

Ruijie Reyee CCTV 1.0

Cookbook



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.



, and other Ruijie networks logos are trademarks of Ruijie Networks.

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

Disclaimer

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

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

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

Preface

Intended Audience

This document is intended for:

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

Technical Support

- The official website of Ruijie Reye: <https://www.ruijienetworks.com/products/revee>
- Technical Support Website: <https://www.ruijienetworks.com/support>
- Case Portal: <https://caseportal.ruijienetworks.com>
- Community: <https://community.ruijienetworks.com>
- Technical Support Email: service_rj@ruijienetworks.com

Conventions

1. GUI Symbols

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

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

Preface	1
1 Overview	1
1.1 Introduction	1
1.2 Specifications.....	2
2 Getting Started	3
2.1 Preparing for Installation.....	3
2.1.1 Project Requirement	3
2.1.2 Network Planning.....	3
3 Configuration	4
3.1 SON and Cloud Deployment	4
3.1.1 Application Scenario	4
3.1.2 Procedure.....	4
3.2 Connection and Configuration of Wireless bridge.....	6
3.3 Creating a VLAN/DHCP.....	7
3.4 Real Topology.....	8
3.4.1 Application Scenario	8
3.4.2 Procedure.....	8
3.4.3 Principle of the Network Topology	11
3.5 Automatic IPC Identification.....	12
3.5.1 Application Scenario	12
3.5.2 Procedure.....	12
3.6 ACL Configuration.....	14
3.6.1 Application Scenario	14

3.6.2 Procedure.....	14
3.7 IPC Access through an Extranet and Server Penetration through an Intranet	16
3.7.1 Application Scenario	16
3.7.2 Procedure.....	16
3.8 Voice VLAN.....	18
3.8.1 Voice VLAN Settings.....	19
3.8.2 OUI Settings.....	19
3.8.3 Port Settings.....	20
3.9 Delivery Report	21
4 Maintenance.....	24
4.1 Remote IPC Operations — IPC Restart and Long-Distance Power Supply	24
4.1.1 Application Scenario	24
4.1.2 Procedure.....	24
4.2 Loop Prevention Configuration	29
4.2.1 Application Scenario	29
4.2.2 Procedure.....	29
5 Troubleshooting.....	33
5.1.1 Ruijie Cloud Cannot Automatically Identify an IPC.....	33
5.1.2 IPC Is Offline	33
5.1.3 Unable to Access the Intranet Server	35
5.1.4 EST Bridging Fails	35
6 FAQ	36

1 Overview

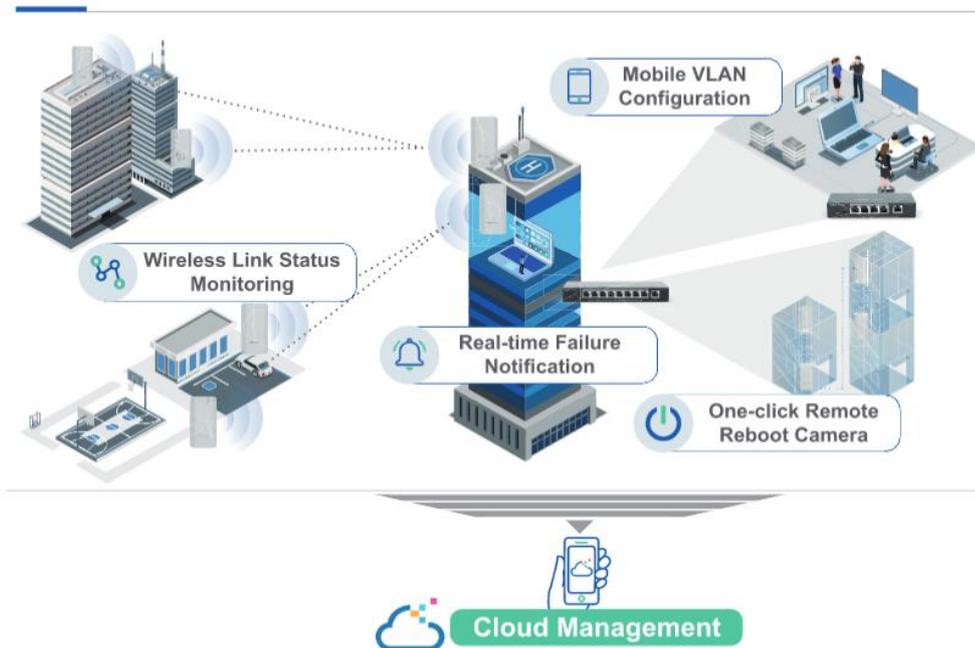
1.1 Introduction

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.

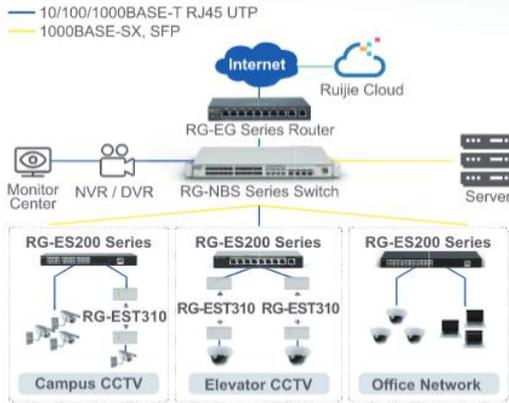
There is a story. One day, confidential documents have been stolen, but the elevator and corridor camera signal lost and couldn't track the thief. Boss was so angry and asked SI to onsite right away to solve his monitoring problem. Two hours later, SI finally arrived the company, when SI tried every 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;
- 250 meters PoE save cabling cost for end-users;
- 5GHz reduce interference and guarantee video quality;
- Meet 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

Product Recommendations

Cloud Managed Switch

RG-ES200 Series Switch



Camera / NVR Recognition



Ports	Icon
4	PoE
8	PoE
16	PoE
24	PoE
16	Non-PoE
24	Non-PoE

=



Once Onsite Taxi Fare

+

Unmanaged Switch Cost

+

- Cloud Management
- Remote Reboot Camera
- 250 Meters PoE
- Mobile VLAN Setting

Wireless Bridge



RG-EST310
1KM Wireless Bridge



Applicable Scenario

- 5GHz Anti-Interference
- Automatic Channel Optimization

- Elevator
- Warehouse
- Office
- Crane
- Bridge
- Factory

- Zero Touch Provisioning
- Self-organizing Network

2 Getting Started

2.1 Preparing for Installation

2.1.1 Project Requirement

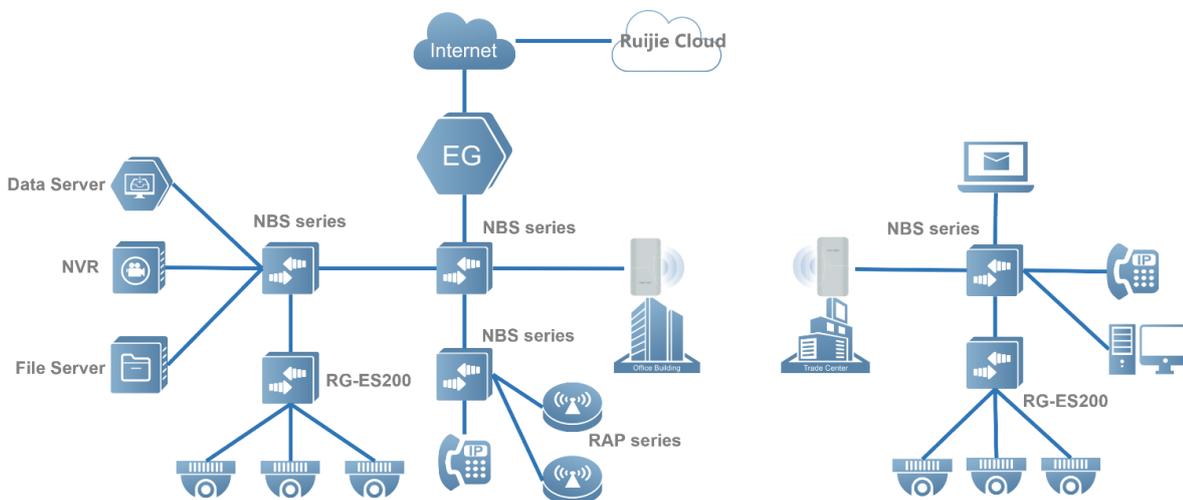
Company Y wants to monitor the whole park and the monitoring data from the cameras should be aggregated to the NVR.

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 Reyeer 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.

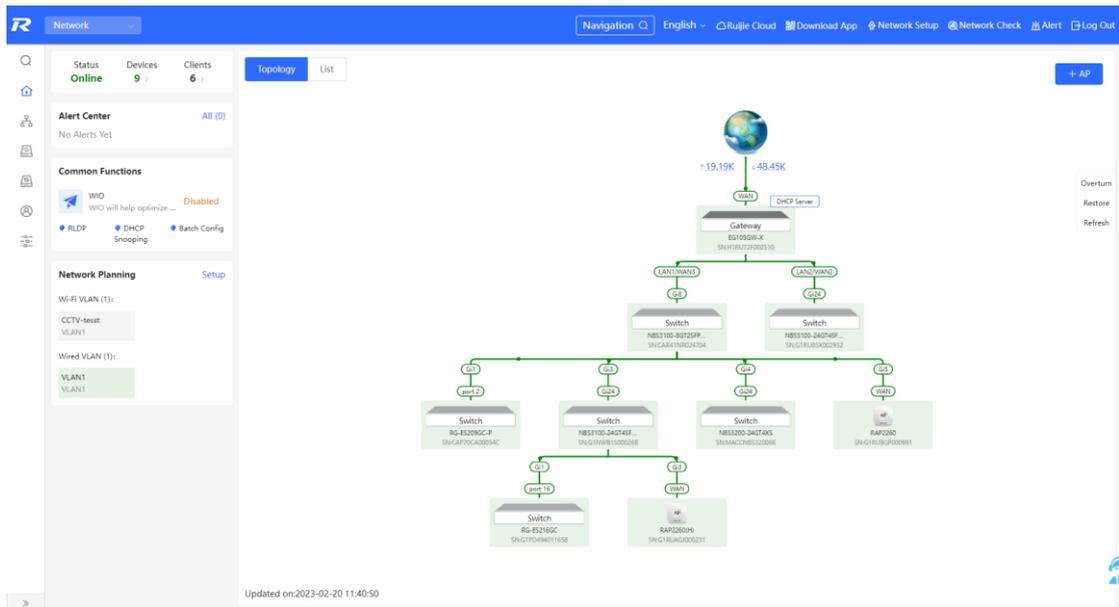
3.1.2 Procedure

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

The screenshot shows the 'Discover Device' interface with a network topology diagram and a table of discovered devices. The topology diagram includes Internet, DHCP, Router (1), Switches (6/8), and APs (1/1). The table below lists the discovered devices:

Model	SN	IP	MAC	Software Ver
Router: EG105GW-X [Master]	H1RLU72F000510	No IP Address Available	28D0F5E33A86	ReyeeOS 1.95.1914
AP: RAP2260(H)	G1RLIAGK00231	192.168.110.147	10823D13E787	ReyeeOS 1.95.2115
Switch: NBS3200-24GT4XS	MACCNBS320066	192.168.110.5	00D0F8DE9CA3	ReyeeOS 1.210.2428
Switch: NBS3100-24GT4SFP-P	G1NWB1500026B	192.168.110.251	00D0F3333861	ReyeeOS 1.86.2021
Switch: NBS3100-8GT2SFP-P	CAR41NR024704	192.168.110.7	5416513A3088	ReyeeOS 1.206.2216
Switch: NBS5100-24GT4SFP-P	G1RLB5X002932	192.168.110.29	28D0F5FF9A9D	ReyeeOS 1.212.2322
AP: RAP2260	G1RUR9P000991	192.168.110.166	7042D301A0FD	ReyeeOS 1.219.1407
Switch: RG-ES2165C	G1PD49A011658	192.168.110.144	30D09E497E85	ESW_1.0(1)B1P20.Release(09201814)
Switch: RG-ES2095C-P	CAP70CA00054C	192.168.110.57	30D09ED087C2	ESW_1.0(1)B1P7.Release(08202314)

