Ethernet Switch (Managed Switch)

User Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.1

Foreword

General

This manual introduces the functions and operations of the Ethernet switch (hereinafter referred to as the "device"). Please read carefully before using the product. After reading, please save the document properly for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Frequently Used Functions

Icon/Parameter	Description
/	Edit an item.
/ /**Delete**	Delete items one by one or in batches.
/	Enable or disable items one by one or in batches.
Refresh /	Refresh the content.
Auto Refresh	Automatically refresh the content at regular intervals.

Revision History

Version	Revision Content	Release Time
V1.0.1	Update Login, Quick Configuration, Maintenance, Network Settings, PoE Management, Security, Control Policy and Authentication.	March 2026
V1.0.0	First release.	September 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited to: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Table of Contents

Foreword I
1 Login 1
1.1 Initializing the Device 1
1.2 Logging in 1
1.3 Main page 2
2 Quick Configuration 4
2.1 Configuring General Information 4
2.2 Viewing Port Information 5
2.3 Viewing IPC and NVR 6
3 Maintenance 7
3.1 Configuring System Time 7
3.2 Viewing Legal Information 7
3.3 Changing Password 7
3.4 Configuring Firmware 8
3.5 File Management 8
3.6 Viewing Device Information 9
3.7 Viewing Log Information 9
3.8 Status Monitoring 10
3.9 Diagnosing 10
3.10 Configuring Mirroring 11
4 Network Settings 13
4.1 Configuring Ports 13
4.1.1 Edit Ports 13
4.1.2 Port Details 15
4.2 Configuring EEE 16
4.3 Configuring VLAN 17
4.4 Configuring VLAN Interface 20
4.5 Configuring Routing 20
4.6 Viewing Routing Table 21
4.7 ARP Management 22
4.8 Configuring ERPS 23
4.8.1 One-Click Configuration 23
4.8.2 Advanced Configuration 26
4.9 Configuring IGMP Snooping 33
4.10 Configuring STP 34
4.10.1 STP 34
4.10.2 Port Instance 35

4.11 Configuring Link Aggregation....36
4.12 Configuring SNMP Protocol....37
4.12.1 Configuring SNMP V1 and V2....38
4.12.2 Configuring SNMP V3....38
4.13 Configuring MAC Table....40
4.13.1 Adding MAC Table....40
4.13.2 Filtering Port MAC....40
4.14 Configuring LLDP....41
4.15 Configuring Loopback Detection....42
4.16 Configuring DHCP....42
4.16.1 Configuring DHCP Server....42
4.16.2 Configuring Static Binding....44
4.16.3 Viewing List of Bound Addresses....45
4.17 DHCP Snooping....45
4.17.1 Global Configuration....45
4.17.2 Port Configuration....46
4.17.3 Option 82 Configuration....48
4.18 Virtual Cable Test....49
5 PoE Management....50
5.1 Configuring PoE Settings....50
5.2 Configuring Perpetual PoE....51
5.3 Configuring Long Distance PoE....51
5.4 Viewing PoE Event Statistics....52
5.5 Configuring Green PoE....52
5.6 Configuring Force PoE....54
5.7 Configuring PoE Watchdog....54
6 Security....55
6.1 Basic Services....55
6.1.1 Configuring Basic Services....55
6.1.2 Configuring HTTPS....55
6.2 Enabling Telnet....56
6.3 Configuring CA Certificate....56
6.3.1 Installing Device Certificate....56
6.3.2 Installing Trusted CA Certificates....57
6.4 Configuring Attack Defense....58
6.4.1 Configuring Firewall....58
6.4.2 Configuring Anti-DoS Attack....59
6.5 Configuring Port Isolation....59
6.6 Configuring Security Authentication....60
7 Control Policy....61

7.1 Configuring Port Priority....61
7.2 ACL....61
7.2.1 Configuring ACL....61
7.2.2 Configuring Period....71
7.2.3 ACL Binding....73
7.3 Configuring Priority Mapping Table....74
7.4 Configuring Queue Scheduling....74
7.5 Configuring Port Speed Limit....75
7.6 Configuring Storm Control....76
8 Authentication....77
8.1 Configuring 802.1x....77
8.2 Configuring Radius....77
Appendix 1 Security Commitment and Recommendation....79

1 Login

1.1 Initializing the Device

Prerequisites

- Make sure that the device is powered on.
- Make sure that the device is connected to the computer, and the IP address of the computer is on the same network as the IP address of the device.

Procedure

Step 1 Open the browser, enter the IP address (192.168.1.110 by default) of the device in the address bar of the web browser, and then press the Enter key.

Step 2 Set the language, and then click **OK**.

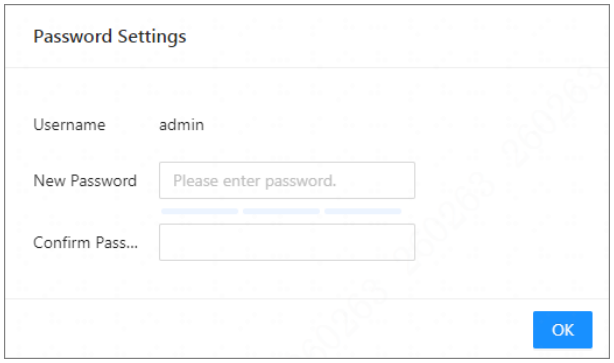
Step 3 Set the time zone, and then click **OK**.

Step 4 Read **Software License Agreement** and **Privacy Policy**, click **I have read and agree to the terms of the Software License Agreement and Privacy Policy**, and then click **OK**.

Step 5 Set the password.

The password must consist of 8 to 32 non-blank characters and contain at least 2 types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

Figure 1-1 Set password



Step 6 Click **OK**.

1.2 Logging in

Prerequisites

- Make sure that the device initialization is complete.
- Make sure that the IP address of the computer is on the same network as the IP address of the device.

Procedure

Step 1 Enter the IP address (192.168.1.110 by default) of the switch in the address bar of the web browser, and then press the Enter key.

Step 2 Enter the user name and password.

Step 3 Click **Login**.

1.3 Main page

Log in to access the home page.

The page might vary depending on the product model. Please refer to the actual device.

Figure 1-2 Home page

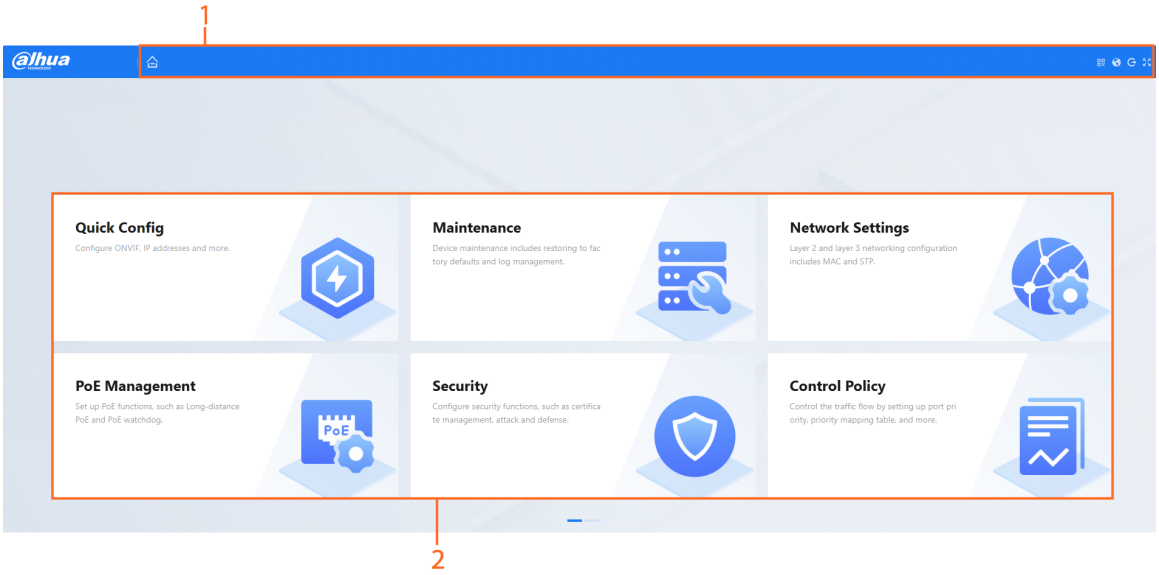


Table 1-1 Description of the home page

No.	Name	Description
1		Go back to the home page.
		Scan the QR code viewing the device's information.
		Switch the system languages. Supports multiple languages.
		Log out, and then return to the login page.
		Full-screen displays the webpage.
2	Quick Config	Configure quick settings, including ONVIF, IP address and more.
	Maintenance	Configure maintenance settings, including restoring to factory defaults and log management.
	Network Settings	Configure network settings, including MAC and STP settings.
	PoE Management	Configure PoE settings, including long-distance PoE and PoE watchdog. Non-PoE devices do not support this feature.

No.	Name	Description
	Security	Configure security settings, including certificate management, attack and defense, and more.
	Control Policy	Configure traffic flow settings, including setting port priority, priority mapping table, and more.
	Authentication	Configure authentication management, including 802.1x and RADIUS.

2 Quick Configuration

You can view the system information, and configure the device parameters including ONVIF, IP address and more. The pages on the manual are for reference only, and might differ from the actual pages.

2.1 Configuring General Information

You can view and configure the general information, including name, IP address and subnet mask.

Procedure

Step 1 Select **Quick Config** > **General**.

Step 2 (Optional) Click to enable the DHCP function.

Step 3 Set the device name, IP address and subnet mask.

Figure 2-1 General information

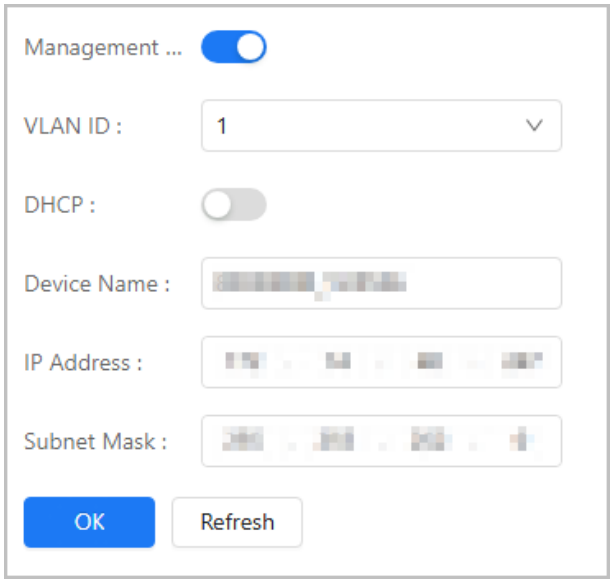


Table 2-1 Description of general information

Parameter	Description
Management VLAN	After **Management VLAN** is enabled, you can only access the webpage through the IP from managed VLAN.
VLAN ID	Displays the current the managed VLAN ID.
DHCP	Supports enabling DHCP. After enabling DHCP, new IP will be automatically acquired and assigned. Once DHCP is enabled, the router or the DHCP server connected with the switch will automatically assign an IP address to the switch. The original IP address will fail to access the webpage.
Device Name	Displays the current device name. Supports changing the name.

Parameter	Description
IP Address	Displays the current IP address and the subnet mask. Supports manual configuration.
Subnet Mask	

Step 4 Click **OK**.

2.2 Viewing Port Information

You can view information including port, type, link status, speed/duplexing, VLAN, RX usage, TX usage and media type of the device.

Procedure

Step 1 Select **Quick Config** > **Port Info**.

Step 2 View the port information of the device.

A green port indicates a successful connection, while a blue port indicates no connection or a failed connection.

Figure 2-2 Port information

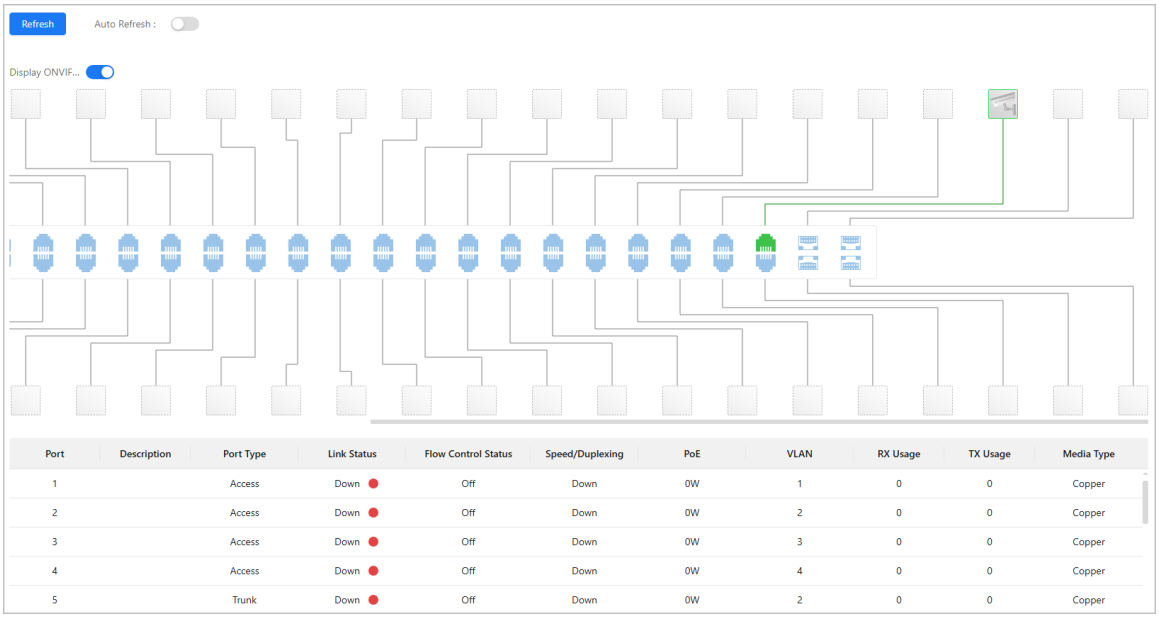


Table 2-2 Description of port information

Parameter	Description
Port	Displays all ports of the device.
Description	Displays the port description. Supports entering number, letter, special character, regardless of upper case and lower case. Up to 16 non-blank characters can be used. No description is by default.
Port Type	Includes 3 types: **Access** , **Hybrid**, and **Trunk**.
Link Status	Includes 2 types: **Up** and **Down**. ● Up: The port is connected. ● Down: The port is not connected or the connection fails.

Parameter	Description
Flow Control Status	Displays the status of the flow control function.
Speed/Duplexing	• Online: Displays the speed and the duplex mode. • Offline: Displays **Down**.
PoE	Displays the PoE power consumption value. • Non-PoE devices do not support this feature. • The number of PoE ports supported varies by product model. Please refer to the actual device.
VLAN	VLAN ID. VLAN 1 by default.
RX Usage	Displays the receiving usage. The value of the current receive rate divided by the actual negotiated rate over a period (usually 5 minutes).
TX Usage	Displays the sending usage. The value of the current transmit rate divided by the actual negotiated rate over a period.
Media Type	Includes 2 types: **Copper** and **Fiber**. • Copper: RJ-45 port. • Fiber: Fiber port.

Related Operations

Click next to **Auto Refresh** to enable the automatic refreshing.

Click next to **Display ONVIF Devices** to enable the ONVIF device display feature, allowing you to visually view types of devices connected under the ports.

Hover the mouse over the image of a connected device to display information about the device, including the connected port number, IP address, MAC address, and more.

2.3 Viewing IPC and NVR

Select **Quick Config** > **IPC&NVR**, you can view the information of the IPC, NVR and other devices connected to the device.

3 Maintenance

3.1 Configuring System Time

You can view and configure the system time of the device.

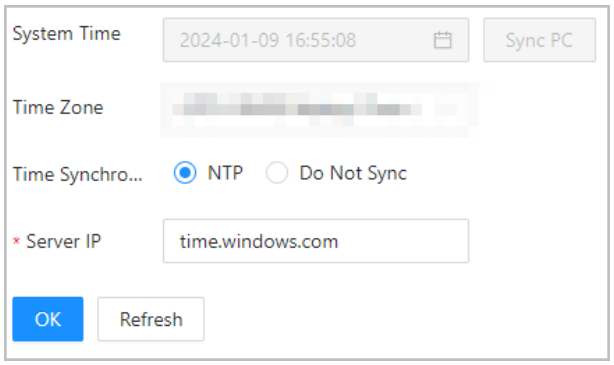
Procedure

Step 1 Select **Maintenance** > **System Time**.

Step 2 Configure the system time.

- Manually configure the **System Time** and **Time Zone**, and then click **OK**.
- Click **Sync PC** to synchronize the device time to the computer time, and then click **OK**..
- Click next to **NTP** and set the server IP to synchronize the device time to the server time, and then click **OK**.
- Click next to **Do Not Sync** to disables automatic time synchronization. System time must be set manually and remains unchanged unless adjusted by the user.

Figure 3-1 Configure time



3.2 Viewing Legal Information

Select **Maintenance** > **Legal Info**, and then you can view **Software License Agreement** , **Privacy Policy** and **Open Source Software Notice**.

3.3 Changing Password

Changing the login password for the device webpage.

Procedure

Step 1 Select **Maintenance** > **Change Password**.

Step 2 Enter **Old Password** , **New Password** and **Confirm Password**.

The password must consist of 8 to 32 non-blank characters and contain at least 2 types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

Step 3 Select time that the password expires in the list of **Password Expires in**.

You can select **Password Expires in** from never, 30 days, 60 days, 90 days, and 180 days.

Step 4 Click **OK**.

3.4 Configuring Firmware

Select **Maintenance** > **Firmware Config**, you can restore the device, update system and restart switch.

Restore Factory Default

Click **Factory Defaults** , enter the password, and then click **OK**.

All parameters restore to default settings except the IP address of the VLAN1.

Update Software

Click **Browse** to import the update file, and then click **Update Now**.

It might take 3 minutes to update the software. After the update, the system will automatically restart.

Restart Device

Click **Restart Now** , and then click **OK** in the pop-up prompt box to restart the device.

3.5 File Management

You can configure the backup file and restore file.

Backup Configuration

Select **Maintenance** > **File Management** > **Backup Config**, click **Export Configuration File** to export the file.

