Interface	Interface	SSID
Monitoring	ACL	Routing	VLAN	Radio
윪 Network-Wide >	IP-MAC Binding	NAT	Routing	Radio Planning
Devices	SNMP	VPN	Loop Prevention	Rate Limit
	Project Password	Portal Auth	DHCP Snooping	AP Mesh
. Clients	CLI Config Task	Dynamic DNS	Interface Rate Limit	Load Balancing
🗑 Logs >	Batch CLI Config	Session Limit	Voice VLAN	Wireless Block/Allow
🔆 Delivery Center 🔿		IPTV	Hot Standby	AP VLAN
, 		PPPoE Server	IP Source Guard	
			Interface Protection	

1. Voice VLAN Settings

Enable voice VLAN, set VLAN, Aging Time, and COS Priority, and click Save.

EGW_20230111 V	Please select the device: G1PD49A005359(-)
俭 Workspace	Settings OUI Port Settings
你 Smart Config	
Configuration	When the voice VLAN feature is enabled, the CoS priority of voice data should be higher than that of service data, so as to reduce delay and packet loss during the transmission.
Network-Wide	Switch:
幸 Devices >	
\bigotimes Authentication $>$	VLAIV. V AGO VLAIV
Monitoring	• Aging Time: 1440
备 Network-Wide >	COS Priority: 6 V
🚇 Devices >	
🖞 Clients >	Save
Logs >	
😂 Delivery Center 🔅	
Add	×
	* VLAN ID: 4
	Cancel
	Cancer

2. OUI Settings

The device identifies the source MAC address of the input message and configures the OUI address to identify the voice data stream of the specified voice device. The enabled globally port will automatically add the corresponding OUI when receiving an LLDP packet that is identified as telephone.

Enter the MAC address and click <Add> to add the OUI address.

EGW_20230111		Please select the device : G1PD49	A005359(-)	
硷 Workspace		Settings OUI Po	ort Settings	
Nort Config		The enabled globally port will	automatically add the corresponding QUI when recei	iving an LLDP packet that is identified as telephone. Up to 24 entries can be added
Configuration		OUIs		
Network-Wide		MAC Address	Description	Action
 Authentication 				+ Add
Monitoring				
8 Network-Wide	>			
Devices	2			
Clients				
Logs				
Selivery Center				

Settings	OUI Port Set	ttings	
1 The enabl	ed globally port will autor	matically add the corresponding OUI when receiving an LLDP packet	that is identified as telephone. Up to 24 entries can be added.
OUIs			
WAC Address		Description	Action
00:22:33		Description	Action Delete

3. Port Settings

The port can be set to the automatic mode only when the port VLAN is in the trunk mode.

When the port is in the automatic mode, the port will exit the voice VLAN first, and automatically join the voice VLAN until it receives voice data again.

A Caution

To ensure the normal operation of voice VLAN on port, please do not switch the port mode (trunk/access mode). To switch the mode, please disable the voice VLAN first.

Select a port and click Edit. Configure Voice VLAN Mode and Security Mode and click Confirm.

EGW_20230111 V	Please select the device	e: G1PD49A005359(-)	\[\] \[
G Workspace	Settings OU	JI Port Settings			
% Smart Config Configuration	The port can be s first, and automa mode (trunk/acce	et to the automatic mode on tically join the voice VLAN un ass mode). To switch the mod	ly when the port VLAN is in the trunk mode. W til it receives voice data again.To ensure the nc e, please disable the voice VLAN first.	/hen the port is in the automatic mode, the por rmal operation of voice VLAN on port, please o	t will exit the voice VLAN do not switch the port
Network-Wide Devices	Port List				🖉 Batch Edit
⊘ Authentication >	Port	Enable	Voice VLAN Mode	Security Mode	C
Monitoring	Gi1	Disabled	Auto Mode	Enabled	Edit
Devices >	Gi2	Disabled	Auto Mode	Enabled	Edit
🖞 Clients >	Gi3	Disabled	Auto Mode	Enabled	Edit
🗑 Logs >	Gi4	Disabled	Auto Mode	Enabled	Edit
Delivery Center	Gi5	Disabled	Auto Mode	Enabled	Edit
Edit					Х
	Ena	abled: 🚺			
	Voice VLAN N	Mode: Auto Mode	V		
	Security N	Node: 🚺			
				Cancel	Confirm

10 Wireless Configuration

10.1 AP Mesh

Overview

- When wired uplink is unavailable in the deployment area, wireless uplink is used for mesh networking to prevent coverage holes.
- An AP automatically scans and selects the best uplink AP. When an uplink fails, the AP will automatically switch to another uplink AP.
- When the wired network fails, a wired AP will automatically switch to the wireless uplink to ensure high availability.

Limitations

The function is only supported on **Reyee APs**.

Configuration

- (1) Power on all devices.
- (2) Place the root AP and Mesh AP within each other's Wi-Fi coverage radius (RSSI > -70 dBm).
- (3) Log in to Ruijie Cloud, choose Configuration > Devices > Wireless > AP mesh, and select a network in this account.
- (4) Confirm that the mesh function (enabled by default) is enabled. If the mesh function is disabled, click Enable Mesh Wi-Fi.

Mesh



Mesh Wi-Fi

1. When wired uplink is unavailable in the deployment area, wireless uplink is used for mesh networking to prevent coverage holes.

2. An AP automatically scans and selects the best uplink AP. When an uplink fails, the AP will automatically switch to another uplink AP.

3. When the wired network fails, a wired AP will automatically switch to the wireless uplink to ensure high availability.



(5) Click Scan to Add Mesh AP.

🛕 Caution

- Up to 8 APs can be paired at a time.
- You are advised to use a maximum of 16 APs to set up a mesh network.

- The Mesh AP must be a Reyee AP.
- The AP is powered on.
- The distance between Root AP and Mesh AP should be less than 2 m.
- A provisioned AP is restored to factory defaults.

		>-70 dBm
1	. Make sure all devices are powered on.	2. Make sure both root AP and Mesh APs are within each others Wi-Fi coverage radius (RSSI > -70dBm).
		Scan to Add Mesh AP

(6) Select the AP to be paired in the scanning result and click Pair. Wait for pairing completion.

Mesh Wi-Fi 🛈		×	Mesh Wi-Fi 🛈		Mesh Wi-Fi 🛈		Х
			0%			MAC: 00:d2:f8:00:50:21	
1	AP(s) are detected		Pairing.				
Please enter the pro the device the Select All	oject management password to ver at has been configured before.	ify					
✓ RAP2260(G)	MAC: 00:d2:f8:00:50:21						
	Scan again Pair			lone		Do	ne
After pairing	, you can view infor	mati	on about the mesh device on	the Al	P Mesh page.		
Mesh 🔵	Mesh Quality Excellent					Scan M	lesh AP

								0
Online Status	SN	MAC	AP Name	AP Model	Uplink AP	Mesh Status	Quantity	Operation
Online	NAEK0050H0012	00:d2:f8:00:50:21	<u>Empty</u>	RAP2260(G)	NAEK0050H0011	Connected	Excellent	Detail

10.2 SSID

10.2.1 SSID Basic Settings

 Log in to Ruijie Cloud, choose Project > Configuration > Devices > Wireless > SSID, and select a network in this account.

(2) On the S	SSID setting pag	e, click • next	to SSID to	create an SSIE) for device	s on the network	ς.
WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Protocol	Operation
			No	Data			

(3) On the SSID setting page, you can create an SSID and fill in parameters as needed. After configuration, click OK.

 SSID: Enter a combination of letters, digits, underscores, das • Frequency Band: 2 2.46 2 56 Encryption Option: Option: Do Not Encrypt C Encrypt • Encryption Method: OPEN (Open) Advanced Wireless mode: 802.11be(Wi-Fi7) Ø Forward Mode: Bridge VLAN: User and AP in the sa Hidden: 56-Prior Access: 	
 Frequency Band: 2.46 56 Encryption Option: Do Not Encrypt Encrypt Encryption Method: OPEN (Open) Advanced Mireless mode: 802.11be(Wi-Fi7) Advanced Wireless mode: Bridge VLAN: User and AP in the sa Hidden: 56-Prior Access: 	
Encryption Option: Do Not Encrypt Encrypt Copen Cope	
 Encryption Method: OPEN (Open) Advanced Wireless mode: 802.11be(Wi-Fi7) ③ Forward Mode: Bridge VLAN: User and AP in the sa Hidden: 5G-Prior Access: 	
Advanced Wireless mode: 802.11be(Wi-Fi7) Image: Image	
Wireless mode: 802.11be(Wi-Fi7) Softward Mode: Bridge VLAN: User and AP in the sa Hidden: 5G-Prior Access:	
 Forward Mode: Bridge VLAN: User and AP in the sa Hidden: 5G-Prior Access: 	
VLAN: User and AP in the sa \vee Hidden:	
Hidden : 5G-Prior Access :	
5G-Prior Access:	
) Single-Client Speed Limit:	
Rate Limit for SSID Users:	
⑦ Portal Authention: Go to the "Captive Portal" page	

Table 10-1	Description	of SSID	Configuration	Parameters
------------	-------------	---------	---------------	------------

Parameter	Description
	In apartment and quasi-apartment scenarios (AP-based independent SSID scenarios), Enable Apartment WiFi can be enabled.
Enable Apartment Wi-Fi	Recommended deployment for apartments: Deploy one AP in each room
	and name each AP using the room number. Each room has an independent SSID.
WLAN ID	It indicates the sequence number to represent an SSID. Up to 32 SSIDs are supported, and there may be differences between diverse models.
Hidden	It indicates whether to disable SSID broadcasting.
SSID	In general scenarios (that is, Enable Apartment WiFi is disabled), this parameter is valid. It indicates the Wi-Fi name.
SSID prefix	In apartment and quasi-apartment scenarios (that is, Enable Apartment WiFi is enabled), this parameter is valid, indicating the Wi-Fi name prefix. The SSID consists of the SSID prefix and AP name (you are advised to name APs after room numbers). For example, when you set SSID prefix to RUIJIE- and the AP name is 301, the SSID for the AP is RUIJIE-301. Note: Configure the apartment SSID password and alias on the AP details page. The default password is 88888888, which does not affect other SSID passwords. The SSID password here is just the apartment SSID password.
Forward Mode	It indicates the NAT mode or bridge mode. If you are not familiar with the live network design, the NAT mode is recommended. For details, see <u>Configuration Description</u> of Forward Mode.
Encryption Mode	The following encryption modes are supported: OPEN, WPA-PSK, WPA2- PSK, WPA/WPA2-PSK, WPA2-Enterprise (802.1x). For details, see <u>Encryption Mode</u> .
	In most cases, Radio1 represents 2.4 GHz and Radio2 represents 5 GHz, and Radio3 represents 2.4 GHz and 5 GHz. (Radio3 is supported on some models.) When you select Radio3 , you can click Configure Radio 3 Working Mode .
Radio	Radio 3 X
	Mode:
	Scan mode: Radio 3 of the AP is used to listen for surrounding RF information and cannot be accessed by users
	 Access mode: Radio 3 of the AP is used for wireless coverage and can be accessed by users
	Cancel

Parameter	Description				
	Specify whether to enable Wi-Fi 6 .				
Enable Wi-Fi 6	On Reyee APs, Wi-Fi 6 can be enabled based on the SSID.				
	Fi 6 is enabled, Wi-Fi 6 is applied to the radio corresponding to the SSID.				
	Detect clients capable of 5 GHz and steer them to that frequency, while				
5G-Prior Access	leaving 2.4 GHz available for legacy clients. Enabling this function is not				
	recommended if most of clients only support 2.4 GHz.				
Single-Client Speed Limit	It indicates the upload and download speed limiting for each client on this				
	SSID.				
Rate Limit for SSID Users	It indicates the total throughput (upload & download) on this SSID.				
	Specify whether to conduct authentication when Encryption Mode is set to				
	a value other than WPA2-Enterprise (802.1x) . After authentication is				
Auth	enabled, the following authentication protocols are supported: WiFiDog and				
	WeChat Connect Wi-Fi (3.X). For details, see Authentication				
	Configuration Description.				

(4) View the SSID list.

SSID 🕀

WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Protocol	Operation
2	Test_Ruijie1	open	No	bridge	1,2	Auth Disabled	Edit Delete
3	Ruijie- Apartment SSID Prefix	open	No	bridge	1,2	Auth Disabled	Ed Del Synchronize it ete Apartment SSID

The **Operation** column is described as follows:

- Edit: Click this button to modify SSID configuration parameters except WLAN ID.
- **Delete**: Click this button to delete a specified SSID.
- Synchronize Apartment SSID: If the AP name is changed, you must click this button to access the **Synchronize SSID** in **Apartment** page, and then click the **Batch Update SSID** button to update the SSIDs involved.

Sy	nchronize SSID in Apa	irtment			×
	Batch Update SSID			Device SN, alias	, MAC Q
	在线状态	设备序列号	MAC	设备名称	SSID名称
	Online	NAEK0055H0007	00d2.f800.5571	301	Ruijie-Ruijie
	Online	NAEK0055H0008	00d2.f800.5581	302	Ruijie-Ruijie
	Online	NAEK0055H0009	00d2.f800.5591	303	Ruijie-Ruijie
	Online	NAEK0055H0010	00d2.f800.5501	304	Ruijie-Ruijie
	Online	NAEK0055H0011	00d2.f800.5511	305	Ruijie-Ruijie
				5 in to	tal < 1 > 10 / page >

1. Configuration Description of Forward Mode

Parameter Description

The following forwarding modes are supported: bridge, nat.

- NAT mode: An AP will serve as a router and use the DHCP pool to provide IP addresses for stations (STAs).
 - Common NAT: All devices can be configured with the same address pool. Otherwise, the current or default one will be used, 192.168.23.0/24.
 - Cloud NAT: In NAT roaming scenarios, this mode should be applied. You can configure a range for the cloud NAT address pool. Ruijie Cloud will distribute different address pools to different devices according to the range.

If SSIDs in both NAT mode and Cloud NAT mode are configured, Ruijie Cloud will only deliver the Cloud NAT pool (that is, assign a pool to each device), but not the NAT pool.

- Bridge mode: An AP will function as a switch and allow all traffic to pass through. You need to specify the VLAN ID for users. The users and AP can use the same VLAN or different VLANs.
 - Users and the AP use the same VLAN: The users and AP share the address pool. It is applicable to the case, in which the address pool of the AP is also a DHCP address pool.
 - Users and the AP use different VLANs: The user VLAN and IP address pool are a part of the local network. It is applicable to the case, in which the local network can separately assign VLANs and addresses to users.

Configuration Example

• Forward Mode is set to bridge and users and the AP are in the same VLAN.

* WLAN ID:	2	~	Hidden:	
SSID:	Test_Ruijie		⑦ Forward Mode:	bridge V
	Chinese Character Encoding ③		VLAN :	User and AP in the sa \vee

• Forward Mode is set to bridge and users and the AP are in different VLANs. The client connected to the SSID will seek the DHCP server with VLAN 10 on the network to obtain the address.

* WLAN ID:	2	V	Hidden:		
SSID:	Test_Ruijie		⑦ Forward Mode:	bridge	~
	Chinese Character Encoding ⑦		VLAN :	Other VLAN V 10	

 When the NAT mode is configured, click Configure a NAT Pool to access the address pool configuration interface.

* WLAN ID:	2	\vee	Hidden:		
SSID:	Test_Ruijie		⑦ Forward Mode:	nat	×
	Chinese Character Encoding ③		Config	ure a NAT pool	

 Uniformly configure the device address pool: Select General Address Pool and click Click here to uniformly configure device address pool. to customize the address pool. After configuration, click OK.

NAT Pool Config		Х
Note:		
1. NAT pool configur	ations will only be delivered after	an SSID with NAT forwarding mode is configured.
2. If the device addre new address pool.	ss pool changes, the original asso	ciated users must actively re-associate with the SSID to obtain an address in the
 General Address 	Pool (for most scenarios)	
Not delivered by def address pool.	fault. The device's current or defau	ult address pool (192.168.23.0/24) is used. Click here to uniformly configure device
 NAT Roaming Ad configuration is gene 	ldress Pool (MACC will assign an a erally used in networks with dual-b	ddress pool to each device. This requires the AP to support layer 3 roaming. This band APs.)
Automatically assign	ed by server (Range: 10.233.0.0/2	4 to 10.254.254.0/24) , Click here to customize the address pool range.
		Cancel OK
 General Addres 	s Pool (for most scenarios)	
Not delivered by d address pool.	efault. The device's current or de	fault address pool (192.168.23.0/24) is used., Click here to use the device's default
* Default IP Rang	192.168.1.0	
* Subnet Mask:	255.255.255.0	
Primary DNS Add	Please enter the DNS address	
Secondary DNS:	Please enter the DNS address	

 When there are multiple APs on a network and Layer 3 roaming is enabled, select NAT Roaming Address Pool Mode and click Click here to customize the address pool range. to configure the address pool range. After configuration, click OK.