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



Gateway (0) AP (2) Switch (6) AC (0) Router (1)

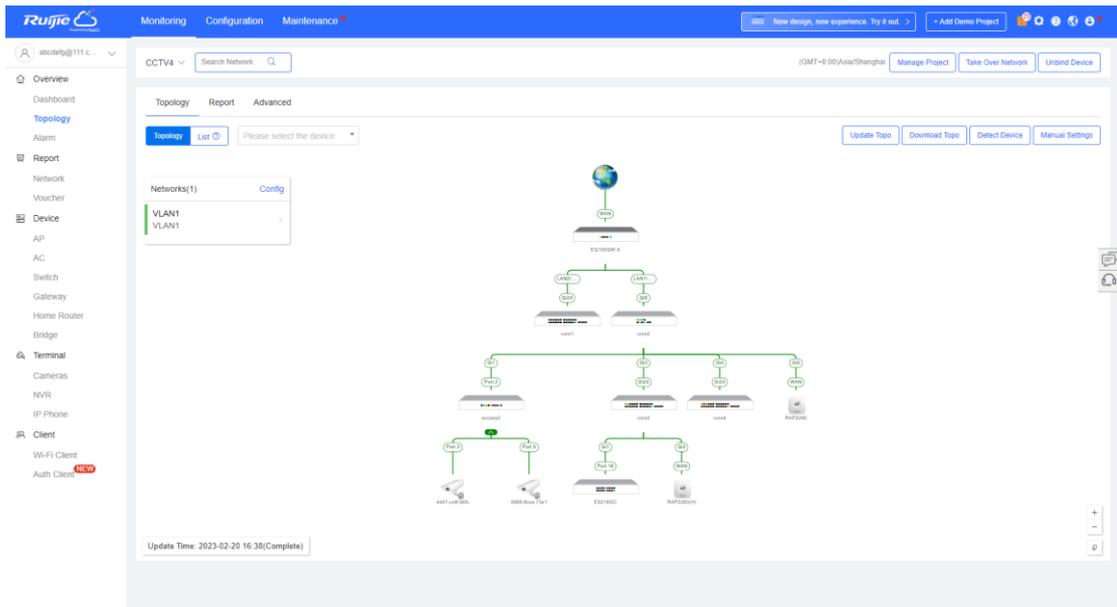
Device List

IP/MAC/hostname/SN/S... Delete Offline Devices Batch Upgrade

	SN	Status	Hostname	MAC	IP	Software Ver	Model
<input type="checkbox"/>	CAP70CA0054C	Online	rujje_2	30:0D:9E:DD:87:C2	192.168.110.57	ESW_1.0(1)B1P7,Release(08202314)	RG-ES2090C-P
<input type="checkbox"/>	G1PD494011658	Online	rujje_2	30:0D:9E:49:7E:85	192.168.110.144	ESW_1.0(1)B1P20,Release(09201814)	RG-ES2160C
<input type="checkbox"/>	H1RU72F000510	Online	Ruijie [Master]_2	28:00F5:E3:3A:86	192.168.110.1_2	ReyeeOS 1.95.1914	EG1050W-X
<input type="checkbox"/>	G1RU83X002932	Online	Ruijie_2	28:00F5:FF:9A:9D	192.168.110.29_2	ReyeeOS 1.212.2322	NBS5100-24GT4SF-P
<input type="checkbox"/>	G1NW815000268	Online	Ruijie_2	00:D0F3:33:3B:51	192.168.110.251_2	ReyeeOS 1.86.2002 new	NBS3100-24GT4SF-P
<input type="checkbox"/>	MACCNBS320066	Online	Ruijie_2	00:D0F8:0B:9C:A3	192.168.110.5_2	ReyeeOS 1.218.2428	NBS3200-24GT4XS
<input type="checkbox"/>	CAR41NR024704	Online	Ruijie_2	54:1651:3A:30:8B	192.168.110.7_2	ReyeeOS 1.206.2216	NBS3100-8GT25FP-P
<input type="checkbox"/>	G1RUAG000231	Online	Ruijie_2	10:82:3D:13:E7:87	192.168.110.147_2	ReyeeOS 1.95.2111 new	RAP22600H
<input type="checkbox"/>	G1RU9GP000991	Online	Ruijie_2	70:42:D3:01:A0:FD	192.168.110.166_2	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**.



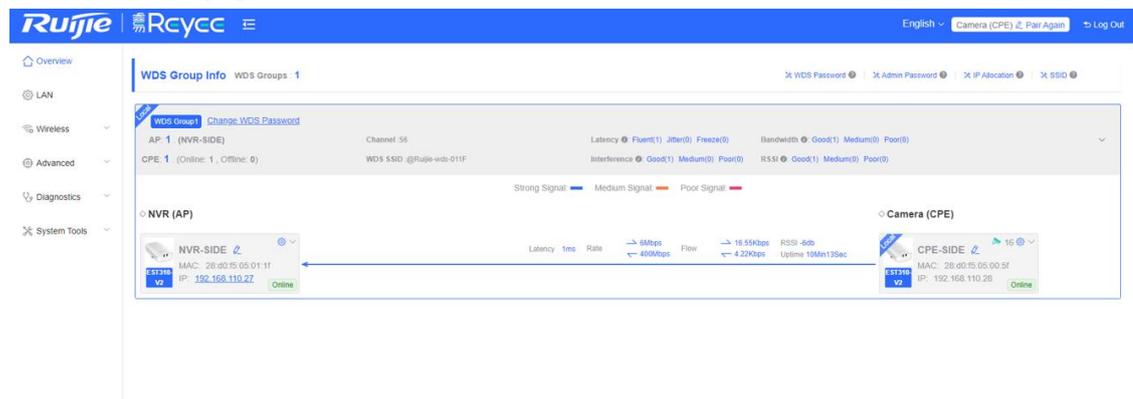
3.2 Connection and Configuration of Wireless bridge

Application Scenario

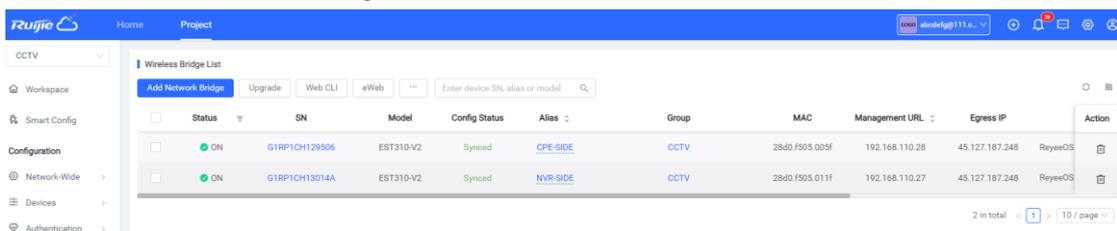
RG-EST series wireless bridge can build up tunnel to transmit video for elevator and long range. It can not only monitor the wireless status in real time, but also save cost for end-users.

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.



- (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 Ruijie Cloud.



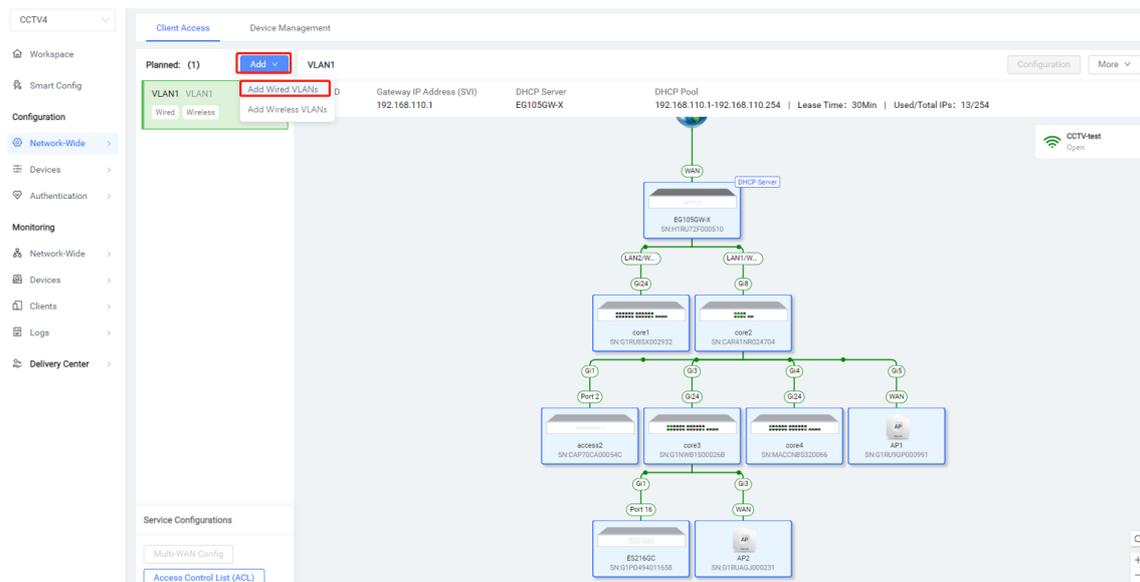
3.3 Creating a VLAN/DHCP

Application Scenario

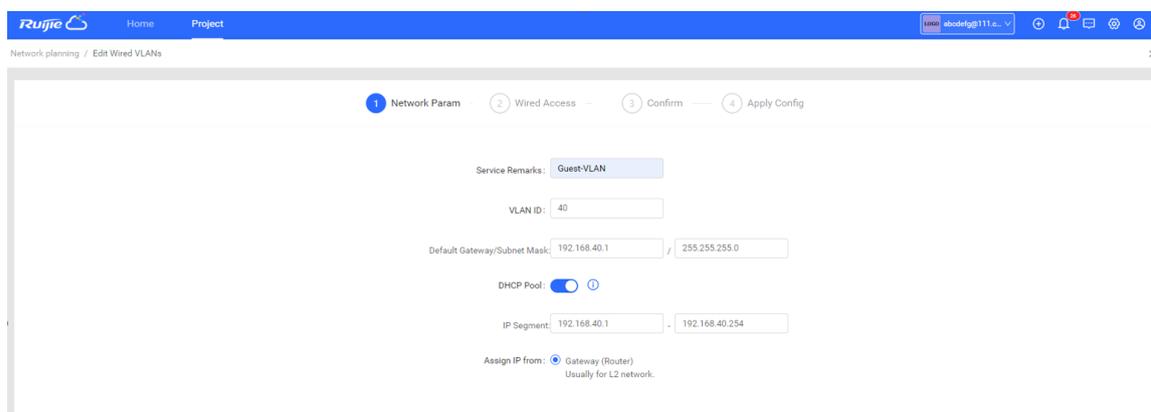
Different clients exist on a network, such as PCs and cameras. When a camera is running, broadcast or abnormal traffic often occurs, imposing negative effects on the service network. The administrator wants to isolate the broadcast and abnormal traffic of the camera from the running service network.

