

Ruijie Reyee CCTV 1.0

Cookbook



Document Version: V1.0 Date: 2023-03-27 Copyright © 2023 Ruijie Networks

Copyright

Copyright © 2023 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

- The official website of Ruijie Reyee: <u>https://www.ruijienetworks.com/products/reyee</u>
- 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 items	Select System > Time.

2. Signs

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

🕕 Warning

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

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. Instruction

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

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

Contents

PrefaceI
1 Overview1
1.1 Introduction1
1.2 Specifications2
2 Getting Started
2.1 Preparing for Installation
2.1.1 Project Requirement
2.1.2 Network Planning
3 Configuration
3.1 SON and Cloud Deployment4
3.1.1 Application Scenario4
3.1.2 Procedure4
3.2 Connection and Configuration of Wireless bridge6
3.3 Creating a VLAN/DHCP7
3.4 Real Topology8
3.4.1 Application Scenario8
3.4.2 Procedure
3.4.3 Principle of the Network Topology11
3.5 Automatic IPC Identification12
3.5.1 Application Scenario12
3.5.2 Procedure12
3.6 ACL Configuration14
3.6.1 Application Scenario14

3.6.2 Procedure14
3.7 IPC Access through an Extranet and Server Penetration through an Intranet16
3.7.1 Application Scenario16
3.7.2 Procedure
3.8 Voice VLAN
3.8.1 Voice VLAN Settings19
3.8.2 OUI Settings19
3.8.3 Port Settings20
3.9 Delivery Report21
4 Maintenance24
4.1 Remote IPC Operations — IPC Restart and Long-Distance Power Supply24
4.1.1 Application Scenario24
4.1.2 Procedure24
4.2 Loop Prevention Configuration29
4.2.1 Application Scenario29
4.2.2 Procedure
5 Troubleshooting
5.1.1 Ruijie Cloud Cannot Automatically Identify an IPC
5.1.2 IPC Is Offline
5.1.3 Unable to Access the Intranet Server
5.1.4 EST Bridging Fails
6 FAQ

1 Overview

1.1 Introduction

In a CCTV scenario, protecting the safety of personnel and property is the core requirement of users. Therefore, smoothly surveillance video transmission, real-time alarm notification and fast recover from camera failure are expected.

There is a story. One day, confidential documents have been stolen, but the elevator and corridor camera signal lost and couldn't track the thief. Boss was so angry and asked SI to onsite right away to solve his monitoring problem. Two hours later, SI finally arrived the company, when SI tried every means to check the system. They only found that unmanaged switch use in the network cannot figure out failure switch ports location. Second, the elevator was unable to transmit video due to damaged cables. During testing, SI found while the employee downloading the camera video would jam. In the end, he had to restart the switch, all the network interrupted.

Reyee Cloud Managed CCTV Network Solution, your CCTV network expert won't disappoint you. Reyee RG-ES200 series cloud managed switch and RG-EST310 wireless bridge are designed for CCTV business. Mobile VLAN configuration, one-step to separate your CCTV and production network, the video won't jam anymore; Real-time Failure Notification, would notice users that camera failure in the first place; Remote Reboot Camera, helps you one-click to restart the camera at home, no need onsite anymore.



CCTV Network Solution

Typical Solution Topology



Solution Benefits for End Users:

- Fair price replace unmanaged to cloud managed switch;
- Protect users property and safety at any time;
- 1 250 meters PoE save cabling cost for end-users;
- 5GHz reduce interference and guarantee video quality;
- Heet difference CCTV requirements in various scenarios.

Benefit for SIs:

- Multiple models optional of RG-ES200 series switch;
- Cloud to remote troubleshooting and maintenance;
- Mobile to set VLANs for different service traffic;
- Easy deployment via Self-Organizing Network technology.

1.2 Specifications



2 Getting Started

2.1 Preparing for Installation

2.1.1 Project Requirement

Company Y wants to monitor the whole park and the monitoring data from the cameras should be aggregated to the NVR.

The headquarters and its branch of Company Y are all in city A, but no wires are connected between them. The staffs from the branch need to get the data by accessing the documents server and data server at the headquarters, and the camera data from the branch needs to be aggregated to the headquarters' NVR.

- (1) The CCTV network is isolated from the other network.
- (2) Support logging into NVR for video surveillance anytime and anywhere.
- (3) Real-time alarms are required, such as CCTV is offline, then the CCTV problems can be solved remotely.
- (4) IP phone access switches need to plan a separate voice VLAN.

2.1.2 Network Planning

Topology:



3 Configuration

3.1 SON and Cloud Deployment

3.1.1 Application Scenario

After physical connections of devices are connected based on the topology, all Reyee devices on the same network automatically complete self-organizing network (SON). After SON is complete, devices can be managed and configured in a unified manner through the main device. In addition, the entire network can be deployed on the cloud by deploying one device on the cloud, which simplifies the deployment.

3.1.2 Procedure

(1) Complete physical connections between devices based on the actual topology. The devices complete SON connections locally.

Net Status (Online Devices / Total)						Refresh Q
(ver addits (online devices / roan)	DHCP Internet	Router	6/6 Switches	令 1/1 APs		New Street
My Network						
CCTV-Test (9 devices)						Ű,
Model	SN	(p	MAC		Software Ver	
Router EG1D5GW-X [Master]	H1RU72F000510	No IP Address Available	28:D0:F5:E3:3A:86		ReyeeOS 1.95.1914	
A P RAP2260(H)	G1RUAGJ000231	192.168.110.147	10:82:3D:13:E7:87		ReyeeOS 1.95.2115	
Switch NBS3200-24GT4XS	MACCNBS320066	192.168.110.5	00:D0:F8:D8:9C:A3		ReyeeOS 1.218.2428	
Switch NBS3100-24GT4SFP-P	G1NWB15000268	192.168.110.251	00:D0:F3:33:38:61		ReyeeOS 1.86.2021	
Switch NBS3100-8GT2SFP-P	CAR41NR024704	192.168.110.7	54:16:51:3A:30:BB		ReyeeOS 1.206.2216	
Switch NBS5100-24GT4SFP-P	G1RU85X002932	192.168.110.29	28:D0:F5:FF:9A:9D		ReyeeOS 1.212.2322	
AP RAP2260	G1RU9GP000991	192.168.110.166	70:42:D3:01:A0:FD		ReyeeOS 1.219.1407	
Switch RG-ES216GC	G1PD494011658	192.168.110.144	30:0D:9E:49:7E:85		ESW_1.0(1)81P20,Release(09201814)	
Switch RG-ES209GC-P	CAP70CA00054C	192.168.110.57	30:0D:9E:D0:87:C2		ESW_1.0(1)B1P7,Release(08202314)	

(2) View the actual network topology and device list on the local eWeb management system.