NAT Pool Config										×
Note:										
1. NAT pool configurations will only be delivere	d after	an SSID with I	NAT f	orwarding	j mode	is co	nfigured.			
2. If the device address pool changes, the origin new address pool.	nal asso	ciated users n	nust a	actively re-	-associa	ate w	th the SSID t	o obtain a	an address in the	
O General Address Pool (for most scenarios)										
Not delivered by default. The device's current of address pool.	or defau	ılt address po	ol (19	2.168.23.0	0/24) is	useo	., Click here t	o uniform	ly configure devic	ce
 NAT Roaming Address Pool (MACC will assi configuration is generally used in networks with 	gn an a 1 dual-b	ddress pool to and APs.)	o eac	n device. T	This req	uires	the AP to su	pport laye	er 3 roaming. This	
Automatically assigned by server (Range: 10.23	33.0.0/2	4 to 10.254.25	64.0/2	4) Click h	here to	cust	mize the add	dress pool	range.	
NAT Roaming Address Pool (MACC will ass configuration is generally used in networks wit	ign an a	address pool band APs.)	to ea	ch device.	. This r	equi	es the AP to	support la	Cancel C	<mark>)К</mark> This
Automatically assigned by server (Range: 10.2	33.0.0/2	24 to 10.254.2	254.0	(24) , CIICK	c nere t	o us	e the server's	default a	iaaress pool.	
Note: The address pool configured below will t	take eff	ect for the		enti	ire netv	vork.				
Start IP Range:	10.	1		1		. 0				
End IP Range:	10.	1		10		. 0				
Primary DNS Address: Please enter the DNS address										
Secondary DNS: Please enter the DNS address										

2. Configuration Description of Encryption Mode

- **OPEN**: Open the SSID. The password is not required.
- WPA-PSK: Use the WPA algorithm to encrypt the SSID. The password is required. After **PPSK** is selected, each client connected to the network will be assigned a separate Wi-Fi key and an account.
- WPA2-PSK: Use the WPA2 algorithm to encrypt the SSID. The password is required. After **PPSK** is selected, each client connected to the network will be assigned a separate Wi-Fi key and an account.
- WPA/WPA2-PSK: Use the WPA/WPA2 algorithm to encrypt the SSID. The password is required. After PPSK is selected, each client connected to the network will be assigned a separate Wi-Fi key and an account.
- WPA2-Enterprise(802.1x): 802.1X authentication and the external RADIUS server are required.
 - a Set Encryption Mode to WPA2-Enterprise(802.1x) and click \bigcirc in the Primary Server line.

	Encryption Mode: WPA2-Enterprise(802.1X)	\sim
	Primary Server: Select a server \lor \bigcirc	C
	Jitter Prevention: Open	
	Advanced Settings: Advanced Settings	
b	Set parameters of the standby RADIUS server and click OK	
	RADIUS Server Configuration X	
	* Server Name:	
	radius_1	
	* Server IP:	
	192.168.1.1	
	Authentication Por:	
	1812	
	Accounting Port:	
	1813	
	* Communication Key:	
	ruijie	
	Cancel	

c If the standby RADIUS server exists, click in the **Standby Server** line. Set parameters of the standby RADIUS server and click **OK**

RADIUS Server Configuration	×
* Server Name:	
radius_2	
* Server IP:	
192.168.1.2	
Authentication Por:	
1812	
Accounting Port:	
1813	
* Communication Key:	
ruijie	
Cancel	OK

d In order to prevent users from repeatedly requesting authentication in a short period of time, you can enable **Jitter Prevention** and set the jitter prevention duration (0–600s).

Jitter Prevention:	✓ Open 0-600	
* Time:	Please enter the time.	s

e Click Advanced Settings to check the radius server list.
nmon Paramete	ers				
	N	AS IP:			
	Accounting Upd	ate Inte 5	mir	nute	
ver Group List		Update			
ver Group List Server Name	wirelessConfig.server Ip	Update Authentication Port	Accounting Port	Communication Key	Acti
ver Group List Server Name radius_1	wirelessConfig.server Ip 192.168.1.1	Update Authentication Port 1812	Accounting Port	Communication Key ruijie	Acti

3. Authentication Configuration Description

Two authentication protocols are supported:

- **WiFiDog**: The protocol sends random dynamic passwords to users' mobile phones in the form of SMs. When the users use the wireless network, they enter the dynamic passwords on the authentication portal page to complete their identity real name verification, thereby ensuring the security of the wireless network.
- WeChat Connect Wi-Fi (3.X): It is an authentication way that can quickly connect to a Wi-Fi hotspot through WeChat. By scanning the QR code in WeChat, users can quickly connect to the Wi-Fi network provided by merchants for free Internet access. After the connection is successful, a status prompt "Connecting to Wi-Fi" will appear at the top of the main page of users' WeChat. Users can click this prompt to view the merchant's official account and special offer and use online functions and services provided by the merchant.

You can use the authentication component of Ruijie Cloud or an external authentication server for authentication.

• Using the authentication component of Ruijie Cloud

To use the authentication component of Ruijie Cloud, configure authentication for the network on Ruijie Cloud. For details, see <u>11.1 Captive Portal</u>.

		Auth:	✓ Open
		Auth Protocol:	WeChat Connect Wi-Fi (3.X)
Auth:	✔ Open	 Use MACC Use an ext 	C authentication component ⑦ for authentication settings ternal auth server
Auth Protocol:	WiFIDog V		
Use MACC Use an extremely set of the set of th	authentication component ⑦ for authentication settings	Seamless Online :	Open(This feature can be enabled only after it is
0			confirmed that this feature is supported by the
Seamless Online :	Open(This feature can be enabled only after it is		authentication server, and that in the authentication)
	confirmed that this feature is supported by the		
	authentication server, and that in the authentication)	STA Escape:	Open
User Offline Detection :	Open	User Offline Detection :	Open

Table 10-2	Description of Authentication Configuration Parameters

Parameter	Description
Auth Protocol	Set it to WiFiDog or WeChat Connect Wi-Fi (3.X).
Seamless Online:	Users only need to pass 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. To use this function, ensure that MAB authentication is enabled for the network so that authentication and Internet access can be normally performed.
	This parameter is valid when Auth Protocol is set to WeChat Connect Wi- Fi (3.X) .
STA Escape	After the feature is enabled, if the server is unavailable, users can automatically go online when no authentication page is displayed.
	You are not advised to enable it. Network packet loss can easily trigger escape.
User Offline Detection	After it is enabled, inactive users will go offline automatically. It is disabled by default, indicating that the device uses the default configuration.

Using an external authentication server

Auth:	✓ Open		
Auth Protocol:	WiFIDog V	Auth:	V Open
Use MACUse an ex	C authentication component ⑦ for authentication settings tternal auth server	Auth Protocol:	WeChat Connect Wi-Fi (3.X)
* ⑦Portal Server URL:		Use MACC	Cauthentication component ⑦ for authentication settings ternal auth server
* ⑦ Portal IP:		* Portal Server URL:	
* Gateway IP:		* Portal Server IP:	
Gateway ID(optional) (op	tí	* Nas IP:	
Portal Port (optional):		* Key:	
Redirect Mode :	JS Script Mode 🗸	Seamless Online :	Open(Enable(advised))
Seamless Online :	Open(Available only when Auth server supports the		
	function)	STA Escape :	Open
User Offline Detection :	Open	User Offline Detection:	Open

Table 10-3 Description of WiFiDog Authentication Configuration Parameters

Parameter	Description
Portal Server URL	It indicates the URL of the external wifidog portal server. After authentication is enabled on the device, unauthenticated users will be redirected to the URL when accessing the Internet.
Portal IP	It indicates the IP address of the portal server. Device communicates with the Portal server configured with this IP address.
Gateway IP	It indicates the gateway IP for wifidog.
Gateway ID	It indicates the gateway ID for wifidog.
Portal Port:	It indicates the port number for landing page redirection.
Redirect Mode	It supports JS Script Mode and HTTP302.
Seamless Online	It indicates seamless authentication on STAs connected to an SSID. The authentication server that supports the seamless feature is required.
User Offline Detection	After it is enabled, inactive users will go offline automatically. It is disabled by default, indicating that the device uses the default configuration.

Parameter	Description
Portal Server URL	It indicates the URL of the external wifidog portal server. After authentication is enabled on the device, unauthenticated users will be redirected to the URL when accessing the Internet.
Portal IP	It indicates the IP address of the portal server. Device communicates with the Portal server configured with this IP address.
NAS IP	It indicates the source IP address used by the device to send RADIUS packets.
Кеу	It indicates the communication key.
Seamless Online:	It indicates seamless authentication on STAs connected to an SSID. The authentication server that supports the seamless feature is required.
STA Escape	This parameter is valid when Auth Protocol is set to WeChat Connect Wi- Fi (3.X) . After the feature is enabled, if the server is unavailable, users can automatically go online when no authentication page is displayed. You are not advised to enable it. Network packet loss can easily trigger escape.
User Offline Detection	After it is enabled, inactive users will go offline automatically. It is disabled by default, indicating that the device uses the default configuration.

Table 10-4 Description of Wechal Connect Wi-11 (S.A) Authentication Connectation Faramete	Table 10-4	Description of WeChat Connect Wi-F	i (3.X) Authentication	Configuration Parameter
---	------------	---	------------------------	--------------------------------

10.2.2 Radio Settings

- Log in to Ruijie Cloud, choose Project > Configuration > Devices > Wireless > SSID, and select a network in this account.
- (2) On the **Radio** setting page, click reaction to **Radio** and set parameters. Up to 3 Radios can be added.

Radio			
Radio1(2.4GHz)	Radio2(5GHz)	Radio3 @ (2.4GHz or 5GHz)	Scan 🔿 Access
ON/OFF	ON/OFF	ON/OFF	
Max Clients	Max Clients	Max Clients	

ON/OFF: If this RF switch is turned off, all SSIDs in this frequency will be disabled and the clients can not access the Internet.

Max Clients: The maximum number of users set will take effect as the maximum number of users if it exceeds the maximum number of users actually supported by the AP; leave it blank to turn off the user limit.

Radio3: It is supported on some models. Supports configuring the operating mode.

Scan: Radio3 is used for collecting RF information around an AP. The client access service is unavailable.

Access: Radio3 is used for wireless coverage. The client access service is available.

(3) After configuration, click Save.

							Save More -
Wireless Configurati	on						~
SSID O							
WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Mode	Action
1	ruijie_test	Open	No	Bridge	1,2	Auth Disabled	e ji
		First Previous	Page 1	of 1 Next Last			10 a 1 in total
Radio							
Radio1(2.4GHz)		Radio2(5GHz)			Radio3	Scan 🔿 Access
ON/OFF		ON/OFF				ON/OFF	
Max Clients		Max Clients				Max Clients	
Note: The "Teinet Settings",	"Client Isolation" and "Wireless Intr	usion Detection" functions can only be	enabled on Ruijie E	nterprise devices.			
Security							~
eWeb 🛛							
eWeb 🔍							
Password	← Configure	Password					

10.3 Radio

Overview

The country code ensures each radio's broadcast frequency bands, interfaces, channels, and transmit power levels conform to country-specific regulations. The frequency bandwidth determines how many non-overlapping channels can be used for your AP to reduce RF interference.

The best practice for user experience is 2.4 GHz in 20 MHz and 5 GHz in 40 MHz.

Procedure

Log in to Ruijie Cloud. Choose **Project** > **Configuration** > **Devices** > **Wireless** > **Radio** and select a network in this account. Set parameters in the **Radio settings** area and **Manual Planning** area.

Radio settings

Configures parameters in the Radio settings area. After configuration, click Save.

Radio settings		
Country or Region:	America(US)	\sim
RF1(2.4G) Default Channel Width :	20MHz	\vee
RF2(5G) Default Channel Width :	40MHz	\sim
RF3(5G) Default Channel Width :	40MHz	\vee

2110
 ave

Country or Region: Select a country code.

RF1(2.4G) Default Channel Width: Configure the default channel width of RF1.

RF2(5G) Default Channel Width: Configure the default channel width of RF2.

RF3(5G) Default Channel Width: Configure the default channel width of RF3.

Manual Planning

O Configure a single device: Select an AP and configure the channel and power of radios. After configuration, click **Apply**.

	SN	MAC	Allac	RF 1 (2.	.4G)	RF 2 (5G)	RF 3 (5G)	configuration details
	an	mAAC.	Alids	Channel	Power	Channel	Power	Channel	Power	SN: NAEK009FH0007
۲	NAEK009FH0007	00d2.f800.9f71								Country or Region: America(US) • RadioFrequence 1(2.4Ghz)
	NAEK009FH0008	00d/2.f800.9f81								Channel: 2
	NAEK009FH0009	00d2.f800.9f91								Power: 100
	NAEK009FH0010	00d2.f800.9f01								RadioFrequence 2(5Ghz)
	NAEK009FH0011	00d2.f800.9f11								Power: 90
							5 in tot	al < 1 > (10 / page 🗸	RadioFrequence 3(SGhz) Channel: Default Configuration
										Power:

SN: indicates the SN of an AP.

MAC: indicates the MAC address of an AP.

Device Name: indicates the AP name.

RadioFrequence > **Channel**: Check the current channel of radios.

RadioFrequence > Power: Check the local power of radios.

O Bulk configure devices (all devices) in a band: Click **Bulk set power for device groups**, select a band, and configure power. After configuration, click **OK**.

Bulk set power for device groups							
RadioFrequence:	RF 2 (5G)						
Power:	95	%					
	Cancel	ОК					

O Bulk configure devices (specified devices) in multiple bands: Click Import Data to go to the configuration import page. Click Download Template to download the template and fill in the template (SN is mandatory). After filling, save the file and click Please select an .xls or .xlsx file to complete configuration import.

SN	Import Data	DE 4 75 461	DF 3 /F 2)	×
NAEK009FH0007	Please fill in the file with locatio	n information before import	t(Up to 500 records can be imported each	n time.)
NAEK009FH0008				
NAEK009FH0009		企		
NAEK009FH0010				
NAEK009FH0011				

O Export current configuration: Click Export Data to export configuration data to an .xlsx file.



10.4 Rate Limit

10.4.1 Overview

It supports User Rate Limit, Wireless Rate Limit, AP Rate Limit, and Packet Rate Limit. If multiple rate limit modes are configured for one client, their priorities are as follows: User Rate Limit > Wireless Rate Limit > AP Rate Limit.

- User Rate Limit: You can configure wireless STA-based rate limit to limit or guarantee the required bandwidth for specific STAs. The maximum number of supported rules is 512 users.
- Wireless Rate Limit: You can configure per-user rate limit, dynamic rate limit, and other functions for designated SSIDs.
 - O Per-user rate limit indicates that all STAs associated with the SSID equally share the rate limit.
 - o All-user rate limit indicates that all STAs associated with the SSID equally share the configured rate limit.
- AP Rate Limit: You can use this function to configure network-wide client rate limit. All clients on the network will share the configured rate limit.
- Packet Rate Limit: You can use this function to set downlink rate limit for broadcast and multicast packets. If the Internet is frozen without heavy traffic during normal use, you are advised to adjust the rate between 1 kbit/s and 512 kbit/s. A lower rate ensures better Internet experience.

10.4.2 User Rate Limit

- Log in to Ruijie Cloud, choose Project > Configuration > Devices > Wireless > Rate Limit, and select a network in this account.
- (2) Confirm that Wireless Rate Limit (enabled by default) is enabled.
- (3) On the **User** tab, click (+) to go to the configuration page.

Wireless Rate Limit												
User	Wireless	AP Pa	acket									
User Rat	e Limi 🕀											
You can cor The maximu	nfigure wireless S um number of su	TA-based rate limit t apported rules is 512	o limit or guarantee the requi users.	ired bandwidth for specifi	ic STAs.							
Client M	AC Address	Uplink (kbps)	Downlink (kbps)	Description	Action							
			No Data									
			NU Data									

(4) Configure the MAC address of the client whose rate needs to be limited and the rate limit value. After configuration, click **Save**.