Procedure

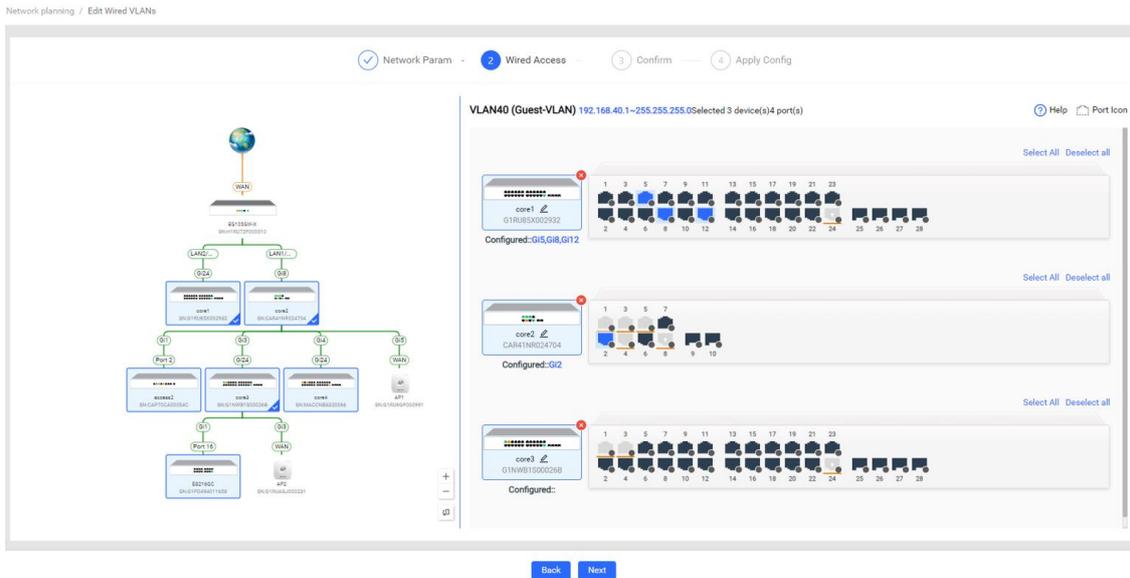
- (1) Adding a wired VLAN: Click **Add** and select **Add wired VLANs** to add wired VLAN configuration for the current network or select an existing wired VLAN and click **Configuration**.



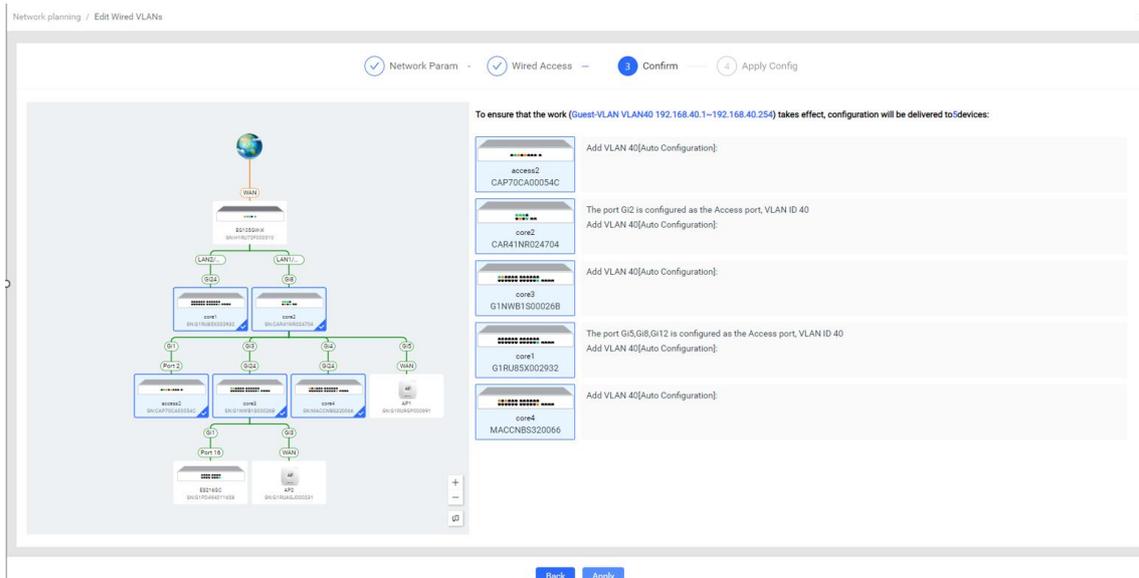
- (2) Setting service parameters: Set the VLAN for wired access and create a Dynamic Host Configuration Protocol (DHCP) address pool for devices in the VLAN to automatically obtain IP addresses. The gateway can serve as the address pool server to assign addresses to access clients. If a core switch supporting 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**.



- (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.



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



3.4 Real Topology

3.4.1 Application Scenario

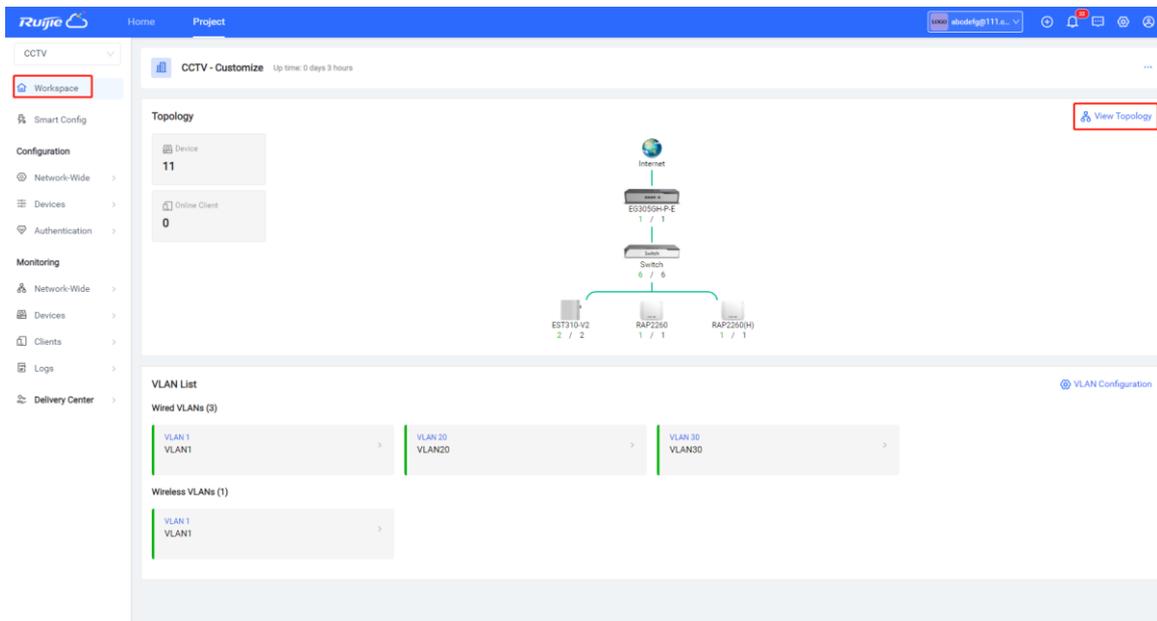
The real topology displays the actual network topology, which helps understand the device status, physical link connection between devices, and information about connected ports. When a fault occurs in the customer's network environment, the real topology helps quickly locate the fault, improving the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

3.4.2 Procedure

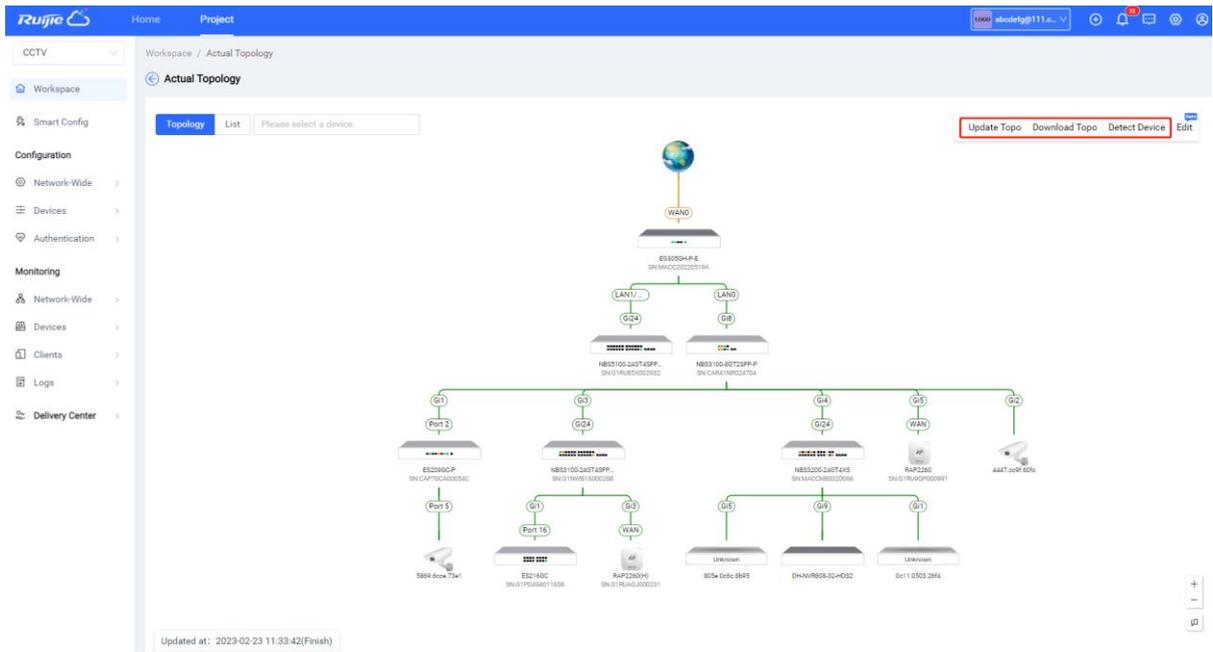
(1) Click a project name to open the project page.

Network Name	Scenario	Alarms	Online Guests	AP	AC	Gateway	Switch	Home Router	Network Bridge	Running Time	Action
shiyun		0	0	1/1	-	1/1	1/1	-	-	0 days	[-] [-] [!]
DemoProject2		0	0	5/5	-	1/1	5/5	-	-	0 days	[-] [-] [!]
DemoProject1		0	0	5/5	-	1/1	5/5	-	-	0 days	[-] [-] [!]
School		0	0	0/0	-	-	-	-	-	0 days	[-] [-] [!]
CCTV		2	0	2/2	-	1/1	6/6	-	2/2	0 days	[-] [-] [!]
CCTV5		0	0	0/0	-	-	-	-	-	2 days	[-] [-] [!]
CCTV11		0	0	0/0	-	-	-	-	-	2 days	[-] [-] [!]
EG105GW-X		2	0	1/2	-	1/1	1/1	-	-	2 days	[-] [-] [!]
TestEG209		0	0	0/0	-	-	-	-	-	3 days	[-] [-] [!]
test123_1		0	0	0/0	-	-	-	-	-	5 days	[-] [-] [!]