All (9)	Gateway (0) AP (2)	Switch (6) AC	(0) Router (1)				
🥡 De	evice List						
Device	e List 😋					IP/MAC/hostname/SN/Sr Q	Offline Devices Batch Upgrade
	SN \$	Status 💠	Hostname \$	MAC \$	IP \$	Software Ver	Model \$
	CAP70CA00054C	Online	ruijie 🖉	30:0D:9E:D0:87:C2	192.168.110.57	ESW_1.0(1)B1P7,Release(08202314)	RG-ES209GC-P
	G1PD494011658	Online	ruijie &	30:0D:9E:49:7E:85	192.168.110.144	ESW_1.0(1)B1P20,Release(09201814)	RG-ES216GC
seal	H1RU72F000510	Online	Ruijie [Master] 🖉	28:D0:F5:E3:3A:86	192.168.110.1 <i>&</i>	ReyeeOS 1.95.1914	EG105GW-X
	G1RU85X002932	Online	Ruijie 🗸	28:D0:F5:FF:9A:9D	192.168.110.29 🌊	ReyeeOS 1.212.2322	NBS5100-24GT4SFP-P
	G1NWB1S00026B	Online	Ruijie 🖉	00:D0:F3:33:38:61	192.168.110.251 🖉	ReyeeOS 1.86.202	NBS3100-24GT4SFP-P
	MACCNBS320056	Online	Ruijie 🖉	00:D0:F8:D8:9C:A3	192.168.110.5 &	ReyeeOS 1.218.2428	NBS3200-24GT4XS
	CAR41NR024704	Online	Ruijie 🖉	54:16:51:3A:30:BB	192.168.110.7 <i>d</i> _	ReyeeOS 1.206.2216	NBS3100-8GT2SFP-P
	G1RUAGJ000231	Online	Ruijie Z	10:82:3D:13:E7:87	192.168.110.147 <i>&</i>	ReyeeOS 1.95.211	RAP2260(H)
	G1RU9GP000991	Online	Ruijie &	70:42:D3:01:A0:FD	192.168.110.166 🌊	ReyeeOS 1.219.1407	RAP2260
< 1) > 10/page >						Total 9

(3) Add devices to Ruijie Cloud. The devices go online, and the topology is displayed under **Topology**.



3.2 Connection and Configuration of Wireless bridge

Application Scenario

RG-EST series wireless bridge can build up tunnel to transmit video for elevator and long range. It can not only monitor the wireless status in real time, but also save cost for end-users.

Procedure

- (1) Power on the paired wireless bridges and install them in the right place.
- (2) Ensure that is no shelter between the wireless bridges.
- (3) Check the LED status of the wireless bridges to ensure that the device is bridging successfully. You also can check the bridging status on the device's eWeb.

Ruíjie	l ≜Rcycc ≖					English ~	Camera (CPE) & Pair Again	
	WDS Group Info WDS Groups : 1				X WDS Password 🕖	X Admin Password 🜒	X IP Allocation 🕘 🕺 X SSID	0
② LAN								
% Wireless	WDS Group1 Change WDS Password AP: 1 (NVR-SIDE)	Channel :56	L	stency (): Fluent(1) Jitter(0) Freeze(0)	Bandwidth @: Good(1) Medium	0) Poor(0)		~
Advanced	CPE: 1. (Online: 1, Offline: 0)	WDS SSID @Ruljie-wds-011F	In	terference (0: Good(1) Medium(0) Poor(0)	RSSI @. Good(1) Medium(0) Po	or(0)		
♀ Diagnostics			Strong Signal: -	Medium Signal: — Poor Signal: —				
	◇ NVR (AP)					ି Camera (CPI	=)	
≫ System Tools ~	NVR-SIDE 2 MAC: 28:d015:05:01:11 P 192:168:110:27 Online		Latency tims Ra	te → 6Mbps Flow → 16.5 ← 400Mbps Flow ← 4.22	5Kbps RSSI-6db Uptime 10Min13Sec	CPE-S EST310 V2 IP: 192	NDE ℓ > 16 ⊕ ~ 28. d0:15. 05. 00: 51 2. 168. 110. 28 Online	

(4) Add the SN of wireless bridge to Ruijie Cloud. After wireless bridge is online on Ruijie Cloud, the connection status of wireless bridge could be monitored via Ruiie Cloud.

Ruíjie 📥		Project							LOGO abcdefg	e ^{111.e} ∨ ⊕	¢ <mark>©</mark> ⇔	@ 8
CCTV	Wireless	Bridge List										
G Workspace	Add Netv	work Bridge	Upgrade Web CLI	eWeb	Enter device SN, alia	as or model Q						0 88
🖏 Smart Config		Status	₩ SN	Model	Config Status	Alias 💠	Group	MAC	Management URL 👙	Egress IP		Action
Configuration		😋 ON	G1RP1CH129506	EST310-V2	Synced	CPE-SIDE	CCTV	28d0.f505.005f	192.168.110.28	45.127.187.248	ReyeeOS	Ē
Network-Wide		🙂 ON	G1RP1CH13014A	EST310-V2	Synced	NVR-SIDE	CCTV	28d0.f505.011f	192.168.110.27	45.127.187.248	ReyeeOS	Ē
Devices >										2 in total <	1 > 107	page 🗸
Authentication											_	

3.3 Creating a VLAN/DHCP

Application Scenario

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.

Procedure

(1) Adding a wired VLAN: 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**.



(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**.

Ruífe 📥 Home Project		1000 abcdefg@111.c 🗸 🕣 💭 💭 🛞 🔕
Network planning / Edit Wired VLANs		×
	1 Network Param 2 2 Wired Access – 3 Confirm — 4 Apply Config	
	Service Remarks: Guest-VLAN	
	VLAN ID: 40	
	Default Gateway/Subnet Mask: 192.168.40.1 / 255.255.255.0	
	IP Segment: 192.168.40.1 . 192.168.40.254	
	Assign IP from: (Gateway (Router) Usually for L2 network.	

(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.

Getwork planning / Edit Wied YLANs	
VLAN40 (Guest-VLAN) 192.168.40.1-255.255.255.0Selected 3 device(s)4 port(s)	Help Port Icon
Image: Configured: 0:05,08,012 Image: Configured: 0:05,08,012	Select All Deselect all Select All Deselect all
	Select All Deselect all
Image: Configured: 1 3 5 7 9 11 13 15 17 19 21 22 Image: Configured: Image: Configured	

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

	Network planning / Edit Wired VLANs	Wired Access	– S Confirm (4) Apply Config	×
	(ma)	To ensure that the work (G access2 CAP70CA00054C	uest-YLAN VLAN40 192.168.40.1–192.168.40.254) takes effect, configuration will be delivered to:idevices: Add VLAN 40[Auto Configuration]: The sets 6/0 is setforward as the Assessment VLANID 40	
5		CAR41NR024704	The port suc is compared as the Access port, VLAN ID 40 Add VLAN 40[Auto Configuration]: Add VLAN 40[Auto Configuration]:	
		core1 G1RU85X002932	The port GIS/GI8/GI12 is configured as the Access port, VLAN ID 40 Add VLAN 40[Auto Configuration]. Add VLAN 40[Auto Configuration].	
		core4 MACCNBS320066		
		Back	Apply	

3.4 Real Topology

3.4.1 Application Scenario

The real topology displays the actual network topology, which helps understand the device status, physical link connection between devices, and information about connected ports. When a fault occurs in the customer's network environment, the real topology helps quickly locate the fault, improving the troubleshooting efficiency.

3.4.2 Procedure

(1) Click a project name to open the project page.

Ruijie 🛆 Home Proje	ct								LOGO abodefg@1	11.e∨ ⊙ Ω	• • •
Project Devi 145 5 24	ce	Alarm 22		8							
Created (145) Received Sh	ared										
Add V Project Management En	ter project name Q										i≣ &
Network Name	Scenario	Alarms	Online Guests	AP	AC ¢	Gateway 👙	Switch 👙	Home Router 👙	Network Bridge 👙	Running Time	Action
🚖 shiyan	h	0	0	1/1		1/1	1/1			0 days	E- < ∶
* DemoProject2	品	0 🕶	0	5/5		1/1	5/5			0 days	ŀ < :
* DemoProject1	品	0 🕶	0	5/5		1/1	5/5			0 days	0- < ∶
* School	lh.	0	0	0/0						0 days	0- < ∶
CCTV	a	2	0	2/2		1/1	6/6		2/2	0 days	0- < ∶
* CCTV5	<u>a</u>	0	0	0/0						2 days	B- < ∶
÷ CCTV11	A	0	0	0/0						2 days	B- < :
★ EG105GW-X	品	2	0	1/2		1/1	1/1			2 days	ē- < ∶
* TestEG209	<u>a</u>	0	0	0/0						3 days	B- < :
★ test123_1	<u>n</u>	0	0	0/0						5 days	G- < :
									147 in to	tal < 1 2 3 4	5 15 >

(2) Click Workspace and click View Topology to view the real topology of the project.