Add		>
* Client MAC Address	Format: 00:11:22:33:44:55.	
* Uplink rate limit	No limit by default. Range: Kbps V Current rate is 0 kbit/s. Range: 1-1700000 kbit/s.	
* Downlink rate limit	No limit by default. Range: Kbps Current rate is 0 kbit/s. Range: 1-1700000 kbit/s.	
Description	Please enter the description	
	Cancel	Save

10.4.3 Wireless Rate Limit

- Log in to Ruijie Cloud, choose Project > Configuration > Devices > Wireless > Rate Limit, and select a network in this account.
- (2) Confirm that Wireless Rate Limit (enabled by default) is enabled.
- (3) On the **Wireless** tab, select the Wi-Fi service whose rate needs to be limited and click **Change** in the **Action** column to go to the configuration page.

I	Wireles	Rate Limit		
	User	Wireless	AP	Packet
W	/ireless	Rate Limit	Group:	AuTo1676 ∨

You can configure per-user rate limit, dynamic rate limit, and other functions for designated SSIDs. Per-user rate limit indicates that all STAs associated with the SSID equally share the rate limit. All-user rate limit indicates that all STAs associated with the SSID equally share the configured rate limit.

The priority of this rate limiting mode is lower than that of user-based rate limiting mode.

WiFi Name / SSID	Uplink rate limit	Downlink rate limit	Action
@Ruijie-sD1E9	No limit	No limit	Change Clear
22	No limit	No limit	Change Clear
公寓6	No limit	No limit	Change Clear
准出测试WLAN8	No limit	No limit	Change Clear
		4 in 1	total < 1 > 10 / page <

(4) Configure the rate limit modes for the uplink and downlink directions and rate limit values. After configuration, click **Save**.

Uplink rate limit	Per-user rate limit Share	d by all users
* Rate limit	No limit by default.	Kbps 🗸
	Current rate is 0 kbit/s. Range: 1-17	00000 kbit/s.
Downlink rate limit	• Per-user rate limit O Share	d by all users
Downlink rate limit * Rate limit	Per-user rate limit Share No limit by default.	d by all users Kbps V

10.4.4 AP Rate Limit

- Log in to Ruijie Cloud, choose Project > Configuration > Devices > Wireless > Rate Limit, and select a network in this account.
- (2) Confirm that Wireless Rate Limit (enabled by default) is enabled.
- (3) On the AP tab, enable the uplink and downlink rate limit functions and configure the rate limit values. After configuration, click Confirm.

Wireless	s Rate Limit 🧲	D								
User	Wireless	AP	Packet							
AP Rate	Limit									
You can use limit. The priority mode.	this function to co of this rate limitin	onfigure net g mode is lo	work-wide clien wer than that c	t rate limit. A	All clients rate limi	on the n	etwork v le and S	vill share SID-base	e the con ed per-us	figured ra
Up	olink rate limit	D								
	0			Kbps 🗸	0					
	Cu	rrent rate is () kbit/s. Range:	1-1700000 k	dbit/s.					
Down	nlink rate limit 🧲	D								
	0			Kbps 🗸	0					
	Cu	rrent rate is () kbit/s. Range:	1-1700000 k	cbit/s.					
		Confirm								

10.4.5 Packet Rate Limit

- Log in to Ruijie Cloud, choose Project > Configuration > Devices > Wireless > Rate Limit, and select a network in this account.
- (2) Confirm that Wireless Rate Limit (enabled by default) is enabled.
- (3) On the **Packet** tab, select the type of broadcast/multicast packets whose rate needs to be limited, and configure the rate limit value. After configuration, click **Confirm**.

User	Wireless	AP	Packet
Packet R	ate Limit		
l'ou can usi you are adi	e this function to set rised to adjust the ra	downlink ra te between	te limits for broadcast and multicast packets. If the Internet is frozen without heavy traffic during normal use, 1 kbit/s and 512 kbit/s. A lower rate ensures better Internet experience.
Restric	t broadcast packets	O Disable	d 🔘 Restrict all 💿 Restrict part
		ARP Pac	kets DHCP Packets
Restri	ct multicast packets	 Disable 	d 🔘 Restrict all 💿 Restrict part
		MDNS F	Packets SSDP Packets
	* Restrict limit	0	Kbps 🗸
		Current rate	e is 0 kbit/s. Range: 1-1700000 kbit/s.

10.5 Load Balancing

Overview

Load balancing ensures that clients are evenly distributed across member APs, thereby using resources efficiently.

Load balancing can be achieved by assigning all the APs in the same area to the same load balancing group to control the access of wireless clients. For example, there are 15 clients associated with AP1, 10 associated with AP2, and the current threshold configured is 2. The client different between the two APs is 5, which is greater than the threshold. Therefore, subsequent users will be associated with AP2.

Limitations

Load balancing is only supported by Reyee Network and AP with P32 or a higher version, and there must be a Reyee EG on the network.

Procedure

- Log in to Ruijie Cloud, choose Project > Configuration > Devices > Wireless > Load Balancing, and select a network in this account.
- (2) Click $\textcircled{\oplus}$ to add a load balancing group.

Load Balancing 🕒 Supported by Reyee Network and AP with version P32 and later

Type

Note: Load balancing can be achieved by assigning all the APs in the same area to the same load balancing group to control the ac with AP2, and the current threshold configured is 2. The client different between the two APs is 5, which is greater than the threshold configured is 2.

Group Name

Rules

(3) Configure parameters for the load balancing group, including **Group Name**, **Type**, **Rule**, and **AP Member**. After configuration, click **OK**.

ad Balancing Group)							
* Group Name:								
Type:	Client Loa	ad Balancing					~	
Rule:	When an	AP is associat	ed with 3	, clients and the diff	erence between the o	currently associated	client count and client count on	
	the AP wi	th the lightest for 10	times, the client will b	, clients can associ e allowed to associat	ate only to another A ed to the AP upon th	P in the group. Afte e next attempt.	r a client association is denied	
AP Member: Selected(0 Selected) Show only grouped								
	Device	Name or SN					Q,	
		Alias	SN	IP	Model	AP Group	Firmware Version	
		Ruijie	NAEK0060H0007	10.170.0.41	RAP1260(G)	No Data	ReyeeOS 1.202.1915	
		Ruijie	NAEK0060H0008	10.170.0.41	RAP1260(G)	No Data	ReyeeOS 1.202.1915	
		Ruijie	NAEK0060H0009	10.170.0.41	RAP2260(G)	No Data	ReyeeOS 1.206.2020	
		Ruijie	NAEK0060H0010	10.170.0.41	RAP2260(G)	No Data	ReyeeOS 1.206.2020	
		Ruijie	NAEK0060H0011	10.170.0.41	RAP2260(G)	No Data	ReyeeOS 1.206.2020	
						5 in te	otal < 1 > 10 / page >	

Cancel OK

Group Name: indicates the load balance group name.

Type: indicates the type of load balancing (client or traffic).

Rule: indicates the rule of load balancing group.

AP Member: indicates the AP added to the group.

Implementation of client and traffic load balancing are as follows:

o Client Load Balancing: When an AP is associated with *n* clients and the difference between the currently associated client count and client count on the AP with the lightest load reaches *n*, clients can be associated only with another AP in the group. After a client association is denied by an AP for *n* times, the client will be allowed to be associated with the AP upon the next attempt.

Add Load Balancing Group								×					
* Group Name:	client												
Type:	Client Loa	id Balancing											
Rule:	When an	AP is associat	red with 3	, clients and the diff	erence between the c	urrently associated	client count and client count on						
	the AP wit	ne AP with the lightest load reaches 3 , clients can associate only to another AP in the group. After a client association is denied y an AP for 10 times, the client will be allowed to associated to the AP upon the next attempt.											
AP Member:	Selected(2 Selected) Name or SN					Show only grouped APs						
		Alias	SN	IP	Model	AP Group	Firmware Version						
		Ruijie	NAEK0060H0007	10.170.0.41	RAP1260(G)	No Data	ReyeeOS 1.202.1915						
		Ruijie	NAEK0060H0008	10.170.0.41	RAP1260(G)	No Data	ReyeeOS 1.202.1915						
		Ruijie	NAEK0060H0009	10.170.0.41	RAP2260(G)	traffic	ReyeeOS 1.206.2020						
		Ruijie	NAEK0060H0010	10.170.0.41	RAP2260(G)	traffic	ReyeeOS 1.206.2020						
		Ruijie	NAEK0060H0011	10.170.0.41	RAP2260(G)	No Data	ReyeeOS 1.206.2020						
						5 in to	otal < 1 > 10 / page >						
							Cancel	ОК					

o Traffic Load Balancing: When the traffic load on an AP reaches *n* multiplied by 100 kbit/s and the difference between the current traffic and the traffic on the AP with the lightest load reaches *n* multiplied by 100 kbit/s, clients can be associated only with another AP in the group. After a client association is denied by an AP for *n* times, the client will be allowed to be associated with the AP upon the next attempt.

	p								
* Group Name:	traffic								
Type:	Traffic Loa	ad Balancing					~		
Rule :	When the lightest lo	e traffic load o pad reaches	n an AP reaches 5 5 *100Kbps, cliu	*100Kbps and the ents can associated o	ne difference betweer nly to another AP in t	n the current traffic ar he group. After a clie	nd the traffic on the AP with the nt association is denied by an		
		a	pbalanceby03ernp4.						
AP Member:	Selected(2 Selected)					Show only grouped APs		
		Device Name or SN Q							
	Device	Name or SN					٩		
	Device	Name or SN Alias	SN	IP	Model	AP Group	Q.		
		Name or SN Alias Ruijie	SN NAEK0060H0007	IP 10.170.0.41	Model RAP1260(G)	AP Group	Q Firmware Version ReyeeOS 1.202.1915		
		Name or SN Alias Ruijie Ruijie	SN NAEK0060H0007 NAEK0060H0008	IP 10.170.0.41 10.170.0.41	Model RAP1260(G) RAP1260(G)	AP Group client client	C Firmware Version ReyeeOS 1.202.1915 ReyeeOS 1.202.1915		
		Name or SN Alias Ruijie Ruijie Ruijie	SN NAEK0060H0007 NAEK0060H0008 NAEK0060H0009	IP 10.170.0.41 10.170.0.41 10.170.0.41	Model RAP1260(G) RAP1260(G) RAP2260(G)	AP Group client client No Data	C Firmware Version ReyeeOS 1.202.1915 ReyeeOS 1.202.1915 ReyeeOS 1.206.2020		
		Alias Alias Ruijie Ruijie Ruijie Ruijie	SN NAEK0060H0007 NAEK0060H0008 NAEK0060H0009 NAEK0060H0010	IP 10.170.0.41 10.170.0.41 10.170.0.41 10.170.0.41	Model RAP1260(G) RAP1260(G) RAP2260(G) RAP2260(G)	AP Group Client Client No Data No Data	C Firmware Version ReyeeOS 1.202.1915 ReyeeOS 1.202.1915 ReyeeOS 1.206.2020 ReyeeOS 1.206.2020		
		Name or SN Alias Ruijie Ruijie Ruijie Ruijie	SN NAEK0060H0007 NAEK0060H0008 NAEK0060H0009 NAEK0060H0010 NAEK0060H0011	IP 10.170.0.41 10.170.0.41 10.170.0.41 10.170.0.41 10.170.0.41	Model RAP1260(G) RAP1260(G) RAP2260(G) RAP2260(G) RAP2260(G) RAP2260(G)	AP Group client client No Data No Data No Data	ReyeeOS 1.202.1915 ReyeeOS 1.202.1915 ReyeeOS 1.202.1915 ReyeeOS 1.206.2020 ReyeeOS 1.206.2020 ReyeeOS 1.206.2020 ReyeeOS 1.206.2020		
		Name or SN Alias Ruijie Ruijie Ruijie Ruijie	SN NAEK0060H0007 NAEK0060H0008 NAEK0060H0009 NAEK0060H0010 NAEK0060H0011	IP 10.170.0.41 10.170.0.41 10.170.0.41 10.170.0.41 10.170.0.41	Model RAP1260(G) RAP1260(G) RAP2260(G) RAP2260(G) RAP2260(G) RAP2260(G)	AP Group Client Client No Data No Data No Data S in ter	ReyeeOS 1.202.1915 ReyeeOS 1.202.1915 ReyeeOS 1.202.1915 ReyeeOS 1.206.2020 ReyeeOS 1.206.2020		
		Name or SN Alias Ruijie Ruijie Ruijie Ruijie	SN NAEK0060H0007 NAEK0060H0008 NAEK0060H0009 NAEK0060H0010 NAEK0060H0011	IP 10.170.0.41 10.170.0.41 10.170.0.41 10.170.0.41	Model RAP1260(G) RAP1260(G) RAP2260(G) RAP2260(G) RAP2260(G)	AP Group client dient No Data No Data S in tot	Q Firmware Version ReyeeOS 1.202.1915 ReyeeOS 1.202.1915 ReyeeOS 1.206.2020 ReyeeOS 1.206.2020 ReyeeOS 1.206.2020 ReyeeOS 1.206.2020 Image: ReyeeOS 1.206.2020 ReyeeOS 1.206.2020 Image: ReyeeOS 1.206.2020		

(4) After configuring the load balancing group, click Save at the upper right corner of the Load Balancing page.

e: Load balancing ca client different betw	an be achieved by assig ween the two APs is 5,	ning all the APs in the same area to the same load balancing group to control the access of wireless clients. For example, there are 15 clients associated with AP1, 10 associated with AP2, and the only is greater than the threshold. Therefore, subsequent users will be associated with AP2.	current threshold co	onfigured is 2.
Group Name	Туре	Rules	AP Member	Action
traffic	Traffic Load Balancing	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 associated 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 associated to the AP upon the next attempt.	2 tip	Edit Delet
client	Client Load Balancing	When an AP is associated with 3,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 association is denied by an AP for 10 times, the client will be allowed to associated to the AP upon the event attempt.	2 tip	Edit Delet

The Action column is described as follows:

- o Edit: Click this button to modify configuration parameters except Group Name.
- o **Delete**: Click this button to delete a specified load balancing group.

After modifying load balancing group parameters or deleting a load balancing group, click **Save** at the upper right corner.

10.6 Client Blocklist and Allowlist

Overview

The purpose of the **Client Blocklist and Allowlist** feature is to deny/allow wireless clients to access Wi-Fi networks. You can configure the global blocklist and allowlist for all Wi-Fi networks or the blocklist and allowlist for a specified SSID. The blocklist and allowlist feature supports matching the MAC address prefixes (OUIs) of clients.

Client Blocklist: Clients on the blocklist are banned from connecting to Wi-Fi networks and clients not on the blocklist are not restricted.

Client Allowlist: When the allowlist is not empty, only clients in the allowlist are allowed to connect to Wi-Fi networks and those not on the allowlist are banned from connecting to the Wi-Fi networks.

🛕 Caution

- The function is only supported on **Reyee APs**.
- When the allowlist is empty, the Wi-Fi allowlist does not take effect, that is, all MAC addresses are allowed to connect to Wi-Fi networks.

Configuration Steps

- Log in to Ruijie Cloud, choose Project > Configuration > Devices > Wireless > Wireless Block/Allow, and select a network in this account.
- (2) Select the scope (SSID-based or Global-based), in which the blocklist or allowlist takes effect, in the list on the left.

Client Blacklist and Whitelist						
The purpose of Wi-Fi blacklist and whitelist feature in Effective Rules: 1. In the blacklist mode, blacklisted of configured.	is to deny/allow wireless clients to access WI-FI. clients cannot connect to Wi FI. 2. In the whitelist mode and	d when the list is not empty, clients not on the whitelist cannot con	nnect to Wi Fi. 3. A maximum of 256 MAC addresses can be			
SSID-based test Global-based	List Type: Prohibit the following MAC addr Only allow the following MAC ac Add MAC Delete MAC	esses to connect to Wi-Fi (blacklist) Idresses to connect to Wi-Fi (whitelist)				
Global Configuration	MAC	Description	Action			

(3) Select the blocklist/allowlist mode. The default mode is blocklist mode. When you switch the mode, click **OK** in the pop-up prompt box to make the mode take effect.

	Only allow the following MAC addr	esses to connect to Wi-Fi (whitelist)	
bal-based	Add MAC Delete MAC		
lobal Configuration	MAC	Description	Action
		No Data	

want to switch to the whitelist mode?



(4) Click Add MAC. On the Add MAC page, add MAC address prefixes or MAC addresses. After adding, click OK.