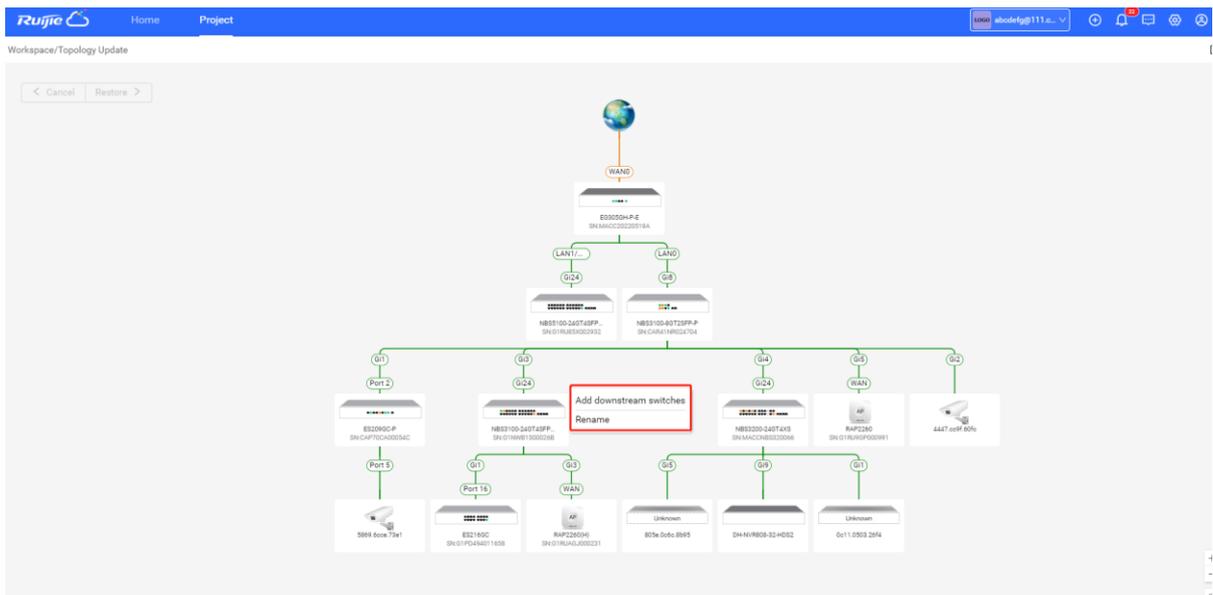
(2) Click **Workspace** and click **View Topology** to view the real topology of the project.



(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.

Online Status	SN	Model	Device Name	MAC Address	Management URL	Sync	Offline Time
ON	G1NWB1S00026B	NBS3100-24GT4SFP-P	Ruijie	00d0.f333.3861	192.168.110.7	Synced	-
ON	MACC20220519A	EG305GH-P-E	Ruijie	00d0.c875.a845	192.168.111.18	Synced	-
ON	CAP70CA00054C	ES209GC-P	ruijie	300d.9e8d.b7c2	192.168.110.12	Synced	-
ON	CAR41NR024704	NBS3100-8GT2SFP-P	Ruijie	5416.513a.30bb	192.168.110.3	Synced	-
ON	G1PD494011658	ES216GC	ruijie	300d.9e49.7e85	192.168.110.8	Synced	-
ON	G1RP1CH129506	EST310-V2	CPE-SIDE	28d0.f505.005f	192.168.110.28	Synced	2023-02-22 16:28:07
ON	G1RP1CH13014A	EST310-V2	NVR-SIDE	28d0.f505.011f	192.168.110.27	Synced	2023-02-22 16:31:07
ON	G1RU8SX002932	NBS3100-24GT4SFP-P	Ruijie	28d0.f5f9.9a9d	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	-

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

Device Information

SN: CAP70CA00054C | Device model: ES209GC-P | Management IP: 192.168.110.12

Monitoring | Configuration | Diagnostics

Overview | Port Rate | PoE List | Search | Log History

Status

1 2 3 4 5 6 7 8 9

Device Resources

Uplink: Port 2, Port Speed: 1000M, Duplex: Full-duplex

Connection Status: Last 24 Hours, Last 7 Days

Uplink/Downlink: 0.00Kbps, Speed: 9.00Kbps, Uplink/Downlink Traffic: 4.00KB, 43.00KB

Port Packet Statistics

Updated Time: 2023-02-23 15:19:53

Port	Inbound/Outbound Traffic (KB)	Inbound/Outbound Rate (KB/s)	Number of Packets Received/Sent	CRC/FCS Errors	Fragment/Oversized Packets	Number of Conflicts
Port 4	0/0	0.0/0.0	0/0	0/--	0/0	0
Port 3	0/0	0.0/0.0	0/0	0/--	0/0	0

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

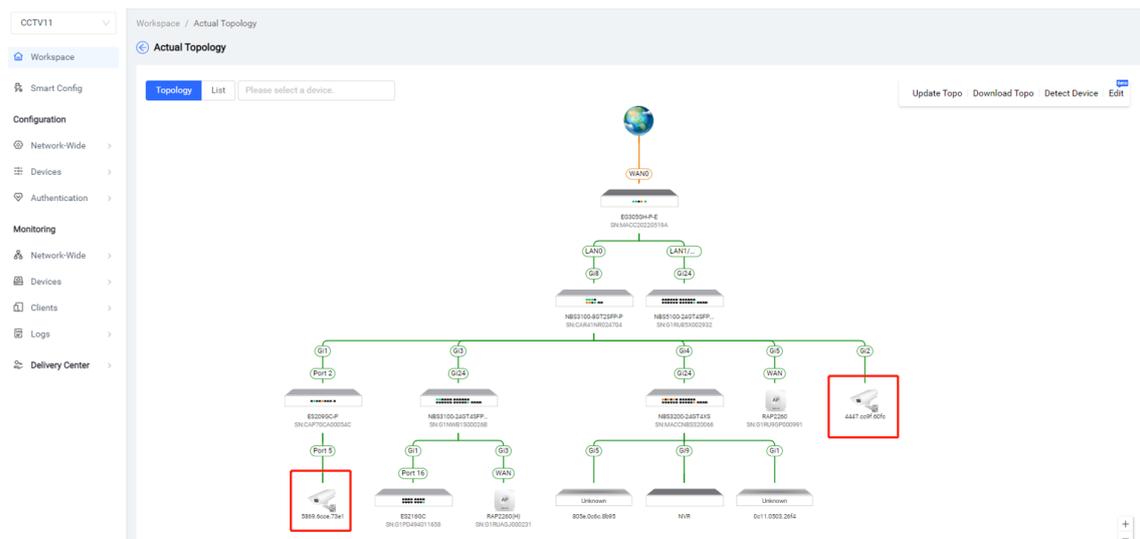
3.5.1 Application Scenario

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**.

1. By using the Ruijie Cloud platform, you must have the management and usage right of the target computer system devices. You are prohibited from using the Ruijie Cloud platform (hereinafter referred to as the "Platform") to log in to any unauthorized device without authorization, and the Platform shall not assume any responsibility arising therefrom.

2. By providing the required credentials to log in to a target computer system device, you shall be deemed as having authorized the Platform to log in to the target computer system device using such credentials and to obtain, transmit, and store information about the system's hardware features and network connectivity status.

3. After the above-mentioned system is connected to the Platform, network security risks may increase. The Platform shall endeavour to ensure the security and integrity of the information transmitted and used in the system, but the relevant information shall be used for operation and maintenance reference only, and the Platform shall not guarantee the integrity and accuracy of the information.

4. The Platform reserves the right to terminate this service if you infringes the copyright of a third party and the Platform is notified by the copyright owner or the legal agent thereof.

5. The service may be adjusted or suspended due to technical development and other external factors, and the Platform shall not be held liable for any loss caused by the discontinuation of service.

I Agree

* IP address:

* Vendor:

* Username:

* NVR Password:

Name:

* IPC - Uplink Switch Type:

Port	PoE Status	Uplink/Downlink Speed
G09		18.37Kbps/9.12Kbps
G12	enable	0.14Kbps/2.08Kbps

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

Status	MAC Address	Channel ID	Channel Name	IP Address	Switch	Port	PoE Status	Uplink/Downlink Speed
Online	-	1	HK-1	192.168.1.1	-	-	-	-/-
Online	-	2	通道21	192.168.1.2	-	-	-	-/-
Online	-	3	Camera 01	192.168.1.24	-	-	-	-/-
Online	-	4	UNV-25	192.168.1.64	-	-	-	-/-
Online	-	5	HK-5	192.168.1.5	-	-	-	-/-
Online	-	6	Camera 01	192.168.1.6	-	-	-	-/-
Online	-	7	Camera 01	192.168.1.7	-	-	-	-/-
Online	-	8	HK-19	192.168.1.8	-	-	-	-/-
Online	-	9	HK-9	192.168.1.9	-	-	-	-/-
Online	-	10	IPC-10	192.168.1.10	-	-	-	-/-

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

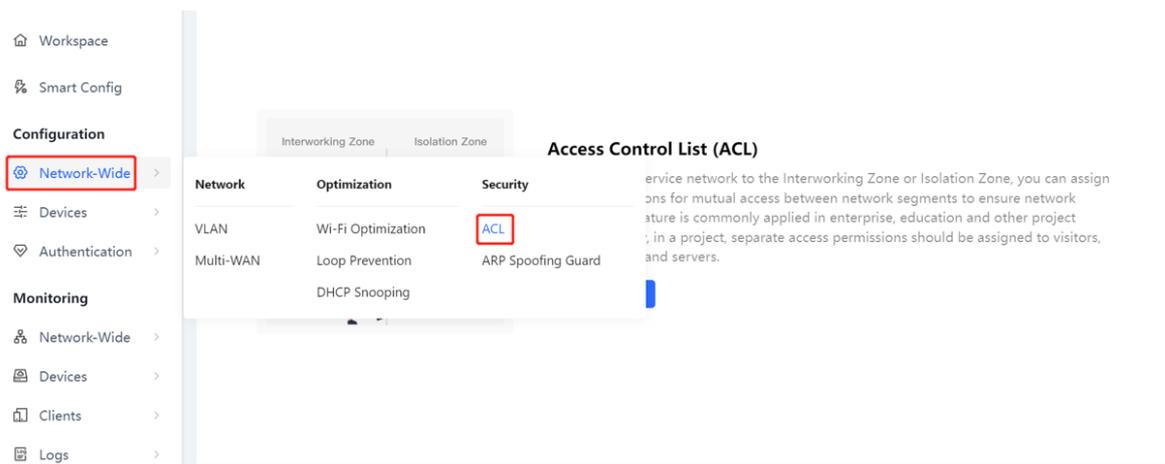
3.6.1 Application Scenario

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**.



- (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

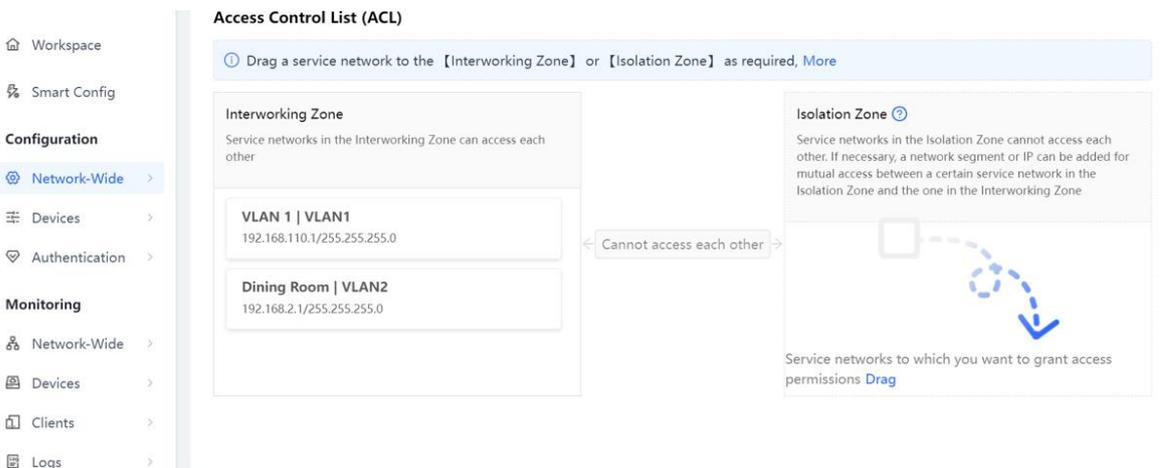
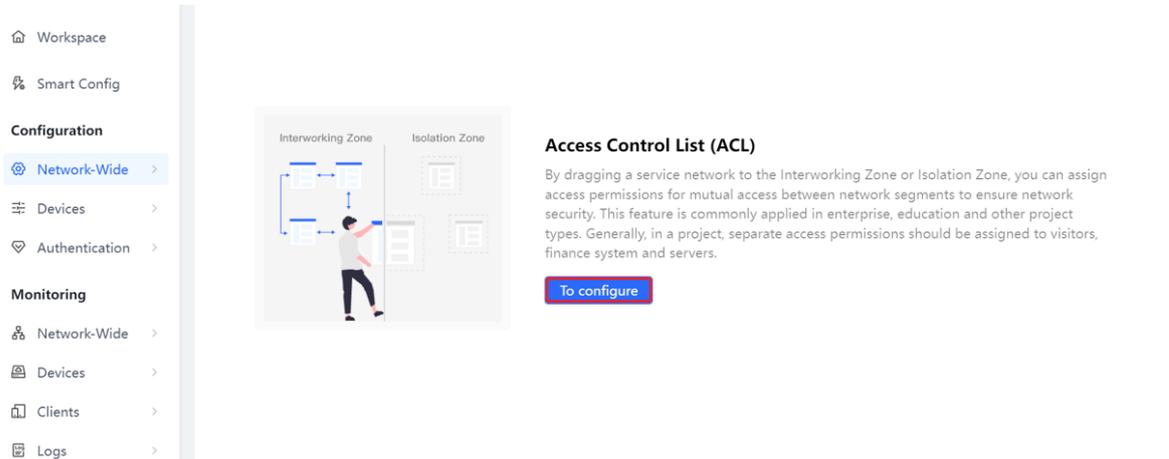
Service networks in the interworking zone can access each other.