(3) Check whether the topology is consistent with the real topology. You can update and download the topology and detect devices.



(4) Click Edit to edit the topology. You can rename devices and add unmanaged devices.



(5) Click List to view the device list and confirm the device status.

Cookbook

Ruíjie 📥		Home I	Project						1060 abcdefg@111.c V	∕ ⊕ ⊈ <mark>®</mark> ⇔ ⊗ ⊗
CCTV	~	Workspace /	Actual Topology							_
Workspace		Actual T	opology							
🛱 Smart Config		Topology	List							
Configuration										C 86
Network-Wide			Online Status	T SN	Model	Device Name 👙	MAC Address	Management URL 👙	Sync	Offline Time
# Devices	>		ON O	G1NWB1S00026B	NBS3100-24GT4SFP-P	Ruijie	00d0.f333.3861	192.168.110.7	Synced	
	>		ON ON	MACC20220519A	EG305GH-P-E	Ruijie	00d0.c875.a845	192.168.111.18	Synced	
Monitoring			ON	CAP70CA00054C	ES209GC-P	ruijie	300d.9ed0.b7c2	192.168.110.12	Synced	
& Network-Wide	>		🕑 ON	CAR41NR024704	NBS3100-8GT2SFP-P	Ruijie	5416.513a.30bb	192.168.110.3	Synced	
Pevices	>		🙂 ON	G1PD494011658	ES216GC	ruijie	300d.9e49.7e85	192.168.110.8	Synced	
Clients	>		🙁 ON	G1RP1CH129506	EST310-V2	CPE-SIDE	28d0.f505.005f	192.168.110.28	Synced	2023-02-22 16:28:07
E Logs			🙂 ON	G1RP1CH13014A	EST310-V2	NVR-SIDE	28d0.f505.011f	192.168.110.27	Synced	2023-02-22 16:31:07
Delivery Center			ON O	G1RU85X002932	NBS5100-24GT4SFP-P	Ruijie	28d0.f5ff.9a9d	192.168.110.2	Synced	
			🙂 ON	G1RU9GP000991	RAP2260	Ruijie	7042.d301.a0fd	192.168.110.10	Synced	
			🙂 ON	G1RUAGJ000231	RAP2260(H)	Ruijie	1082.3d13.e787	192.168.110.11	Synced	
			🙂 ON	MACCNBS320066	NBS3200-24GT4XS	Ruijie	00d0.f8d8.9ca3	192.168.110.4	Synced	
									11 in	total < 1 > 20 / page >

(6) Click a device to view the device details.

Ruíjie 📥	Hom	e Project	1000 abodetgg 111.a V	L <mark>.</mark> ⇔ ⊗ ⊗
CCTV	~ @	Device Information		
G Workspace		TOPOLOGY List	ruijie 🖉 💿 Synced	More V
			SN: CAP70CA00054C Device modle:ES209GC-P Management IP:: 192.168.110.12	Details >
Smart Config		S9	Monitoring Configuration Diagnostics	
Configuration			Overview Port Rate PoE List Search Log History	
Network-Wide	>	WAND	Status	
I Devices	>			Instruction
Authentication	>	EG305GH-P-E SNIMACC20220519A	1 2 2 4 3 4 7 8 1	
Monitoring		(LAN1/		
🖧 Network-Wide	>	(Gi24) (Gi8)	Device Resources	
Pevices	5		Uplink Connection Status Last 24 Hours Last 7 Days	
			Port Port 2	
LLI Cilerita		NB53100-246145PF NB53100-46125PF-P SNEGTRU85X002932 SNEGAR41NR024704	Port speed: 1000M Dunley: Full-dunley	
🗟 Logs	>	G1 G3 G4	Uplink/Downlink 0.00Kbps ↑ 15:00 19:00 23:00 3:00 7:00 11:00	
Delivery Center	>	Port 2) (Gi24) (Gi24)	Speed (0): 9.00Kbps ↓ Uplink/Downlink 4.00K8 ↑	
		+ + +	Traffic 10: 43.00K8 4	
		ES209GC-P NB53100-24GT45FP NB53200-24GT4X5	Port Packet Statistics	
		SN:CAP70CA00034C SN:G1NWB15000268 SN:MACCNB5320066	Updated Time: 2023-02-23 15:19:53	0
		Gil Gil Port 16 WWAN	Port (KB) (KB/s)	Number of Conflicts
			Port 0/0 0.0/0.0 0/0 0/ 0/0	0
		EXCTORE RAP2280(H) SINGTPD494011658 SINGTRUMGD00231 4	Port 0/0 0.0/0.0 0/0 0/ 0/0	0
		đ	Dent	

3.4.3 Principle of the Network Topology

- (1) Make sure that the devices are online on Ruijie Cloud, and the Web CLI is available.
- (2) You require a root node device, which can be the EG or core switch.
- (3) Calculate all connected devices through the root node and update the topology; the data required are MAC, ARP and Routing, etc.

3.5 Automatic IPC Identification

3.5.1 Application Scenario

Ruijie Cloud can automatically identify IP cameras (IPCs) connected to switches in two ways:

- (1) Ruijie Cloud detects IPC traffic to identify IPCs.
- (2) Ruijie Cloud identifies IPCs based on NVRs connected to IPCs and added on Ruijie Cloud.

3.5.2 Procedure

(1) Connect an IPC to an NBS or ES switch. Wait for 20 minutes and log in to Ruijie Cloud to view the topology status.



(2) Add an NVR. Enter the IP address, vendor, username, and password of the NVR as prompted, and click **Save and Detect**.

Ruijie 📥	Home Project	1. By using the Ruijie Cloud platform,	you must have the management and usage right of the target computer		1060 abc			
		system devices. You are prohibited fro	om using the Ruijie Cloud platform (hereinafter referred to as the "Platform")					
CCTV11	IPC NVR Smart Clients	to log in to any unauthorized device	without authorization, and the Platform shall not assume any responsibility					
Workspace		arising therefrom.						
- monopose		2. By providing the required credentia	ils to log in to a target computer system device, you shall be deemed as	All switches				83
🖗 Smart Config	Detection Results	having authorized the Platform to log	in to the target computer system device using such credentials and to					
	IPCs detected by the Cloud	obtain, transmit, and store informatio	n about the system's hardware features and network connectivity status.				Unlink/Downlink	
Configuration	The K	3. After the above-mentioned system	is connected to the Platform, network security risks may increase. The		Port	PoE Status	Speed	· ·
Network-Wide	> IP:102.168.1.108 yendor:Debue	Platform shall endeavour to ensure th	e security and integrity of the information transmitted and used in the					
# Devices		system, but the relevant information	shall be used for operation and maintenance reference only, and the Platform		Gi9		ps	C
	+Add NVR	shall not guarantee the integrity and	accuracy of the information.					
Authentication	(Detect IPC through NVR)	4. The Platform reserves the right to t	erminate this service if you infringes the copyright of a third party and the		Gi2	enable	0.14Kbps/2.08Kbp	С
Monitoring		Platform is notified by the copyright	wher or the legal agent thereof.		_	_		
		5. The service may be adjusted or sus	pended due to technical development and other external factors, and the			2 in tot	al < 1 > 10/page	e v
88 Network-Wide	>	Platform shall not be held liable for a	ny loss caused by the discontinuation of service.					
Devices	>		I Agree					
Clients	>	• IP address:						
🖭 Logs	3 	Vendor:						
Delivery Center	>							
		* Username:						
		NVR Password:	ø					
		Name:						
		• IPC - Uplink Switch Type:						
			Cancel Save and Detect					

(3) After the NVR goes online, the IPC information is displayed in the NVR list.