Restoration Configuration

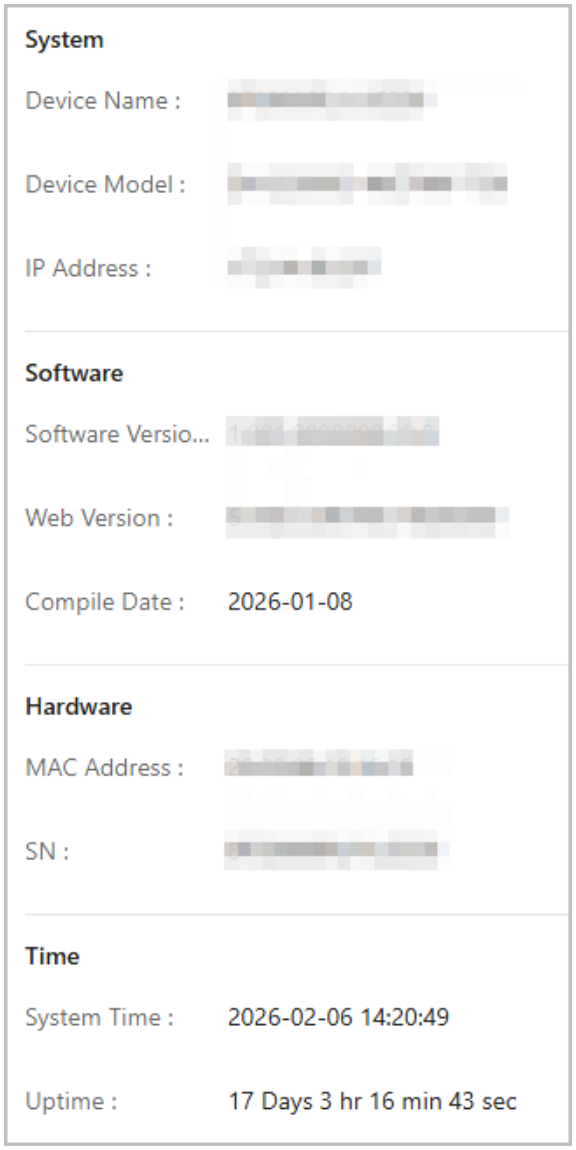
Select **Maintenance** > **File Management** > **Config Restore**, click **Browse** to select the file, and then click **Import Configuration Files** to import the file.

Imported configuration will overwrite previous configuration.

3.6 Viewing Device Information

Select **Maintenance** > **Device Info**, you can view the information on **System** , **Software**, **Hardware** and **Time**.

Figure 3-2 Device information



3.7 Viewing Log Information

You can view the log information on the device operations.

Procedure

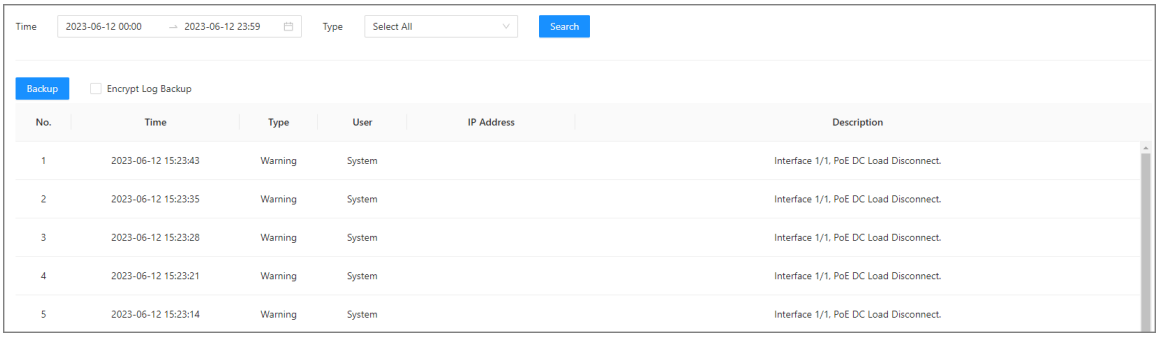
Step 1 Select **Maintenance** > **Log**.

Step 2 Configure **Time** and **Type**, and then click **Search**.

Step 3 You can view the log information.

- Log type includes **Error** , **Warning** and **Message**.
- Backup: Tap to backup the searched logs.
- Encrypt Log Backup: Click the checkbox to encrypt the back-up logs.

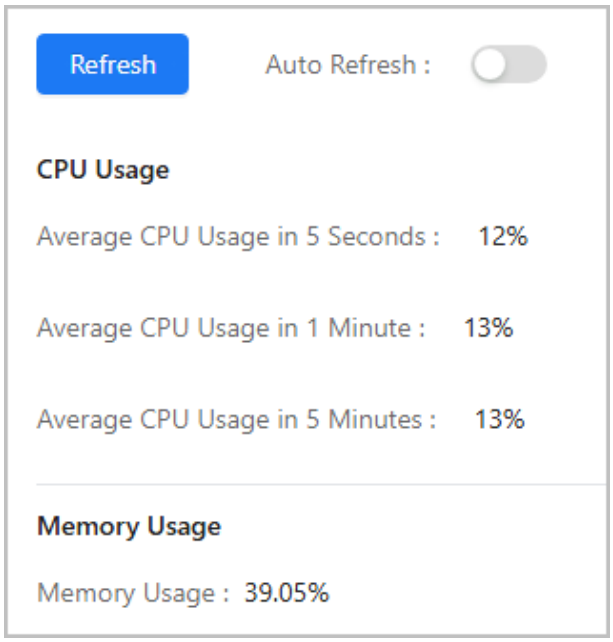
Figure 3-3 Log information



3.8 Status Monitoring

Select **Maintenance** > **Status Monitoring**, and then you can view the CPU usage and memory usage.

Figure 3-4 Status monitoring



3.9 Diagnosing

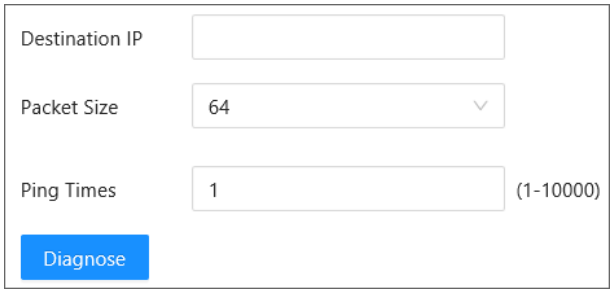
Procedure

Step 1 Select **Maintenance** > **Diagnosis**.

Step 2 Enter the **Destination IP** , and then select **Packet Size** and **Ping Times**.

Step 3 Click **Diagnose**.

Figure 3-5 Diagnosis



3.10 Configuring Mirroring

Mirroring is a packet capture technology. By configuring the device, it allows copying data packets from one or multiple ports (source mirror ports) to a designated ports (destination mirror port). A host running packet analysis software is connected to the destination mirror port to analyze the received packets, thereby achieving network monitoring and troubleshooting purposes.

Procedure

Step 1 Select **Maintenance** > **Mirror**.

Step 2 Click **Add**.

Step 3 In **Add Mirroring Group** page, select **Mirroring Group No.**, **Destination Port**, and then select from **TX**, **RX**, and **Both** according to the actual situation.

Step 4 Click **OK**.

Figure 3-6 Add Mirroring Group

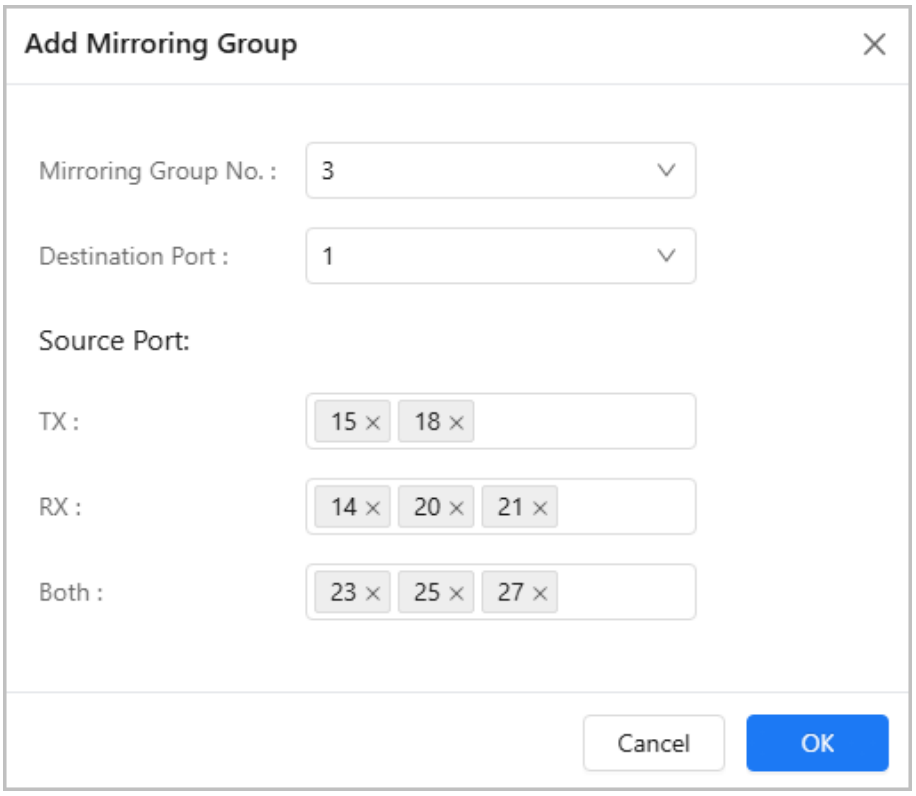


Table 3-1 Description of source port

Name	Description
TX	Only supports sending traffic.
RX	Only supports receiving traffic.
Both	Supports both sending and receiving.

4 Network Settings

4.1 Configuring Ports

4.1.1 Edit Ports

Procedure

Step 1 Select **Network Settings** > **Port**.

You can view the port parameters, including speed/duplexing status, flow control, and other parameters.

Figure 4-1 Port

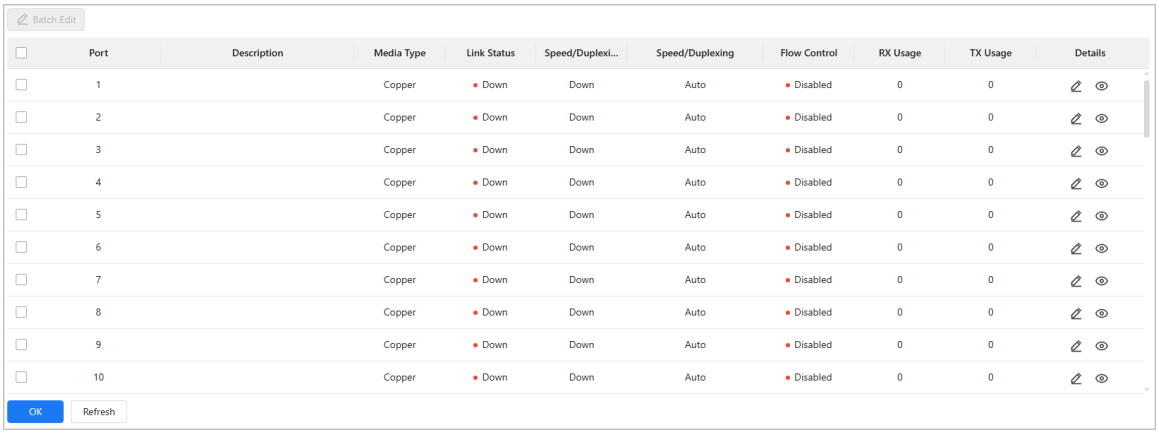


Table 4-1 Description of the port parameters

Parameter	Description
Port	Displays all ports of the device.
Description	Enter the description of the port. The description cannot exceed 16 characters. Only numbers, letters and the following special character (_) are allowed. The first character must be a letter and the last character must not be a special character.
Media Type	Includes 2 types: **Copper** and **Fiber**. ● Copper: Ethernet port. ● Fiber: Optical port.
Link Status	Includes 2 statuses: **Up** and **Down**. ● Up: The port is connected. ● Down: The port is not connected or the connection fails.

Parameter	Description
Speed/Duplexing Status	• Online: Displays the port rate and the duplex mode. • Offline: Displays **Down**.
Speed/Duplexing	Set the speed and the duplex mode from **Down** , **Auto**, **10M Half**, **10M Full**, **100M Half**, **100M Full**, and **1000M Full**. The speed/duplexing is set as **Auto** for combo port.
Flow Control	Click to enable or disable the function.
RX Usage	Displays the receiving usage.
TX Usage	Displays the sending usage.

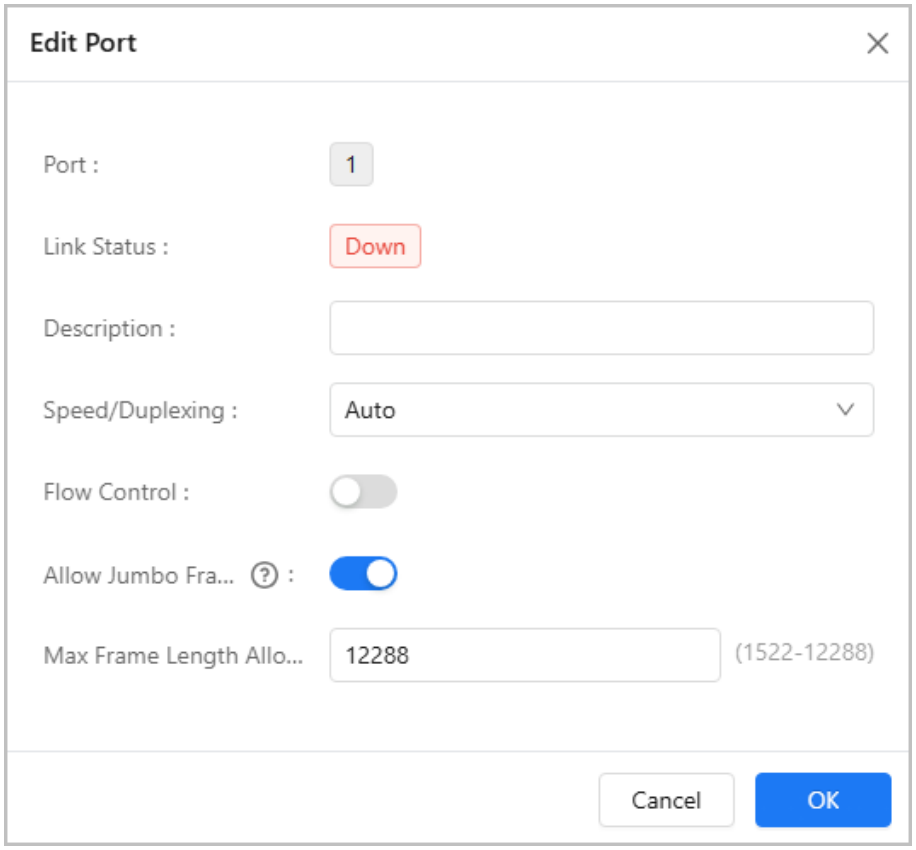
Step 2 Configure the port parameters, including edit the parameters one by one or in batches.

- Click to edit the port parameter, and then click **OK**.

  Allow Jumble Frames , **Max Frame Length Allowed**: Click next to **Allow Jumble Frames** to enable this function, it allows for setting the maximum transmission unit (MTU) to support data frames up to 12,288 bytes.

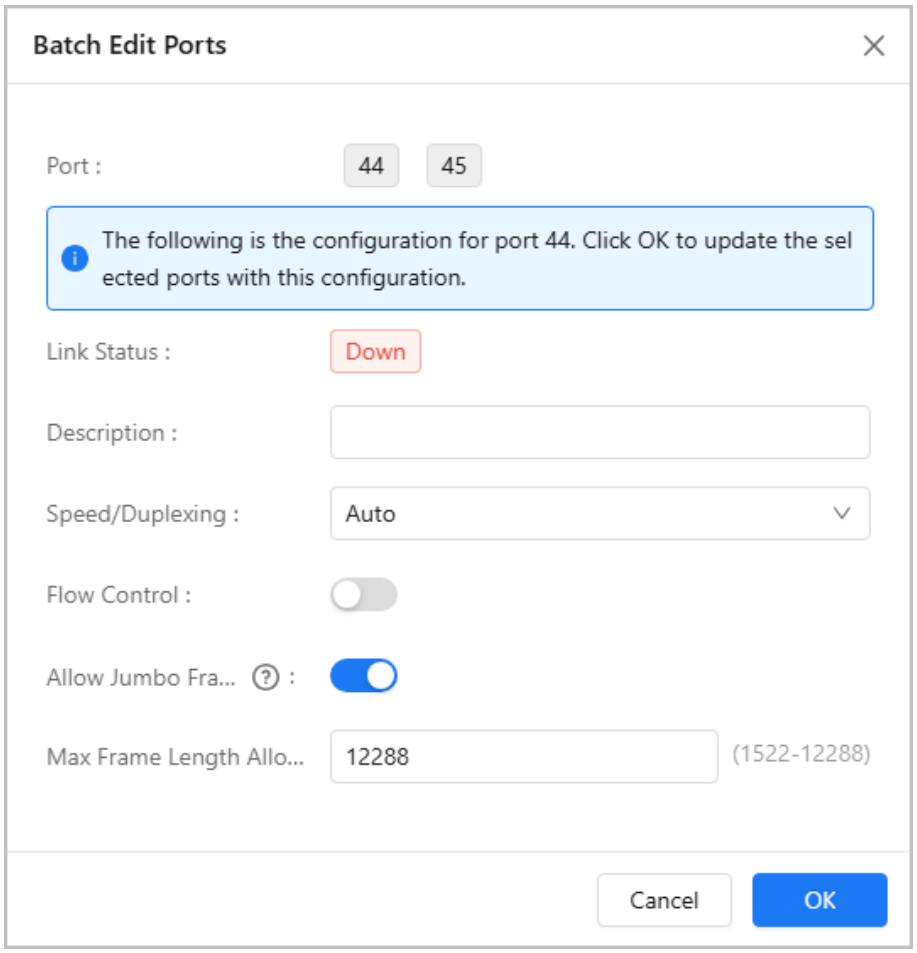
  The max frame length allowed might vary depending on the device. Please refer to the actual device.

Figure 4-2 Edit port



- Select some ports, click **Batch Edit** , edit the port parameters in batches, and then click **OK**.

Figure 4-3 Batch edit ports



Step 3 Click **OK**.