- Isolation Zone

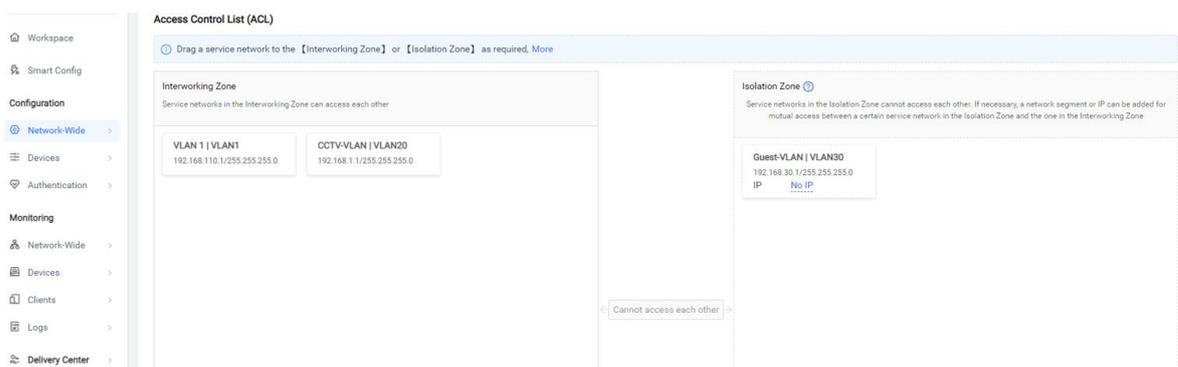
Service network segments in the isolation zone cannot access those in the interworking zone and vice versa.

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.



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

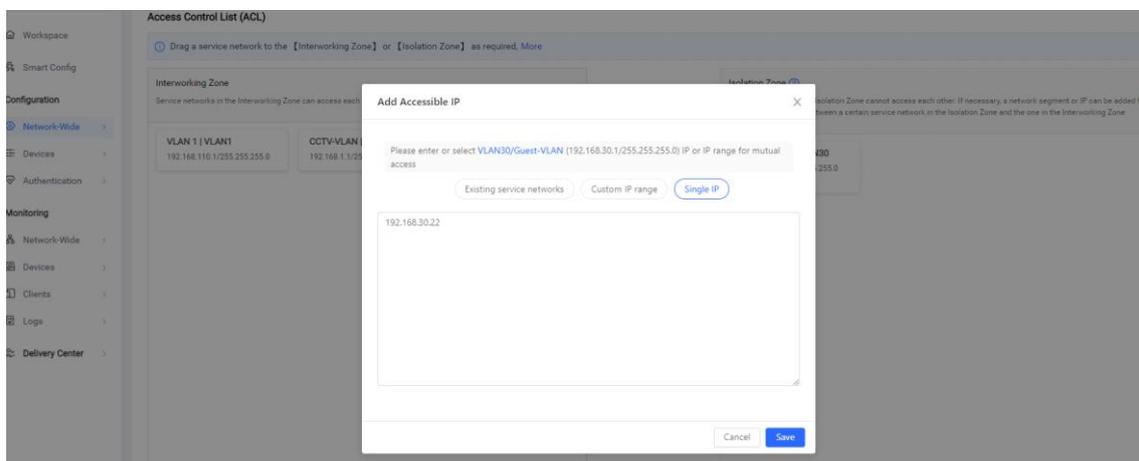


(3) (Optional) In **Isolation Zone**, click **No IP**.

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**.



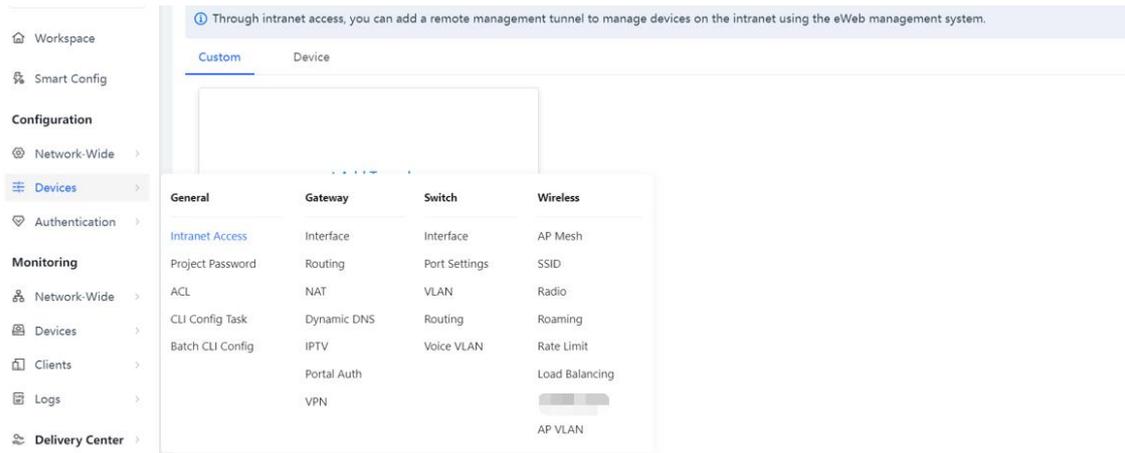
3.7 IPC Access through an Extranet and Server Penetration through an Intranet

3.7.1 Application Scenario

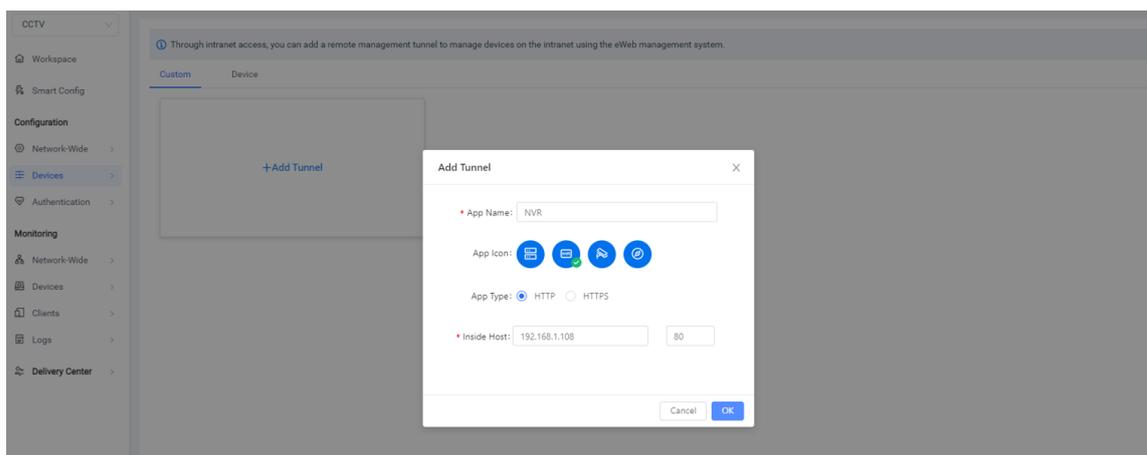
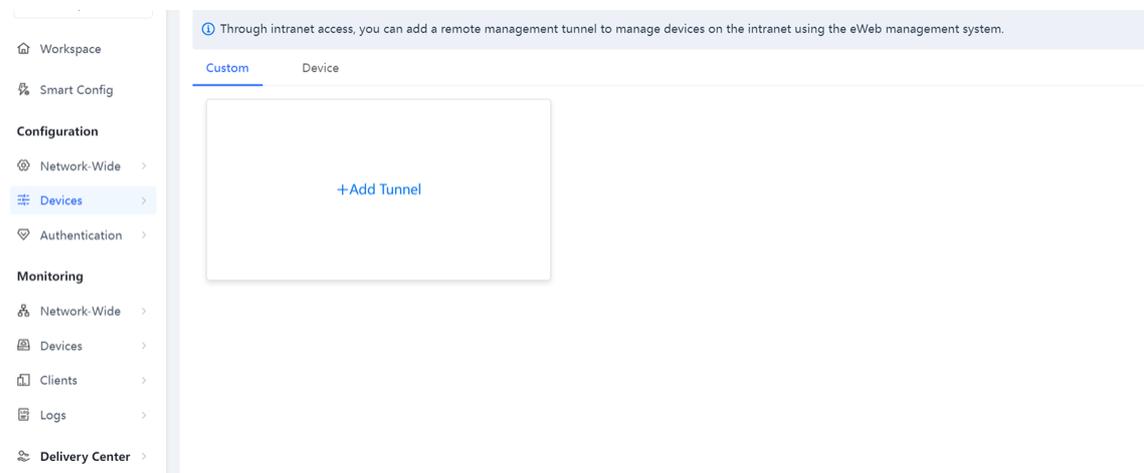
Through intranet access, you can add a remote management tunnel to manage devices on the intranet using the eWeb management system. In addition, you can add a tunnel to access intranet monitoring devices, such as NVRs and IPCs.