Cookbook

	CCTV11		IPC NVR S	mart Client	is k	Key Clients	IP Phone								
	ගි Workspace														
	🐕 Smart Config		Add NVR More V											Q	88
	Configuration		Status		Name	IP as	idress	Vendor	Username	Switch	Port	Quantity	Last Update	Action	
	Network-Wide		Connected		NVR	192.10	58.1.108	Dahua	admin	Ruijie	Gi9	23	2023/02/21 14:16:58	🕑 Edit 🖞 Dr	elete
	Devices														
	Authentication														
1	Monitoring														
	እetwork-Wide														
,	P Devices														
	Clients	>													
	🛱 Logs														
	ab Delivery Center														
	CCTV11		IPC NVR Sn	nart Clients	Ke	ey Clients	IP Phone								
6	බ Workspace				0.00		1.1.5.0.000								
ş	🎖 Smart Config		Detection Results		U NVK C	connection succe	eded. Edit NVR confi	guration						0	88
c	Configuration		IPCs detected by the Cloud		Detect ag	ain Client t	ype 🗸 🛛 More 🧸		(La	ast Update: 2023/02/2	1 14:17:00) All switc	hes	Channel name, IP ad	dre Q	
6	Network-Wide		NVR IP:192.168.1.108 vend	lor:Dahua		Status	MAC Address	Channel ID	Channel Name	IP Address	Switch	Port	PoE Status Upli	nk/Downlink	,
Ξ	# Devices													Speed	
9	Authentication		(Detect IPC through NVR			⊘ Online		1	HK-1	192.168.1.1				-/-	0
Ν	Monitoring					⊘ Online		2	通道21	192.168.1.2				-/-	C
ê	& Network-Wide	>				⊘ Online		3	Camera 01	192.168.1.24				-/-	C
8	Devices					⊘ Online		4	UNV-25	192.168.1.64				-/-	C
ć	Clients	>				⊘ Online		5	HK-5	192.168.1.5				-/-	C
6	E Logs					⊘ Online		6	Camera 01	192.168.1.6				-/-	C
q	Conter Center					Online		7	Camera 01	192.168.1.7				-/-	C
						Online		8	HK-19	192.168.1.8				-/-	Ċ
						Online		9	HK-9	192.168.1.9				-/-	C
						⊘ Online		10	IPC-10	192.168.1.10				-/-	C
												23 in total	1 2 2 2 10/22	co V Co to	

Principle:

Scenarios without NVRs

1. To identify traffic of an IPC, the identification algorithm depends on the following information:

- (1) 30-minute switch traffic data
- (2) MAC address of the switch port connected to the IPC.
- (3) ESW or managed NBS switch directly connected to the IPC.

2. IPC triggering method.

- (1) Proactive triggering: manually click the Ruijie Cloud app.
- (2) Passive triggering: Ruijie Cloud traverses' devices in the early morning every day to identify the IPC.

3. Available information (can be displayed)

- (1) MAC address of the IPC
- (2) Switch port connected to the IPC
- (3) Switch port traffic (presented as IPC traffic externally)
- (4) Switch port status (presented as IPC connection status externally)
- (5) PoE power supply status of the switch port (presented as IPC power supply status externally)

Scenarios with NVRs

1. With the built-in HTTP client, Ruijie Cloud connects to an NVR through a remote tunnel to obtain related information.

2. The NVR identification algorithm depends on the following information:

- (1) A device that supports tunnels exists on the network, and the device can ping the NVR at layer 3.
- (2) NVR information entered by the user: IP address, vendor and model (optional), username, and password of the NVR

3. Triggering method

- (1) When the depending information is available, Ruijie Cloud proactively obtains the IPC information.
- (2) The frontend determines whether to display the latest time for obtaining information and whether to provide an API for users to manually trigger updates.

4. Available information (can be displayed)

- (1) IP address of the IPC
- (2) IPC status
- (3) MAC address of the IPC

3.6 ACL Configuration

3.6.1 Application Scenario

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.

3.6.2 Procedure

Configuring Service Access Control

Choose Configuration > Network-Wide > Security > ACL.

습	Workspace					
5	Smart Config					
Co	nfiguration			nterworking Zone Isolation	n Zone Access C	Control List (ACL)
۲	Network-Wide	>	Network	Optimization	Security	ervice network to the Interworking Zone or Isolation Zone, you can assign
ţ.	Devices	>	VLAN	Wi-Fi Optimization	ACL	stor mutual access between network segments to ensure network ature is commonly applied in enterprise, education and other project
\otimes	Authentication	>	Multi-WAN	Loop Prevention	ARP Spoofing Guard	, in a project, separate access permissions should be assigned to visitors, and servers.
Mo	onitoring			DHCP Snooping		1
品	Network-Wide	>				
0	Devices	>				
Ĺ.	Clients	>				
3h	Logs	>				

(1) Click To configure to go to the Access Control List (ACL) 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.