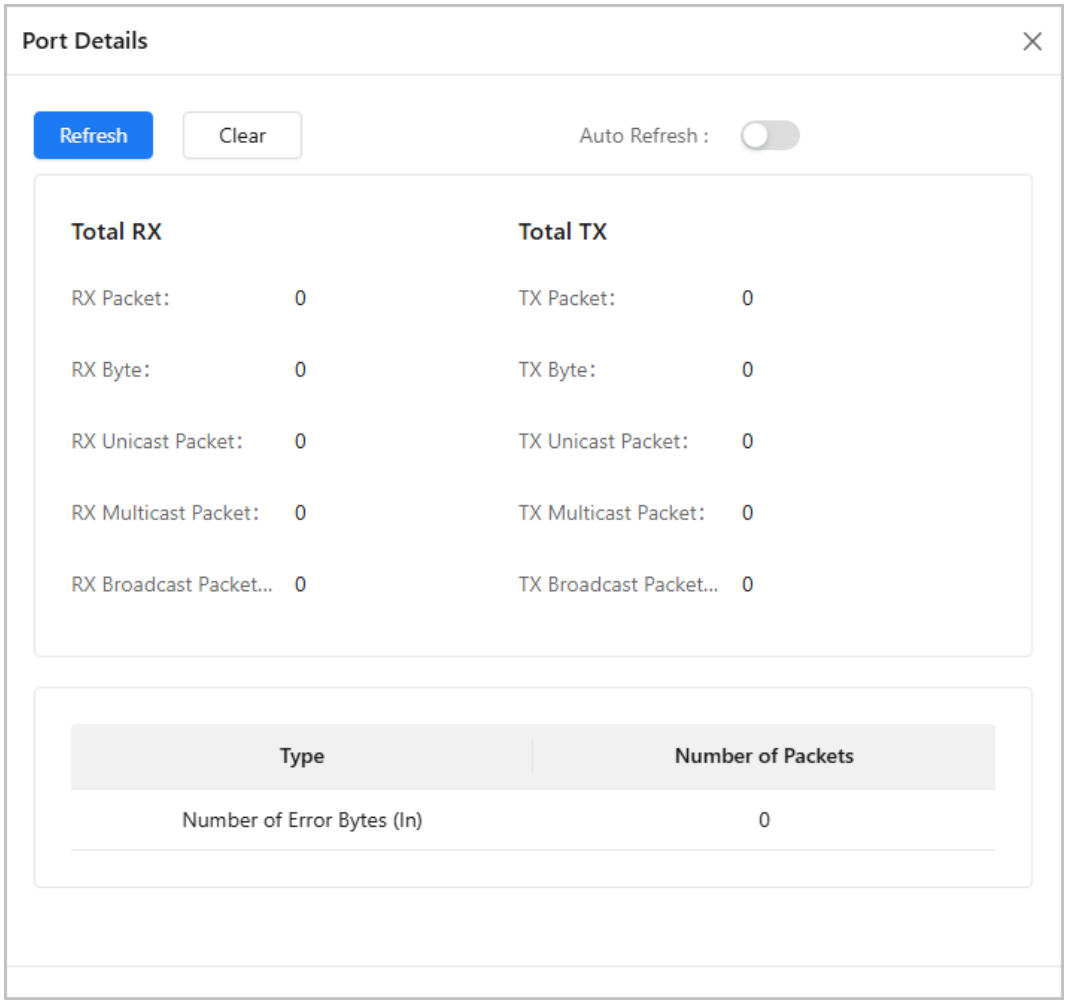
4.1.2 Port Details

Procedure

Step 1 Select **Network Settings** > **Port**.

Step 2 Click to view the detail information of port parameters.

Figure 4-4 Port details



4.2 Configuring EEE

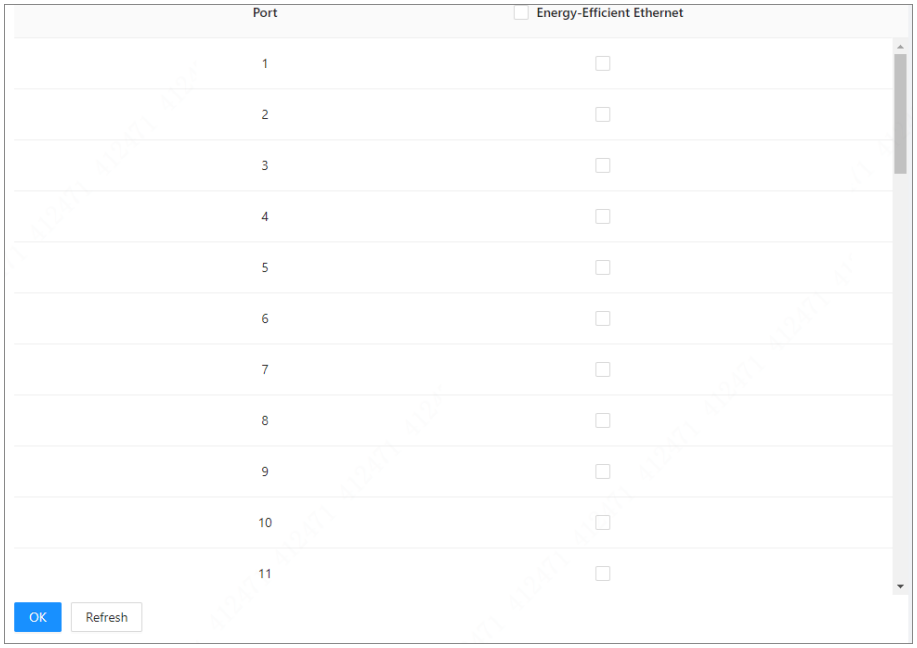
EEE (Energy-Efficient Ethernet) is designed to reduce power consumption of network devices during the periods of low data activity or network idle time.

Procedure

Step 1 Select **Network Settings** > **EEE**.

Step 2 Select the checkbox of the port to enable the **Energy-Efficient Ethernet** function, and then click **OK** to save the configuration.

Figure 4-5 EEE function



4.3 Configuring VLAN

You can add the port to the VLAN, and then configure the information of the VLAN.

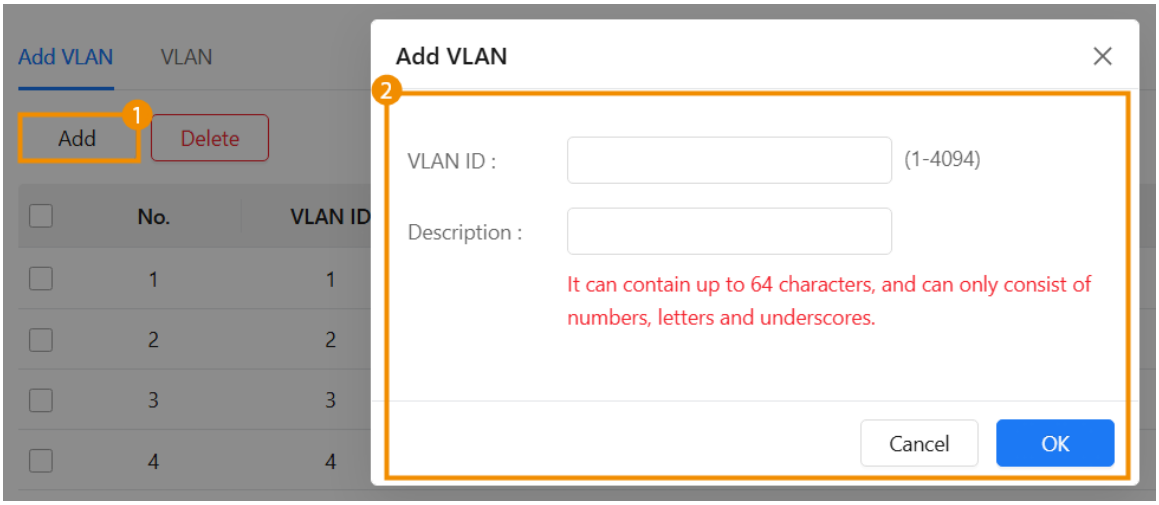
Procedure

Step 1 Select **Network Settings** > **Add VLAN**.

Step 2 Click **Add** , enter the **VLAN ID** and **Description**, and then click **OK**.

- For **VLAN ID** configuration, it supports enter single, multiple, or consecutive values. For example, **2**, **3, 7**, **7**, **2-9**, representing the creation of VLAN2, VLAN 3 and VLAN 7, VLAN 2 through VLAN 9 respectively. The valid VLAN ID range is subject to the actual device.
- For configuring multiple VLAN IDs, separate the numbers with a comma.
- Descriptions cannot be configured when creating multiple VLAN IDs.

Figure 4-6 Add VLAN



Step 3 Select **Network Settings** > **VLAN** to configure the port VLAN parameters.

Figure 4-7 Configure VLAN

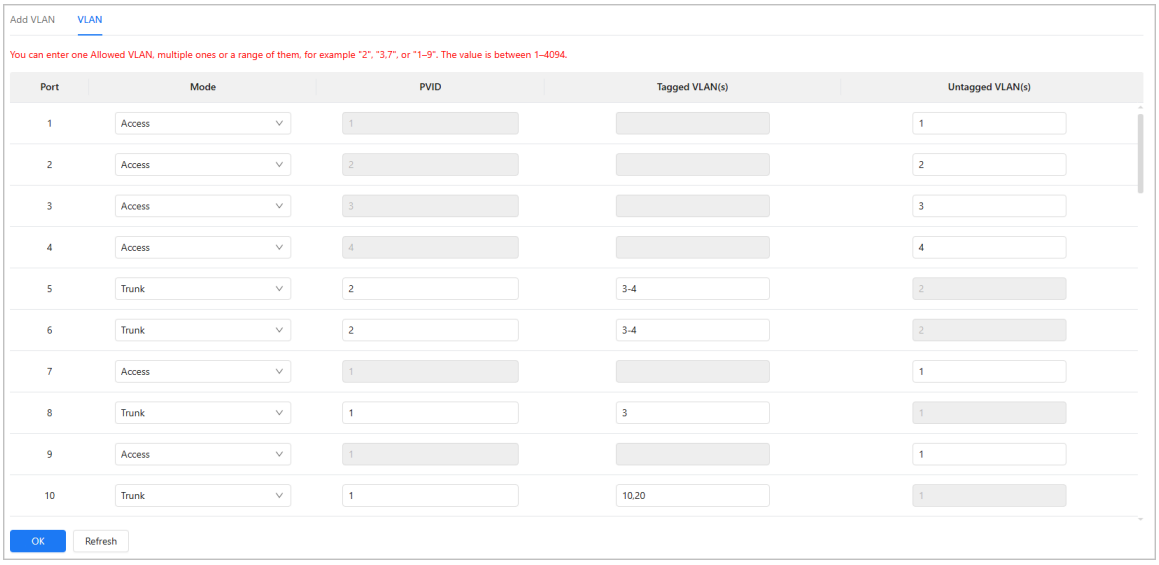


Table 4-2 Description of the port VLAN parameter

Parameter	Description
Port	Displays all ports of the device.
Mode	Includes 3 modes: **Access** , **Trunk**, and **Hybrid**. ● Access: In this mode, only transmit one untagged VLAN packet. **Untagged VLAN(s)** must be configured. ● Trunk: In this mode, allows transmit multiple tagged VLANs packets. **PVID** and **Tagged VLAN(s)** must be configured. ● Hybrid: In this mode, allows transmit multiple untagged and tagged VLANs packets. **PVID** , **Untagged VLAN(s)** and **Tagged VLAN(s)** must be configured.
PVID	Assign the port to a specific VLAN. The port belongs to VLAN 1 by default.

Parameter	Description	
Tagged VLAN(s)	Set this value to transmit tagged VLAN(s) packets.	**Untagged VLAN(s)** and **Tagged VLAN(s)** supports enter single, multiple, or consecutive values. For example, **2**, **3,7**, **2-9**. The valid VLAN ID range is 1 to 4094.
Untagged VLAN(s)	Set this value to transmit untagged VLAN(s) packets.	

Table 4-3 Frame processing comparison

Port Type	Untagged Frame Processing	Tagged Frame Processing	Frame Transmission
Access	Receives an untagged frame and adds a tag with the default VLAN ID to the frame.	• Accepts the tagged frame if the frame's VLAN ID matches the default VLAN ID. • Discards the tagged frame if the frame's VLAN ID differs from the default VLAN ID.	After the PVID tag is removed, the frame is transmitted.
Trunk	• Adds a tag with the default VLAN ID to an untagged frame and accepts the frame if the port permits the default VLAN ID. • Adds a tag with the default VLAN ID to an untagged frame and discards the frame if the port denies the default VLAN ID.	• Accepts a tagged frame if the VLAN ID carried in the frame is permitted by the port. • Discards a tagged frame if the VLAN ID carried in the frame is denied by the port.	• If the frame's VLAN ID matches the default VLAN ID and the VLAN ID is permitted by the port, the device removes the tag and transmits the frame. • If the frame's VLAN ID differs from the default VLAN ID, but the VLAN ID is still permitted by the interface, the device will directly transmit the frame.
Hybrid			If the frame's VLAN ID is permitted by the port, the frame is transmitted. The port can be configured whether to transmit frames with tags.

Step 4 Click **OK**.

Related Operations

In the **Add VLAN** tab, you can edit and delete VLAN information.

VLAN 1 cannot be deleted.

4.4 Configuring VLAN Interface

Background Information

A VLAN interface (Virtual Local Area Network Interface) is a logical interface that is configured based on VLANs but not bound to physical ports. Through VLAN virtual interfaces, virtual local area networks can be created and managed on devices, enabling network segmentation and isolation to enhance network security.

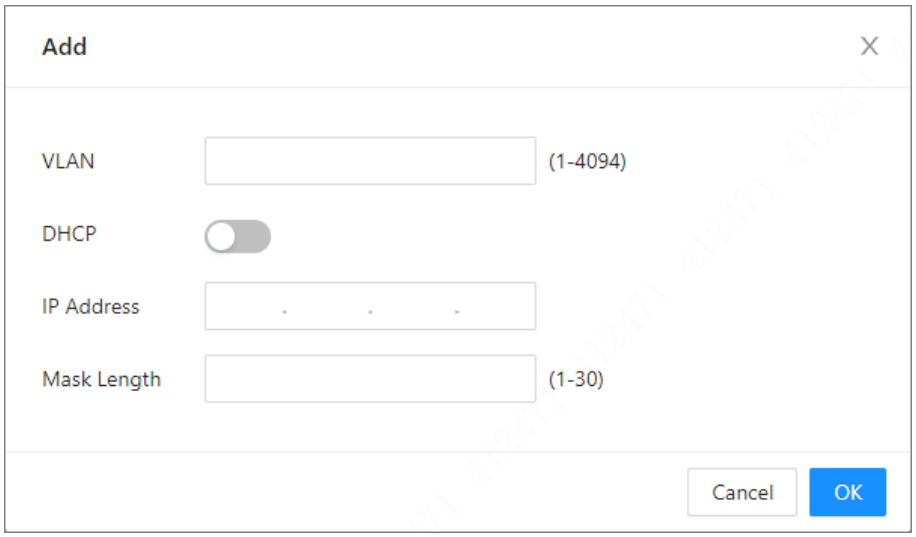
Procedure

Step 1 Select **Network Settings** > **VLAN Interface**.

Step 2 Click **Add** , input **VLAN** number, and then enable **DHCP**.

When **DHCP** disabled, you need to enter **IP Address** and **Mask Length**.

Figure 4-8 Add a VLAN interface



4.5 Configuring Routing

Introduces the IP settings and the routing settings of the device.

Procedure

Step 1 Select **Network Settings** > **Routing Settings**.

Step 2 Click **Add**, and then configure the parameters.

Figure 4-9 Routing settings

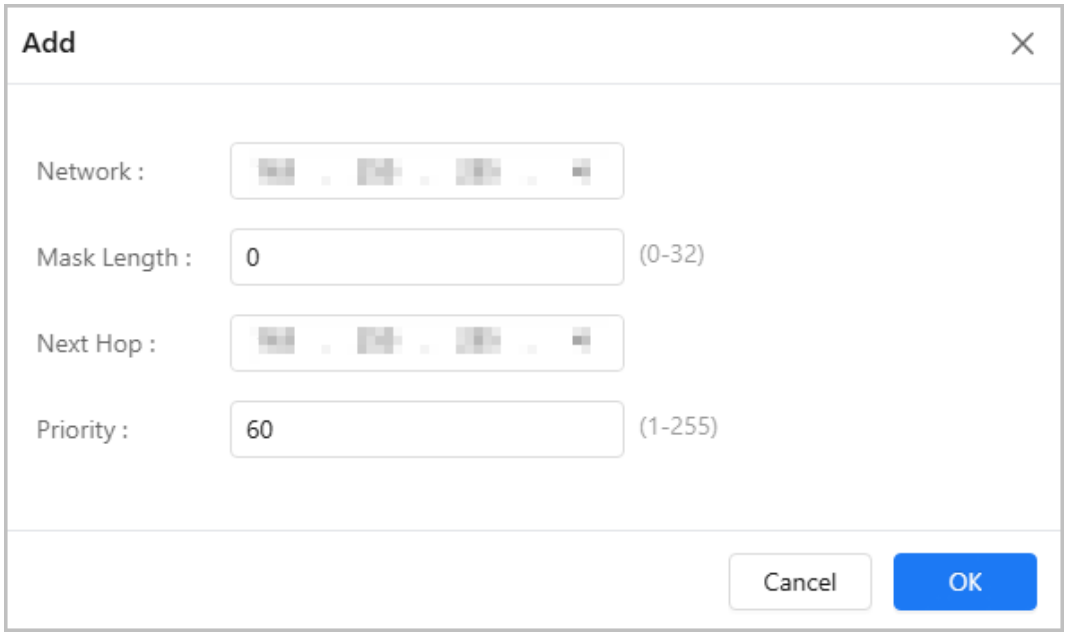


Table 4-4 Description of the routing parameters

Parameter	Description
Network	Enter the destination address or destination network to identify the IP packet.
Mask Length	Set the mask length to define the IP address range.
Next Hop	Set the next hop address of the next device that a packet must pass through before reaching its destination.
Priority	Set the priority to select the optimal path among multiple routing entries. A smaller priority value indicates a higher priority.