Add MAC	×	Add MAC ×
OUI Complete MAC		OUI Complete MAC
Note: For an OUI MAC, you only need to enter the first six digits of the MAC address, and all MAC addresses matching the first six digits will take effect (applicable to the case where the first six digits of the device MAC is the same).	2	Note: For a complete MAC, you must enter the complete MAC address and only the device which match the complete MAC will take effect (applicable to the case where the first six digits of the device MAC are different).
Not more than 16 characters. One Chinese character takes three bytes) separated by commas. One record pe line. Example:00:00:00, Li Yang's Mobile Number 10:00:00:10, Lii's Mobile Number	r	Enter the complete MAC address (uppercase letters) and remarks (Chinese characters, English letters, numbers, underscores, ·, # or @. Not more than 16 characters. One Chinese character takes three bytes) separated by commas. One record per line. Example: 000000020008, Li Yang's Mobile Number:000010:02008, Lill's Mobile Number
Cancel	ж	Cancel

- OUI: For an OUI MAC, you only need to enter the first six digits of the MAC address, and all MAC addresses matching the first six digits will take effect (applicable to the case where the first six digits of the device MAC is the same).
- Complete MAC: For a complete MAC, you must enter the complete MAC address and only the device which match the complete MAC will take effect (applicable to the case where the first six digits of the device MAC are different).
- (5) After completing the blocklist/allowlist configuration, click Save at the upper right corner of the Client Blocklist and Allowlist page.

Client Blacklist and Whitelist				Save
The purpose of Wi-Fi blacklist and whitelis Effective Rules: 1. In the blacklist mode, bla configured.	st feature is to deny/allow wireles acklisted clients cannot connect t	: clients to access Wi-Fi. o Wi Fi. 2. In the whitelist mode and when the list is not em	pty, clients not on the whitelist cannot connect to Wi Fi. 3. A m	aximum of 256 MAC addresses can be
SSID-based	List Type: • Pro	phibit the following MAC addresses to connect to V	Vi-Fi (blacklist)	
test		ly allow the following MAC addresses to connect t	o Wi-Fi (whitelist)	
Global-based		elete MAC		
Global Configuration		MAC	Description	Action
		00:00:01 OUI		Delete
				1 in total $\langle 1 \rangle$ 10 / page \vee

The Action column is described as follows: To delete a rule, click **Delete** in the Action column, click **OK** in the pop-up prompt box, and then click **Save** at the upper right corner.

Client Blacklist and Whitelist				Save
The purpose of Wi-Fi blacklist and whitelist feature Effective Rules: 1. In the blacklist mode, blacklisted configured.	is to deny/allow wireless cli clients cannot connect to W	ents to access WI-FI. I FI. 2. In the whitelist mode and when the list is not e	mpty, clients not on the whitelist cannot connect to Wi Fi.	3. A maximum of 256 MAC addresses can be
SSID-based	List Type: 💿 Prohil	bit the following MAC addresses to connect to	v Wi-Fi (blacklist)	
test	Add MAC Dele	te MAC	to with (wintenst)	
Global-based				Or Are you sure you want to delete this MAC?
Global Configuration		MAC	Description	Cancel OK
		00:00:01 OUI		Delete
				1 in total <1 > 10 / page $>$

10.7 AP VLAN

Overview

This feature can be used to deliver the port VLAN configuration to multiple designated devices.

Limitations

This feature only supports EAPs/RAPs with a version of P32 and later in AP mode.

Procedure

- Log in to Ruijie Cloud, choose Project > Configuration > Devices > Wireless > AP VLAN, and select a network in this account.
- (2) Set parameters on the AP Port VLAN page. After configuration, click Apply to deliver the configuration.

AP Port VLAN

Note: This feature can be used to deliver the configuration to multiple designated devices, This feature only supports EAPs/RAPs with a version of P32 and later in AP mode.

Device:							
	Enter device	alias, SN, or IP ad	Q 3 Selected			t	isplay Never Contigured Device
		Alias		SN	IP	Model	Last Configuration Time
		Ruijie	NAEKOO	7BH0009	192.168.110.9	RAP2260(G)	2023-02-13 16:19:33
		Ruijie	NAEKOO	07BH0010	192.168.110.10	RAP2260(G)	2023-02-13 16:19:33
	193	Duilio	NAFKO	17RH0011	192 168 110 11	P6P2260/G1	2023-02-13 16:19:33
onfiguration:							
			Port Type:	Access			×
			VLAN ID:	50			
			Port:	LAN		U r	selected S elected
					LAN		

Device Model: indicates the AP model.

Device: indicates the device to which the configuration needs to be delivered.

Port Type: indicates the port type, which is access or trunk.

VLAN ID: indicates the VLAN ID of a port.

Selected Ports: Select the port to which the VLAN ID needs to be delivered.

Apply && Clear: Apply the configuration to the device or clear the configuration.

(3) Access the AP's Eweb and check the VLAN ID and port VLAN configuration.

Overview	Basics Y Wireless Y Advanced Y Diagnostics Y System Y		
LAN Settings	Port VLAN		
🥖 LAN S	ttings		
Port VLAN) ngs		- Add 🗇 Delete Selected
Up to 4 er	tries can be added.		
	VLAN ID	Remark	Action
	50	-	Edit Delete

Overview Basics Vireless Advanced Dia	ignostics 🎽 System 🐃
LAN Settings Port VLAN	
Port VLAN Please choose LAN Settings to create a VLAN first and co	onfigure port settings based on the VLAN.
Port VLAN	
Connected Disconnected	
	Port 1
VLAN 1(WAN)	Not Joir 🗸
VLAN 50	UNTAG 🗸

11 Authentication Configuration

11.1 Captive Portal

You can use the **Captive Portal** feature to set authentication policies, including customizing authentication pages, setting authentication network segments, SSID, and other information.

When a user is connected to a wireless or wired network, the system will display a landing or login page that may require authentication, payment, acceptance of an end-user license agreement, acceptable user policy, survey completion, or other valid credentials that both the host and user agree to adhere by.

The network security can be enhanced by configuring the Captive Portal.

Procedure

(1) Choose Configuration> Auth & Accounts > Authentication > Captive Portal.



(2) Click Add Captive Portal to add a captive portal.

Captive Portal ③		
		New Authentication Function New version upgrade, support AP/Gatgeway unified configuration Support multiple login methods, one-click login, Voucher, Account, SMS verification, registered account Support multi-language and flexible customization of Portal pages. Add Captive Portal
Add Captive Portal		
Policy Info		
Policy Name:		
Policy Mode ③:	Inner	
SSID:		
Seamless Online:		
Seamless Online Period:	1 Day	×]
Portal Escape :		
Portal Page ③		
Current Project Shar	ed Portals	
Add Page		
3		
One-click Login		
	the in	
1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1		
Test	1	

a Configure basic information about the captive portal.

Parameter	Description			
Policy name	Indicates the name of a captive portal.			
	Indicates the authentication mode to which the captive portal applies:			
	• Inner: Cloud-based authentication. The built-in authentication server in the public cloud is used for authentication.			
Policy Mode	• Local: Device-based local authentication and acceleration. Portal pages and accounts in the cloud are synchronized with the device for local authentication and acceleration.			
	• External : Third-party authentication, facilitating integration between the device and a third-party authentication server for authentication.			
	Indicates the device that performs the authentication.			
	• When there is a router on the network, you are advised to enable authentication on the router. You can perform authentication on either an access point (AP) or a router.			
	AP: An AP acts as the NAS.			
	• Router: A router or gateway acts as the NAS responsible for performing authentication at the gateway exit.			
Authentication Device	• Reyee AP Authentication: RAP/EWR, ReyeeOS 1.219 or later version.			
	 Reyee EG WiFiDog Authentication: EG/EGW, ReyeeOS 1.202 or later version. 			
	 Reyee EG Local Authentication: EG210G-E, EG210G-P-E, EG310GH-E, EG310GH-P-E, EG305GH-E, EG305GH-P-E, ReyeeOS 1.230 or later version. 			
	Enterprise EGs support local authentication			
	This parameter is not required if the policy mode is Local.			
	Indicates the wired network that requires authentication. Enter the network segment in this field.			
Notwork	Lears connecting to the wired network corresponding to this network cognon			
	must be authenticated			
	This parameter is required if the Authentication Device is Router.			
	Indicates the network name of the Wi-Fi network that requires authentication.			
SSID	Users connecting to this wireless network must be authenticated.			
	This parameter is required if the Authentication Device is AP.			
	After this function is enabled, if the first authentication is successful,			
Seamless Online	subsequent connections to this Wi-Fi network will automatically be			
	authenticated within a certain period of time.			
	Indicates the time period for seamless online.			
Seamless Online Period	If the first authentication is successful, subsequent connections to this Wi-Fi			
	network will automatically be authenticated within this period of time.			

 Table 11-1
 Basic Information About the Captive Portal

Parameter	Description					
	Indicates the portal page that is displayed after portal authentication.					
Dortal Daga	Click Current Project to select the portal page for an existing project.					
Ponal Page	Click Shared Portals to select an existing portal page.					
	Click Add Page to customize a portal page.					

b To customize a portal page, the portal basic settings and portal visual settings of the device is required.

Dorto	Dage
Porta	Pade

Portal Basic Settings	
Portal Name:	
Login Options:	✓ One-click Login
	Access Duration (Min): Unlimited 15 30 60 Custom
	Voucher
	Account
	SMS
	Registration
	Facebook Account
Show Balance Page:	Disable (Available only when Auth server supports the function)
Post-login URL:	

Table 11-2	Basic Information	of the	Portal	Page
------------	--------------------------	--------	--------	------

Parameter	Description
Portal Name	Indicates the name of a captive portal template.
	Indicates the option to perform the desired action.
	One-click Login : indicates login without the username and password. You
Login Options	can set Access Duration and Access Times Per Day.
	Voucher: indicates login with a random eight-digit password.
	Account: indicates login with the account and password.
	SMS: indicates login with the phone number and code.
	Registration:
Show Balance Page	Indicates the available duration, time, or data after portal authentication.
Post-login URL	Indicates the URL that is displayed after portal authentication.

Portal Visual Settings			
Logo:		Mobile	Desktop
Logo Image:	Upload		
Logo Position:	°°		3
Background:	Picture ⑦ Solid Color		R
Background Image:			
	Upload		One-click Login
Background Mask Color:	#999999 10%		
Welcome Message:	● Text ○ Picture ⑦	and the second	the of the states of
English	+		The second
Welcome Text:	Enter less than 60 characters.		
Marketing Message:	Enter less than 60 characters.	5 - 6	
Terms & Conditions:			

Table 11-3 Visual Information of the Portal Page

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

Parameter	Description
Language	Select the language of the portal page.
Welcome Message	Select the welcome message with the image or text.
Marketing message	Enter the marketing message.
Terms & Conditions	Enter terms and conditions.
Copyright	Enter the copyright.
Login Button	Select the login button on the authentication page.
Welcome Message Text Color	Select the welcome message text color. The default value is #ffffff.
Welcome Message Text Size	Select the welcome message text size.
Button Color	Select the button color. The default value is #0066ff.
Button Text Color	Select the button text color. The default value is #ffffff.
Link Color	Select the link color. The default value is #ffffff.
Text Color in Box	Select the text color in the box. The default value is #ffffff.

c Click OK.

1 Note

- Considering the performance and good design of the page, one network supports up to 50 portal templates.
- The portal template supports multiple languages including Chinese (Simplified), Chinese (Traditional), English, German, Indonesian, Japanese, Korean, Malay, Portuguese, Russian, Spanish, Thai, Turkish, and Vietnamese.
- The preview image including mobile and desktop format. The actual effects vary with devices at different resolutions.

After the captive portal is successful configured on the cloud, relevant configurations will be automatically delivered to the device end.

11.2 User Management

11.2.1 Account

Account authentication allows the valid account to access the specified Wi-Fi.

Procedure

Log in to Ruijie Cloud, choose Project > Authentication > User Management, and select a network in this account.

Cancel

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

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

Add account		Х
* User name		
* Password		
* User group		~
Allow VPN connection		
Tips: By enabling this option,	he user can use this account to log in remotely using a VPN.	
User information setting $ \lor $		

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

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

User group: It indicates a user group. Select a user group from the drop-down list or click **Custom** to create a user group.

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

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

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

Step1: Download and fill in the device information in the template. Up to 500 records can be imported each time. Account and Password fields are required. Please enter less than 32 characters, consisting of letters, numbers or underscores.			×
Step1: Download 500 records can b	and fill in the device information e imported each time.	in the template. Up to	
Account and Passwor of letters, numbers or	rd fields are required. Please enter less th r underscores.	nan 32 characters, consisting	
	Please select an .xls or .xlsx file	Download Template	

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

1 Note

- Account, Password, and User Group are mandatory.
- Check that the user group already exists and the added accounts are not duplicate with existing accounts. For details about how to create a user group, see <u>11.2.3</u> User Group.

11	5	~	2	D	A	
Account	Password	First name	Last name	Alias	User group	Email
test2	test2				test	
test3	test3				test	
test4	test4				test	

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

Account	Voucher	User Group	< E-sharing	0							○ ▷ ೫•
Add acco	Add account Bulk import One-click send More v • Total Accounts: 3 • Activated Accounts: 0 • Expired Accounts: 0								Accou	nt Q	
	Account	Password	User group	Status ① =	Period	First name	Alias	Created at	Activated at	Ex	Operation
	test3	test3	test	Not used	30Minutes	Empty	Empty	2023-02-13 16:42:21	-		∠Cō
	test4	test4	test	Not used	30Minutes	Empty	Empty	2023-02-13 16:42:21	-		∠ C O
	test2	test2	test	Not used	30Minutes	Empty	Empty	2023-02-13 16:42:21	-		∠co

3 in total \langle 1 \rangle 10 / page \vee

Follow-up Operations

Account	Voucher	User Group	≪ E-sharing	0							€ ₽ ^{\$\$}
Add acco	Bulk impor	t One-click send	More v • T	otal Accounts: 3 🔹 A	Activated Accounts: () Expired Accounts: 0				Accou	nt Q
	Account	Password	User group	Status 🛈 🗉	Period	First name	Alias	Created at	Activated at	Ex	Operation
	test3	test3	test	Not used	30Minutes	Empty	Empty	2023-02-13 16:42:21			2 C 8
	test4	test4	test	Not used	30Minutes	Empty	Empty	2023-02-13 16:42:21			£ C 8
	test2	test2	test	Not used	30Minutes	Empty	Empty	2023-02-13 16:42:21			∠ C 0

3 in total < 1 > 10 / page \vee

The following figure shows the export result.

Account	Password	User	group		Period	First	narLa	st nam	Alias	Phone	nucreated	Activat	ecExpired	Devices	MAC	Bind	Traffic	Upload/D	VPN	Operat
test3	test3	test	Not	used	30Minute						2023-02	-1-	-	0/3	3		0 MB/10	0 Unlimite	Disabled	
test4	test4	test	Not	used	30Minute						2023-02	-1-	-	0/3	3		0 MB/10	0 Unlimite	Disabled	
test2	test2	test	Not	used	30Minute						2023-02	-1-	-	0/3	3		0 MB/10	0 Unlimite	Disabled	

• Click **One-click send** to email the accounts to employees.

	Passi	vord U	iser group	Status 🕕 🐨	Period	First name	Alias	Created at
test3	One-click	send						×
test4	Are you sur Tip: the foll	e to send emails to owing table lists th	the accounts you be accounts that have	have selected ? ve an email address.				
test2		Account	Password	User group	Created at	VPN	Account Status	Send Status 🐨
		test3	test3	test	2023-02-13 16:42:21	Disabled	Not used	Unsent
							1 in total <	1 > 10 / page ∨

11.2.2 Voucher

Voucher authentication on Ruijie Cloud allows you to charge users for wireless network access using access codes. The number of concurrent users, time, and data quota limit can be customized and offer to your guests.

Procedure

- Log in to Ruijie Cloud, choose Project > Authentication > User Management, and select a network in this account.
- (2) On the Voucher tab, click Add voucher.



(3) Configuring voucher parameters. After configuration, click OK.

Add voucher		×
* Quantity	2	
Quantity		
* User group	^]
	test	
User information setting $ \lor $	Custom	
Advance setting \checkmark		
	Cance	ОК

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

User group: Select a user group or click Custom to customize a new user group.

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

Advance setting:

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

Advance Setting 🔨	
Voucher code type	Alphanumeric 0-9, a-z ^
	Alphanumeric 0-9, a-z
Voucher length	Alphabetic a-z
	Numeric 0-9
	Cancel

O Voucher length: Select the voucher length. The value ranges from 6 to 9.