命 Workspace										
🖏 Smart Config										
Configuration		Interworking Zone	Isolation Zone	Access Control List (ACL)						
Ø Network-Wide	>	r ⊟ ↔ E		By dragging a service network to the Interworking Zone or Isolation Zone, you can assign access permissions for mutual access between network segments to ensure network security. This feature is commonly applied in enterprise, education and other project						
∃ Devices	>		a بریست :							
\bigotimes Authentication	>			types. Generally, in a project, separate access permissions should be assigned to visitors, finance system and servers.						
Monitoring		N		To configure						
品 Network-Wide	>	1 4								
Devices	>									
Clients	>									
딸 Logs	>									
 Logs ᢍ Workspace 	Access	s Control List (ACL)	to the [Interworking Zo	one] or [Isolation Zone] as requir	ed, More					
 Logs Workspace Smart Config 	Access	s Control List (ACL)	to the [Interworking Zo	one] or [Isolation Zone] as requir	ed, More					
 Logs Workspace Smart Config Configuration 	Access D Interviservice	s Control List (ACL) rag a service network to working Zone e networks in the Interworl	to the [Interworking Zo	one] or [Isolation Zone] as require	ed, More Isolation Zone ⑦ Service networks in the Isolation Zone cannot access each					
 E Logs Workspace Workspace Smart Config Contiguration Network-Wide 	> Access ① D Inter Servic other >	s Control List (ACL) rag a service network to working Zone e networks in the Interwork	to the 【Interworking Zone can access each	one] or [Isolation Zone] as requir	ed, More Isolation Zone ⑦ 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					
 Logs Workspace Smart Config Configuration Network-Wide Devices 	> Access Access Interv Servic other VLL VLL	s Control List (ACL) rag a service network t working Zone e networks in the Interworf AN 1 VLAN1	to the 【Interworking Zo	one] or [Isolation Zone] as requir	ed, More Isolation Zone 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					
 E Logs Workspace Workspace Smart Config Contention Network-Wide Devices Authentication 	> Access Access Inter Servic other VL 192 >	s Control List (ACL) rag a service network t working Zone e networks in the Interwork AN 1 VLAN1 2.168.110.1/255.255.255.0	to the [Interworking Zo	one] or [Isolation Zone] as require	ed, More Isolation Zone ③ 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					
 E Logs Workspace Smart Config Smart Config Control Network-Wide Devices Authentication Workspace 	 Access Dintern Servic other VL VL 192 	s Control List (ACL) rag a service network t working Zone e networks in the Interwork AN 1 VLAN1 2.168.110.1/255.255.255.0 ning Room VLAN2 2.168.21.1/255.255.255.0	to the [Interworking Zo	one] or [Isolation Zone] as require	ed, More					
 Logs Workspace Smart Config Smart Config Smart Config Network-Wide Network-Wide Authentication Authentication Motoring Network-Wide 	 Access Di Intervision Servic Other VL 192 Dia 192 Dia 192 	s Control List (ACL) rag a service network t working Zone e networks in the Interwor. AN 1 VLAN1 2.168.110.1/255.255.255.0	to the [Interworking Zo	ene] or [Isolation Zone] as require	ed, More Isolation Zone ⑦ 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 Service networks to which you want to grant access					
 Elogs Workspace Smart Config Smart Config Internation Network-Wide Authentication Authentication Network-Wide Network-Wide Devices 	 Access Intern Servic other VL 192 Dia 192 2 	s Control List (ACL) rag a service network t working Zone e networks in the Interwor AN 1 VLAN1 2.168.110.1/255.255.255.0 ning Room VLAN2 2.168.2.1/255.255.255.0	io the [Interworking Zo	one] or [Isolation Zone] as requir	ed, More Isolation Zone ③ 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 Service networks to which you want to grant access permissions Drag					
 Elogs Workspace Smart Config Smart Config Touriguration Network-Wide Authentication Motoring Network-Wide Povices Network-Wide Devices Devices Clients 	> Access Access Intervise VL VL P Din 192 Din 192 Din 192 Din 192 Din 192 Din	s Control List (ACL) rag a service network t working Zone e networks in the Interwor AN 1 VLAN1 2.168.110.1/255.255.255.0 ning Room VLAN2 2.168.2.1/255.255.255.0	to the 【Interworking Zo	one] or [Isolation Zone] as require	ed, More					

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

	Access Control List (ACL)						
សៃ Workspace	 Drag a service network to the [Interwork] 	king Zone] or [Isolation Zone] as required, More					
Smart Config		the state of the s					
Configuration	Service networks in the Interworking Zone can acc	ess each other		Isolation zone (7) Service networks in the Isolation Zone cannot access each other. If necessary, a network segment or IP can be added for			
Network-Wide				mutual access between a certain service network in the isolation Zone and the one in the interworking Zone			
# Devices	VLAN 1 VLAN1 CCTV 192.168.110.1/255.255.255.0 192.10	FVLAN VLAN20 58.1.1/255.255.255.0		Guest-VLAN VLAN30			
Authentication :				IP NoIP			
Monitoring							
& Network-Wide							
P Devices							
Clients			Cannot access each other				
E Logs							
Delivery Center							

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

No IP:

- 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**.

	Access Control List (ACL)			
Workspace	Drag a service network to the	Interworking Zon	e] or [isolation Zone] as required, More	
🖏 Smart Config				
Configuration	Interworking Zone Service networks in the Interworking Zon	re can access each	Add Accessible IP X	solation Zone cannot access each other. If recessary a network segment or IP can be added fo
Network-Wide				and a second car the internation of the contract work and the second of the track of the
🗄 Devices	VLAN 1 VLAN1 192.168.110.1/255.255.255.0	CCTV-VLAN 192.168.1.1/25	Please enter or select VLAN30/Guest-VLAN (192,168.30.1/255.255.255.0) IP or IP range for mutual access	130 255.0
Authentication			Existing service networks Custom IP range Single IP	
Monitoring			192.168.30.22	
🇞 Network-Wide				
2 Devices				
1) Clients				
🗄 Logs				
2 Delivery Center				
			Cancel Save	

3.7 IPC Access through an Extranet and Server Penetration through an Intranet

3.7.1 Application Scenario

Through intranet access, you can add a remote management tunnel to manage devices on the intranet using the eWeb management system. In addition, you can add a tunnel to access intranet monitoring devices, such as NVRs and IPCs.

3.7.2 Procedure

Choose Configuration > Devices > General > Intranet Access.

Workspace		(1) Through inte	ranet access, you can a	add a remote manag	ement tunnel to manage	devices on the intranet u	using the eWeb man	agement sys
Creat Carta		Custom	Device					
Smart Config								
onfiguration								
Network-Wide	£							
# Devices		General	Gateway	Switch	Wireless			
Authentication	8	Intranet Access	Interface	Interface	AP Mesh			
Monitoring		Project Password	Routing	Port Settings	SSID			
Network-Wide	2	ACL	NAT	VLAN	Radio			
Devices	ŝ	CLI Config Task	Dynamic DNS	Routing	Roaming			
7		Batch CLI Config	IPTV	Voice VLAN	Rate Limit			
Clients	20		Portal Auth		Load Balancing			
E Logs	8		VPN					
Delivery Center	8				AP VLAN			

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

A		① Through intranet access, you can add a remote management tunnel to manage devices on the intranet using the eWeb management system.							
ъ workspace		Custom Device							
% Smart Config									
Configuration									
Ø Network-Wide	>								
🛱 Devices	>	+Add Tunnel							
\bigotimes Authentication	>								
Monitoring									
🖧 Network-Wide	>								
Devices	>								
Clients	>								
🕼 Logs	>								
Delivery Center	>								

CCTV									
A Wadaaaa	Through intranet access, you can add a remote management tunnel to manage devices on the intranet using the eWeb management system.								
workspace	Custom Device								
🕏 Smart Config									
Configuration									
Ø Network-Wide			_						
# Devices	+Add Tunnel	Add Tunnel	×						
		t for Newsy DOP							
Monitoring		* App Name.							
& Network-Wide		App Icon: 😑 📖 💫 🙆							
P Devices									
f] Clients		App Type: HTTP HTTPS 							
		Inside Host: 192.168.1.108 80							
E cogo									
Delivery Center									
		Cancel	ок						

Cookbook

VT22							
		① Through intranet access, you can add a remote management	t tunnel to manage devices on the intranet using th	e eWeb management sy	stem.		
G Workspace		Custom Device					
🖏 Smart Config							
Configuration	onfiguration		NVR		HTTP_Server		
Network-Wide			Inside Host & port		Inside Host & port		
# Devices		+Add Tunnel			192.108.110.43.00		
Authentication							
Monitoring			⊕To configureEdit	🗇 Delete	⊕To configure 🖉 Edit	🗇 Delete	
🗞 Network-Wide					_		
P Devices					×		
Clients			Creating the tunnel conn	ection please wait.			
E Logs							
2 Delivery Center							
😂 Delivery Center							



3 🛦 不安全 34.142.173.36.65467	ピ ☆ □	4
3 A Fréde 134,142,173,3665467 Lopin Immes.contention Size Timestamp Hits Immes.contention Size Timestamp Hits Immes.contention Size Size Timestamp Hits Immes.contention Size Size Timestamp Hits Immes.contention Size Size Size Size Immes.contention Size Size Size Size Immes.contention Size Size Size Size Immes.contention Size Size Size Size Size Immes.contention Size Size Size Size Size Size Immes.contention Size Size	<i>€</i> ☆ □	4
afomation vs 2.5m net 2008-45		

3.8 Voice VLAN

Application Scenario

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.