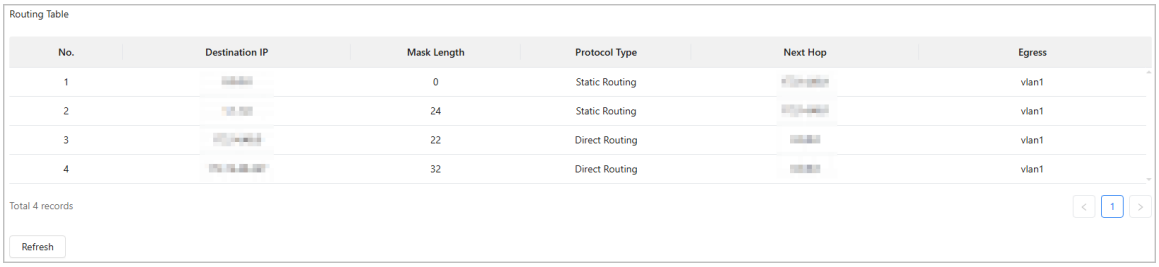
Step 3 Click **OK**.

4.6 Viewing Routing Table

The routing table is a data structure used by network devices to store the information of routing. This table records the optimal path information to reach different networks or subnets, serving as the core basis for networks devices to make packet forwarding decisions.

Select **Network Settings** > **Routing Table** to view the effective routing information, including destination IP, mask length, protocol type, next hop and egress.

Figure 4-10 Routing table



4.7 ARP Management

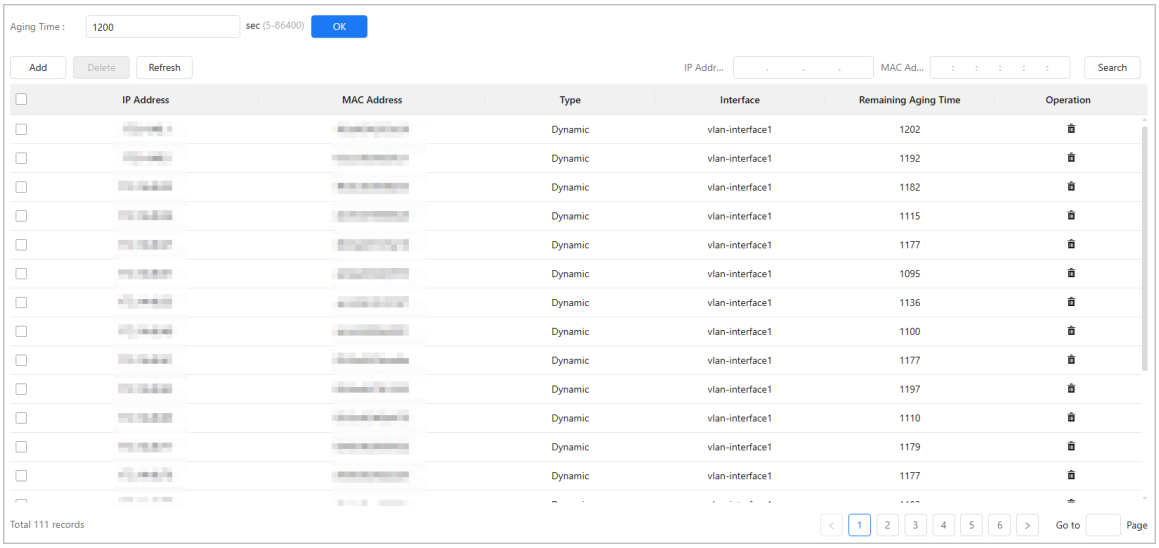
Background Information

Address Resolution Protocol (ARP) is a protocol used to map IP addresses to MAC addresses. There are generally 2 types of ARP entries: static and dynamic. In a local area network (LAN), data transmission requires both the destination IP address and MAC address. To obtain the MAC address corresponding to an IP address, an address resolution protocol is used.

Procedure

Step 1 Select **Network Settings** > **ARP**, and then you can view the information of the IP address and MAC address mapping.

Figure 4-11 ARP

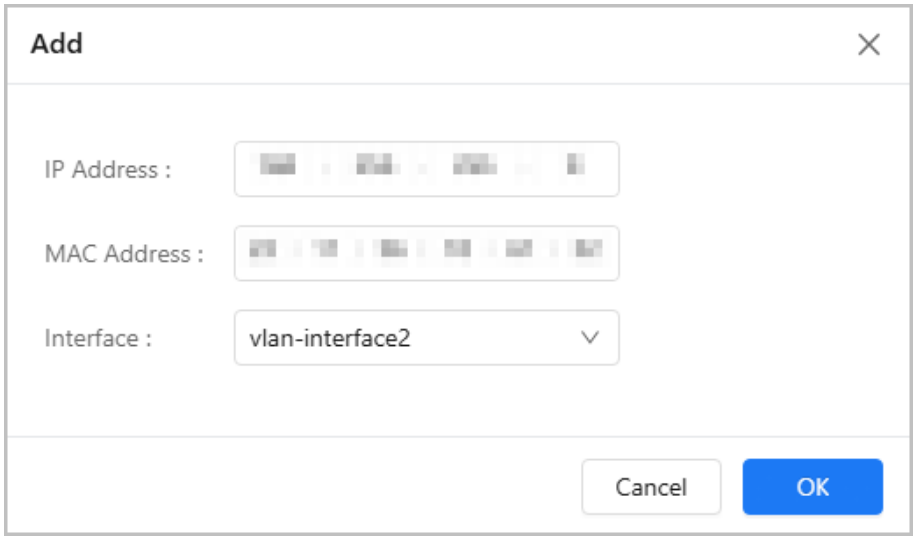


Step 2 Configure the aging time.

1. In the **Aging Time** box, enter the number.
2. Click **OK**.

Step 3 Click **Add**, and then enter the IP address, MAC address and interface.

Figure 4-12 Add the address



Step 4 Click **OK**.

4.8 Configuring ERPS

ERPS is a protocol defined by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) to eliminate loops at Layer 2. Generally, redundant links are used on an Ethernet switching network such as a ring network to provide link backup and enhance network reliability. The use of redundant links, however, might produce loops, causing broadcast storms and rendering the MAC address table unstable. As a result, communication quality deteriorates, and communication services might even be interrupted. ERPS prevents broadcast storms and implements fast traffic switchover on a network where there are loops, provides fast convergence and carrier-class reliability, and allows all ERPS-capable devices on a ring network to communicate.

Some models might not support ERPS function. Please refer to the actual products.

4.8.1 One-Click Configuration

Procedure

Step 1 Select **Network Settings** > **ERPS**.

Step 2 In the **Config Mode** area, select **One-Click ERPS Settings**, and then automatically generates a basic ERPS instance.

Click **Parameter Description**, and then you can view the detail information of the parameter.

Step 3 (Optional) In the **ERPS** area, click to enable **Ring Network**.

Disabling **Ring Network** will automatically delete the configured ERPS network, and then it might cause network storms and affect system stability.

Step 4 In the **ERPS Instance** area, click to edit the information of the basic ERPS instance.

(Optional) Click **More Settings** to view more details of the information.

Loopback Detection cannot be enabled at the same time as ERPS or STP. Only one ERPS ring can be configured.

Figure 4-13 Edit one-click ERPS

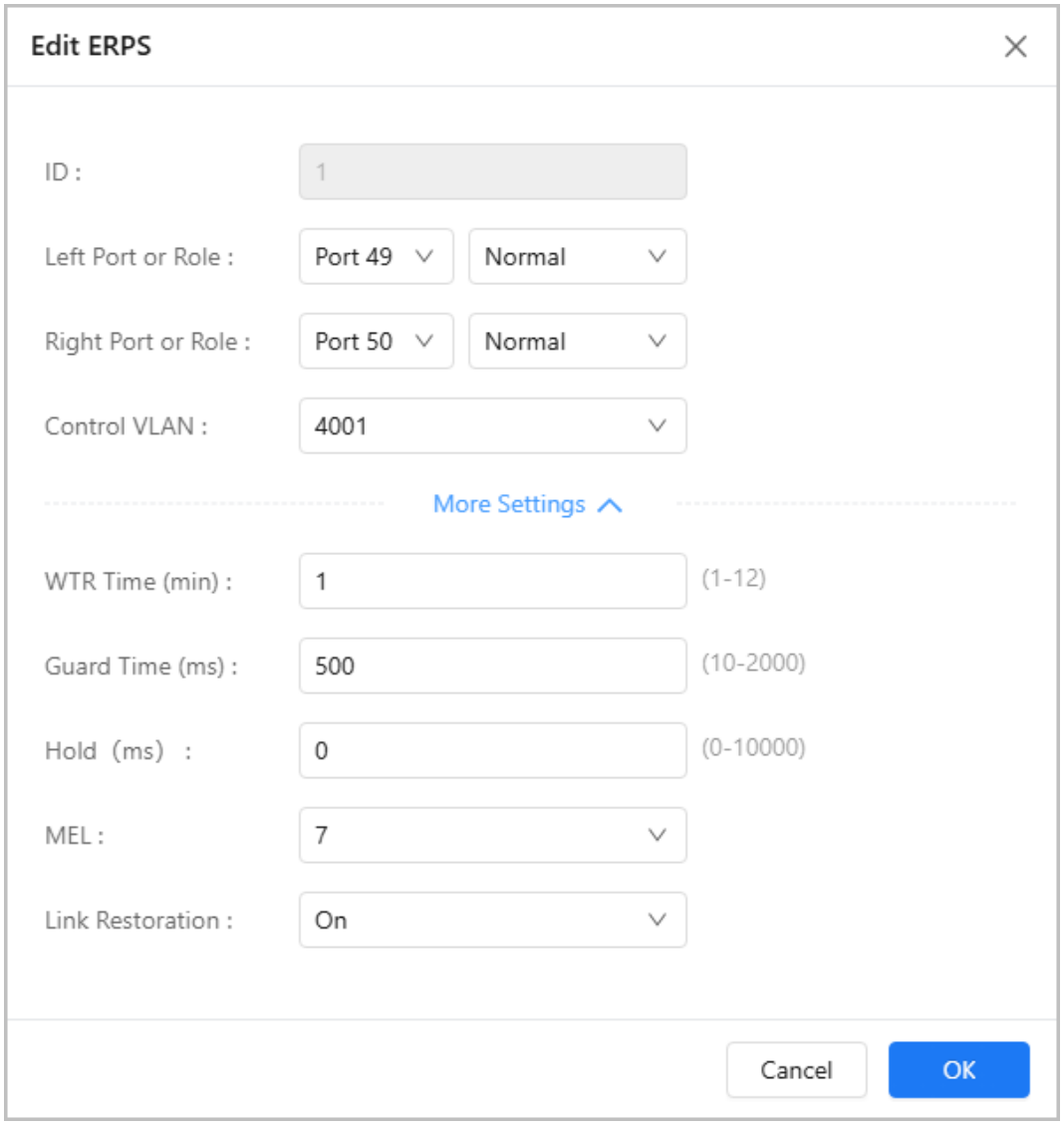


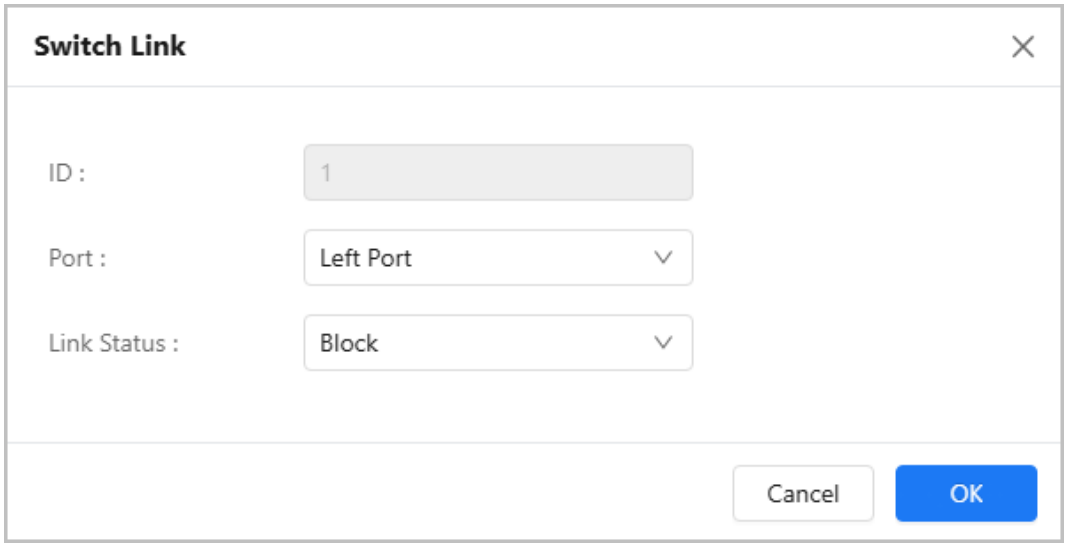
Table 4-5 Description of one-click ERPS parameter

Parameter	Description
ID	The ID number of the ERPS.
Left Port or Role	Set the left port in the ERPS ring and its role. Include 3 roles: **Normal** , **Owner**, and **Neighbour**. • Normal: The regular node. • Owner: The RPL (Ring Protection Link) owner node. • Neighbour: The non-owner node within the RPL link.

Parameter	Description
Right Port or Role	Set the right port in the ERPS ring and its role. Include 3 roles: **Normal** , **Owner**, and **Neighbour**. ● Normal: The regular node. ● Owner: The RPL (Ring Protection Link) owner node. ● Neighbour: The non-owner node within the RPL link.
Control VLAN	Set the VLAN ID for the ERPS protocol to avoid interference with the service traffic.
WTR Time (min)	Set the duration of the WTR (Wait to Restore Time). A higher value increase stability, a lower value enables faster recovery but might cause oscillations.
Guard Time (ms)	Set the duration of the guard time.
Hold (ms)	Set the duration of the hold off time.
MEL	Set the MEL (Maintenance Entity Level) of the ERPS protocol packets. A higher value indicates lower priority.
Link Restoration	● Select **On** to enable automatic restoration of the blocked RPL link state after fault recovery. ● Select **Off** to require manual restoration of the blocked RPL link state after fault recovery.

Step 5 (Optional) Click **Switch Link** to enable simulated fault switching for manual testing of ERPS functionality and network recovery validation.

Figure 4-14 Switch Link



- Port: Select the port to block.
- Link Status: Include **Block** and **Clear**.
  - **Block** : Simulate link failure to trigger port switching.
  - **Clear** : Simulate link failure recovery.

Step 6 Click **OK**.

4.8.2 Advanced Configuration

4.8.2.1 Managing Advanced Configuration

Procedure

Step 1 Select **Network Settings** > **ERPS**.

Step 2 In the **Config Mode** area, select **Advanced Settings**.

Step 3 (Optional) In the **ERPS** area, click to enable **Ring Network**.

⚠

Disabling **Ring Network** will automatically delete the configured ERPS network, and then it might cause network storms and affect system stability.

Step 4 In the **ERPS** area, click **Add**.

Figure 4-15 Add advanced ERPS

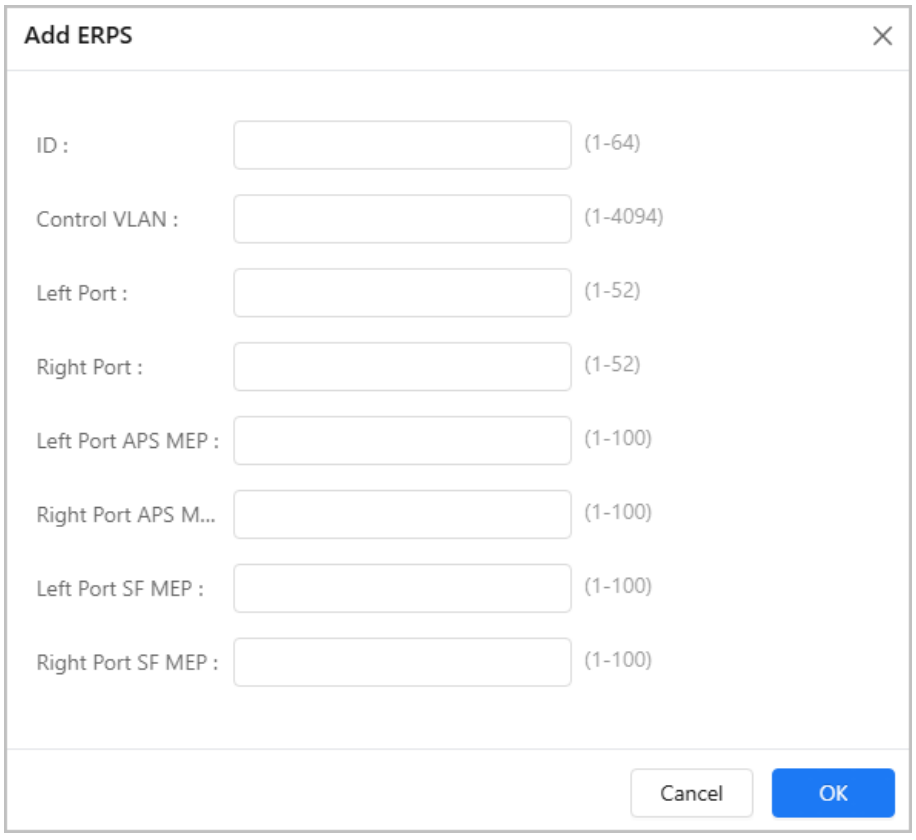


Table 4-6 Description of advanced ERPS

Parameter	Description
ID	The ID number of the ERPS.
Control VLAN	Set the VLAN ID for the ERPS protocol to avoid interference with the service traffic.
Left Port	Set the 2 connected ports for the ERPS ring.

Parameter	Description
Right Port	
Left Port APS MEP	• Port APS MEP (Automatic Protection Switching Maintenance End Point): Set the APS MEP for ERPS port to detect ERPS protocol message interruption. • Port SF MEP (Signal Fail Maintenance End Point): Set the SF MEP for ERPS port to detect signal failure. **Left Port APS MEP** value and **Left Port SF MEP** value must be consistent. **Right Port APS MEP** value and **Right Port SF MEP** value must be consistent. For example, set **Left Port SF MEP** value to 1 and set **Right Port SF MEP** value to 2.
Right Port APS MEP	
Left Port SF MEP	
Right Port SF MEP	

Step 5 Click **OK**.

4.8.2.2 Editing Advanced Configuration

Procedure

Step 1 Select **Network Settings** > **ERPS**.