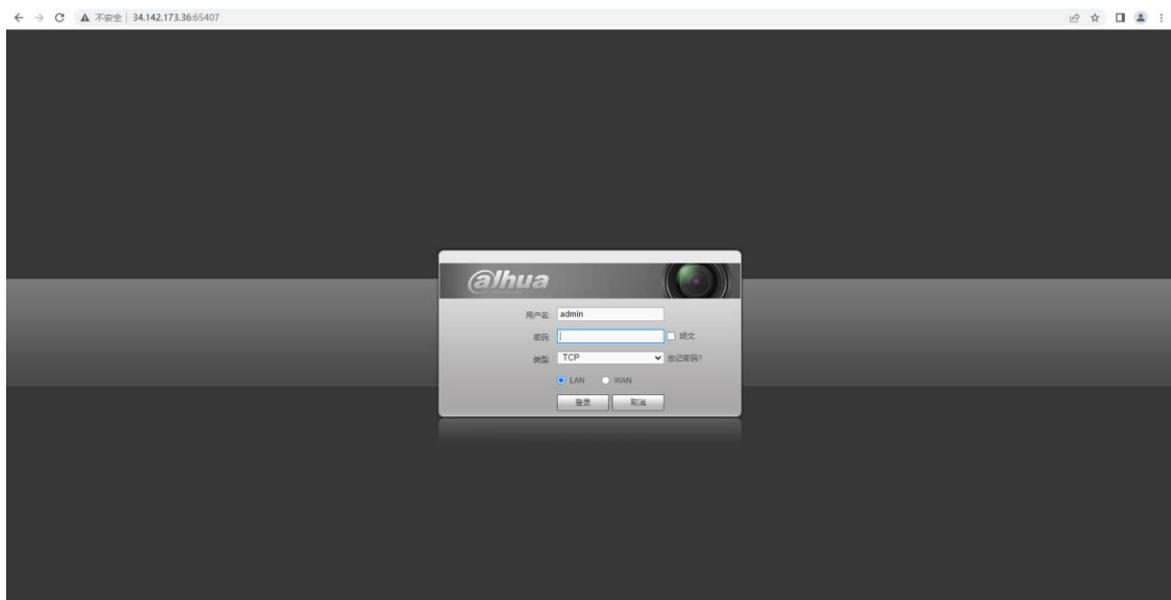
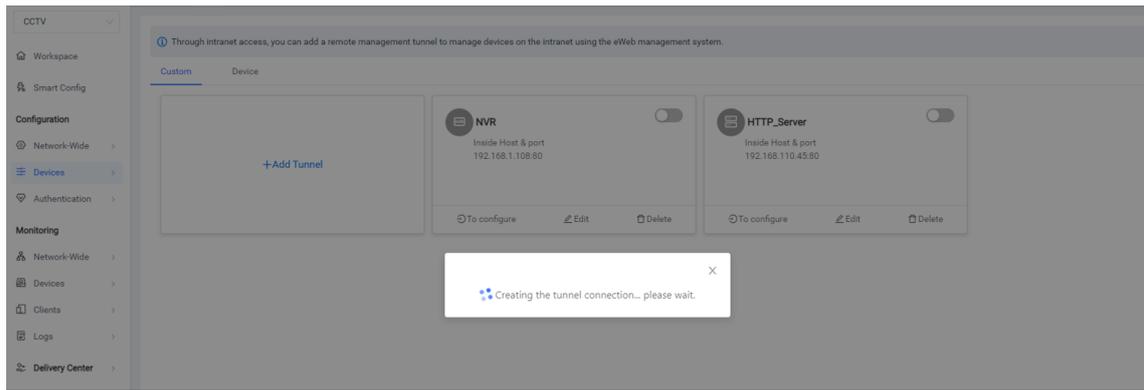
3.7.2 Procedure

Choose **Configuration > Devices > General > Intranet Access**.



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





3.8 Voice VLAN

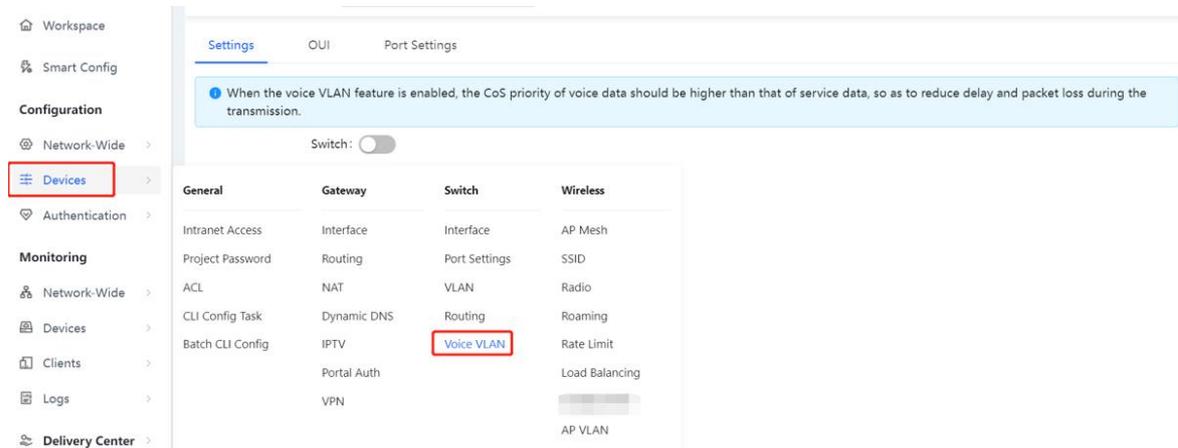
Application Scenario

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.

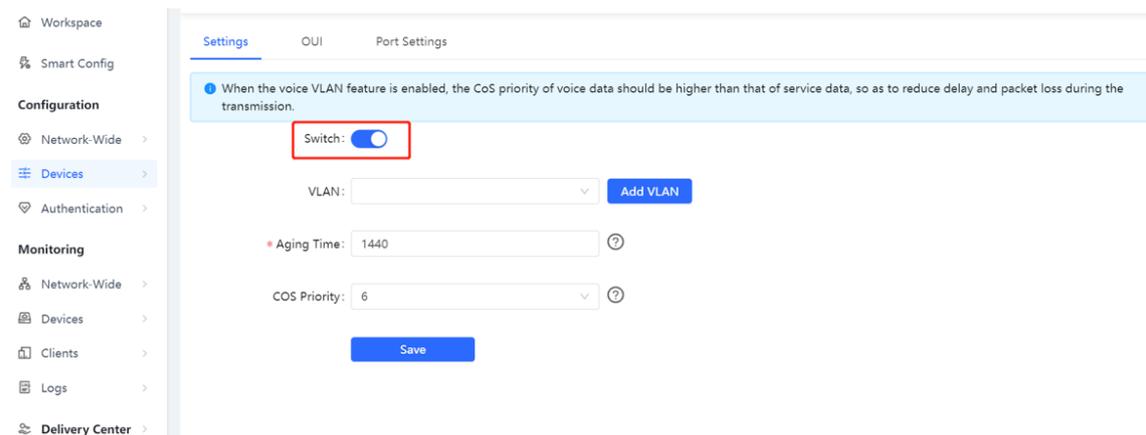
Procedure

Choose **Configuration > Devices > Switch > Voice VLAN**.



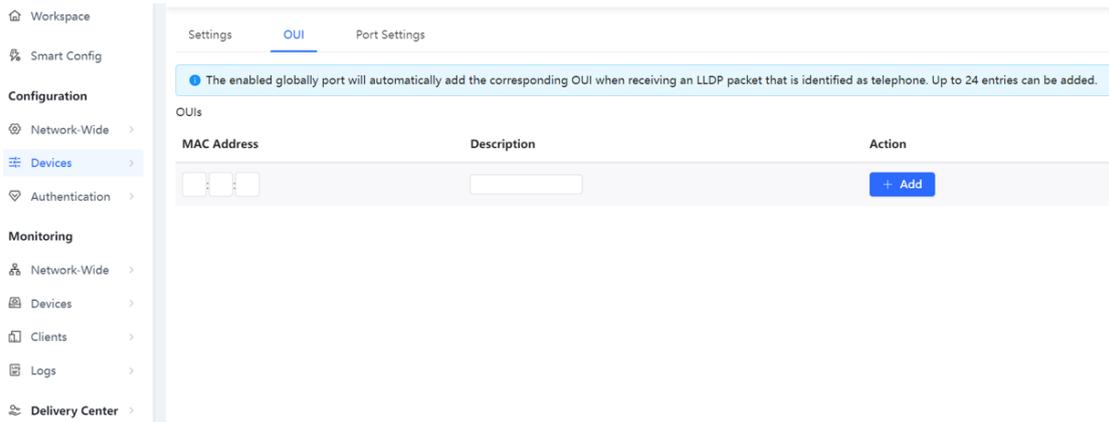
3.8.1 Voice VLAN Settings

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



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.



3.8.3 Port Settings

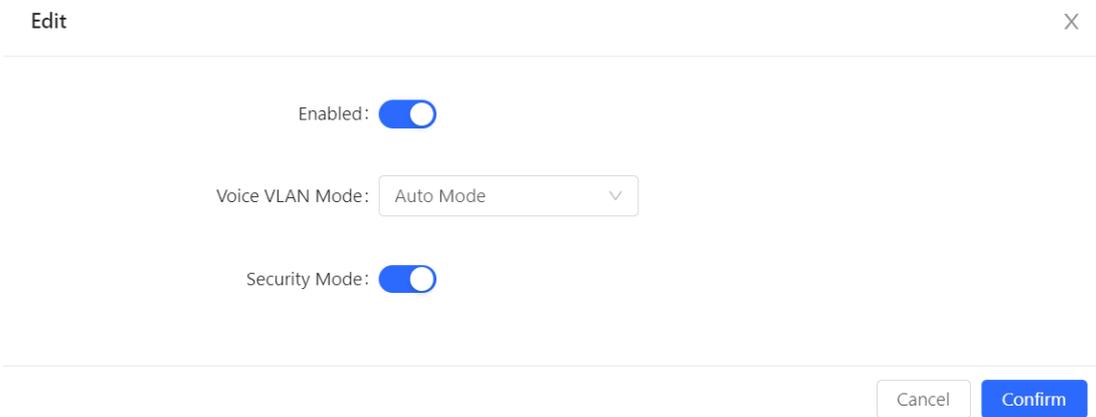
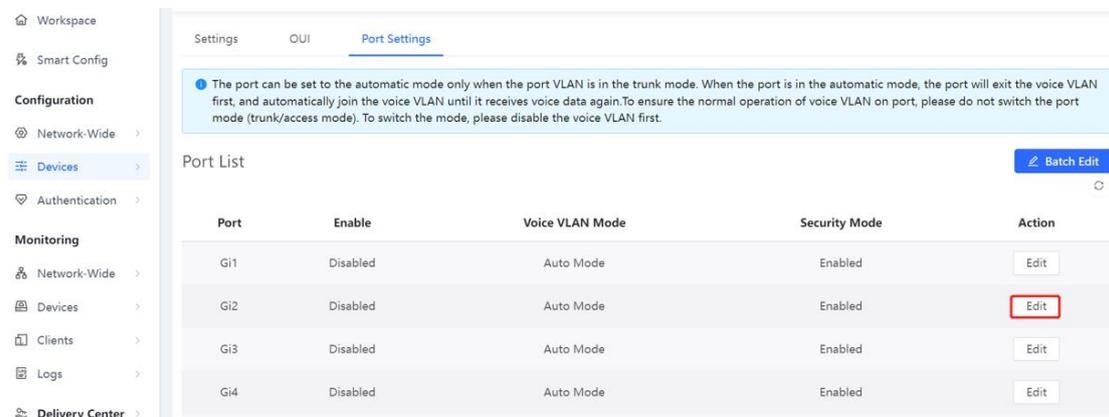
The port can be set to the automatic mode only when the port VLAN is in the trunk mode.

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.

 **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**.



3.9 Delivery Report

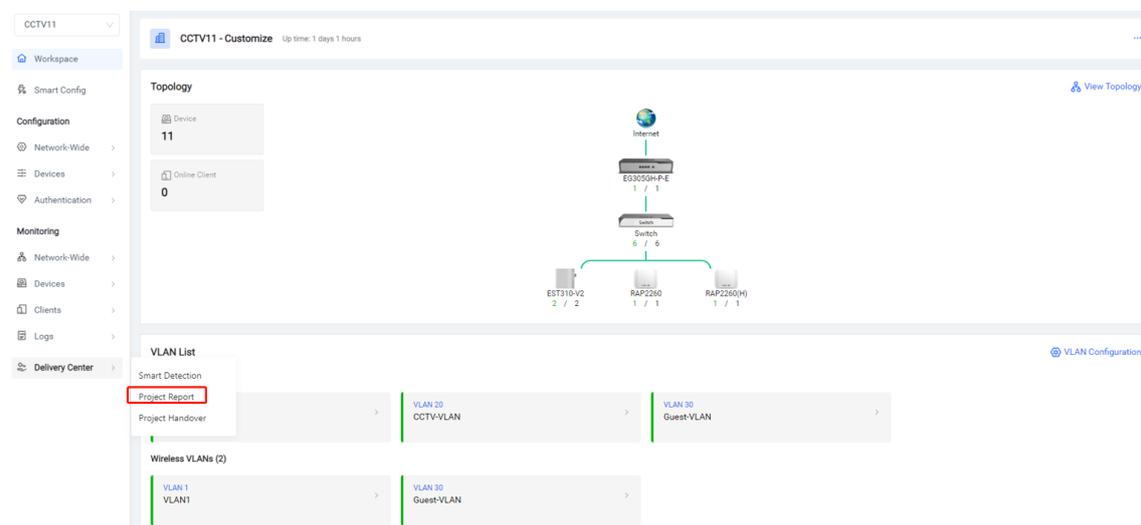
Application Scenario

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, internet 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.