Voucher length	6	
	6	
	7	
	8	
	9	

(4) View the voucher list.

dd vo	ucher Print vouche	r More 🗸 💿	1otal Vouchers: 4	Activated Vouchers: 0	0	Voucher	Q FI
	Voucher code	User Group	Period	Created at	Activated at	Expired a	Operation
	fqyhwg	1	Unlimited	2022-08-12 18:34:31			LCO
	dxwgkh	1 Unlimite		2022-08-12 18:34:31	-	÷	∠ C ū
	t5nq76	t5nq76 1		2022-08-12 11:09:07		-	∠ C ū
	jsz75g	1	Unlimited	2022-08-12 11:09:07			LCO

Follow-up Operations

• Exporting the voucher

Accou	nt Voucher	User Group	≪ E-sharing	1							C 🗗 💱
Add voucher Print voucher More v • Total Vouchers: 222 • Activated Vouchers: 0 • Expired Vouchers: 0										् Filter प्र	
	Voucher code	User group	Status ① =	Price	Period	First name	Alias	Created at	Activated at	Ex	Operation
	22yyxk	test	Not used		30Minutes	Empty	Empty	2023-02-14 14:39:18	-		∠ C O
	23m7ge	test	Not used		30Minutes	Empty	Empty	2023-02-14 14:39:18	-		∠ C Ō
	2admh4	test	Not used		30Minutes	Empty	Empty	2023-02-14 14:39:18	-		∠ C Ö

• Printing the voucher

Click **Printing Voucher** and complete print configurations.

Accou	nt Voucher	Use	Tip: Only vouchers selecter	ed on current page will be printe	ed. ①	
Add vo	ucher Print vouch	er Mo	Print mode	Print (A4) in two columns		×
	Voucher code	User g	Custom Text			
	22yyxk	tes	Logo	default		Θ
	23m7ge	test		Ruijie		
	2admh4	test		default	dayu500KB	
	2crfwm	test		-	(han Shen Kemen She	
	2f7t2v	test		23-32	test	
	2hj7k4	tesi				
	2j5b7t	test		+ Add logo		
	2 6					Đ
			Profiles shown on the v 4 parameters can be selected at	oucher t most		
			Profile name Period Maximum upload rate	Maximum downlo	ad rate Concurrent of MAC binding	devices J

11.2.3 User Group

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

Account	Voucher	User Group	≪ E-sharing	i
+ Add				
			No Data	

(3) Configure user group parameters. After configuration, click **OK**.

Add user group		Х
* User group name	test	
	User Group Policy	
Price		
Concurrent devices	3	~
Period	30Minutes	~
Quota 🛈	100 MB	~
Maximum upload rate	Unlimited	~
Maximum download rate	Unlimited	~
Bind MAC on first use		
		Cancel OK

User Group Name: indicates the user group name.

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

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

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

Quota: indicates the maximum amount of data transfer.

Maximum upload rate: indicates the maximum upload rate.

Maximum download rate: indicates the maximum download rate.

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

(4) View the user group list. Click 🖉 or 📋 for a specified user group to modify or delete the user group.

Account	Voucher	User Group	E-sharing	í		
+ Add						
test		<u> </u>	Ť			
Maximum Maximum	Maximum upload rate: Unlimited ↑ Maximum download rate: Unlimited ↓					

11.3 PPSK

Overview

Per-user PSK (PPSK) is also called as "One Client, One Password". It combines advantages of PSK and 802.1X. Each terminal is bound to a unique Wi-Fi password to ensure secure Wi-Fi.

Limitations

- PPSK only supports import of 1500 passwords.
- PPSK is based on MAC address binding of terminals, and multiple devices of the same user also need to log in with different passwords.
- Each AP can only be configured with a PPSK authentication SSID.
- The PPSK password is generated randomly and does not support the customized password format.
- The AP can support PPSK only after being upgrade to B40P2 or a later version.
- There is no validity date for PPSK, which can be used all the time when it is created.
- PPSK can be created manually or through batch import.
- Only Ruijie AP support PPSK expect the AP130(L).
- Only the sub account user who is assigned with the root group can configure PPSK.

Procedure

- (1) Log in to Ruijie Cloud, choose Project > Authentication > PPSK, and select a network in this account.
- (2) Click **Add** to go to the PPSK account configuration page.

PPSK	E-sharing						
PPSK Ø							
Tip: Please disa	ble Private MAC when using	PPSK on iOS 14.					
Note: The PPSK	function can only be enable	ed on Ruijie Enterprise APs.					
					⊖ ⊵ 쀼・었		
Add	Delete			Account Client I	Q Search		
	Account	Client MAC	Wi-Fi Key	Created At	Action		
	No Data						
		First Previous Pade	0 of 0 Next Last		10 n 0 in total		

(3) You can import PPSK accounts in batches to add accounts or add them directly on the page. The default

account adding mode is batch import. Click	Add Account	or	Batch Import	at the lower left
		,		

corner of the page to switch the account adding mode.

Add Account	×	Add Account	×
Download and fill in the device information in the template.Up to 1500 records can be imported		Account 🛛 🔹 +	
Lipicad Template File Download Template			
Add Account Cion	e	Batch Import CK Cose	

• Adding PPSK accounts manually

On the Add Account page, enter an account name. Click + to add one row. After configuration, click **OK**.

Add Account		×	Add Account				×
Account test1	ê 🔂			Account	test1	ė.	
				Account		8 +	
Batch Import		OK Close	Batch Import				OK Close

- Adding PPSK accounts through batch import
 - a Click **Download Template** to download the template.

Add Account

 \times

Download and fill	I in the device information in	the template.Up to 1500 records can	be imported
	Upload Template File	Download Template	
Add Account			Close
b Edit the template a	and save it.		
Account			
T1			
T2			
T3			
14			
Click Upload Tem	plate File to upload the f	ile. After uploading, users are aut	omatically crea
Add Account			
Download and fil	I in the device information in	the template.Up to 1500 records can	be imported
	ppakTap	nplate (1).xls	
	ppskien		
	рряктен		
	рряктеп	Import	
Add Account	рряктеп	Import	Close

PPS	K E-sharing					
PPSK	0					
Tip: Pleas	se disable Private MAC when using PPSK a PPSK function can only be enabled on R	on iOS 14. uijie Enterprise APs.				
					Ð	⊭ ∷:•33
Add	Delete			Account	Client MAC	Q Search
	Account	Client MAC	Wi-Fi Key	Creat	nd At	Action
	T1	Format:ffff.ffff.ffff Bind	Sbkzhzgb	2023-02-15	16:59:03	B 1
	test1	Format:ffff.ffff.ffff Bind	ahgbm59r	2023-02-15	17:21:18	B 1
	Τ4	Format.ffff.ffff.ffff Bind	aidgcbsn	2023-02-15	16.59.03	B A
	test2	Format.ffff.ffff.ffff Bind	d5irv9q5	2023-02-15	17:21:18	B A
	T2	Format:ffff.ffff.ffff Bind	dj97htrz	2023-02-16	16.59.03	e i
	тз	Format:ffff.ffff.ffff Bind	jt252jif	2023-02-15	16.59.03	B 1
		First Previous Page	1 of 1 Next Last		10	6 in total

Account: indicates the name of PPSK account.

Client MAC: indicates the client's MAC address for this account.

WiFi Key: indicates the randomly generated 8-digit password for a PPSK account.

Created at: indicates the time when a PPSK account was created.

Action: indicates the View or Delete action. You can view the account to check the PPSK synchronization log.

PPSK Synchronize Log						
Synced: 0	Syncing: 0 Unsu Status	pported: 0 🛛 🔴 Fail	led: 0 Update Time	e		
No Data						
First	Previous Page	0 of 0	Next Last	10 🔺 0 in total		

(5) The PPSK key needs to be synchronized to all APs on the same network. Choose MONITORING > Devices > AP, select a device, and click Web CLI. Enter the show sumng user all command to check whether the PPSK Wi-Fi key is synchronized to the AP.

SN									Background color:	
General	>	Web CLI	sh sumng	user all		10				
Connectivity	>		Sumng Tot	tal Sta Num:		1				
Running Status	>		UserNa	ame Wifi	iKey	Account-Time	м	lac-Address	Reg-Time	
Client	>			t3qhkxjk	Mon Feb	28 15:52:11 2022	-	-		
WLAN	>			hn59m63s	Mon Fe	eb 28 15:52:11 2022	b	ce2.659a.8dbe	Mon Feb 28 15:52:11 2022	
Wireless Secu	>			fq6rnxky	Mon Feb	28 15:52:11 2022				
Web CLI	>			d6xff28w	Mon Fe	b 28 15:52:11 2022				
				8r4x53va	Mon Fe	b 28 15:52:11 2022 b 28 15:52:11 2022				
			Ruijie#	2rap88ri	Mon Feb	28 15:52:11 2022				

11.4 Allowlist

Choose **Authentication** > **Allowlist** to go to the allowlist configuration page.

DemoProject2 V	Pre-auth Whitelist			
☆ Workspace	Pre-Authentication Access Server List			
発 Smart Config	Add Delete			Search Q
Configuration	Туре	Information	Description	Action
Network-Wide >				
≇ Devices →				
Authentication >	Authentication	N	D Data	
Monitoring	Captive Portal			
& Network-Wide ⇒	Whitelist Free Client List			
Devices	Add Delete			Search Q
Clients >	Туре	Information	Description	Action
E Logs				
Delivery Center >				

11.4.1 Pre-Authentication Access Server List

(1) Pre-authentication URL list: It lists websites that can be accessed by users even if the users are not authenticated.

Click Add below **Pre-Authentication Access Server List**, select **URL**, and add a website. You can add a description for the website behind the website.

Pre-auth Whitelist Pre-Authentication Access Server List Add Delete			Search Q.
Туре	Information	Description	Action
	baidu.com		Delete
Authentication-Free Client List	Add Pre-Authentication Access Server	×	Total 1 Items < 1 > 10/page ∨ Search Q
Type	URL IP http:///	Cancel OK	Action
9	<u>192.168.110.1</u>	Empty	Delete
	22-22-22-22-22-22	22	Delete
	11:22:33:44:55:66	Empty	Delete

(2) Pre-authentication IP list: It lists external network IP addresses that can be accessed by all users including unauthenticated users.

Click Add below **Pre-Authentication Access Server List**, select **IP**, and add an IP address. You can add a description for the IP address behind the IP address.

Pre-auth Whitelist			
Pre-Authentication Access Server List			
Add Delete			
Туре	Information	Description	Action
	baidu.com		Delete
			Total 1 items < 1 > 10 / page >
Authentication-Free Client List	Add Pre-Authentication Access Server	x	
Add Delete	URL IP	⊕	
Туре	10.	Cancel	Action

11.4.2 Authentication-Free Client List

(1) Authentication-free IP list: IP addresses in the list can access the Internet without authentication.

Click Add below Authentication-Free Client List, select IP, and add an IP address. You can add a description for the IP address behind the IP address.

Pre-auth Whitelist Pre-Authentication Access Server List Add Delete			Search Q
Туре	Information	Description	Action
	baldu.com		Delete
Authentication-Free Client List	Add Authentication-Free Client	× •	Total 1 items < 1 > 10/page > Search Q
Type	19 <mark>5</mark>	Cancel	Action

(2) Authentication-free MAC list: MAC addresses in the list can access the Internet without authentication.

Click **Add** below **Authentication-Free Client List**, select **MAC**, and add a MAC address. You can add a description for the MAC address behind the MAC address.
Х

12 Cloud Account and Project Management

12.1 Adding a Sub Project

Project Management

(1) Choose Home > Project and click Project Management.

(2) Click Add Project Group and enter the Group Name to create a group.

Enter a search term Q	ruijie-opdemo-002@test 🖉	Add Project Group	Add Project
 ruijie-opdemo-002@test.cor Ruijie_PH_Test GTAC_Test DISKOMINFO BEKASI Evan_Test Ruijie-test_Auto Ruijie-test 	Group Name: Enter configGroupNameTip Cancel Confirm		
₩ Demo			

(3) Select a project group and click Add Project. Set basic parameters of the sub project. Then click Next.

Project Management			X
Enter a search term Q V 💠 ruijie-opdemo-002@test.com	Test	Add Project Group Hand Over	Add Project More v
 ♣ FarTest_Network ♦ Test ♣ Ruijie_PH_Test ♣ GTAC_Test ▲ GTAC_Test 	Mgmt Subgroups & Networks (0)		
نظم DISKOMINFO BEKASI الملكم Evan_Test الملكم Ruijie-test_Auto الملكم Ruijie-test			
and Demo			

2040				Basic Information	on
Sasic				Network Alias	
* Network Alias:	Enter the project name			Time Zone	China (GMT+8:00)
				Location	
* Management Password:	Enter the management pas	sword		SSID	
	Note: if the device has been o	configured before, the ma	nagement password		
	should be configured the san	ne with the eWeb passwo	rd.		
Scenario:					
	ARC				
	Office	Hotel	Villa/Home		
	Charles and		Sec. do		
	Factory/Warehouse	Restaurant	School		
		1 Alexandre			
	Retail/Shop	Residence	Customize		
Time Zone:	(GMT+8:00)China				
	Adva	nced T			
	Adva	inced -			

- (4) Add devices manually or through batch import.
- Option 1: Add devices manually.

Enter the device SN and alias.

Add Device			the device model	Add Device	→ Finish X
Switch			Basic		
You can add a switch in one of	the following four modes (click to switch mode):		Device type	Switch	
			Add to	Test	
By entering device SN	By batch adding using an excel file				
			Added devic	es	
1 SN:	Alias:	+	Switch	0	
Back		Cancel Finish			

• Option 2: Add devices through batch import. In the template, up to 500 records can be imported each time.

Add Device	vice model 🔶	Add Device	── + Finish	Х
Switch	Basic			
You can add a switch in one of the following four modes (click to switch mode):	Device type	Switch		
By entering device SN By batch adding using an excel file	Add to	Test		
Download and fill in the davies information in the template line to 500 records can be impacted each time	Added devices			
bownoad and nin in the device information in the tempate of to 500 records can be imported each time.	Switch	0		
Select an sis or sisk me				
Back Cancel Finish				

- a Click Batch Import.
- b Click Download Template to download the template
- c Fill in the device SN and alias in the template and save it.

- d Click **Upload Template File** to upload the edited template file.
- e Click the Import button.
- (5) After the devices are added, click **Save & Next**.

The sub project is added successfully.

Finish	+Add Sub Project	+Add Device Finish		
			Succeeded!	
		AP: 0 , Switch: 0 ,	Gateway: 0 , Wireless Router: 0 , Wireless Bridge: 0	
AP Swit	ch Unauthorized Gateway	Gateway Home Router	Wireless Bridge	
	No	SN	Alias	Action
			No Data	
		First Previous Pa	ege O of O Next Last	10 = 0 in total
				Close

12.2 Managing Cloud Login Accounts

Click (a) at the upper right corner and click **Account**.

User Info	
Username :	ruijie-opdemo-002@test.com
Länguage:	English/English V
Time Zone :	(GMT+1:00)Europe/Paris
Full Name :	
Email:	ruijie-opdemo-002@test.com
Country:	
Company:	ruijie-opdemo-002
Mobile:	
	Save
Two-Factor Authentication	
Two-Factor Authentication ③:	Enable

12.3 Managing Cloud Sub Accounts

Click ⁽²⁾ at the upper right corner, and click **Sub Account**. The **Sub Account List** displays the information of sub accounts. Click ⁽¹⁾ in the **Action** column to edit the sub account. Click ⁽¹⁾ in the **Action** column to delete the sub account.

Sub Account List						⊙ ⋕ - ⊠
Add Sub Account					Username, Full Na	me, Mc Q Search
Username	Role	Network	Full Name	Mobile	Email	Action
ry_xiaoziran@163.com	Admin	Nature_office20210113	123 etse	-	ry_xiaoziran@163.com	区直
ruok@chacuo.net	Operator	eg_test,egtest	ren mei	15986	ruok@chacuo.net	区直
2961167598@qq.com	Operator	default	rui jie		2961167598@qq.com	区直
	First	st Previous Page 1	of 1 Next Last			10 🔺 3 in total

Click **Add Sub Account** to add a new sub account. Select the network, enter the Email in the **Username** box and click **Send Code**. Enter the security code contained in the Email, set the password, language, full name, expiration date, mobile and role, and click **Save**.