Step 2 In the **ERPS Instance** area, click  to edit the information of ERPS, and then click **OK**.

(Optional) Click **More Settings** to view more details of the information.

Loopback Detection cannot be enabled at the same time as ERPS or STP. Only one ERPS ring can be configured.

Figure 4-16 Edit advanced ERPS configuration

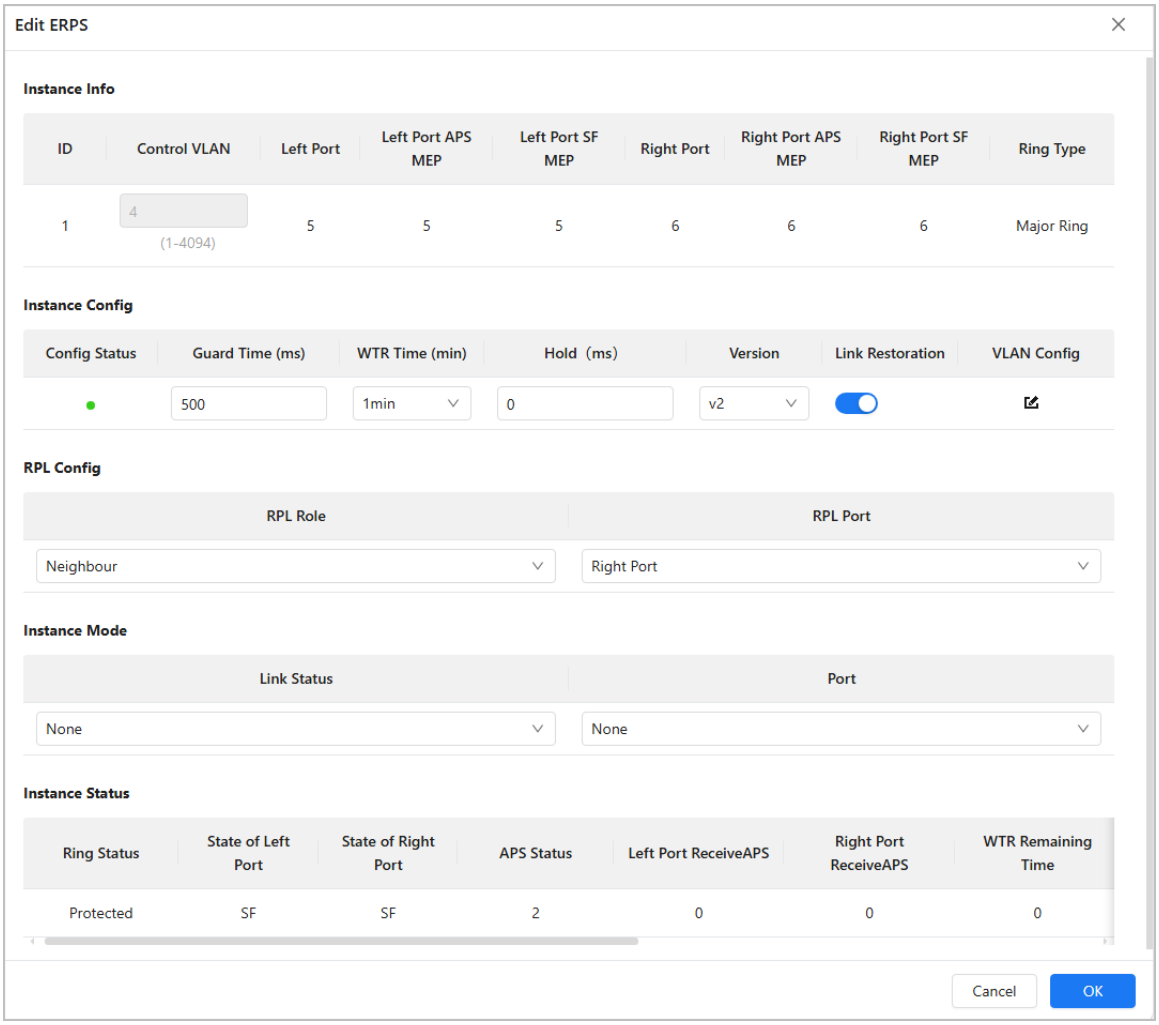
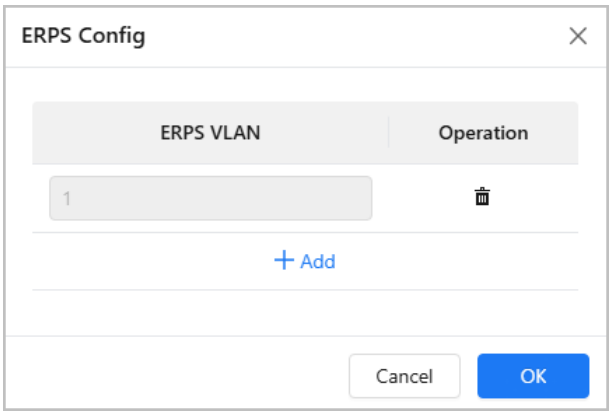


Table 4-7 Description of advanced ERPS configuration

Parameter	Description
Instance Info	Displays the current ERPS instance information. For details, see Table 4-6 .

Parameter	Description
Instance Config	Set the configuration information of ERPS. ● Config Status: The regular node. ● Guard Time (ms), WTR (min), Hold (ms), Link Restoration: Set 4 parameters. For details, see Table 4-5 . ● Version: Set the version of ERPS protocol. ● : Click **Add** to add ERPS VLAN. 
RPL Config	Set **RPL Role** and **RPL Port**. For details, see Table 4-5 .
Instance Mode	Set the EPL link status and corresponding port. ● **Link Status** include 4 types. ◇ **None** : Default status. ◇ **Manually Switch** : Manually switch to the backup port. ◇ **Force Switch** : Switch to the backup port immediately. ◇ **Clear** : Clear the current link status, and then restore to normal status. ● **Port** : Link status switches to the selected port.

Parameter	Description
Instance Status	Displays ERPS instance status and key parameters. ● **Ring Status** includes 4 types. ◇ **Idle** : The normal ring state (with an **Owner** role in the link). ◇ **Pending** : The normal ring state (no **Owner** role in the link). ◇ **Protected** : The ring protection state. ◇ **Forced** : A node in the ring is switched manually or forcibly. ● **State of Left Port** and **State of Right Port**: **SF** (Signal Failure) value indicated signal failure. ● **APS Status** (Automatic Protection Switching) includes 4 types. ◇ **0** : No APS packets have been received. ◇ **1** : An APS packet has been received, but no switch has occurred. ◇ **2** : The switch has occurred or protection is in progress. ◇ **3** : Error. ● **Left Port ReceiveAPS** and **Right Port ReceiveAPS** includes 4 types. ◇ **0** : The left or right port does not receive any APS packet. ◇ **1** : The left or the right port received the APS packet. ● **WTR Remaining Time** includes 2 types. ◇ **0** : The WTR remaining time has elapsed and the main port can be restored. ◇ ≥1: The WTR remaining time has not elapsed and waiting is required. ● **RPL Blocked Status** includes 2 types. ◇ Green dot: RPL link is normally blocked. ◇ Red dot: RPL link is not blocked. ● **No APS Received** includes 2 types. ◇ Green dot: Normal condition (no APS packets have been received). ◇ Red dot: Abnormal condition (no APS packets have been received). ● **Left Port Status** and **Right Port Status** includes 2 types. ◇ Block: The left or right port is blocked. ◇ Unblock: The left or right port is not blocked. ● **FOP Alarm** (Fault OAM Protocol) includes 2 types. ◇ Green dot: No alarm. ◇ Red dot: Alarm active.

Step 3 Click **OK**.

4.8.2.3 Managing MEP Configuration

MEP (Maintenance Entity Group End Point) is a part of the ERPS ring. A node refers to a Layer 2 switching device added to an ERPS ring. A maximum of 2 ports on each node can be added to the same ERPS ring.

Procedure

Step 1 Select **Network Settings** > **ERPS**.

Step 2 In the **Config Mode** area, select **Advanced Settings**.

Step 3 In the **MEP** area, click **Add**.

Figure 4-17 Add MEP

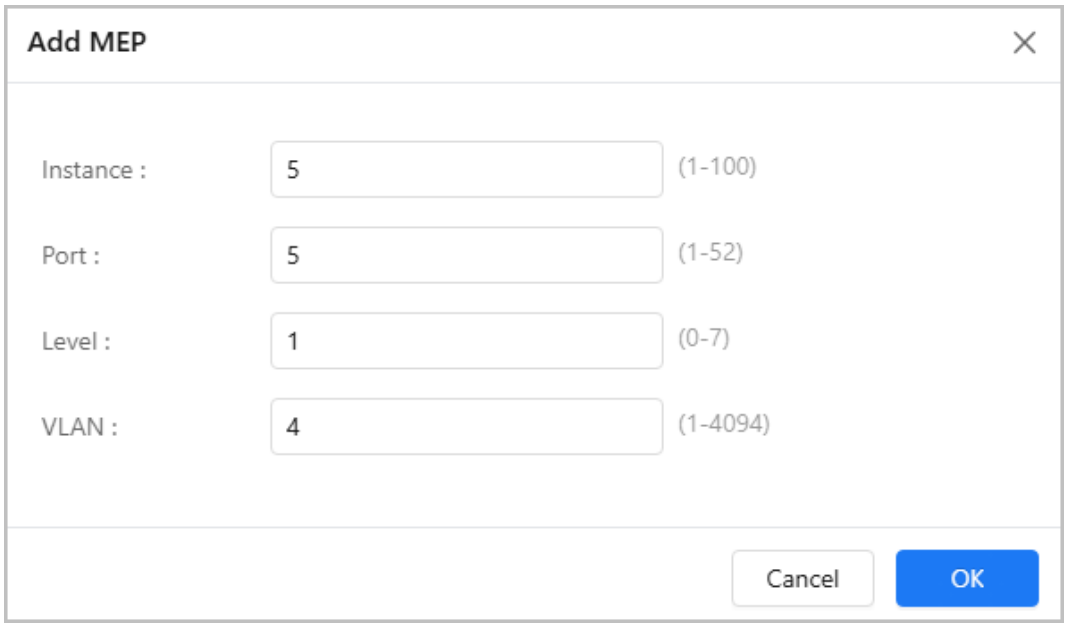


Table 4-8 Description of MEP

Parameter	Description
Instance	The number of the MEP instance.
Port	The port number of MEP.
Level	Maintenance level. We recommend setting as 0.
VLAN	The protocol VLAN number. For example, VLAN 3.

Step 4 Click **OK**.

4.8.2.4 Editing MEP Configuration

Procedure

Step 1 Select **Network Settings** > **ERPS**.

Step 2 In the **Config Mode** area, select **Advanced Settings**.

Step 3 In the **ERPS** area, click  to edit the information of the MEP.

Figure 4-18 Edit MEP

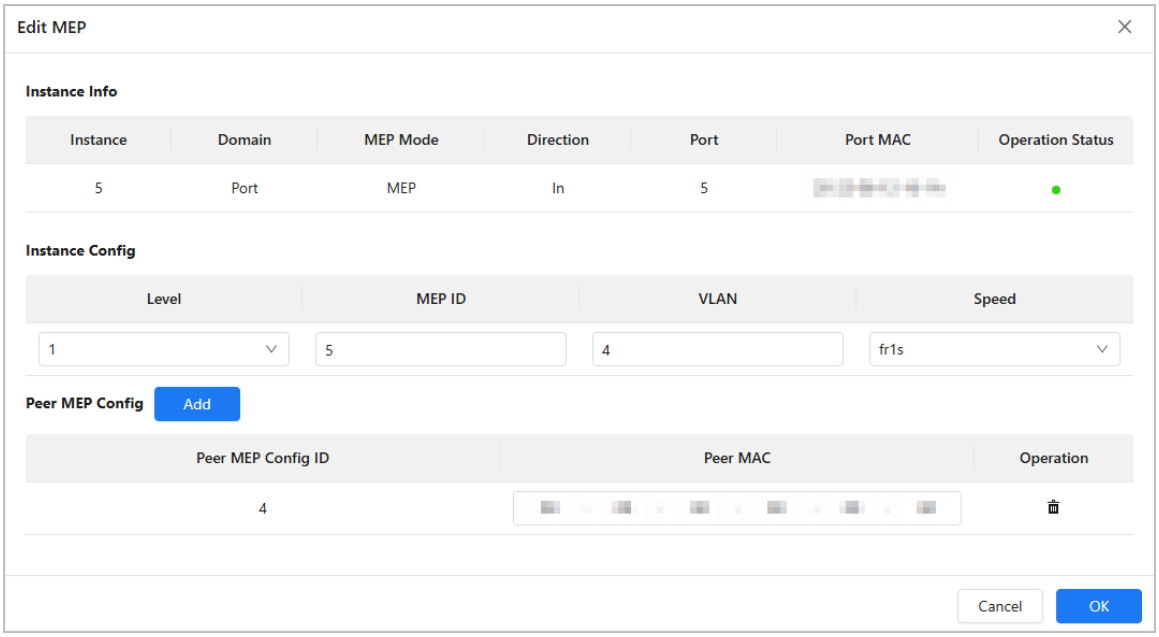
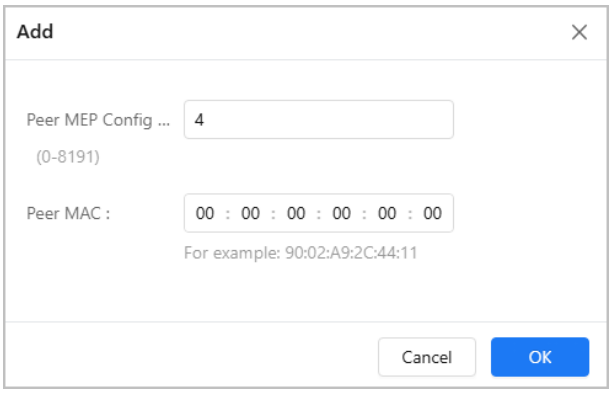


Table 4-9 Description of MEP configuration

Parameter	Description
Instance Info	Displays the information of the current MEP instance. ● **Instance** : The ID of this MEP instance. ● **Domain** (Domain type): The domain type which this MEP belongs. **Port** indicates port-based. ● **MEP Mode** : The mode type of this MEP instance. ● **Direction** : The direction of this MEP instance. **In** indicates entering the device from external. ● **Port** : The port number of this MEP instance. ● **Port MAC** : The MAC address of this port. ● **Operation Status** includes 2 types. ◇ Green dot: Normal condition. ◇ Red dot: Abnormal condition (MEP is inactive or faulty).
Instance Config	Set the configuration information of MEP. ● **Level** : Set the level of this MEP instance. A smaller value indicates a higher priority. ● **MEP ID** : Set the ID number of this MEP instance. ● **VLAN** : Set the VLAN number of this MEP instance. ● **Speed** : Set the recovery time of this MEP instance. Includes **fr1s** and **fr10s**.

Parameter	Description
Peer MEP Config	Set the configuration information of peer MEP. You can only add 1 Peer MEP. Click **Add** to add the configuration information of peer MEP. • **Peer MEP Config ID** : Set the peer MEP ID to bidirectional communication. • **Peer MAC** : Set the MAC of peer MEP to identifying the peer device. 

Step 4 Click **OK**.

4.9 Configuring IGMP Snooping

IGMP Snooping (Internet Group Management Protocol Snooping) is the multicast constraint mechanism running on the device of layer 2, for managing and controlling the multicast. Through analyzing the received IGMP packet, the device of layer 2, which runs IGMP Snooping, creates the mapping between the port and the MAC multicast address, and forwards the multicast data according to the mapping.

Procedure

Step 1 Select **Network Settings** > **IGMP Snooping**.

Step 2 Click next to **IGMP Snooping** to enable the function.

Step 3 Click next to **IGMP Leave Group Messages** to enable the function.

- Enable the function: Once the function is enabled, if the switch receives group messages that are not registered, it leaves the messages. The bandwidth will be saved, and then the forwarding rate will be increased.
- Disable the function: If the group messages are not registered, the messages will be broadcast in the VLAN. The bandwidth will be occupied, and then the forwarding rate will be decreased.

Please be advised on enabling **IGMP Leave Group Messages**, otherwise the multicast might fail.

Step 4 Click **OK**.

4.10 Configuring STP

Spanning Tree Protocol (STP) builds a loop-free logical topology for LANs. It blocks redundant links between any 2 network devices and leaves a single active link between them so as to eliminate loops.

STP and RSTP provide the following capabilities:

- STP: A management protocol at the data link layer, is used to detect and prevent loops on a Layer 2 network. It, however, converges the network topology slowly.
- RSTP: An enhancement to STP, allows for rapid network topology convergence. However, both RSTP and STP have a defect that all the VLANs on the same LAN share the same spanning tree.

4.10.1 STP

Background Information

When spanning tree is enabled, iLinkView cannot be used.

Procedure

Step 1 Select **Network Settings** > **STP**.

Step 2 Click next to **STP** to enable STP function.

Step 3 Select a working mode.

Step 4 Click **Advanced**, and then configure the advanced parameters.

Figure 4-19 Configure STP

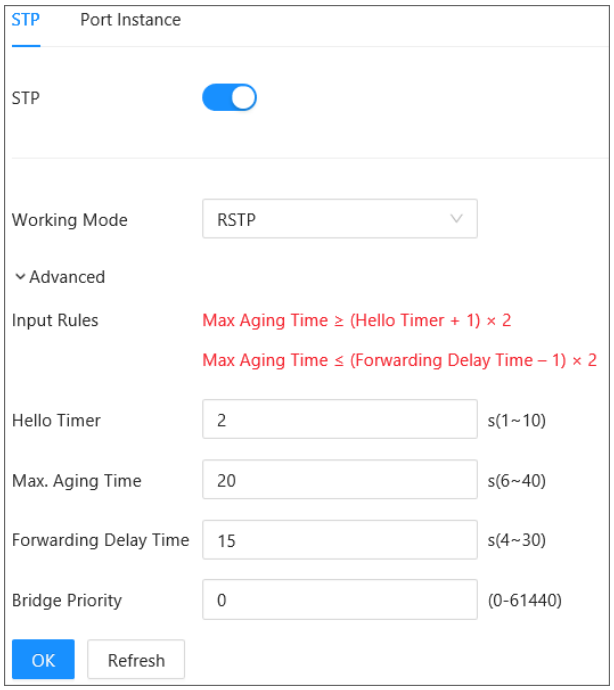


Table 4-10 Description of the advanced parameters

Parameter	Description
STP	The basic spanning tree protocol.