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

Wired Network Planning	IP Address Range	VLAN ID	IP Address Allocation Mode
VLAN1	192.168.110.0/24	1	DHCP

App Name	Description
DHCP Snooping	DHCP Snooping can prevent network failure caused by unauthorized routers or DHCP servers.
Smart Flow Control	Limit the network speed of clients flexibly.

(4) Check the network topology.

ID	Device Name	Model	MAC	IP	Action	
4	Ruijie	G1PD494011658	ES216GC	300d 9e49 7e85	192.168.110.8	Add
5	CPE-SIDE	G1RP1CH129506	EST310-V2	28d0 f505 005f	192.168.110.28	Add
6	NVR-SIDE	G1RP1CH13014A	EST310-V2	28d0 f505 011f	192.168.110.27	Add
7	Ruijie	G1RU85X002932	NBS5100-24GT45FP-P	28d0 f5f1 9a9d	192.168.110.6	Add
8	Ruijie	MACC20220519A	EG305GH-P-E	00d0 c875 a845	192.168.111.18	Add
9	Ruijie	MACCNBS320066	NBS3200-24GT4XS	00d0 f8d8 9ca3	192.168.110.4	Add

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

Update Time: 2023-02-22 11:41:30 [Refresh](#) | [Preview](#) | [Download Report](#)

- Report.pdf
- Report.docx

1. Cover
2. Basic Information
3. VLAN and Address Pool
4. Diagnosis
5. Device
6. Topology
7. Appendix

4 Maintenance

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

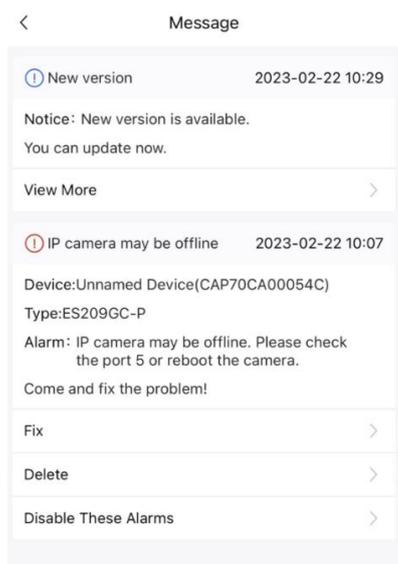
4.1.1 Application Scenario

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.

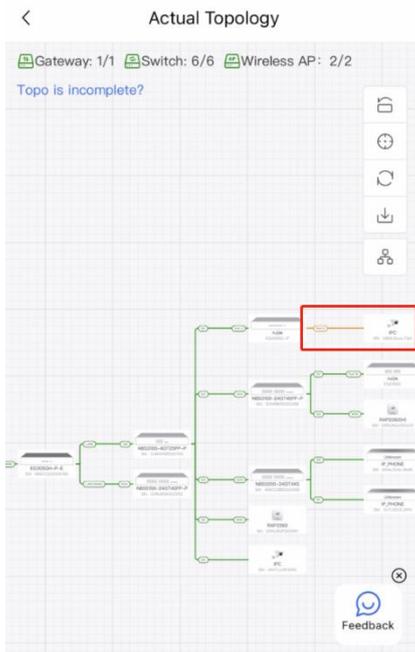
4.1.2 Procedure

- (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.



You can view offline IPCs through the topology.



(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.

Port Status: Copper | PoE | 100M
Speed: 0Mbps | Power Status: On
Packets: 0 | Power: 2.8W

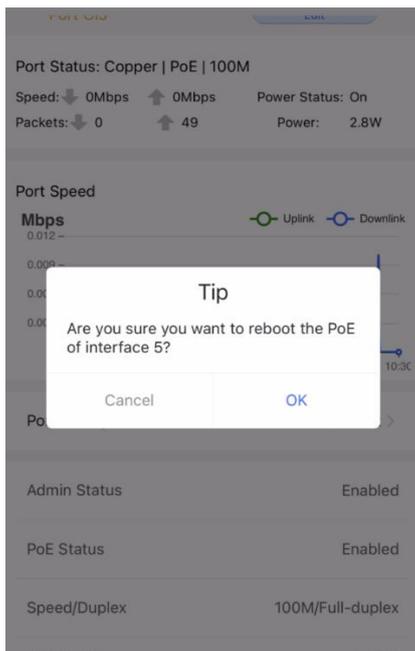
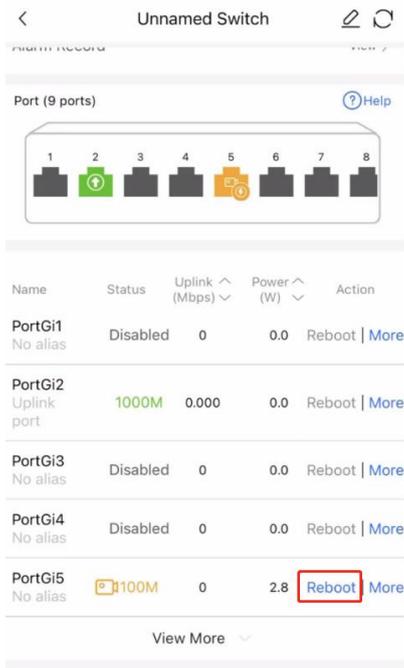
Port Speed graph showing Uplink and Downlink speeds over time.

Port Configuration Edit >

Admin Status	Enabled
PoE Status	Enabled
Speed/Duplex	100M/Full-duplex
Port VLAN VLAN: 20	Access

Cable Test Restart

Restart the IPC.



The IPC goes online again.



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

The screenshot shows the "Unnamed Switch" configuration page in the Ruijie Cloud app. It displays a port configuration table and a list of settings. The "Long-distance Transmission" option is highlighted with a red box.

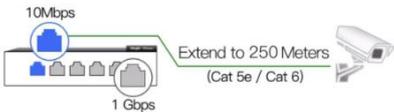
Name	Status	Uplink (Mbps)	Power (W)	Action
PortGi1 No alias	Disabled	0	0.0	Reboot More
PortGi2 Uplink port	1000M	0.000	0.0	Reboot More
PortGi3 No alias	Disabled	0	0.0	Reboot More
PortGi4 No alias	Disabled	0	0.0	Reboot More
PortGi5 No alias	100M	0	2.8	Reboot More

View More

- VLAN Settings
- Long-distance Transmission**

< Long-distance Transmission

Long-distance Transmission
After long-distance data transmission is enabled, the transmission and speed of port will be changed to full-duplex/10Mbps



Selected Ports Port 5 (No alias) Occupied by MGMT VLAN



■ Available ■ Unavailable ■ Configured

Save

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

< Unnamed Switch  



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	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 No alias	Disabled	0	0.0	Reboot More

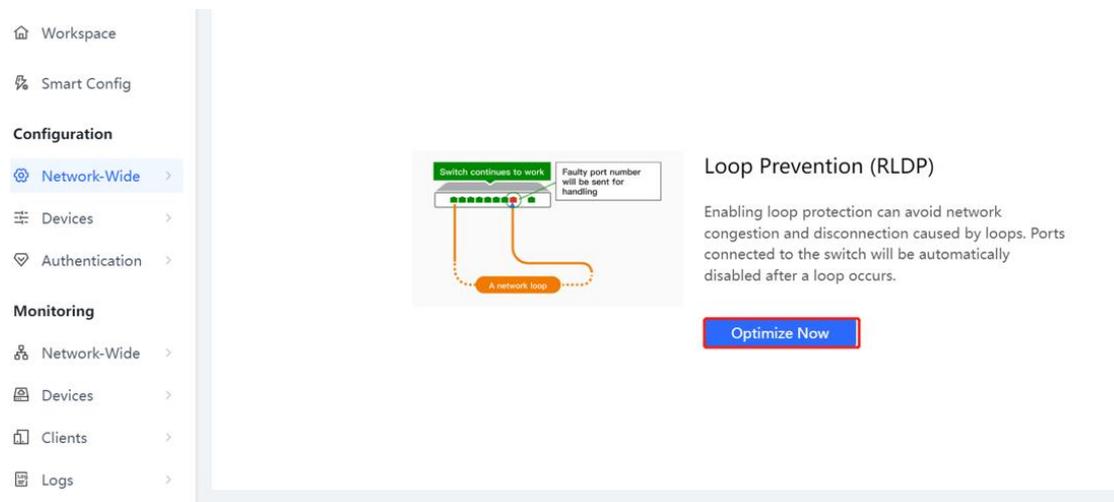
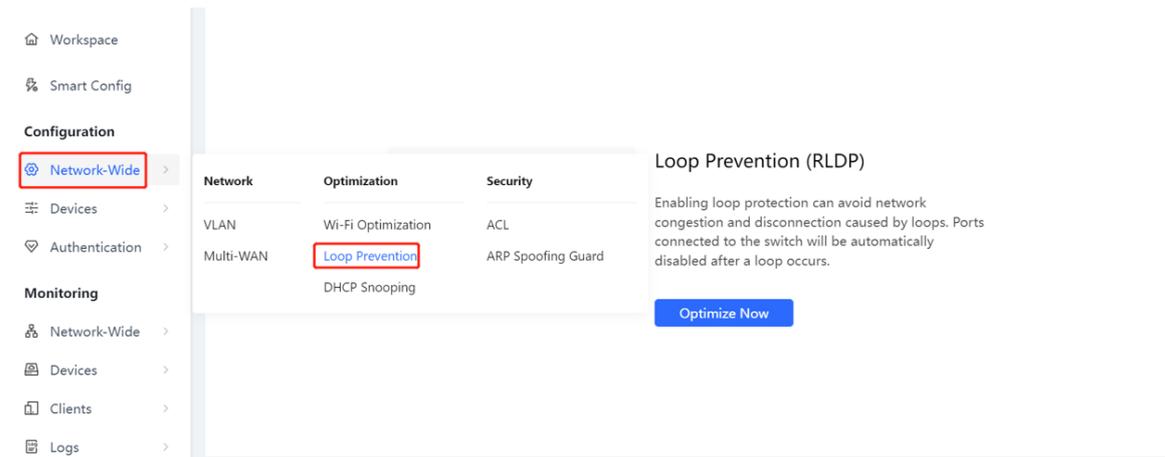
4.2 Loop Prevention Configuration

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**.