Procedure

Choose Configuration > Devices > Switch > Voice VLAN.

12						
₩ ₪	/orkspace					
			Settings	OUI Port S	settings	
% Sn	mart Config					
6			When the volume	oice VLAN feature is e	nabled, the CoS prior	rity of voice data should
Config	guration		transmission	1.		
@ Ne	etwork-Wide			Switch:		
击 De	evices		General	Gateway	Switch	Wireless
	uthentication					
V H	anientication		Intranet Access	Interface	Interface	AP Mesh
Monit	toring		Project Password	Routing	Port Settings	SSID
	5			nouting	, or coordings	0010
& Ne	etwork-Wide	3	ACL	NAT	VLAN	Radio
			CLI Config Task	Dynamic DNS	Routing	Roaming
E De	evices	2	Batch CLI Config	IPTV	Voice VLAN	Rate Limit
бП Cli	lients		Sector Sector Sector			
				Portal Auth		Load Balancing
E Lo	ogs	20		VPN		
						AP VLAN
2 De	elivery Center					

3.8.1 Voice VLAN Settings

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

☆ Workspace	Settings OUI Port Settings
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:
章 Devices >	VLAN: YLAN
Monitoring	• Aging Time: 1440 ⑦
윦 Network-Wide >	COS Priority: 6 V
P Devices	
Clients >	Save
Logs >	
😂 Delivery Center >	

3.8.2 OUI Settings

The enabled globally port will automatically add the corresponding OUI when receiving an LLDP packet that is identified as telephone.

Cookbook

俭 Workspace	Settinas OUI Pa	rt Settings	
🖏 Smart Config			
Configuration	• The enabled globally port will	automatically add the corresponding OUI when receiving a	an LLDP packet that is identified as telephone. Up to 24 entries can be added.
⊗ Network-Wide >	OUIs		
r Devices →	MAC Address	Description	Action
			+ Add
Monitoring			
🖧 Network-Wide >			
Devices			
1 Clients			
E Logs			
📚 Delivery Center 💚			

3.8.3 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.

硷 Workspace		Settings	OUI Port Settings			
🖏 Smart Config						
Configuration		The port c first, and a mode (true	an be set to the automatic mod utomatically join the voice VLA nk/access mode). To switch the	le only when the port VLAN is in the trunk mode. Wi N until it receives voice data again.To ensure the nor mode, please disable the voice VI AN 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 to not switch the port
Network-Wide	×.	mode(tru	nyaccess modej. To switch the	nice, please disable the voice vibra hist.		
I Devices	>	Port List				∠ Batch Edit O
	×	Port	Enable	Voice VLAN Mode	Security Mode	Action
Monitoring		Tort	Lindoc	Voice Vent mode	Scenty mode	Action
🖏 Network-Wide	>	Gi1	Disabled	Auto Mode	Enabled	Edit
P Devices	>	Gi2	Disabled	Auto Mode	Enabled	Edit
Clients	2	Gi3	Disabled	Auto Mode	Enabled	Edit
🕼 Logs	>	Gi4	Disabled	Auto Mode	Enabled	Edit
Delivery Center	×.					
Edit						Х
			Enabled :			
		Voice	VLAN Mode: Auto	Mode v		
		Se	curity Mode: 🗾			
					Cancel	Confirm

3.9 Delivery Report

Application Scenario

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.

Procedure

(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.



Cookbook

CCTV11		Edit						SRefresh @Preview @Download Report
硷 Workspace								
🖏 Smart Config					CCTV11Report 🖍			
Configuration		1. Cover						1. Cover 2. Basic Information
Network-Wide	>							 VLAN and Address Pool Diagnosis
Devices	>	Project Report						5. Device 6. Topology
\oslash Authentication	>							7. Appendix
Monitoring		2. Basic Information						
🗞 Network-Wide	>	LOGO	You are advised to upload the image with t	he size of 420 x 112.				
Pevices	>		Only files in PNG, JPG, JPEG, and BMP for	rmats are supported.				
Clients	>		The image cannot exceed 100 KB.					
E Logs	>		Project	Tenant	Default			
Se Delivery Center	>		Upload	Upload	Ruíjie	Reyce		
		Copyright	All Rights Reserved®XXX					
		Delivery Time	2023-02-21	110				
		Description	XX Project					
								le la
		Team 🗹	Display in Report					
		Na	ame	Job		Phone	Action	
					No Data			

(3) You can view service configuration of the general solution in the delivery report.

3. Office Service Configuration						
3.1 Wired Network Planning						
Wired Network Planning		IP Address Range	v	'LAN ID IP	Address Allocation Mode	
VLAN1		192.168.110.0//24	1	Dł	HCP	1.Select report theme 2.Basic information
3.2 WLAN Network Planning						3.Common Solutions Service configuration 4.Configuration smart
WLAN Network Planning	SSID	Password	IP Address Range	VLAN ID	IP Address Allocation Mode	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	prevent network failure c	aused by unauthorized rou	ters or DHCP servers.		
Smart Flow Control	Limit the network sp	eed of clients flexibly.				

(4) Check the network topology.

CCTV11		4	ruijie	G1PD494011658	ES216GC	300d.9e49.7e85	192.168.110.8		Ad	1		Ad	1
A		5	CPE-SIDE	G1RP1CH129506	EST310-V2	28d0.f505.005f	192.168.110.28		Ad	1		Ad	1
1㎡ Workspace		6	NVR-SIDE	G1RP1CH13014A	EST310-V2	28d0.f505.011f	192.168.110.27		Ad	1		Ad	1
🖏 Smart Config		7	Ruijie	G1RU85X002932	NBS5100-24GT4SFP-P	28d0.f5ff.9a9d	192.168.110.6		Ad	1		Ad	1
Configuration		8	Ruijie	MACC20220519A	EG305GH-P-E	00d0.c875.a845	192.168.111.18		Ad	1		Ad	1. Cover 2. Basic Information
Network-Wide	5	9	<u>Ruijie</u>	MACCNBS320066	NBS3200-24GT4XS	00d0.f8d8.9ca3	192.168.110.4		Ad	1		Ad	3. VLAN and Address Pool 4. Diagnosis
I Devices	>	6. Top	plogy										5. Device 6. Topology
	>						Topology						7. Appendix
Monitoring													Iorizontal Vertical
备 Network-Wide	>							Gil	Port 2	ES209GC-P	-Port 5		5869.6cce.73e1
Pevices	>												
Clients	5										GI	Port 16	Switch
E Logs	5									Switch			ES216GC
2. Delivery Center	,							GI3	- Gi24)	NBS3100-24GT4SF	-		
ap bennen y bennen											63	WAN	RAP2260(H)
						(LANO) Gi8)	Switch				(65)		
					Gateway		NBS3100-8GT2SF						805e.0c6c.8b95
				WAN (WAN	eg305GH-P-E		Dullah			Culture			NB/D
						Gi24	NBS5100-24GT4SF	Gi4	-Gi24	NBS3200-24GT4XS	- Gi9		NVR +
													-
		7. App	endix 🗆 Ad	d to PDF appendix				Gis	WAN	AP 	GII		0c11.0503.28/4

(5) Click **Download** at the upper right corner to download the delivery report in PDF and Word formats.