Add Sub Account			Х
Default Project Group ③:	ruijie-opdemo-002@test.com		
* Username :			
* Verification Code:		Send Code	
* Password :			
Language :	English	~	
* First Name :			
* Last Name :			
* Mobile:			
Role :	Employee	 © 	
			Cancel Save

Role:

- Admin owns the permissions to create an account.
- **Employee** owns the permissions to edit data.
- **Operator** owns the permissions to print voucher and view account data.
- **Guest** owns the permissions to view data.

12.4 Switching Accounts

Click ______ at the upper right corner.



13 Monitoring

13.1 Viewing all the Device

^{troject}		Device 44 • 1 device	s have new version.	Alarm 26						
en-testas	-001@yopmail.com	m								
All(44)	Gateway(8) Switch(14)	AP(11)	AC(4) Home Route	r(5) Network Bridge(2)					
🛞 Upgra	de Web CLI	eWeb	Enter device SN, alias	or model Q						
	Status T	SN	Model	Alias 0	Group	MAC	Management URL 👙	Egress IP	Firmware Version	Actio
	ON ON	CAN90TZ047159	EST310	Add	MaCc1640659167465	300d.9e02.5b11	192.168.110.4	45.127.187.248	AP_3.0(1)B2P28,Release(07211415)	Đ
	ON ON	G1PQ5MH004203	ES226GC-P	ES226	MaCc1663838993846	300d.9e5c.e549	192.168.111.18	45.127.187.248	ESW_1.0(1)B1P20,Release(09201814)	Đ
	ON ON	MACC112528831	NBR6120-E	Rujje	88888888	00d0.f822.9384	192,168,200,13	45.127.187.248	NBR_RGOS 11.9(6)B15 Latest	Û
	ON ON	MACCEG1689832	EG105G-P	Rujje	test_1	00d0.f815.0844	192 168 200 29	45.127.187.248	ReyeeOS 1.85.1906 Latest	Û
	ON ON	MACCWS6816001	WS6816	ws6816	123fsdf	00d0.f822.33f1	192.168.100.22	220.250.41.86	AC_RGOS 11.9(5)B1, Release(06240613)	Ē
	O OFF	H1P600K001010	EG3230	Te云1667978895664	3355	300d 9e80 ad13	192.168.111.8	112.49.232.23	EG_RGOS 11.9(6)815, Release(09211923	Û
	O OFF	18C4942570104	S2915-24GT4MS-P-L	Ruije	3355	00d0.1824.56f7	100.100.100.2	112 49 232 86	S2915-L_RGOS 11.4(1)B82 Latest	Ē
	OFF	CANL51U003134	ES205C-P	ruje	ap_mesh_001	8005.8857.d3e3	192.168.110.2	220.250.41.86	ESW_1.0(1)B1P10,Release(09152116)	Đ
	O OFF	CAP60EY05939C	ES209GC-P	ES209GC	lsw_now	300d.9e91.cb3d	192.168.111.135	220.250.41.86	ESW_1.0(1)B1P3,Release(07200415)	Đ
	O OFF	CAP70CA00054C	ES209GC-P	ruile	noeg	300d.9ed0.b7c2	192.168.110.57	220.250.41.86	ESW 1.0(1)81P7 Release(08202314)	雨

13.2 Viewing all the Alarm

oject 42	b .	Device 44 • 1 devices have new	version.							
n-testa	s-001@yopmail.com									
Ignore	Alarms Export Alarms	SN	Q				Not cleared Cleared	Start Date	~ End Date	
	Alarm Type 🛛 🖓	Alarm Severity 🖓	Group	Alarm Source	Device SN	Alias	Generated at	Cleared at	Updated at	Action
	Device goes online/offline frequently	Moderate	ren-testas- 001@yopmail.com/8888 8888	Device	MACC112528831	Ruijie	2023-01-29 16:35:10		2023-01-29 16:35:09	6
	Device offline alarm	Moderate	ren-testas- 001@yopmail.com/EGW _20230111	Device	G1MQAWQ00077C	AP840	2023-01-13 21 28:07		2023-01-13 21 28 07	ß
	All device offline	Moderato	ren-testas- 001@yopmail.com/EGW _20230111	Organization			2023-01-13 21 28:07		2023-01-13 21:28:07	ß
	Device offline alarm	Moderate	ren-testas- 001@yopmail.com/EGW _20230111	Device	G1R118N002987	Ruijie	2023-01-13 21:14:07		2023-01-13 21:14:07	6
	All device offline	Moderate	ren-testas- 001@yopmail.com/22	Organization			2023-01-13 21:10:07		2023-01-13 21:10:07	6
	Device offline alarm	Moderate	ren-testas- 001@yopmail.com/22	Device	H1M722K000263	ruijie	2023-01-13 21:10:07		2023-01-13 21 10 07	ß
			ren-testas-							

13.3 Viewing Topology

Topology displays the overall network status on the GUI, including the network topology and device status, and offers the project report.

Requirements on the Network Topology

- (1) Ensure that devices are online on the Ruijie Cloud and the web CLI is accessible.
- (2) A root node that can be an EG or a core switch is required.
- (3) The number of connected devices is calculated based on the root node and the topology is refreshed. Data such as MAC addresses, ARP entries, and routing entries is required.

The topology cannot be displayed in the following situations:

- You cannot access the device web CLI.
- An EG is deployed on the network, but it does not support the **show mac** command or the version is not the latest.
- Multiple switches at the same level together with non-Ruijie products serve as the egress.
- The core switch, access switches, and Aps are deployed. The core switch runs OSPF and has no static routing entries, so its routing table is incomplete.
- Device offline, port change, static route modification, device addition or deletion, etc.
- Switches constitute a network using Virtual Switching Unit (VSU).
- Switches constitute a network using Virtual Router Redundancy Protocol (VRRP).
- Only APs exist in the network group.

Procedure

Click Project > Workspace > View Topology

Demo_Project_1 V	Demo_Project_1 - Customize Up time: 0 days 5 hours		
Workspace			
Smart Config	Topology		🖧 View Topology
Configuration	Device	(See See See See See See See See See See	
Network-Wide			
Devices	D Online Client	EG3100H-E	
Authentication	0		
Monitoring		Switch 5. / 5	
& Network-Wide			
Devices		RAP1260(0) RAP2260(0)	
ជា Clients ្		2 / 2 3 / 3	
🗟 Logs >	VIANList		W M AN Configuration
2 Delivery Center	Wired VLANs (4)		C. Construction
	VLAN1 VLAN5 VLAN1 11	VLAV 23 Finance	VLAN 25 Guest
	Wireless VLANs (0)		
		No Data	

Update Topology: refreshes the topology when devices are added or deleted.

Download Topo: downloads the topology in .png format.

	: Click any device in the topolo	gy to view or configure the corresponding device.
Demo_Project_1	© Device Information	
Workspace	TOPOLOGY List	Ruije Z. • Synchronize Failed Web More v SN: NAEKOO4H0002 Desice modie/N853200-48GT4X5 Management IP: 192.106.110.2 Details >
Smart Config	S	Monitoring Configuration Diagnostics
Configuration		Overview Port Rate Search Log History
Network-Wide	(WAN1)	Status
I Devices		Instruction
Authentication >	EG310GH-E 51694/KD040H0001	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 17 19 41 43 45 47 49 31
Monitoring	(LANO)	
& Network-Wide	Gil	2 4 6 8 10 12 14 16 18 20 22 24 26 28 10 12 14 16 18 20 22 .
Devices	Ţ.	Device Resources
Clients >	NB53200-48GT4X5	Uplink CPU8/Memory Usage More> Connection Status Last 7 Days
E Logs		Port Speed
2 Delivery Center		Duplen None None
	(G124) (G124) (Port 1)	Upinou Ovinina Unitoria 5 300 9:00 13:00 5:00 9:00 13:00 5:00 9:00 13:00
		Uplinit/Dominik Unknown + CPU Utilization Memory Usage Traffic (t): Unknown +
	NBS3100-240745PP NBS3100-240745PP NBS3100-240745PP ES2160C-P SNINAEXONBH0003 SNINAEXONBH0004 SNINAEXONBH0005 SNINAEXONBH0005	Port Packet Statistics
	G1-2 G12 G1	Updated Time: O
		Port Inbound/Dutbound Traffic Inbound/Outbound Rate Number of Packets CRC/PCS Fragment/Oversized Number of (XB) (XB/x) Received/Sent Errors Packets Conflicts
	AP Group AP Group R422566G + - DENABLOORPOTH -	

13.4 Detecting Device

Detect Device: After the detection is completed, the detection result will be displayed.

Procedure

Click **Project** > **Workspace** > **View Topology**, Click Detect Device.

A Sukhum+Punnikul A	SK_Networ	onflict Network Take over Network Unbind Device
OVERVIEW		
Dashboard	Topology LoadingPlease wait.	
Topology		
Alarm		Update Topo Download Topo Manual Settings
REPORT		 A new device is detected. Click here is add.
Network	Network	
Voucher		
習 DEVICE	VLAN1 VLAN1	
AP		
AC		C
Switch		

After the detection is completed, the detection result will be displayed.

2 new devices of other network are detected									
Detection Time: 2022-09	-09 16:57:06 Detect again								
Mama		Add to Network							
RAP2260(G)	SN: G1QF	MAC: ecb ² 98b							
RAP2260(G)	SN: G1C A	MAC: ec e							

When you add a device to the network, you are required to enter the device password. If the password is incorrect, the system will refuse to add it to the network.

Ruijie Cloud refreshes the topology by default when a device is added to the network. When Ruijie Cloud fails to detect the added devices, click **Detect again** to update the topology.

13.5 Wi-Fi Experience

The bar chart displays the experience status in a given period of time and collects data approximately every 5 minutes.

EQperience: Parameters include the client delay, packet loss, and signal strength, and the SVM algorithm is used to calculate the score.

Color	Experience Type	Experience						
	Excellent	The HDV and internet game are available						
	Good	The communication application, web page, and VoIP are available						
	Fair	The client goes offline frequently						
	Poor	The client is difficult for the client to go online						
	No radio	Check whether a client is inactive according to the traffic and power usage						

EGW_20230111		Wi-Fi Experience	(Only supported by Rey	reeOS 1.206 and later)				2.4G 5G	Today Y	esterday Custom period
ක Workspace										
🚯 Smart Config		AP Channel and	I User Experience			📰 No radio 💼 Excellent 💼 G	ood 🛑 Fair			
Configuration		165 161								
Network-Wide		157 153 149								
I Devices	5	64 60								
Authentication	2	50 52 48								
Monitoring 2		44 40 36								
& Network-Wide		Wi-Fi Experience 3	:53 14:00 14:07 14:14 14:	21 14:28 14:35 14:42 14:49	14:56 15:03 15:1	0 15:17 15:24 15:31 15:38 15:45	15:52 15:59 16:06 16	i:13 16:20 16:27 16:34 16:41 16:48 1	6:55 17:02 17:0	09 17:16 17:23 17:30
Devices	×	Upgrade			-O- Experi	rience Score 💼 Excellent 🚞 Go	od 📒 Fair 🧰 Poor			User Experience Sc 100
Clients		Alarm								80
E Logs		Layout								60
Delivery Center	2									40
										20
		1230 1246 1	in the the the th	a also also also also	they also also	n alar alar alar alar alar	der der der u	an alam alam alam alam alam a	les alor als	0
		13:59 13:46 1.	3155 14300 14307 14014 143	1 14220 14232 14242 14249	14030 13303 1301	0 15:17 15:24 15:31 15:30 15:45	13:32 13:39 10:00 10	(13 10:20 10:27 10:34 10:41 10:40 1	0.35 17302 173	9 17:10 17:25 17:30
		Device Details(C	Click AP Channel Busyness a	ind Interference or User Expe	rience Histogram I	to switch time period)				AP Client
Device Details(C	ick AP	Channel Busyness and In	iterference or User Experier	nce Histogram to switch time	e period)					AP Client
										88
Device SN	Ra	dio Channel	Width (MHz)	Transmit Power (%)		Channel Utilization% (TX R)	(OBSS)	Background Noise(dBr	1)	Experience Quality
						No Data				

	Client MAC	Username	Uptime	IP	Experien ce Score	Experien ce Quality	Reason	chan nei	Uplink Traffic (MB)	Downlink Traffic (MB)	Rate (Up and Down) Mbps	RSSI (dBm)	backgrou nd noise (dBm)	Channel Usage (%)	AP	,		s
																	8	6
I	Device Details	(Click AP Channel Busyn	ess and Interference or	User Experience	e Histogram to	switch time pe	riod)							Enter the MAC addre	ss. Q	AP	Client	
CI	ient																	

13.6 Data insights

DemoProject1	□田四英 ∨ □ 遠行状态 ∨ ■ EG31	0GH-E (NAEK0074H0001) : 查看设备详情								
☑ Workspace			Request failed: Request failed with status or	ode7cb240dc						
% Smart Config	 Online Clients O 	None CPU Utilization			None	mory Usage 0				
Configuration										
Network-Wide	View history trend								1小时▼ 今天	0
III Devices	2023-02-11~2023-02-12 Clients			Connectivity						
Authentication										
Monitoring										
& Network-Wide				19:00	23:00	3:00	7:00	11:00	15:00	
圆 Devices										
① Clients										
E Logs										
2 Delivery Center										
			No D	uta						
	2023-02-11~2023-02-12 Speed Summary									
				No Data						

13.7 Edit Topology

Procedure

Click Project > Workspace > View Topology and click Edit

Edit: For different devices, you can perform different operations. Hover the mouse over the device to check the operations that can be performed on the device. The following are for reference only.

• For the gateway detected by the network, you can edit the alias of the device or add the downlink device.

Back Network >	Manual Setting				
				Horizontal Vertical	Instruction
					Configure Virtual Device
					1. Point to the virtual device and click Configure Device Type.
		(G000) (G000) EG2100P	GEdf Alas GAdd Downlink Device		Stelet Device Type Device Type Device Device Device Type Device Device
	(007)	(Gi0/2-2)	(0.0/2-4)		Linemanand Puelter (New Reuse)
	I	T	T		ES05
	(60/23)	WAN	(WAN)		ES05G
					EONO
	\$2910-24GT4SFP	A720	AP180		ОК

• For the device added manually, you can rename the device, select the device model, or remove the device form the network. The models include Reyee ES series and unmanaged switches (non-Reyee).



13.7.1 Common Troubleshooting

1. What can I do if the system displays "No Data" in the topology?

- (1) If there is only one AP on the network, the topology cannot be displayed.
- (2) The egress device is not the Ruijie device and no core switch is deployed.
- (3) Try to refresh the topology manually.

2. What can I do if there is only an EG in the topology?

- (1) If the version is not the latest one, you need upgrade it to the latest version.
- (2) If the web CLI is unavailable, other devices cannot be displayed.

3. What can I do if some devices are not displayed in the topology?

- (3) show mac/show arp/show ip route: If the output of any of the preceding commands contains the configuration with S*, static bindings exist.
- (4) Dynamic routing protocols such as OSPF are configured for the topology.

(5) The switches in the topology are configured with VSU.

4. What can I do if virtual devices are displayed in the topology?

- (6) The network device is not on the Ruijie Cloud or is offline.
- (7) The network device is not the Ruijie device.
- (8) If the network device is an unmanaged switch, you are advised to edit the name and the port manually.

13.8 Upgrade

13.8.1 Upgrade

Select products to upgrade the software versions of the products in batches.