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

CCTV11

- Workspace
- Smart Config
- Configuration
 - Network-Wide
 - Devices
 - Authentication
- Monitoring
 - Network-Wide
 - Devices
 - Clients
 - Logs
 - Delivery Center

Loop Prevention

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

Loop Protection

[Configure](#)

CCTV11

- Workspace
- Smart Config
- Configuration
 - Network-Wide
 - Devices
 - Authentication
- Monitoring
 - Network-Wide
 - Devices
 - Clients
 - Logs
 - Delivery Center

Loop Prevention / Loop Prevention Config

← Loop Prevention Config

Please click switches on which you want to enable the Loop Protection feature:

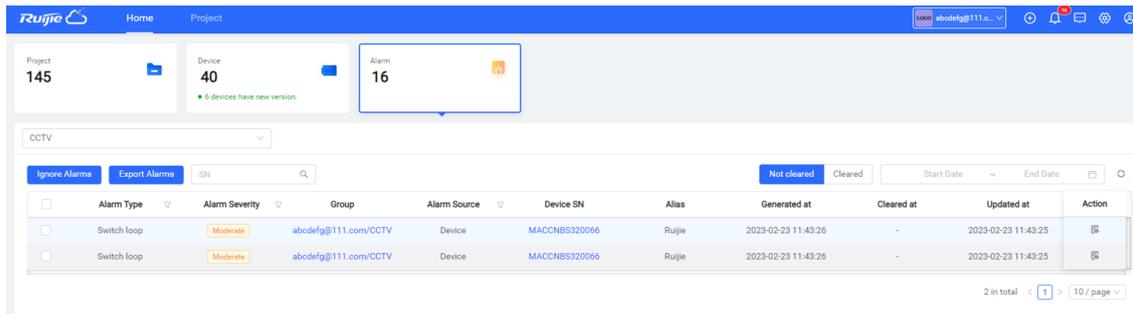
Recommendation
Enable on all identified access switches in the project

Custom
Manually select access switches

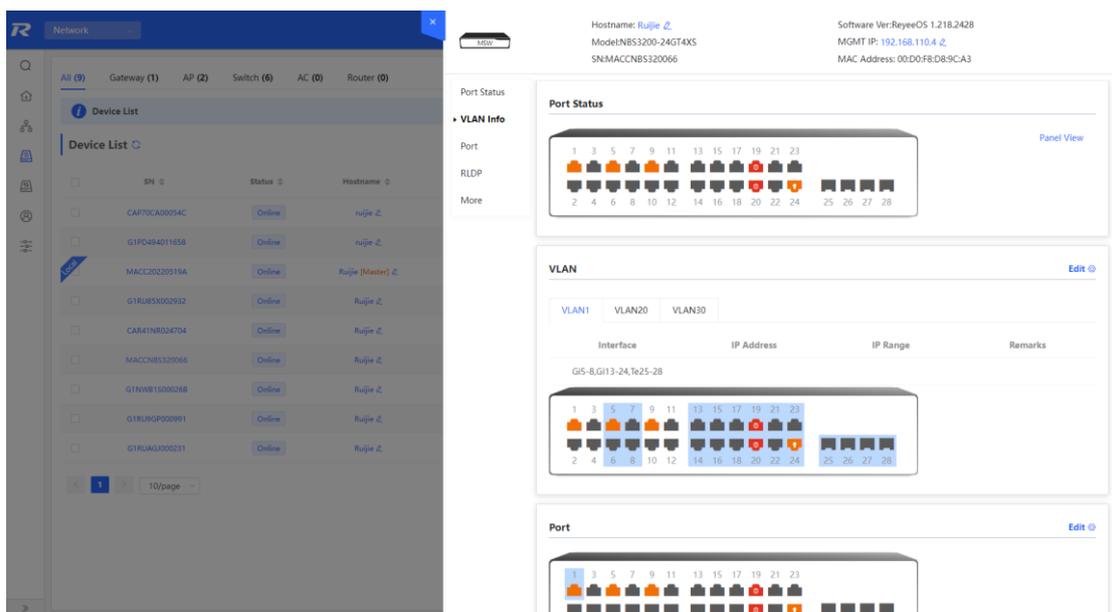
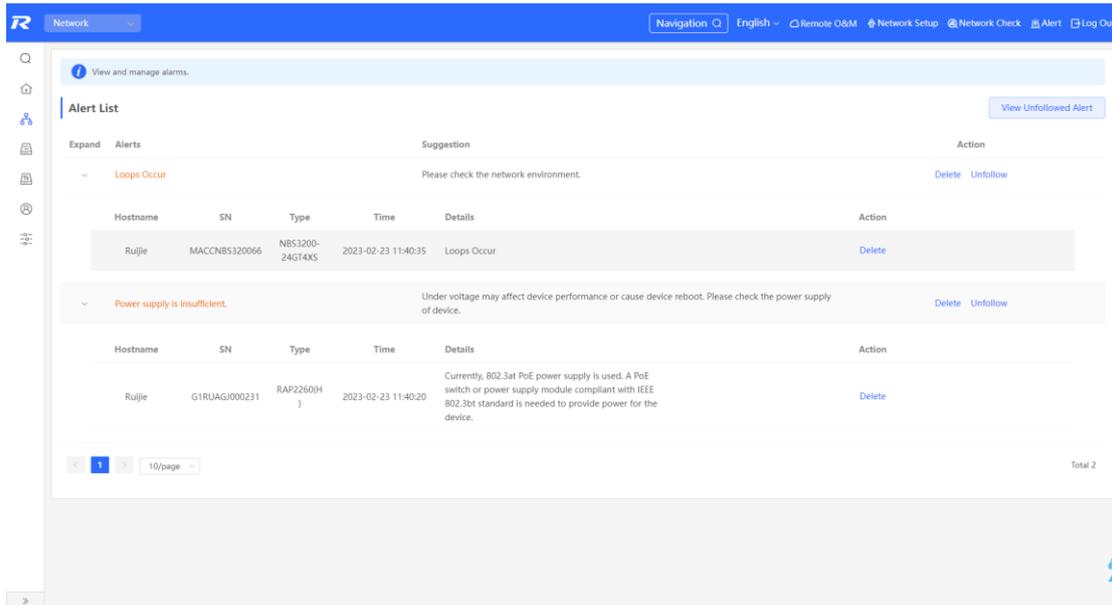
Selected: 4 device(s)

[Deliver Config](#)

When a loop occurs, an alarm is reported.



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



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

The screenshot displays the Ruijie Cloud network management interface. The main view is titled "Device Information" and shows a network topology on the left and monitoring data on the right.

Topology: A hierarchical network diagram starting with a "WAN" connection at the top. Below it is a switch labeled "EG0504-P-E" (SN: MACCNB53202978A). This switch has two LAN ports: "LAN1" (G24) and "LAN2" (G8). LAN1 is connected to two switches: "NB53100-24G24KFP..." (SN: R8B5K029352) and "NB53100-8G222FP-P" (SN: CA84198024704). LAN2 is connected to "NB53100-8G222FP-P". The "NB53100-24G24KFP..." switch has three ports: "Port 2" (G1), "G3", and "G4". "G1" is connected to "ES2096C-P" (SN: CAP70CA00054C). "G3" is connected to "NB53100-24G24KFP..." (SN: 1NWB10002028B). "G4" is connected to "NB53200-24G74KS" (SN: MACCNB5320066). The "NB53100-24G24KFP..." switch has two ports: "Port 16" (G1) and "WAN" (G8). "Port 16" is connected to "ES2186C" (SN: 70P049011658). "WAN" is connected to "BAP2800H" (SN: 70AG0000231).

Monitoring Panel: The right side of the interface shows monitoring data for the selected device (Ruijie, SN: MACCNB5320066, Device model: NB53200-24G74KS, Management IP: 192.168.1.104).
- **Status:** A row of 24 indicator lights, with the 12th light (port 12) highlighted in yellow.
- **Device Resources:** Includes "Uplink" (Port: G24, Port Speed: 100M, Duplex: Full-duplex, Uplink/Downlink Speed: 25.54Kbps / 15.28Kbps), "CPU&Memory Usage" (CPU Utilization: 10%, Memory Usage: 13%), and "Connection Status" (Last 24 Hours, Last 7 Days).
- **Port Packet Statistics:** A table with columns: Port, Inbound/Outbound Traffic (KB), Inbound/Outbound Rate (KB/s), Number of Packets Received/Sent, CRC/FCS Errors, Fragment/Overized Packets, and Number of Conflicts. The table shows "No Data".

Right-Hand Panel: A vertical sidebar on the far right contains various status icons and labels: Role, Status, poE, 1G/2.5G/5G/10G, Power Error, 10M/100M, Blocking, Disconnected, Uplink, Close, Copper, Abnormal, SFP, and Instruction.

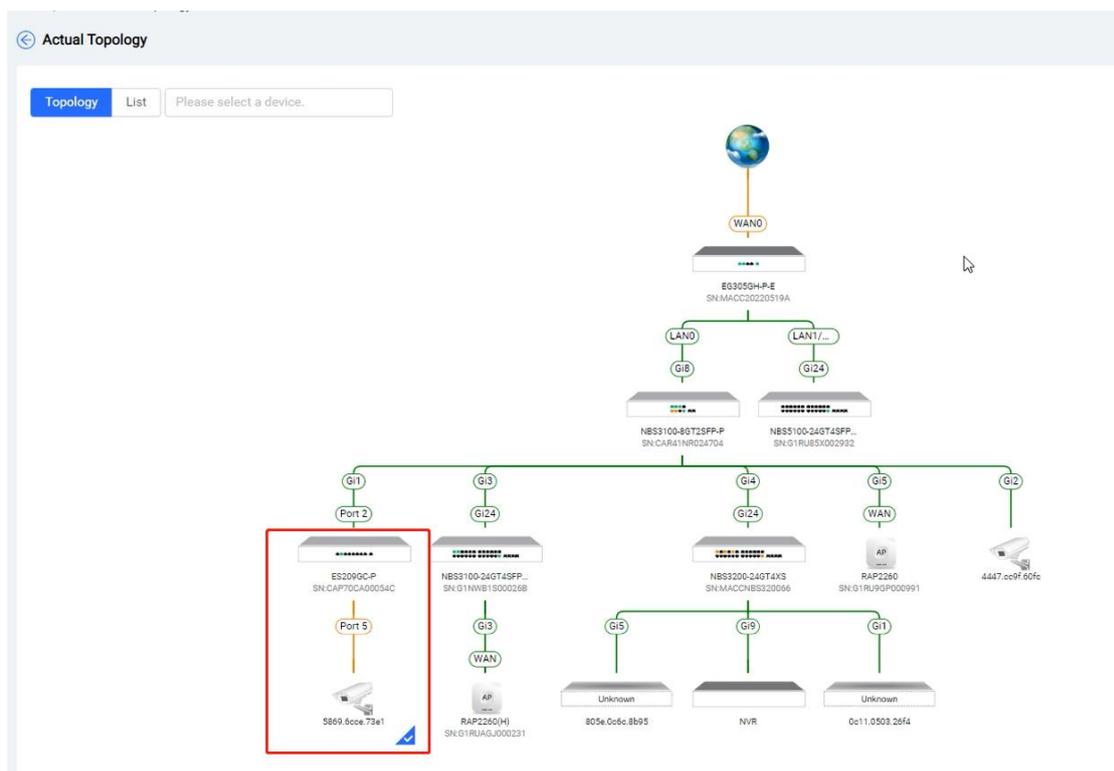
5 Troubleshooting

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.

Device Information

TOPOLOGY List

EG305GH-P-E
SN:MACC20220519A

LAN0 LAN1/...

Gi8 Gi24

NBS3100-8GT25FP-P
SN:CAR41NR024704

NBS5100-24GT45FP...
SN:G1RU85X002932

Gi3 Gi4 Gi5

Gi24 Gi24 WAN

NBS3100-24GT45FP...
SN:G1NWB15000268

NBS3200-24GT4XS
SN:MACCNBS330066

AP
RAP2260
SN:G1RUJRG000991

ruijie Synced

SN: CAP70CA00054C Device model: ES209GC-P Management IP: 192.168.110.2

Monitoring Configuration Diagnostics

Overview Port Rate PoE List Search Log History

PoE Port List

Total PoE Power:120.00 W, Current Power:2.71 W, Time: 2023/2/22 10:27:23

Port	PoE-capable	PoE Status	Power	PD class
Port 1	Open	Disabled	0.00 W	0
Port 2	Open	Disabled	0.00 W	0
Port 3	Open	Disabled	0.00 W	0
Port 4	Open	Disabled	0.00 W	0
Port 5	Open	Open	2.71 W	3
Port 6	Open	Disabled	0.00 W	0
Port 7	Open	Disabled	0.00 W	0
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.

Unnamed Switch

Port (9 ports) ? Help

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	1000M	0	2.8	Reboot More

View More

- (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?

- (1) 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.