4 Maintenance

4.1 Remote IPC Operations — IPC Restart and Long-Distance Power Supply

4.1.1 Application Scenario

Real-time Failure Notification would notice users that camera failure in the first place; Remote Reboot Camera helps you one-click to restart the camera at home, no need onsite any more.

4.1.2 Procedure

(1) Real-time Failure Notification: When an IPC is offline, Ruijie Cloud provides real-time alarm information, helping master the real-time IPC status.

The app receives an IPC offline alarm.

<	Message	
() New version		2023-02-22 10:29
Notice: New versio You can update nov	n is available v.	e.
View More		>
() IP camera may b	be offline	2023-02-22 10:07
Device:Unnamed D	evice(CAP7	0CA00054C)
Type:ES209GC-P		
Alarm: IP camera m the port 5 o	nay be offlin r reboot the	e. Please check camera.
Come and fix the pr	roblem!	
Fix		>
Delete		>
Disable These Alarr	ns	>

You can view offline IPCs through the topology.

<	Act	ual To	pology		
Gateway:	1/1 Switc	h: 6/6	Wirele	ss AP: 2	2/2
Topo is inco	mplete?				6
					Θ
					Q
					৶
					윦
			C NET O		
100954-8-4 per successions			Mentors -	ster	Vitram P.Prot.
		6	10000 10 10000 10 10000	90 	8
					0

(2) Remote Reboot Camera: Remotely operate an IPC through the Ruijie Cloud app, for example, restart the IPC and set long-distance power supply.

When an IPC is abnormal, check the network cable status.

<	No alias		0
FULL UID		Luit	
Port Status: Copp Speed: J OMbps Packets: J 0	oer PoE 100M	Power Status: Power:	On 2.8W
Port Speed Mbps 0.012 - 0.009 - 0.006 - 0.003 - 0 0 06:18 06:18 06:18	46 07:17 07:53 08:	- O - Uplink - O 21 08:53 09:24	Downlink
Port Configurati	on		Edit >
Admin Status			Enabled
PoE Status		I	Enabled
Speed/Duplex		100M/Full	-duplex
Port VLAN VLAN: 20			Access
Cable 7	Test	(¹) Resta	rt

Restart the IPC.

<	0	D						
Port (9 por	2 3	4 5	6	7	Help 8			
Name	Status	Uplink ^ Mbps) ~	Power ^ (W) ~	Acti	on			
PortGi1 No alias	Disabled	0	0.0	Reboot	More			
PortGi2 Uplink port	1000M	0.000	0.0	Reboot	More			
PortGi3 No alias	Disabled	0	0.0	Reboot	More			
PortGi4 No alias	Disabled	0	0.0	Reboot	More			
PortGi5 No alias	100M	0	2.8	Reboot	More			
View More $$								

Port Status: Copp Speed: John OMbps Packets: John O	oer PoE 100	M Power Status: • Power:	On 2.8W		
Port Speed Mbps 0.012		- O- Uplink - O -	- Downlink		
0.00	Tin				
0.00	TIP				
^{0.00} Are you su of interfac	ire you want to e 5?	o reboot the PoE	10:30		
Canc	el	ОК	>		
Admin Status		E	nabled		
PoE Status		Enabled			
Speed/Duplex		100M/Full-	duplex		
Dent MI AN					

The IPC goes online again.

< Actual Topology



If an IPC needs long-distance power supply, configure it in the Ruijie Cloud app.

< 	Unna	amed Sw	itch	20
Port (9 port	ts)			(?) Help
	2 3	4 5		7 8
Name	Status	Uplink ^ (Mbps) ~	Power ^ (W) ~	Action
PortGi1 No alias	Disabled	0	0.0	Reboot More
PortGi2 Uplink port	1000M	0.000	0.0	Reboot More
PortGi3 No alias	Disabled	0	0.0	Reboot More
PortGi4 No alias	Disabled	0	0.0	Reboot More
PortGi5 No alias	100M	0	2.8	Reboot More
	Vie	w More		
	V Settings			
€; Long	-distance Tra	nsmissior	1	



The negotiated rate of the corresponding switch port is changed to 10 Mbps.

<	Unn	amed Swi	tch	<u></u> 20
1	2 3	4 5	6	7 8
Name	Status	Uplink ^ (Mbps) ~	Power ^ (W) ~	Action
PortGi1 No alias	Disabled	0	0.0	Reboot More
PortGi2 Uplink port	1000M	0.001	0.0	Reboot More
PortGi3 No alias	Disabled	0	0.0	Reboot More
PortGi4 No alias	Disabled	0	0.0	Reboot More
PortGi5 No alias	1 10M	0	2.6	Reboot More
PortGi6 No alias	Disabled	0	0.0	Reboot More
PortGi7 No alias	Disabled	0	0.0	Reboot More
PortGi8 No alias	Disabled	0	0.0	Reboot More
PortGi9	Disabled	0	0.0	Reboot More

4.2 Loop Prevention Configuration

4.2.1 Application Scenario

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.

4.2.2 Procedure

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

습	Workspace						
5	Smart Config						
Co	onfiguration						
0	Network-Wide	>	Network	Optimization	Security	Loop	p Prevention (RLDP)
ħł	Devices	>	VLAN	Wi-Fi Optimization	ACL	Enabli conge	ng loop protection can avoid network stion and disconnection caused by loops. Ports
\otimes	Authentication	>	Multi-WAN	Loop Prevention	ARP Spoofing Guard	conne disabl	cted to the switch will be automatically ed after a loop occurs.
М	onitoring			DHCP Snooping		0	atimize Now
8	Network-Wide	>					Junize Now
	Devices	>					
Ó.	Clients	>					
	Logs	>					
습 尽 Cor	Workspace Smart Config figuration						
0	Network-Wide	×		Switch	Faulty port number will be sent for		Loop Prevention (RLDP)
抖	Devices	>			handling		Enabling loop protection can avoid network
\otimes	Authentication	>		L.	A network loop		congestion and disconnection caused by loops. Ports connected to the switch will be automatically disabled after a loop occurs.
Мо	nitoring						Ontimize Now
ጽ	Network-Wide	Σ					Optimize Now
	Devices	×					
ſ.	Clients	×.					
192	Logs	>					

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



When a loop occurs, an alarm is reported.

πυίπο 📥	Home	Project					L060 abo	lefg@111.c > 🕀 🗘	° © ©
Project 145	•	Device 40 • 6 devices have new version.							
CCTV									
Ignore Alarm	s Export Alarms	SN Q				Not cleared Cleared	Start D	ate ~ End Date	0
	Alarm Type 🛛 🖓	Alarm Severity 🙄 Group	Alarm Source 🛛 🖓	Device SN	Alias	Generated at	Cleared at	Updated at	Action
	Switch loop	Moderate abcdefg@111.com/CCTV	Device	MACCNBS320066	Ruijie	2023-02-23 11:43:26		2023-02-23 11:43:25	3
	Switch loop	Moderate abcdefg@111.com/CCTV	Device	MACCNBS320066	Ruijie	2023-02-23 11:43:26		2023-02-23 11:43:25	6
								2 in total < 1 >	10 / page ∨

Log in to the eWeb management system of the device to view the device port status and alarm information.