Demo_Project_1 V	Upgrade Firmwar	e Version							
	Upgrade								
Smart Config	Model	Model		Current Versio	n: Current Version		Hardware Version:	Hardware Version	Q Search
Configuration	Device Adding Time	: Start Time	~ End Time	SI	N: Enter the device SN. Us	e a line break to	Description :	Enter the device description here. Use a line break to separate each device description	
Network-Wide >	Keword: Enter Device SN or Description								
I Devices	Keyword						ti.	li li	
	Upgrade selected	Upgrade all 10s	elected						0 88
Monitoring		Status 👻	Device SN	Group	Model	Hardware Version	Current Version	Recommended Version	Description
Network-Wide		Online	NAEK0048H0001	Demo_Project_1	EG310GH-E	1.00	ReyeeOS 1.206.202	3	
Climate		 Online 	NAEK0048H0002	Demo Project 1	NBS3200-48GT4XS	1.00	ReveeOS 1.202.181	8	
		Online	NAEK0048H0003	Demo Project 1	NBS3100-24GT4SFP-P	1.00	ReveeOS 1.202.181	8	
er cogo		Online	NAEK0048H0004	Demo Project 1	NR\$3100-24GT4SFP.P	1.00	ReveeOS 1 202 181	-	
Delivery Center >		College	NA 5/0040/00005	Domo Drojost 4		1.00	Devec00 1 202 101	0	
		• Online	NAEN0040H0000	Demo_Project_1	NB53100-24G145PP-P	1.00	Reyeeus 1.202.101	0	
		 Online 	NAEKUU48HUUU6	Demo_Project_1	ES218GC-P	1.00	ESW_1.0(1)B1P20,Release(0	9200219)	
		Online	NAEK0048H0007	Demo_Project_1	RAP1260(G)	1.00	ReyeeOS 1.202.191	5	
		Online	NAEK0048H0008	Demo_Project_1	RAP1260(G)	1.00	ReyeeOS 1.202.191	5	
		Online	NAEK0048H0009	Demo_Project_1	RAP2260(G)	1.00	ReyeeOS 1.206.202	D	
		Online	NAEK0048H0010	Demo_Project_1	RAP2260(G)	1.00	ReyeeOS 1.206.202	D	
								11 in total < 1 2	> 10 / page > Go to

13.8.2 Firmware Version

Demo V	Upgrade Firmware Version					
Workspace	Version Details Personal software version					
Smart Config	Enter device model software y 9. Search					0 8
Configuration	Cristia davida upadal darrega x(1)					00
Network-Wide	Model	Current Version	Hardware Version	Devices	Recommended Version	Action
⊞ Devices →	NBS3100-24GT4SFP-P	ReyeeOS 1.202.1818	1.00	3		Go To Upgrade
Authentication >	RAP2260(G)	ReyeeOS 1.206.2020	1.00	3		Go To Upgrade
Monitoring	RAP1260(G)	ReyeeOS 1.202.1915	1.00	2		Go To Upgrade
å Network-Wide →	EG310GH-E	ReyeeOS 1.206.2023	1.00	1		Go To Upgrade
Devices	NBS3200-48GT4XS	ReyeeOS 1.202.1818	1.00	1		Go To Upgrade
☐ Clients ⇒						
E Logs					5 in total < 1	> 10 / page ∨
Delivery Center >						

This page lists device version files that are manually uploaded by users.

Demo	Upgrade	Firmware Version									
☑ Workspace	Version Detail	Personal software version									
🛱 Smart Config		-	_								
Configuration		model_software ver 9. Se	arch				Oselected Delete Version Upload Version File O &				
Network-Wide		Firmware Version	Version Size(MB)	Released at	Release Note		Applicable Model				
III Devices		ReyeeOS 1.216.1318	13.49	2023-02-06 17:35		EG105G-E :1.00.EG105G-E :1.xx.EG1	105G-P-E 1.00.EG105G-P-E 1 xx,EG105G-P-E 2.00.EG105G-P-E 2 xx,				
Authentication		ReyeeOS 1 218 2428	Upload	Version File		×	1-P-E-1.00.EG105G-P-E-1.xx.EG105G-P-E-2.00.EG105G-P-E-2.xx,				
Monitoring			Unload a	tay or or his file. (Note:	Unload a far or file for upper	ading the estausu or firewall. The bin file unloaded	8200-48GT4XS 1 2X.NBS5200-48GT4XS 1 3X.NBS5200-48GT4XS 1 4X.NBS5200-				
& Network-Wide			by an ind	lividual cannot be used f	for upgrade on Ruijie Cloud.	aunig the gateway of mewait. The birt he uproaded	-24GT4X8 1 0x.NB55200-24GT4X8 1 1x.NB55200-24GT4X5 1 2x.NB55200- IGT4X8 2.0x.NB55200-24GT4X5 2 1x.NB55200-24SFP/8GT4X5 1 0x.NB55200-				
Devices		ReyeeOS 1 218 1302			.L. Select a tar oz o	v bio file	2x.NB55200-245FP/6GT4XS 1 3x.NB55200-245FP/6GT4XS 1 4x.NB55200- 5100-48GT4SFP 1 0x.NB55100-48GT4SFP 1 1x.NB55100-48GT4SFP 1 2x.NB55100				
Clients							46GT45FP 2.0x.N855100-48GT45FP 2.1x.N855100-24GT45FP 1.0x.N855100- 24GT45FP 1.0x.N855100-24GT45FP 1.4x.N855100-24GT45FP 2.0x.N855100-				
聞 Logs							24GT4SFP: 2.1x				
😂 Delivery Center		ReyeeOS 1 218 2428	12.66	2023-01-05 19:43	RAF	(2260(G): 1.00,RAP2260(G): 1.xx,RAP2260(G): 2.00, AP262(G): 2.00,	RAP2250(G): 2 xx RAP2250(G): 3 00 RAP2250(G): 3 xx EAP262(G): 1 00 EAP262(G): 1 xx EAP262(G): 2 xx EAP262(G): 3 00 EAP262(G): 3 xx				
		ReyeeOS 1.202.2423	11.61	2022-12-27 14:48		EG105G 1.00.EG105G-P.1.	00.EG105G-1.xx,EG105G-P1.xx,EG105G-2.xx,EG105G-P2.xx				
		ReyeeOS 1 204 2414	9.66	2022-12-22 10.12		EW1200G-PR0	0.1.00.EW1200G-PRO.1.xx,EW1200G-PRO.2.xx,				
		ReyeeOS 1 205 2216	11 66	NBS5000 940T4X65-1 bx NBS5200 940T4X65-1 1x NBS5200 940T4X65-1 2x NBS5200 940T4X65-1 0x							



13.9 Configuring Alarms

Click Ci at the upper right corner, and click **Alarm**. When no alarm is configured, global settings are used. On the **Alarm Settings** page, you can specify whether to enable or disable alarms and how the alarms should be received.

Procedure

(1) Click **O** at the upper right corner and click **Alarm Settings**.

L0G0 ru V	÷	С <mark>в</mark>	œ	۲	8
				Ala	arms
				lice	ense
				Co	ntacts

(2) Select one project in this account.

Ruijie-test_Auto		
Enter a search term	٩	
∨ 💠 ruijie-opd om		
品 Ruijie_PH_Test		
品 GTAC_Test		
品 DISKOMINFO BEKASI		
品 Evan Test		
品 Ruijie-test_Auto		m type
品 Ruijie-test		
ሔ Demo		

(3) Set alarm parameters.

e-test_Auto V			
Nam Sattings Natification Padalasts			
Notification Recipients			
Common Switch Gateway AC			4
Alarm type	Alarm Enabling	Alarm Threshold Email Alarm	
Device offline alarm			
All device offline			
Device configuration changes			Batch Apply
System indicator (CPU, memory usage, etc.) beyond threshold			To batch apply alarm settings of
Switch loop redundancy			click Copy and Apply.
Multiple DHCP servers			Copy and Apply
Multiple DHCP servers on LAN port			
Multiple DHCP servers on WAN port			
Device interface IP conflict			
Terminal IP conflict			
AP(4G) link switch			
RGOS Configuration Change Alarm			
Smart community client offline			

Type: indicates the type of alarms.

Alarm Enabling: indicates whether to enable the function. If the function is enabled, alarm information is displayed on the alarm page.

Alarm Threshold: indicates the alarm threshold.

Email Alarm: indicates that alarms will be pushed to the contacts in **Contact Group List** of the network through the email when **Email Alarm** and **Status** are enabled.

A	larm Settings	Notification Recipients			0
Ec	lit Contact				
		Group	Description	Enable	
			No Data		

13.10 Managing Contacts

Procedure

Click Contact to access Notification Recipient List and Notification Recipient List and Notification Recipient Group.

1060 n V	⊕	@ @
		Alarms
Alarm		license
3	())	Contacts

• Notification Recipient List

In the **Notification Recipient List** area, you can add contacts and contact groups that will receive the alarm emails.

Notification Recipient List	otification Recipient Group				o
+ Add Notification Recipient					
Name	Phone	Email	Group	Description	Action

Name: displays the customized name of a recipient.

Phone: displays the mobile number of a recipient.

Email: displays the email address of a recipient.

Group: indicates the group of a recipient.

Description: describes the recipient.

Action: indicates the operation for the recipient. The value is **Edit** or **Delete**. After clicking **Edit**, you can edit recipient information in the displayed window.

Add Notification Recipient: adds a recipient to the notification recipient list.

• Notification Recipient Group

In the Notification Recipient Group area, you can add a group and move the recipients to the group.

Notification Recipient List Notification Recipient Gro	up	٥
+ Add Group	_	
Group	Description	Action
test		<i>_</i> ∉Edit ⊜Delete
		1 in total < 1 > 10 / page >

Group: displays the customized name of the group.

Description: displays some words to describe the recipient group.

Action: indicates the operation for the recipient group. The value is Edit or Delete.

Add Group: adds a recipient group to the notification recipient list.

After clicking **Edit**, you can edit recipient group information in the displayed window. The value is **Add to Group** or **Delete from Group**.

• Add to Group: adds the selected recipients to current group.

Edit Contact Gro	oup			×
* Group Name:	test			
Description :				
✓ 1/1 it Enter se	ems All Contacts		0 items Contact Gr Enter search content	roup Q
▼ test		>	No data.	
			Can	ncel

o Delete from Group: deletes the selected recipients from the current group.

Edit Contact Gro	bup	Х
* Group Name:	test	
Description:	ns All Contacts arch content Q test	
	Cancel	OK

13.11 Viewing the Number of Global Alarms Quickly



Click Home > Alarm

13.12 Viewing Details About Global Alarms

Project 243		Device 42 • 1 devices have new w	Alarm 15 Arsion.	8						
ren-testas-	-001@yopmail.com			•						
Ignore A	larms Export Alarms	SN	Q,				Not cleared Cleare	d Start Dat	e ~ End Date	8
	Alarm Type 🛛 🖓	Alarm Severity	☑ Group	Alarm Source	Device SN	Alias	Generated at	Cleared at	Updated at	Action
	Device offline alarm	Moderate	ren-testas- 001@yopmail.com/MaCc16 40659167465	Device	CAN90TZ047159		2023-02-08 16:41:07		2023-02-08 16:41:07	5
	All device offline	Moderate	ren-testas- 001@yopmail.com/MaCc16 40659167465	Organization			2023-02-08 16:41:07		2023-02-08 16:41:07	6
	All device offline	Moderate	ren-testas- 001@yopmail.com/22	Organization			2023-01-13 21:10:07		2023-01-13 21:10:07	[]
	Device offline alarm	Moderate	ren-testas- 001@yopmail.com/22	Device	H1M722K000263	ruijie	2023-01-13 21:10:07		2023-01-13 21:10:07	6
	All device offline	Moderate	ren-testas- 001@yopmail.com/xx_Aut 0	Organization			2023-01-12 17:36:00		2023-01-12 17:36:00	(L
	All device offline	Moderate	20220420_lsw/lsw1_Auto	Organization			2023-01-12 10:46:44		2023-01-12 10:46:44	5
	All device offline	Moderate	ren-testas- 001@yopmail.com/enet	Organization			2023-01-04 14:57:10		2023-01-04 14:57:09	(5
								15 in tot	al < 1 2 > 107 page >	Go to

13.13 Viewing Alarms of a Project

Choose Project > Monitoring > Network-Wide > Alarm.

Alarm Lis	t									
Ignore /	Alarms Export Alarm	SN	Q				Not cleared Cleared	Start Date	~ End Date	C 8
	Alarm Type 🛛 🖓	Alarm Severity 🛛 🖓	Group	Alarm Source	V Device SN	Alias	Generated at	Cleared at	Updated at	Action
	Device offline alarm	Moderate	DISKOMINFO BEKASI	Device	G 11	TCF-14652	2023/11/10 14:52:07	-	2023/11/10 06:52:07	E\$
									1 in total < 1 >	10 / page \vee

13.14 Layout

Layout is used to identify the AP location.

Procedure

- (1) Choose CONFIGURATION > WIRELESS > Layout and select a network in this account.
- (2) Click Config Layout in the Layout area.

Layou	ut			
Layout :		~ (Config Layout	Device

(3) Click **ADD Layout** on the **Config Layout** page.

C	onfig Layout	×
	Name	Action
	No	Data
		Add Layout

(4) Set parameters of the layout and click **Save**.

Add/Edit Layout	2	×
Layout Name	Please enter up to 18 characters, consisting of letters, numbers and underline (_).	
Layout Source	😔 Local Layout	
	Мар	
Please select a picture	Select e in the format of gif, jpg, jpeg, bmp or png. The size of the picture cannot exceed 5M	1.
	Save]

Layout Name: Enter up to 18 characters, consisting of letters, numerals, and underlines (_).

Layout Source: Select a local layout or map.

- Local Layout: Select a picture in the format of gif, jpg, jpeg, bmp, or png on the local PC. The size of the picture cannot exceed 5 MB.
- Map: Enter a location name for Bind Location.

14 Delivery Center

14.1 Smart Detection

Choose Delivery Center > Smart Detection > Check Now to generate a project delivery report.



After a project delivery report is generated, click View Report to view the report.

DemoProject2			
硷 Workspace			
🕏 Smart Config			
Configuration		Smart Cherk Passed	
Ø Network-Wide	>	This network has passed smart check and is ready to be delivered. A project delivery report has been generated. The project delivery report has been generated. The project delivery report has been generated.	
幸 Devices	>	You are advised to deliver this report to the network owner for better management.	
\otimes Authentication	>	View Report Back	
Monitoring			
Monitoring නී Network-Wide	>	Link Status	^
Monitoring & Network-Wide Devices	>	Link Status O Port percentiation rate and duraley text	^
Monitoring & Network-Wide @ Devices 1 Clients	>	Link Status O Port negotilation rate and duplex test O Bott flow negotilation	^
Monitoring [®]	> > >	Link Status O Port negotiation rate and duplex test O Port flow monitoring	^
Monitoring [®]	>	 Link Status Port negotilation rate and duplex test Port flow monitoring Layer 2 and 3 Connectivity 	^

14.2 Project Report

14.2.1 Applicable Scenarios

After project deployment is completed, a delivery report needs to be submitted to the owner, which often requires considerable testing and writing time. This function can conduct intelligent check, summarize all types of information and check results, and automatically generate a project delivery report in both PDF and Word formats. The report covers basic information, general solution, intelligent configuration check results, device list, and topology.

After the project deployment is completed, a report can be offered to the owner. The report can provide the revised project network device overview and delivery time, customized company logo, company name, and

project introduction, show the topology of the whole project, and supplement other vendors' devices to the device list. The report can be in PDF and Word formats.