Parameter	Description
RSTP	An enhancement to STP, allows for rapid network topology convergence.
Hello Timer	The period of root bridge sending BPDU. The time ranges from 1 second to 10 seconds.
Max. Aging Time	The aging time of current BPDU. The time ranges from 6 seconds to 40 seconds.
Forwarding Delay Time	After setting topological change, the bridge maintains the time of snooping and study state. The time ranges from 4 seconds to 30 seconds.
Bridge Priority	The value ranges from 0 to 61440.

4.10.2 Port Instance

Procedure

Step 1 Select **Network Settings** > **STP** > **Port Instance**.

Step 2 Enter **Priority** and **Root Path Cost** of each port.

- The value of **Priority** ranges from 0 to 240, and must be an integral multiple of 16.
- The value of **Priority** is 128 by default.

Figure 4-20 Port instance

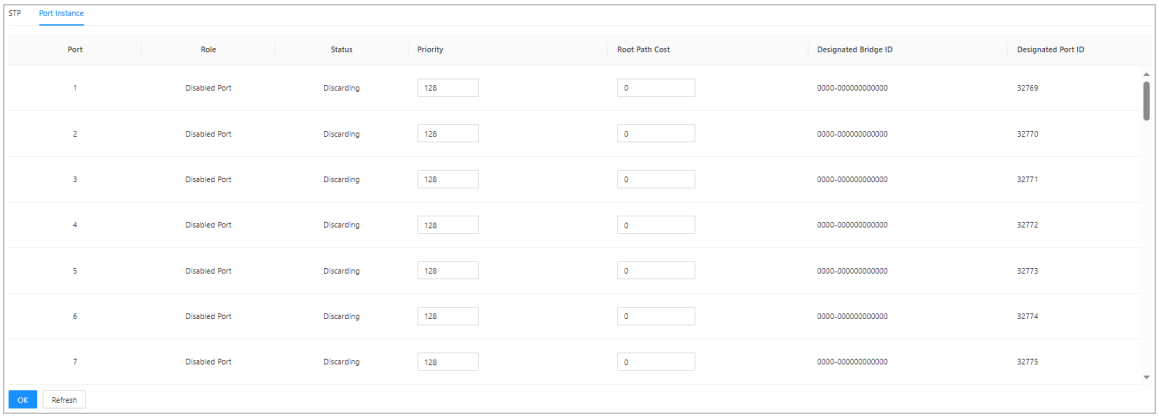


Table 4-11 Description of the port instance

Parameter	Description
Role	The basic STP.
Status	An enhancement to STP, allows for rapid network topology convergence.
Priority	The priority of the port.
Root Path Cost	The root path cost of the port.
Designated Bridge ID	The designated bridge ID of the port.
Designated Port ID	The designated port ID of the port.

4.11 Configuring Link Aggregation

Link aggregation is to form multiple physical ports of the device into the logical port. The multiple links in the same group can be regarded as a logical link with a larger bandwidth. Through aggregation, the ports in the same group can share the communication flow, to make a larger bandwidth. Besides, the ports in the same group can back up reciprocally and dynamically to enhance the link reliability.

Background Information

Link aggregation includes 2 types: Static aggregation and dynamic aggregation.

- **Static aggregation mode**: Manually adding multiple member ports to an aggregation group. All ports remain in the forwarding state and share the traffic load.
- **Dynamic aggregation mode**: The aggregation devices exchange aggregation information through LACPDU (Link Aggregation Control Protocol Data Unit) packets. Matching links are aggregated to transmit and receive data. The addition and removal of ports within the aggregation group are automatically handled by the protocol, providing high flexibility and load-balancing capabilities.

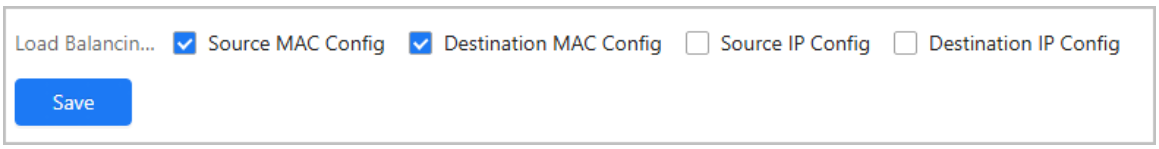
Procedure

Step 1 Select **Network Settings** > **Link Aggregation**.

Step 2 In the **Load Balancing** box, select the type and click **Save**.

- **Source MAC Config** : Indicates the load balancing algorithm based on source MAC address.
- **Destination MAC Config** : Indicates the load balancing algorithm based on destination MAC address.
- **Source IP Config** : Indicates the load balancing algorithm based on source IP address.
- **Destination IP Config** : Indicates the load balancing algorithm based on destination IP address.

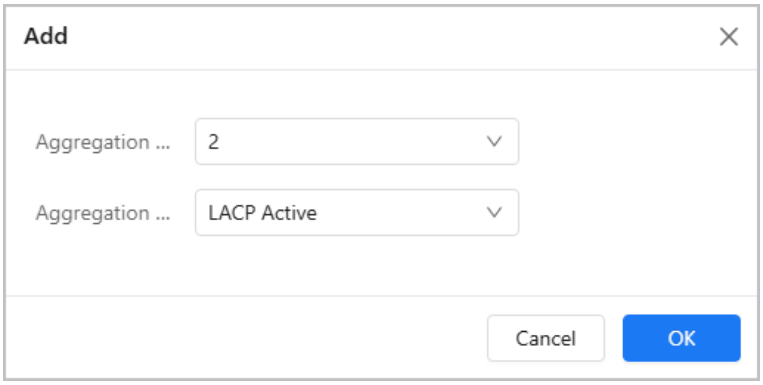
Figure 4-21 Link mode



Step 3 Click **Add** , configure parameters, and then click **OK**.

- **Aggregation Group No.** : The ID used to distinguish different link aggregation groups.
- **Aggregation Group Mode** include 3 modes.
  - **Static** : Manually configure link aggregation without using any protocol for automatic negotiation and management of the aggregation group.
  - **LACP Active** : Actively sends LACP packets to initiate aggregation negotiation.
  - **LACP Passive** : Dose not actively send LACP packets but only receives and responds to LACP packets from the peer device.

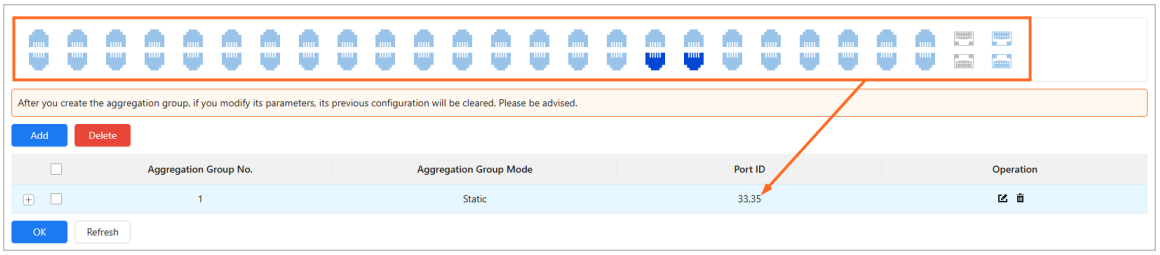
Figure 4-22 Add link aggregation



Step 4 Select ports to be added to the aggregation group.

Only ports with identical speed, duplex, long-distance, and VLAN configurations can join the same aggregation group.

Figure 4-23 Select ports



Step 5 Click **OK**.

4.12 Configuring SNMP Protocol

SNMP (Simple Network Management Protocol) is the standard protocol for network management in Internet, and it is widely applied for accessing and managing the managed devices. SNMP has the following features:

- It supports intelligent management for network device. By using the network management platform based on SNMP, the network administrator can query the running status and the parameters of the network device, and can configure the parameter, find the error, perform fault diagnosis, and then plan the capacity and create the report.
- SNMP supports to manage the devices of different physical features. SNMP provides only the most basic function library. It makes the management task and the physical feature and the networking technology of the managed device independent, to manage the devices from different manufacturers.

SNMP network provides 2 elements, NMS and Agent.

- NMS (Network Management System) is the manager in SNMP network, and it provides friendly human-machine interface to help the network administrator to finish most of the network management work.
- Agent is the managed role in SNMP network, and it receives and handles the request packet from NMS. In some emergency circumstances, for example, if the port status changes, Agent can send alarm packet to NMS proactively.

4.12.1 Configuring SNMP V1 and V2

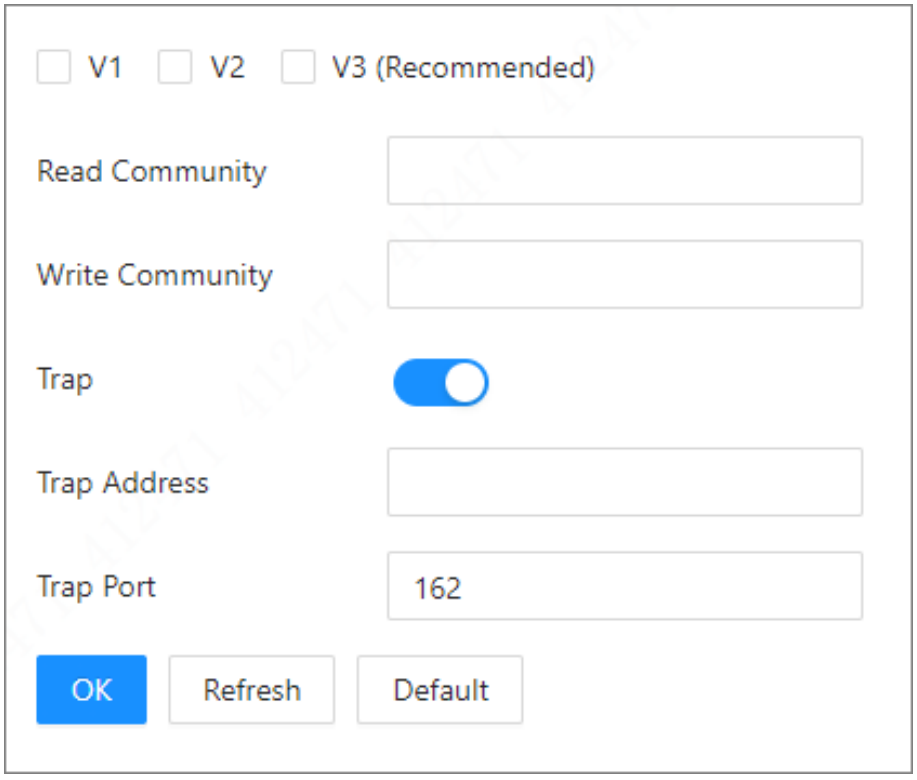
Procedure

Step 1 Select **Network Settings** > **SNMP**.

Step 2 Select **V1** or **V2** version.

Step 3 Configure parameters, including **Read Community** , **Write Community**, **Trap Address**, and **Trap Port**.

Figure 4-24 SNMP



Step 4 Click **OK**.

4.12.2 Configuring SNMP V3

Procedure

Step 1 Select **Network Settings** > **SNMP**.

Step 2 Select **V3**.

Step 3 Configure parameters.

Figure 4-25 SNMP V3

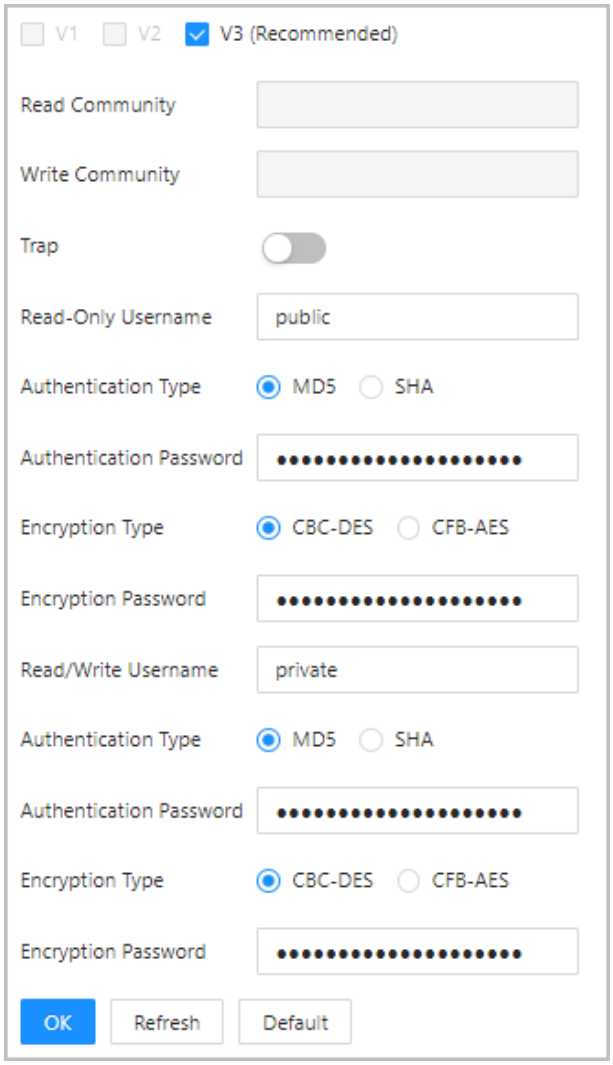


Table 4-12 Description of SNMP parameters

Parameter	Description
Read Community	Read community supported by the agent programs.
Write Community	Write community supported by the agent programs.
Trap Address	The destination address of trap information sent by the agent program.
Trap Port	The destination port of trap information sent by the agent program.
Read-only Username	Set the read-only username. It is for V3 only.
Authentication Type	Set authentication mode when the security level is **Authentication no encryption** or **Authentication and encryption**. The authentication mode includes **MD5** and **SHA**.
Authentication Password	Set authentication password.
Encryption Type	Set encryption mode when the authentication mode is **Authentication and encryption**.

Parameter	Description
Encryption Password	Set the encryption password when the authentication mode is **Authentication and encryption**.
Read/Write Username	Set read and write user.

Step 4 Click **OK**.

4.13 Configuring MAC Table

MAC (Media Access Control) Table records the relationship between the MAC address and the port, and the information including the VLAN that the port belongs to. When the device is forwarding the packet, it queries in the MAC address table for the destination MAC address of the packet. If the destination MAC address of the packet is contained in the MAC address table, the packet is forwarded through the port in the table directly. And if the destination MAC address of the packet is not contained in the MAC address table, the device adopts broadcasting to forward the packet to all the ports except the receiving port in VLAN.

4.13.1 Adding MAC Table

You can bind the MAC address to the port on certain VLAN.

Procedure

Step 1 Select **Network Settings** > **MAC Table**.

Step 2 On the **MAC Table** tab, click **Add**.

Step 3 Set the MAC address, VLAN, and Port.

For example, bind the MAC address 00:00:00:00:00:01 to the port 3 in VLAN 2.

Step 4 Click **OK**.

Figure 4-26 Add MAC table

Related Operations

- Clear dynamic MAC address: Click **Clear Dynamic MAC**.
- Search for MAC address and port: Enter the MAC address or port number on the upper-right corner, and then click **Search**.

4.13.2 Filtering Port MAC

Background Information

After enabling port MAC filtering, the following MAC devices can communicate with the port.

- Devices in the MAC allowlist.

- The static MAC devices changing from the dynamic MAC devices.

After enabling port MAC filtering, the port cannot access the managing address or login.

Procedure

Step 1 Select **Network Settings** > **MAC Table**.

Step 2 On the **MAC Filtering** tab, select the port, and then click to enable the filtering function.

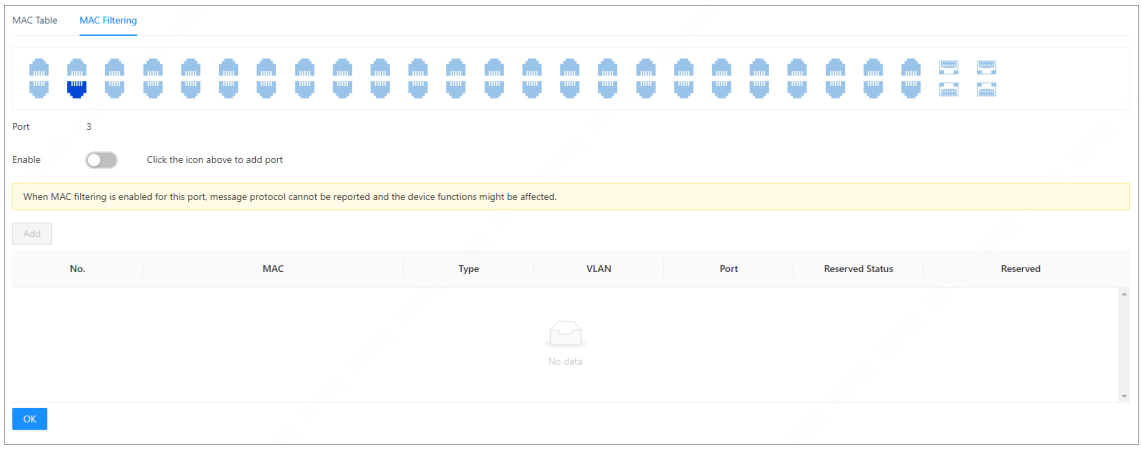
Step 3 Configure the MAC filtering of the port.

- Change from dynamic to static.
  1. Select one record, and then select next to **Reserved**.
  2. Click **OK**.

     The type changes from **Dynamic** to **Static**.

     Static MAC devices can communicate with the port normally.
- Create MAC allowlist.
  1. Click **Add**.
  2. Set MAC address and VLAN.
  3. Click **OK**.

Figure 4-27 MAC filtering



4.14 Configuring LLDP

LLDP (Link Layer Discovery Protocol) is a standard link layer discovery way. It can form its main capabilities, management address, device number and port number as TLV (Type Length Value), encapsulate it in LLDPDU (Link Layer Discovery Protocol Data Unit), and release it to its neighbor. The neighbor will keep the received information in the form of standard MIB (Management Information Base), so that the network management can query and judge the communication state of the link.

Procedure

Step 1 Select **Network Settings** > **LLDP**.