R	Network	~				Nav	vigation Q English ~ 🛆	Remote O&M 🛛 🐣 Network	Setup @Network Check	蓝 Alert □ Log Out
a A	🚺 Vie	w and manage ala	arms.							
መ ጽ	Alert L	ist							View U	Infollowed Alert
	Expand	Alerts			Su	ggestion			Action	
11	~	Loops Occur			Ple	ase check the network environment.			Delete Unfollow	
8		Hostname	SN	Туре	Time	Details		Action		
-0- -0-		Ruijie	MACCNBS320066	NBS3200- 24GT4XS	2023-02-23 11:40:35	Loops Occur		Delete		
	Ŷ	Power supply	is insufficient.		Un	der voltage may affect device performance or cause device device.	reboot. Please check the power	r supply	Delete Unfollow	
		Hostname	SN	Туре	Time	Details		Action		
		Ruijie	G1RUAGJ000231	RAP2260(H)	2023-02-23 11:40:20	Currently, 802.3at PoE power supply is used. A PoE switch or power supply module compliant with IEEE 802.3bt standard is needed to provide power for the device.		Delete		
	< 1	> 10/pa	ge v							Total 2
										e
>										

Device List Port Statu Device List © Port EN © ENE(0) Port	Port Status
Device List C Port	Panel Vie
- SN © Status © Hostname ©	
Mare	
CAP70CA00054C Online nuijie 2	2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28
G1PD494011658 Online ruijie &	
MACC20220519A Online Ruije (Master) 2	VLAN Ec
G1RU85X002932 Online Ruijie 2	VLAN1 VLAN20 VLAN30
CAR41NR024704 Online Ruijie &	Interface IP Address IP Range Remarks
MACCN85320066 Online Ruijie 2	Gi5-8,Gi13-24,Te25-28
G1NW815000268 Online Ruijie 2	
G1RU9GP000991 Online Ruijie 2	
G1RUAGJ000231 Online Ruijie 2	2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28

View switch details and confirm the port status on Ruijie Cloud.



5 Troubleshooting

5.1.1 Ruijie Cloud Cannot Automatically Identify an IPC

- (1) After an IPC is powered on, wait for about 20 minutes and then check whether it can be identified by Ruijie Cloud.
- (2) Log in to the switch connected to the IPC and check whether the traffic over the switch port is normal and stably uploaded to Ruijie Cloud.
- (3) Check whether the device connected to the IPC is an NBS or ES series switch.
- (4) If an NVR is deployed, you are advised to identify the IPC through the NVR. Ensure that the IP address, username, and password of the NVR are correct, a device that supports tunnels exist on the network, and the device can interconnect with the NVR.

5.1.2 IPC Is Offline

(1) Based on the real topology on Ruijie Cloud, locate the switch connected to the offline IPC and the corresponding port number.



(2) Log in to the switch and view the port details.

E Device Information					
TOPOLOGY List	ruijie ∠ Synced	D	Device modle:ES209GC-P	Managem	ent IP:: 192.168.110.2
se 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 19	Monitoring	Configuration	Diagnostics		
	Overview Pr	ort Rate PoE List	Search Log	History	
WAND	PoE Port List				
	Total PoE Power:120.00	W, Current Power:2.71 \	N, Time: 2023/2/22 10:27:23		
SN:MACC20220519A	Port	PoE-capable	PoE Status	The Power	PD class
LAND LAN1/	Port 1	Open	Disabled	0.00 W	0
	Port 2	Open	Disabled	0.00 W	0
	Port 3	Open	Disabled	0.00 W	0
NBS3100-8GT25P-P- NBS5100-24G145FP SN:CAR41NR024704 SN:G1RU85X002932	Port 4	Open	Disabled	0.00 W	0
G3 G4 G5	Port 5	Open	Open	2.71 W	3
Gi24 Gi24 (WAN)	Port 6	Open	Disabled	0.00 W	0
AP	Port 7	Open	Disabled	0.00 W	0
S4C ShiGTNU/2401937/ ND5200-2401937/ ND5200-240193/ ShiGTNU/2401937/ ShiGTNU/2401937/ ShiGTNU/2401937/	Port 8	Open	Disabled	0.00 W	0

- (3) If the port status is **down** and the PoE status is **Disabled**, check the physical connection and network cable quality of the device.
- (4) If the port status and PoE status are normal but the IPC is offline, try to restart the PoE port.



(5) After the port is restarted, wait for a period of time and check whether the IPC goes online again. If the IPC is still offline, check the IPC status.

5.1.3 Unable to Access the Intranet Server

- (1) Check whether the IP address and port of the intranet server are correctly configured.
- (2) Check whether the server can access the Internet. If not, configure the server network.
- (3) Check whether the server can be accessed directly. Use an intranet device in the same network segment to log in to the server. If the login fails, check the server.
- (4) Check whether the number of tunnels created on Ruijie Cloud has reached the limit. Up to 10 tunnels can be created for each project. Check whether the tunnels expire. A tunnel expires after it is created for 3 hours.

5.1.4 EST Bridging Fails

- (1) View the LED indicators of the bridged devices to determine the bridging status of the devices.
- (2) Confirm the maximum distance supported by the devices (EST310: 1 km; EST350: 5 km). Adjust the distance between the devices to ensure that the front panels of the devices face each other and ensure that the devices can receive Wi-Fi signals.
- (3) Check the bridge environment: whether the distance between devices is too far, whether there is any obstruction between them, or whether the wireless radio is disturbed.
- (4) Check the working mode of the device. Ensure that one side is AP mode, and the other side is CPE mode.
- (5) Restore the devices to factory settings and test them again.

6 FAQ

6.1 What should I do if I want to add the NVR to the topology?

- (1) Add IP address to Ruijie Cloud.
- (2) Add the username/password of NVR to Ruijie Cloud.
- (3) Make sure the NVR is available.

6.2 Which manufacturers of NVRs can be added in Ruijie Cloud?

Hikvision, Dahua, Tiandy, Uniview and Huawei can be added in Ruijie Cloud.

6.3 What information of the NVR can be displayed on the cloud?

The information including Status, IP, Vender, Username, Switch port connect with, Camera Qty and Update time will be displayed on Ruijie Cloud.

6.4 What information of the IPC can be displayed on the cloud?

- Speed up the recognition (based on the IPC MAC) of IPC under ESW/NBS managed switches. Supported vendors: Dahua, Hikvision, Honeywell, TE Connectivity, and Tiandy.
- (2) Camera is connected with ESW or NBS switch, with 30-mins stable flow to Ruijie Cloud.
- (3) Get IPC info by logging in to NVR: Ruijie Cloud can access to NVR to get IPC related info by tunnel.

6.5 Which manufacturers of IP cameras can be recognized by Ruijie Cloud?

Ruijie Cloud will recognize the IP cameras based on port traffic automatically. In theory, all cameras can be recognized.

6.6 What information of the IP camera can be displayed on the Cloud?

The information including Status, MAC, IP, Switch port connected with and Uplink/Downlink Speed will be displayed on Ruijie Cloud.

6.7 Which switch mode will recognize the IP camera automatically?

Reyee ES and NBS series will recognized the IP camera automatically.

6.8 What can I do if the topology shows" No Data"?

- (1) If there is only one AP in the network, the topology cannot be displayed.
- (2) The egress device is not the Ruijie device and doesn't have a core switch.
- (3) Try manually refreshing the topology.

6.9 What can I do if there is only an EG device on 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 not available, other devices cannot be displayed as well.

6.10 What can I do if some devices are missing on the topology?

- (1) Show mac/show arp/show ip route of the device. The results of these 3 commands including "S*" will make the device miss.
- (2) Dynamic routing protocols such as OSPF exist in the topology.
- (3) The switches in the topology are configured with VSU.

6.11 What can I do if the virtual devices are shown on the topology?

- (1) The device is not on the Ruijie Cloud or is offline.
- (2) The device is not the Ruijie device.
- (3) If the device is an un-managed switch, it is recommended to edit the name and the port manually.