14.2.2 Configuration Steps

1. Choose Project > Delivery Center > Project Report to view the latest delivery report of the current project.



2. Click Edit at the upper right corner to edit basic information in the project report.

DemoProject1	V		
	DemoProject 1 Project ReportPreview Opdate Time:2023-02-03 02:31:47		Bear Bear Myse Edownload
🕏 Smart Config	2-		
Configuration			
Network-Wide	>		
	>		
Authentication	>		
Monitoring		DemoProject1	
& Network-Wide		Project Report	
Devices	>		
Clients	>		
🗄 Logs	>		
2 Delivery Cente		Report Time: 2023-02-03	
			•
			+
			•
[DemoProjec	t1 Project ReportEdit Update Time:2023-02-03 02:31:47		Download @Preview Download @Preview Download
DemoProjec	t1 Project ReportEdit Update Time:2023-02-03 02:31:47 nation		@Preview @Edit in WPS⑦ 쇼Download
2. Basic inform	11 Project ReportEdit Update Time:2023-02-03 02:31:47 nation An image with an aspect ratio of 43 is recommended.		BPreview BEdit in WPSØ BDownload
DemoProjec	1) Project ReportEdit Update Time:2023-02-03 02:31:47 nation An image with an aspect ratio of 4.8 is recommended. Only PNG, JPG, JPGG or BMP format images are allowed.		은Preview 을Edit in WPS® 쇼Download
[DemoProjec 2. Basic inform LOGO:	till Project ReportEdit Update Time/20/23-02-03 02:31:47 nation An image with an aspect ratio of 4/3 is recommended. Only PNG, JPG, JPEG or BMP format images are allowed. The image file must be less than 100 KB, Click Upload Again.		은Preview 을Edit in WPS® 쇼Download
[DemoProjec 2. Basic inform LOGO:	till Project ReportEdit Update Time:2023-02-03 02:31:47 nation An image with an aspect ratio of 43 is recommended. Only PNG, JPG, JPGG or BMP format images are allowed. The image file must be less than 100 KB, Click Upload Again. Wasse Upload Again		Preview &Edit in WPS® &Download 1.Select report theme 2.Basic information
[DemoProjec 2. Basic inform LOGO:	till Project ReportEdit Update Time:2023-02-03 02:31:47 nation An image with an aspect ratio of 4.3 is recommended. Only PNG, JPG, JPG or BMP format images are allowed. The image file must be less than 100 KB, Click Upload Again. When Upload Again		Preview &Edit in WPSO &Download I.Select report theme 2.Basic information 3.Common Solutions Service conformation
[DemoProjec 2. Basic inform LOGO: Copyright:	till Project ReportEdit Update Time:2023-02-03 02:31:47 nation An image with an aspect ratio of 43 is recommended. Only PNG, JPG, JPGG or BMP format images are allowed. The image file must be less than 100 KE. Click Upload Again. Mum Upload Again All Rights Reserved©rmp		Preview &Edit in WPSO &Download I.Select report theme 2.Basic information 3.Common Solutions Service configuration 4.Configuration smart
[DemoProjec 2. Basic inform LOGO: Copyright: Delivery time:	tl project ReportEdit Update Time:2023-02-03 02:31:47 nation An image with an aspect ratio of 43 is recommended. Only PNG, JPG, JPGG or BMP format images are allowed. The image file must be less than 100 KE, Click Upload Again. Mame Upload Again All Rights Reserved©rmp 2023/02/03		Preview &Edit in WPSC &Download I.Select report theme 2.Basic information 3.Common Solutions Service configuration 4.Configuration smart check results 5.Device list
DemoProjec 2. Basic inforr LOGO: Copyright: Delivery time Project	Lt J. Project ReportEdit Update Time:2023-02-03 02:31:47 nation An image with an aspect ratio of 4.3 is recommended. Only PNG, JPG, JPEG or BMP format images are allowed. The image file must be inso than 100 KE. Click Upload Again. Mum Upload Again All Rights Reserved©rmp 2023/02/03 Enter project description		Preview &Edit in WPSC &Download I.Select report theme 2.Basic information 3.Common Solutions Service configuration 4.Configuration smart check results 5.Device list 5.Topology 7.anonembers
Copyright: Delivery time: Project description:	tl J Project ReportEdit Update Time:2023-02-03 02:31:47 nation An image with an aspect ratio of 43 is recommended. Only PNG, JPG, JPEG or BMP format images are allowed. The image file must be inso than 100 KE. Click Upload Again. Mam Upload Again All Rights Reserved©rmp 2023/02/03 Enter project description		Preview BEdit in WPS® Boownload I.Select report theme 2.Basic information 3.Common Solutions Service configuration 4.Configuration smart check results 5.Device list 6.Topology 7.Appendixes (configuration details)
Copyright: Copyright: Delivery time: Project description:	tl J Project ReportEdit Update Time:2023-02-03 02:31:47 nation An image with an aspect ratio of 4.3 is recommended. Only PNG, JPG, JPEG or BMP format images are allowed. The image file must be less than 100 KE. Click Upload Again. Mam Upload Again All Rights Reserved©rmp 2023/02/03 Enter project description		Preview BEdit in WPS® BOownload I.Select report theme 2.Basic information 3.Common Solutions Service configuration smart check results 5.Device list 6.Topology 7.Appendixes (configuration details)
DemoFroject	Lt J. Project ReportEdit Update Time:2023-02-03 02:31:47 nation An image with an aspect ratio of 4.3 is recommended. Only PNG, JPG, JPEG or BMP format images are allowed. The image file must be into the into the ION KE, Click Upload Again. Mum Upload Again All Rights Reserved Crmp 2023/02/03 Enter project description Show in the report		Preview BEdit in WPS® Boownload I.Select report theme 2.Basic information 3.Common Solutions Service configuration smart check results 5.Device list 6.Topology 7.Appendixes (configuration details)
DemoProject Basic infon LOGO: Copyright: Delivery time: Project description: Project team Name	tl J Project ReportEdit Update Time:2023-02-03 02:31:47 nation An image with an aspect ratio of 4.3 is recommended. Only PNG, JPG, JPEG or BMP format images are allowed. The image file must be less than 100 KE. Click Upload Again. Mam Upload Again All Rights Reserved©rmp 2023/02/03 Enter project description Show in the report Title	Phone	Preview &Edit in WPSC &Download I.Select report theme ZBaic information Scormon Solutions Service configuration Action Action
[DemoFrojec 2. Basic infon LOGO: Copyright Delivery time Project team Project team Name	tl J Project ReportEdit Update Time:2023-02-03 02:31:47 nation An image with an aspect ratio of 4.3 is recommended. Only PNG, JPG, JPEG or BMP format images are allowed. The image file must be less than 100 KE, Click Upload Again. Mam Upload Again All Rights Reserved©rmp 2023/02/03 Enter project description Show in the report	Phone	Preview &Edit in WPSC &Download I.Select report theme 2.Basic information Service configuration 4.Configuration smart check results S.Topology 7.Appendixes (configuration details) Action
DemoProject Basic infon LOGO: Copyright: Delivery time: Project description: Project team Name	tl J Project ReportEdit Update Time:2023-02-03 02:31:47 nation An image with an aspect ratio of 4.3 is recommended. Only PNG, JPG, JPEG or BMP format images are allowed. The image file must be into the into the 100 KE. Click Upload Again. Mam Upload Again All Rights Reserved©rmp 2023/02/03 Enter project description Show in the report	Phone	Action Action Action Action Action
DemoProject Basic infon LOGO: Copyright: Delivery time: Project description: Project team Name	tl J Project ReportEdit Update Time:2023-02-03 02:31:47 nation An image with an aspect ratio of 4:3 is recommended. Only PNG, JPG, JPEG or BMP format images are allowed. The image file must be less than 100 KE. Click Upload Again. Main Upload Again All Rights Reserved©rmp 2023/02/03 Enter project description Title Title 	Phone	Action Action Action
[DemoProject 2. Basic infon LOGO: Copyright: Delivery time Project team Name	tl J Project ReportEdit Update Time:2023-02-03 02:31:47 nation An image with an aspect ratio of 4.3 is recommended. Only PNG, JPG, JPEG or BMP format images are allowed. The image file must be less than 100 KE. Click Upload Again. Main Upload Again All Rights Reserved©rmp 2023/02/03 Show in the report Title	Phone	Action Action Action
DemoProject Basic infon LOGO: Copyright: Delivery time: Project description: Project team Name + Add team me	tl) Project ReportEdit Update Time:2023-02-03 02:31:47 nation An image with an aspect ratio of 4.3 is recommended. Only PNG, JPG, JPEG or BMP format images are allowed. The image file must be into the into the 100 KE. Click Upload Again. Image: Start and the into the intothe into the into the into the intothe into	Phone	Action Action Action

3. You can view service configuration of the general solution in the delivery report.

[DemoProject1] Project ReportEdit Update Time:2023-02-03 02:31:47									lit in WPS⑦ 쇼Download
3.	Office Service Configuration 3.1 Wired Network Planning Wired Network Planning		IP Address Range		VLAN ID	IP Address	Allocation Mode		
	VLAN1		192.168.110.0//24		1	DHCP			1.Select report theme 2.Basic information
	3.2 WLAN Network Planning WLAN Network Planning	SSID	Password	IP Address Range	e VLAN	ID	IP Address Allocation Mode		3.Common Solutions Service configuration 4.Configuration smart check results 5.Device list
				No Data					6.Topology 7.Appendixes (configuration details)
	3.3 Office Application								
	App Name	Description							
	DHCP Snooping	DHCP Snooping can	n prevent network failure cau	sed by unauthorized	routers or DHCP servers.				
	Smart Flow Control Limit the network speed of clients flexibly.								

4. Checking the network intelligently: Click **Configure smart check immediately**. The page automatically redirects to **Smart Detection**.

You	have not configu	red smart check]
Device	e list					
No.	Device Type	Device modle	Product description	Quantity	Action	1.Select repor 2.Basic inform 3.Common So
1	AP	RAP1260(G)	Enter product description	2		Service config 4.Configuration
	AP	RAP2260(G)	AX1800 Wi-Fi 6 dual-band Gigabit ceiling mount AP, dual Gigabit LAN uplink ports, built-in antennas, dual-band 2.4GHz/5GHz, 802.11az, 80	3		 check results 5.Device list
	Gateway	EG310GH-E	Rack-mountable 10-port full gigabit router, providing one WAN port, 6 LAN ports, and 3 LAN/WAN ports; recommended concurrency of 300, maxi mum 1.5 Gbps throughput; cloud remote management supported.	1		6.Topology 7.Appendixes (configuration
	Switch	NBS3200- 48GT4XS	48-Port L2 Managed 10G Uplink Switch, 48 Gigabit RI45 Ports,4 *10G SFP+ Slots,19-Inch Rack-mountable Steel Case	1		
	Switch	ES218GC-P	18-Port. Gigabit Smart POE Switch, 16 Gigabit RI45 Ports including 16 POE/POE+ Ports, 2 SFP Slots, 240W PoE power budget,13-inch Rack-mounta bie Steel Case	1		
;	Switch	NBS3100- 24GT4SFP- P	24-Port Gigabit L2 Managed POE Switch, 24 Gigabit RI4S POE/POE+ Ports, 4 SEP Slots, 370W POE power budget, 19-inch Rack-mountable Stell Cas g	3		

5. Click Check Now.

Smart Check Passed This network has passed umart check and is ready to be delivered. A project delivery report has been generated. The project delivery report contains Wi-Fi password, network configuration details, mart check result, device information, and other configurations you have made during network deployment. You are advised to deliver this report to the network owner for better management. View Report	
S Layer 2 and 3 Connectivity	^
⊘ Address pool and VLAN test	
Link Status O Port negotiation rate and duplex test	^
© Port flow monitoring	

 After check, go to Project > Delivery Center > Project Report > Edit. The check results of functions supported by the network will be automatically incorporated into the delivery report.

	[DemoProject1] Project F	ortEdit Update Time:2023-02-03 02:31:47		@Pre	view 🔂Ed	it in WPS@ க்Do
e	4. Configuration smart che	results				
nfig	Configuration smart check re-	s: Pass 🥑 Hide vulnerabilities				
,	Туре		Details		Result	
Vide	Layer 2 and 3 Connectivity		Address pool and VLAN test		Pass	1 Columna
	Link Status		Port negotiation rate and duplex test		Pass	2.Basic informa
ion $ ightarrow$			Port flow monitoring		Pass	3.Common Sol Service configu
	5. Device list					4.Configuration check results
Vide	Device overview					 5.Device list 6.Topology
	No. Device Type De	Product description		Quantity	Action	7.Appendixes (configuration
	1 AP RA	60(G) Enter product description		2		
enter	2 AP RA	60(G) AX1800 WI-FI 6 dual-band Gigabit celling wave2/wave1, up to 1775Mbps; support /	mount AP, dual Gigabit LAN uplink ports, built-in antennas, dual-band 2.4GHz/5GHz, 602.11ax, 802.11ac P and routing mode, L3 roaming, Ruijie Cloud app management, Support PoE and local power supply	3		
	Smart Detection Project Report EG	GH-E Rack-mountable 10-port full gigabit route mum 1.5 Gbps throughput; cloud remote	r, providing one WAN port, 6 LAN ports, and 3 LAN/WAN ports; recommended concurrency of 300, maxi management supported.	1		
	Project Handover NE 48	48-Port L2 Managed 10G Uplink Switch, 4	8 Gigabit RI45 Ports,4 *10G SFP+ Slots,19-inch Rack-mountable Steel Case	1		
	5 Switch ES	GC-P 18-Port Gigabit Smart POE Switch, 16 Gig ble Steel Case	abit RI45 Ports including 16 POE/POE+ Ports, 2 SEP Slots, 240W PoE power budget, 13-inch Rack-mounta	1		
	6 Switch 24	00- SFP. 24-Port Gigabit L2 Managed POE Switch,	24 Gigabit RJ45 POE/POE+ Ports, 4 SFP Slots, 370W PoE power budget, 19-inch Rack-mountable Stell Cas	3		

7. Check the network topology.

DemoProject1 V	[DemoProject1] Project Report	Edit Update Time:2023-02-	03 02:31:47				@Preview @Edi	t in WPS② L 쇼Download
Workspace								
Smart Config	5 Ruijie NAEK0037H0005	NBS3100-24GT4SFP-P	00d0.f800.3750	192.168.110.5	Enter product description	Enter product description		
	6 Ruljie NAEK0037H0006	ES218GC-P	00d3.f800.3762	192.168.110.6	Enter product description	Enter product description		
Configuration	+ Add Device Information							
Ø Network-Wide >	6. Topology							1 Select report theme
⊕ Devices →								2.Basic information
$\ensuremath{igsilon}$ Authentication $\ensuremath{\ >}$				6				3.Common Solutions Service configuration
Monitoring				(Amar)				4.Configuration smart check results
& Network-Wide								5.Device list 6 Toppinger
Devices				(chee)				7.Appendixes
Clients >				-				(configuration details)
E Logs				Manager and and				
Delivery Center >							63 + - 0	
	7. Appendixes (configuration de	tails) As a PDF appendix						

8. Click **Download** at the upper right corner to download the delivery report in PDF and Word formats.

DemoProject1 V	Physical Research Burnet Research Haussen 2022 02 02 02 02 147	
G Workspace		PDF
Smart Config	5 Ruijie NAEK0037H0005 NB53100-24GT45FP-P 0040.4800.3750 192.168.110.5 Enter product description Enter product description	WORD
	6 Ruijie NAEK0037H0006 ES2186C-P 00d3/800.3762 192.168.110.6 Enter product description Enter product description	
Configuration	+ Add Device Information	
Ø Network-Wide >	6. Topology	1.Colord connect theme
		2.Basic information
	9	3.Common Solutions Service configuration
Monitoring		4.Configuration smart check results
🔏 Network-Wide >	and a second sec	5.Device list 6.Topology
圖 Devices >	÷	7.Appendixes (configuration details)
fi Clients →		(comganation actums)
E Logs		
So Delivery Center 🔿		

14.3 Project Handover

14.3.1 Applicable Scenarios

After-sales technical personnel of channels may be unable to solve some problems during maintenance. In this case, channel technicians generally seek support from Ruijie technical support engineers, who will temporarily need network management permissions for troubleshooting.

You can transfer your network (including devices on the network and device-related configuration) to other accounts. You can also share a network with other accounts. Read/write permission and read-only permission can be configured for sharing. The read-only permission is used for monitoring requirements while the read/write permission is used for troubleshooting requirements.

14.3.2 Configuration Steps

Choose Delivery Center > Project Handover to hand a project over to a contact in Current Tenant.



You can also click **Other Tenant**. Enter a complete account for search, select the target account, and hand the project over to the account.

DemoProject1	~	Project Handov	er
		Hand over to	Current Tenant Other Tenant
🕏 Smart Config			Enter the account. If the account belongs to multiple organizations, the name of these organizations will be "Account - Organization Name". In this case, select an organization.
Configuration			Account: Enter the account.
Network-Wide	>		Hand Over
	>		
	>		
Monitoring			
& Network-Wide	>		
Devices	>		
Clients	>		
🗑 Logs	>		
😂 Delivery Center	>		

15 Appendix: Frequently-Used Controls

15.1 Notification

You can view device go-online and go-offline reminders.



15.2 Add

Add \vee

15.3 Delete

Ū

15.4 Quickly locate the table entry you want to find by entering keywords

	Enter	device model, so	oft	Q Search			
	Upgrade Model:	Model	Current Version :	Current Version	Hardware Version:	Hardware Version	Q Search
	Device Adding Time : Keyword :	Start Time ~ End Time	SN :	Enter the device SN. Use a line break to separate each device SN.	Description :	Enter the device description here. Use a line break to separate each device description.	
15.5	Status Disabled:	; enabled:	O . You c	an click it to switch th	e status.		

15.6 Change Project Name or Password

Demo_Project_1 V	Demo_Project_1 - Cust	omize Up time: 0 days 5 hours			
Workspace					Change project name
Smart Config	Тороlogy				Change project password
Configuration	圆 Device				
Network-Wide >	11		and the second		
I Devices	Online Client		EG310GH-E		
	0		1 / 1		
Monitoring			Switch		
å Network-Wide >			5 / 5		
Devices			# # RAP1260(G) RAP2260(G)		
Clients >			2/2 3/3		
E Logs	V/I AN I 1-4				
2 Delivery Center	VLAN LIST				VLAN Configuration
	Wired VLANs (4)				
	VLAN 1 VLAN1	> VLAN 5 11	> VLAN 23 Finance	> VLAN 25 Guest	
	Wireless VLANs (0)				
			No Data		