Step 2 On the **LLDP Remote Device** tab, view the information of LLDP remote device.

Figure 4-28 LLDP remote device

4.15 Configuring Loopback Detection

This function can detect the loop between ports. If a loop is detected, the loop will be disconnected.

Procedure

Step 1 Select **Network Settings** > **Loopback Detection**.

Step 2 Click to enable loopback detection.

Loopback Detection cannot be enabled at the same time as ERPS or STP.

Step 3 Click **OK**.

4.16 Configuring DHCP

Enable the DHCP function of the device and use it as a DHCP server. The DHCP server supports allocating IP addresses to devices within the network and ensures that each device is assigned a different IP address, greatly simplifying the way of network configuration management.

DHCP servers are typically used in the following situations.

- Large-scale networks: When the network scale is large, manually configuring the IP addresses involves a huge workload and is difficult to manage centrally. In such cases, using DHCP can simplify management work.
- Insufficient IP addresses: When the number of hosts in the network exceeds the available IP addresses and it is impossible to assign fixed IP addresses to each host, DHCP can dynamically allocate the IP addresses. For example, Internet service providers might limit the number of users who can access the network simultaneously, and users need to obtain the IP addresses dynamically to achieve connection.
- A small number of fixed IP requirements: In a network, only a few hosts require fixed IP addresses, while the majority do not. In such cases, DHCP can effectively meet these requirements and reduce management complexity by dynamically allocating IP addresses.

4.16.1 Configuring DHCP Server

Procedure

Step 1 Select **Network Settings** > **DHCP Server** > **DHCP Server**.

Step 2 Click next to **DHCP Server**.

Step 3 Create a new address pool.

1. In the **Address Pool List** area, click **Add**.
2. Set the parameters.

Figure 4-29 Add address pool

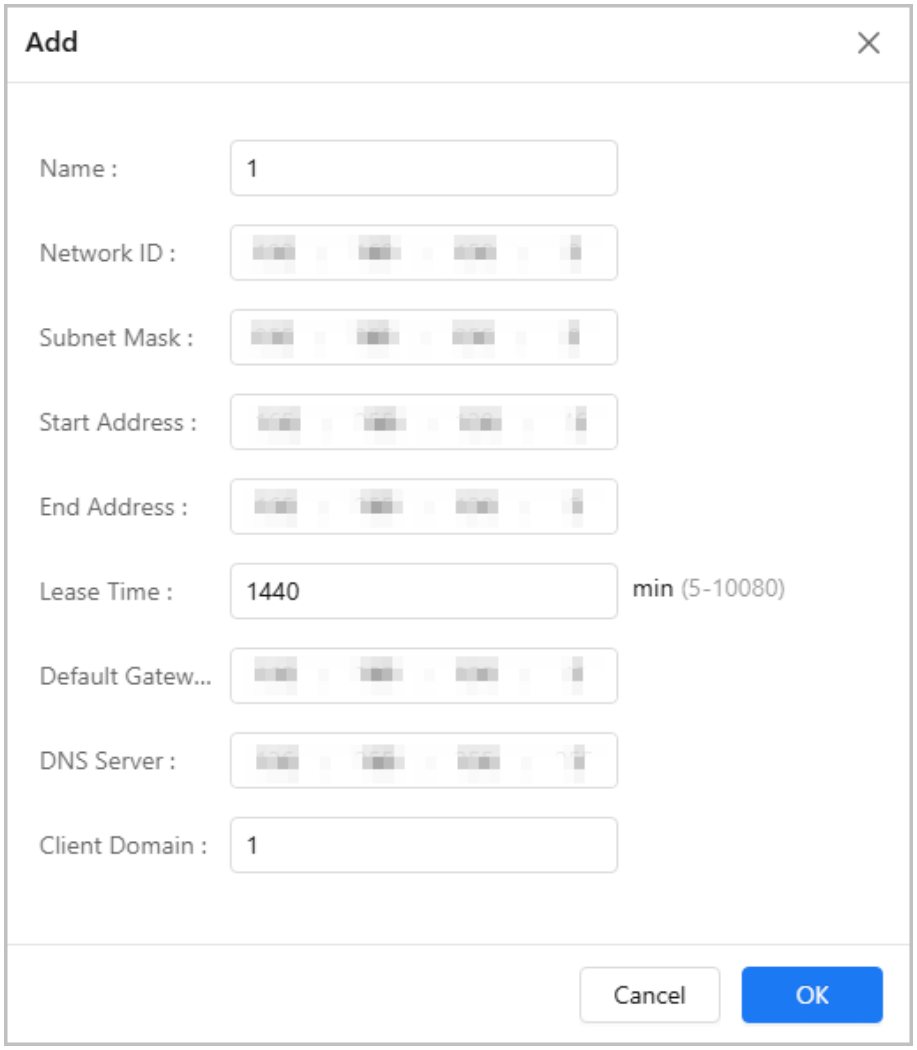


Table 4-13 Description of address pool parameters

Parameter	Description
Name	Set the name of the DHCP address pool. For example, pool1.
Network ID	Set the IP address that can be assigned to hosts or networks.
Subnet Mask	Set the subnet mask for hosts or networks.
Start Address	Set the starting address of the IP address range that can be assigned to devices in the address pool. The start address must be within the defined network range and less than or equal to the end address.
End Address	Set the ending address of the IP address range that can be assigned to devices in the address pool. The ending address must be within the defined network range and greater than the starting address.
Lease Time	Set the usage period of the IP address assigned by the DHCP server to the client. After the lease period expires, the client must request renewal from the DHCP server or obtain a new IP address.

Parameter	Description
Default Gateway	Set the default gateway address (usually the IP address of the router) for network access. This address must be within the subnet range.
DNS Server	Set the IP address of the DNS server for domain name resolution on the client device.
Client Domain	Set the DNS domain name for the client device to identify its logical domain.

3. Click **OK**.

Step 4 Configure reserved IP segments.

Reserved IPs are designated for servers only and will not be assigned to clients.

1. In the **Reserved IP** area, click **Add**.
2. Enter the IP address range. For example, **192.168.100.2** - **192.168.100.50**.
3. Click **OK**.

4.16.2 Configuring Static Binding

Procedure

Step 1 Select **Network Settings** > **DHCP Server** > **Static Binding**.

Step 2 Click **Add** to add a static IP binding.

Figure 4-30 Add a static IP binding

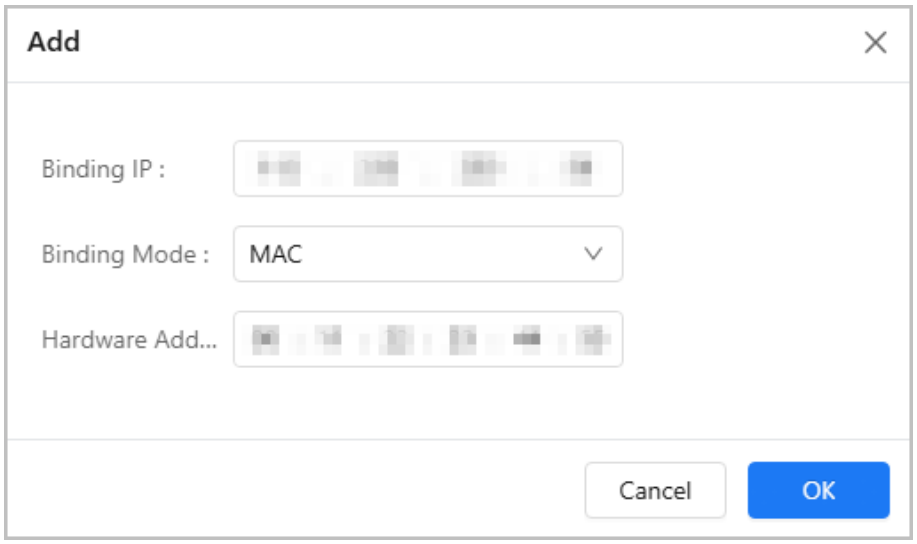


Table 4-14 Description of static IP binding parameter

Parameter	Description
Binding IP	Set the binding IP address to the client device. This address must be within the network range of the current DHCP address pool.

Parameter	Description
Binding Mode	Includes **MAC** and **Name_ASCII**.
Hardware Address/ Client ID	• **MAC** : Use the physical MAC address of the hardware device as the client device identifier for address binding. 1. In the **Binding IP** list, select **MAC**. 2. In the **Hardware address** box, enter the physical MAC address. • **Name_ASCII** : Use the client ID of the virtualized environment as the client device identifier for address binding. 1. In the **Binding IP** list, select **Name_ASCII**. 2. In the **Client ID** box, enter the client ID of the virtualized environment.

Step 3 Click **OK**.

4.16.3 Viewing List of Bound Addresses

Select **Network Settings** > **DHCP Server** > **List of Bound Addresses** to view the configured dynamic IP address and static IP address in **DHCP Server** and **Static Binding** tabs, including the client ID, MAC address, IP type, and the remaining time of the address pool lease.

4.17 DHCP Snooping

4.17.1 Global Configuration

Procedure

Step 1 Select **Network Settings** > **DHCP Snooping** > **Global Config**.

Step 2 Set the parameters of **Global Config**.

Figure 4-31 Global configuration

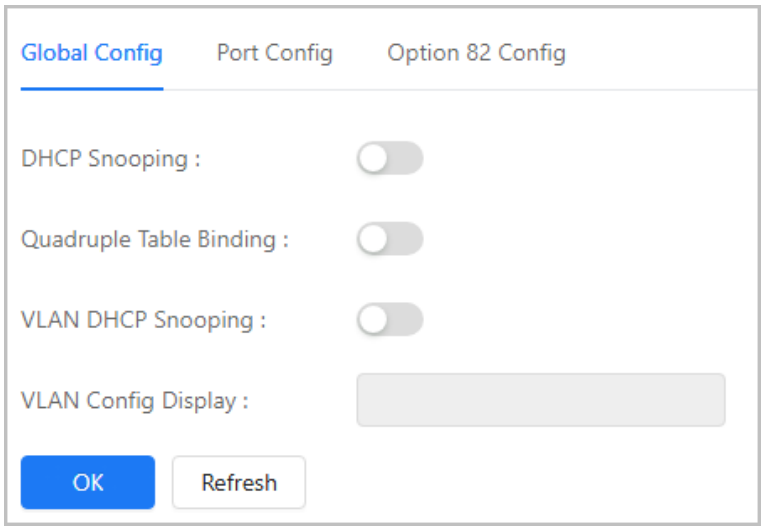


Table 4-15 Description of global configuration parameters

Parameter	Description
DHCP Snooping	Click next to **DHCP Snooping** to enable monitoring and filtering of DHCP packets on all ports to identify legitimate DHCP servers. To enable global DHCP Snooping, VLAN DHCP Snooping must be disabled.
Quadruple Table Binding	Click next to **Quadruple Table Binding** to enable the recording of the DHCP client IP address, MAC address, port and VLAN information for security protection.
VLAN DHCP Snooping	• **VLAN DHCP Snooping** : Use to enable DHCP Snooping for a specific VLAN on the device, providing targeted protection for that VLAN. • **VLAN ID** : Enter the specific VLAN number for where DHCP Snooping will be enabled. To enable VLAN DHCP Snooping, global DHCP Snooping must be disabled.
VLAN Configuration Display	Displays the VLAN number which DHCP Snooping has been enabled.

Step 3 Click **OK**.

4.17.2 Port Configuration

Procedure

Step 1 Select **Network Settings** > **DHCP Snooping** > **Port Config**.

Step 2 Set the parameters of **Port Config**.

Port Config : Used to perform granular configuration for each port, enabling more secure and flexible DHCP protection.

Figure 4-32 Port configuration

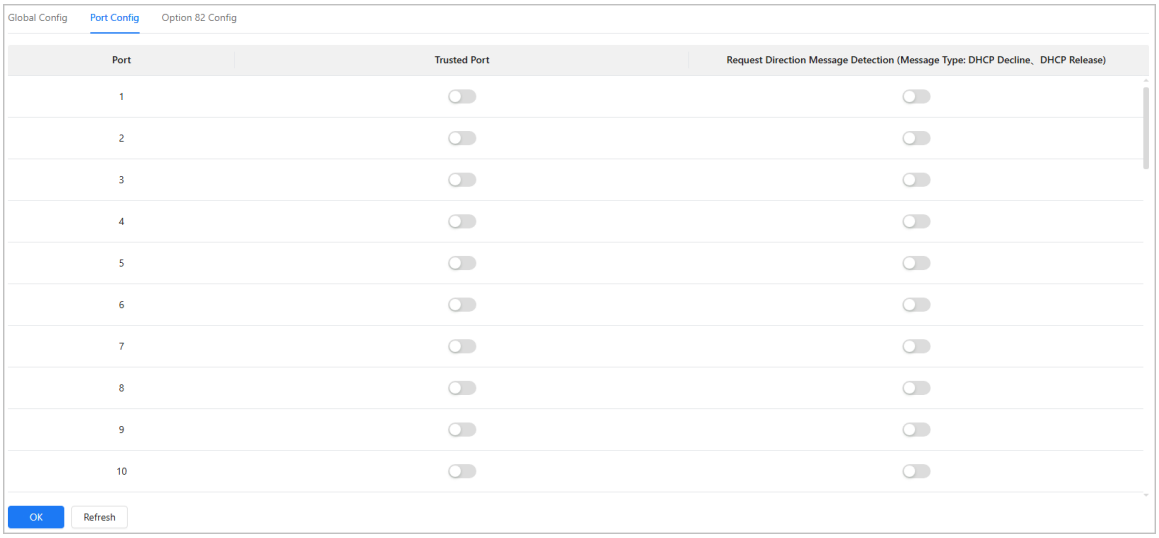


Table 4-16 Description of port configuration parameters

Parameter	Description
Port	Displays all ports of the device.
Trusted Port	Set this parameter to ensure DHCP clients can only obtain IP addresses from authorized DHCP servers, preventing forged server attacks. ● Trust: Click to enable trusted port mode, allowing normal reception of DHCP Offer, DHCP Ack, and DHCP Nak packets from DHCP servers. ● Untrust: Click to disable trusted port mode, causing all DHCP packets from servers to be discarded.
Request Direction Message Detection (Message Type: DHCP Decline, DHCP Release)	Set this parameter to enable detection, which monitors whether this port sends unauthorized DHCP requests. ● Click to enable detection. When the device receives a DHCP Decline or DHCP Release packet, it checks whether a matching entry exists locally. ◇ If the entry exists and the packet details match, it is valid packet and will be forwarded to the DHCP server. ◇ If the entry does not exists, it is a valid packet and will be forwarded to the DHCP server. ◇ If the entry exists but the packet details do not match, it is forged packet and will be discarded. ● Click to turn off detection.

Step 3 Click **OK**.

4.17.3 Option 82 Configuration

Procedure

Step 1 Select **Network Settings** > **DHCP Snooping** > **Option 82 Config**.

Step 2 Set the parameters of **Option 82 Config**.

Option 82 (DHCP Relay Agent Information Option) is an optional parameter in the DHCP protocol and is used to carry relay agent information in DHCP requests.

Figure 4-33 Option 82 configuration

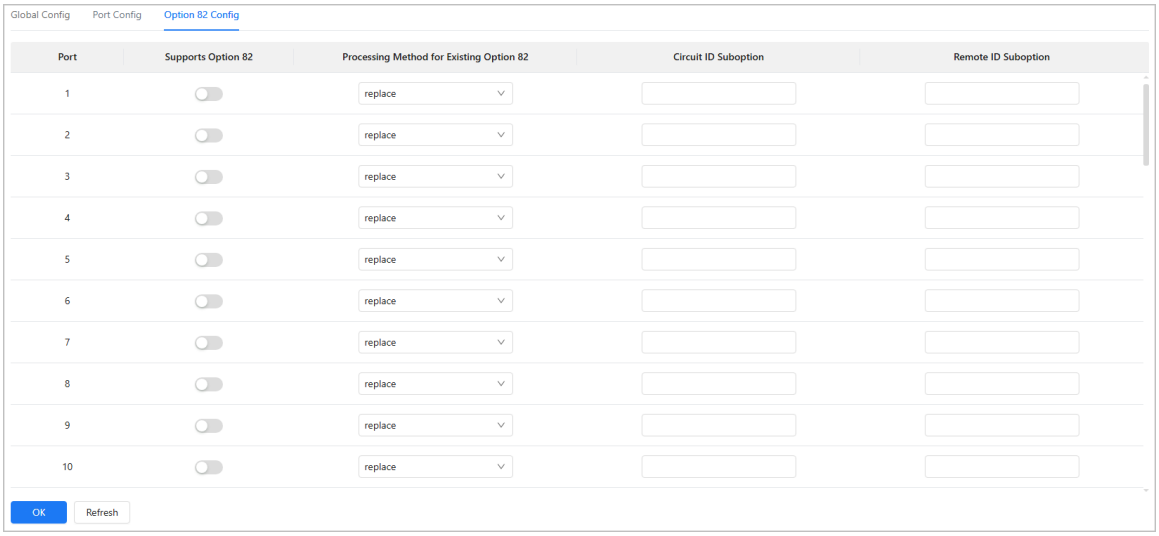


Table 4-17 Description of Option 82 configuration parameters

Parameter	Description
Port	Displays all ports of the device.
Supports Option 82 Port	Click to enable this function to the specific port, the device will add Option 82 information to the forwarded DHCP requests.
Processing Method for Existing Option 82	Configure how the device handles DHCP request with Option 82 information when received on a particular port. When the received packet does not contain Option 82 information, the device will insert Option 82 according to the preconfigured DHCP Snooping settings (including filling mode, content, and format), add it to the packet, and then forward it. • **replace** : Insert Option 82 according to the preconfigured DHCP Snooping settings (including filling mode, content, and format), replacing any existing Option 82 information, and then forward the packet. • **keep/append** : Preserve the existing Option 82 information in the packet, and then forward the packet. • **drop** : Discard the packet.
Circuit ID Suboption	Fill in the specific information to identify the physical location of the client access.

Parameter	Description
Remote ID Suboption	Fill in the specific information to identify the physical location of the relay agent itself.

Step 3 Click **OK**.

4.18 Virtual Cable Test

Procedure

Step 1 Select **Network Settings** > **Virtual Cable Test**.

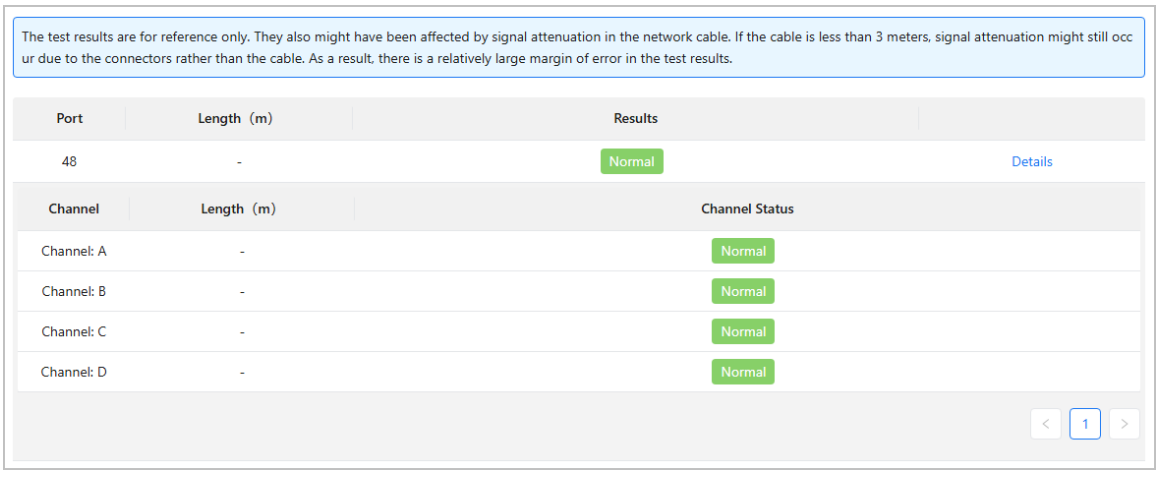
Step 2 Click **Check** of the corresponding port to detect and view the specific test results.

Step 3 (Optional) Click **Details** to view the link status of the 4 wire pairs.

Displays the port detection results through color coding and text labels.

- **Port** : Displays the port number.
- **Length (m)** : Base on the **Bucket Theory** (where the shortest channel determines the overall length), it displays the minimum valid channel length among the 4 channels.
- **Results** : The detection results include 5 statuses.
  - ◇ **Normal** : All 4 channels are properly connected.
  - ◇ **Open Circuited Channel** : At least one channel has an open circuit (broken connection).
  - ◇ **Short Circuited Channel** : At least one channel has a short circuit fault.
  - ◇ **Abnormal** : Multiple channels exhibit mixed fault. For example, partial open or short circuits.
  - ◇ **Test Failed** : Indicating the port link status is **down** or other issues caused detection failure.

Figure 4-34 Virtual cable test



5 PoE Management

PoE refers to that the device uses network cables to externally connect PD (Powered Device) for remote power supply through Ethernet electrical ports. PoE function enables centralized power supply and convenient backup. Network terminals do not need external power supply, but only one network cable. Complied with IEEE 802.3af, IEEE 802.3at and IEEE 802.3bt standards, the device uses a globally unified power port. It can be used in IP phones, wireless AP (Access Point), portable power charger, credit card machine, network camera, data collection.

- Non-PoE devices do not support this function.
- Only some models of PoE devices comply with IEEE 802.3at standard. Single BT port supports up to 90 W. Please refer to the actual products.

5.1 Configuring PoE Settings

Procedure

Step 1 Select **PoE Management** > **PoE Settings**.

Step 2 In **Power Settings** area, you can view the total power and configure the available power.

Step 3 In **Power Status** area, you can view the consumed power and remaining power.

Step 4 In **Port Status and Control** area, select from the list below the **PoE Management** to enable or disable PoE of the corresponding port.

Figure 5-1 PoE settings

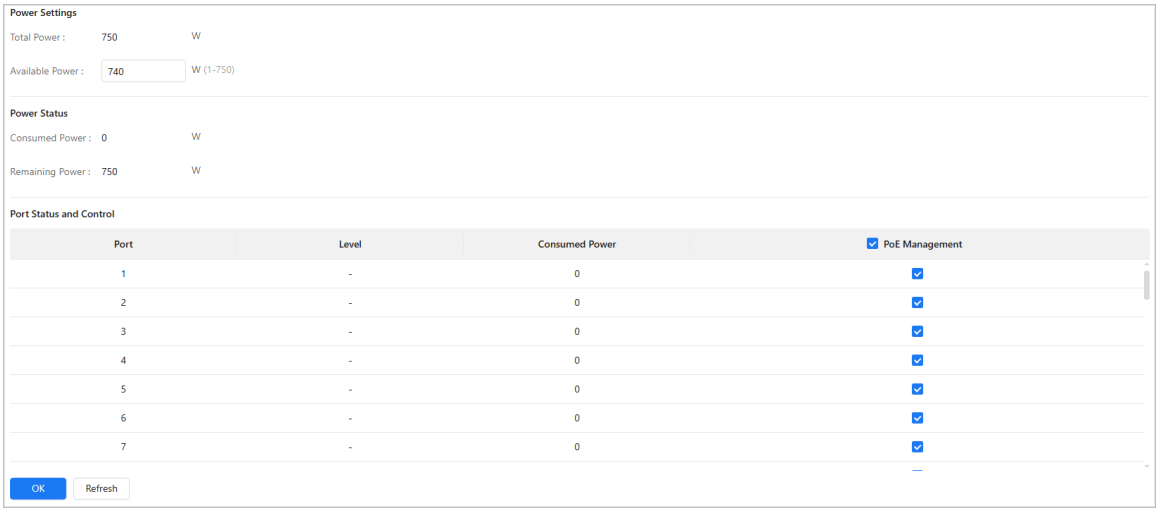


Table 5-1 Description of PoE parameters

Parameter		Description
Power Settings	Total Power	Displays the total PoE power.
	Available Power	Configure the available PoE power.
Power Status	Consumed Power	Displays the current PoE power consumed by all ports.
	Remaining Power	Displays the current remaining PoE power.
Port Status and Control	Level	Displays the power supply level of the terminal devices. The power supply level ranges from 0 through 8, and the Hi-PoE power supply standard level is displayed as 5+.

Parameter		Description
	Consumed Power	Displays the current PoE power consumed by the corresponding single port.
	PoE Management	Enable or disable the PoE power supply function of the port. By default, PoE is disabled on a PoE port. PSE power overload: When the total amount of the power consumption of all ports exceeds the maximum power of PSE, the system considers the PSE is overloaded.

Step 5 Click **OK**.

5.2 Configuring Perpetual PoE

Enable perpetual PoE, which continues to supply power to the powered devices even when the device reboots.

Procedure

Step 1 Select **PoE Management** > **Perpetual PoE**.

Step 2 Click to enable **Global Config**.

Step 3 Click **OK**.

5.3 Configuring Long Distance PoE

After you enable long distance PoE, the maximum transmission distance will change from 100 m to 250 m, and the transmission speed will be reduced from 1 Gbps to 10 Mbps.

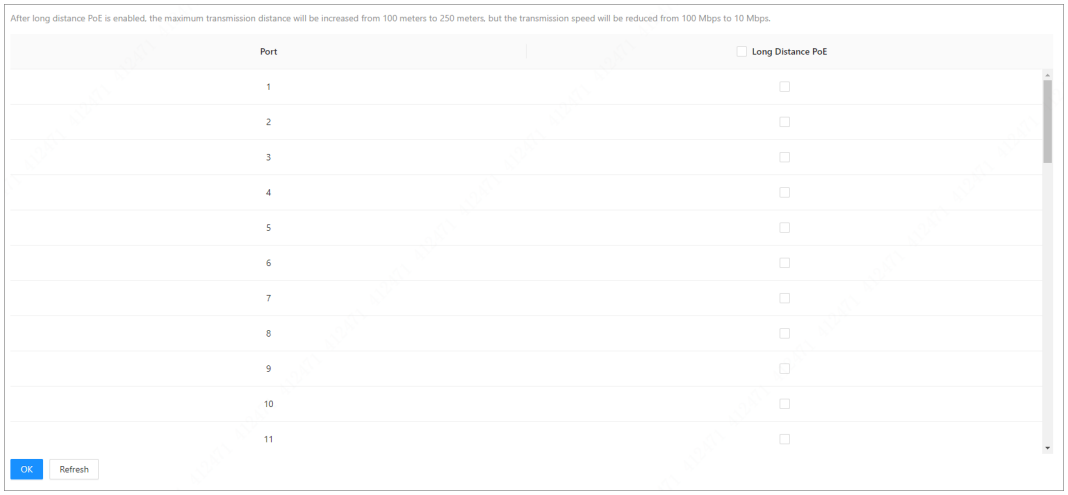
Procedure

Step 1 Select **PoE Management** > **Long Distance PoE**.

Step 2 Click of the corresponding port to enable long distance PoE.

Step 3 Click **OK**.

Figure 5-2 Long distance PoE



5.4 Viewing PoE Event Statistics

Select **PoE Management** > **PoE Event Statistics** to view PoE event statistics.

Table 5-2 Description of PoE event statistics

Parameter	Description
Overload	Single port boots up when the power current has exceeded the current threshold.
Short Circuited	When the powering chip sends power to the port, it becomes short-circuit.
DC Disconnection	Single port power is off.
Short Circuit During startup	The power is short-circuit when the powering chip sends out power.
Overheat Protection	Single port boots up when the temperature of powering chip has exceeded the threshold.

5.5 Configuring Green PoE

Green PoE can reduce power consumption while retaining full compatibility with existing equipment.

Procedure

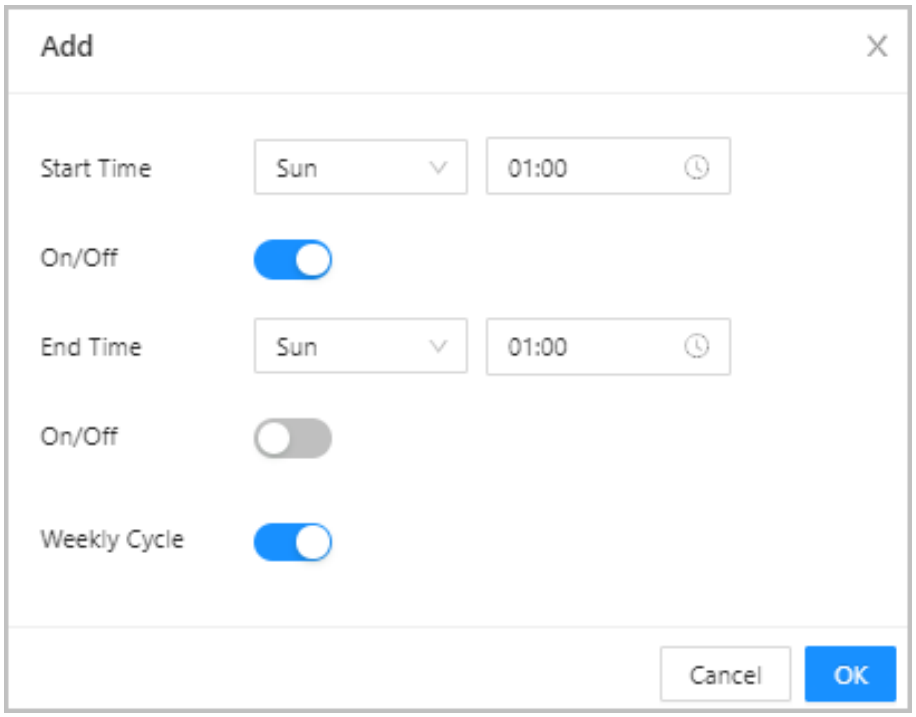
Step 1 Select **PoE Management** > **Green PoE**.

Step 2 Click **Add Energy Saving Plan** or to add and edit the energy saving plan.

- Start Time: The day and time when the plan starts.
- On/Off: The device state after the start time.
- End Time: The day and time when the plan ends.
- On/Off: The device state after the end time.
- Weekly Cycle: Whether the plan repeats weekly.

- **Start Time** and **End Time** must be set to opposite states.
- If **On/Off** of **Start Time** is set to and **On/Off** of **End Time** is set to , then during the period from **Start Time** to **End Time**, the green PoE will be turn off.

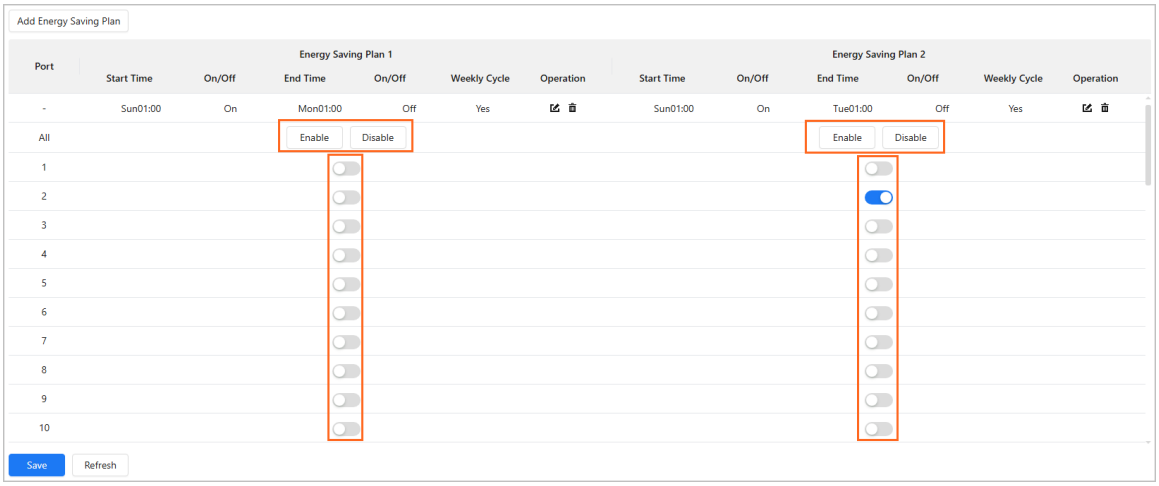
Figure 5-3 Add energy saving plan



Step 3 Click the corresponding port to enable green PoE.

- Each port can enable only one energy saving plan.
- Click **Enable** under a specific energy saving plan to apply it to all ports.
- Click **Disable** under a specific energy saving plan to deactivate this plan to all ports.

Figure 5-4 Green PoE



Step 4 Click **Save**.

5.6 Configuring Force PoE

Background Information

- After force PoE is enabled, connecting a non-PoE device to a forced PoE port might result in PD (Powered Device) damage.
- After force PoE is enabled, the port will force supply to the powered device, whether or not the device connected to the port meets the requirements. Please be advised.
- **Force PoE** and **PoE watchdog** cannot be enabled at the same time.

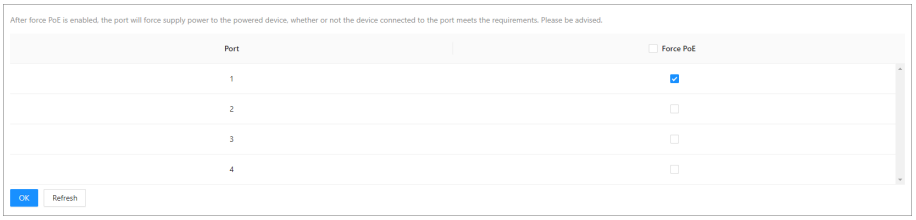
Procedure

Step 1 Select **PoE Management** > **Force PoE**.

Step 2 Click of the corresponding port to enable force PoE.

Step 3 Click **OK**.

Figure 5-5 Force PoE



5.7 Configuring PoE Watchdog

Background Information

With **PoE Watchdog** is enabled, you can check the status of the PD every 60 seconds. If no data transmission is detected, the device will automatically power off and restart the PoE port, ensuring port monitoring and keeping the PD device online.

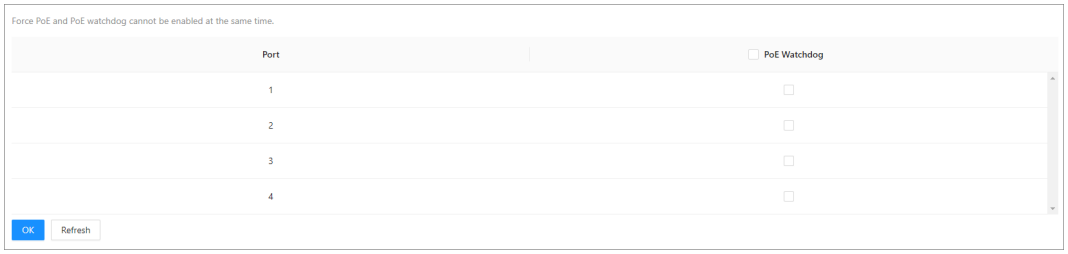
Force PoE and **PoE watchdog** cannot be enabled at the same time.

Procedure

Step 1 Select **PoE Management** > **PoE watchdog**.

Step 2 Click of the corresponding port to enable PoE watchdog as needed.

Figure 5-6 PoE watchdog



Step 3 Click **OK**.

6 Security

6.1 Basic Services

6.1.1 Configuring Basic Services

Procedure

Step 1 Select **Security** > **Basic Services**.

Step 2 Enable TLS, private protocols, or SSH protocols as needed.

- **TLS1.1** : The secure transport layer protocol (TLS) is used to guarantee confidentiality and data integrity between 2 communication applications. This protocol consists of 2 layers: TLS Record and TLS Handshake. TLS1.1 uses a weak encryption algorithm. We recommend you disable it.
- **Private Protocol** : Disabling this protocol might affect the functionality of related configurations such as **ConfigTool**.
- **SSH** : SSH is a reliable protocol that provides security for remote login sessions and other network services. Using SSH can effectively prevent information leakage during remote management.

Step 3 Click **OK**.

6.1.2 Configuring HTTPS

HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer) is a service entry based on Transport Layer Security (TLS). HTTPS provides web service, ONVIF access service and RTSP access service.

Procedure

Step 1 Select **Security** > **HTTPS**.

Step 2 (Optional) On the **Basic Services** tab, click to enable TLS1.1 as needed, and then click **OK**.

By default, the webpage only supports TLS1.2. If you need to use TLS1.1, you must enable it on the webpage. Please be advised that TLS1.1 poses security risks. We recommend you disable TLS1.1 to avoid unexpected risks.

Step 3 On the **HTTPS** tab, click to enable HTTPS.

Step 4 Select a device certificate.

Step 5 Select **Certificate Management** and the page will turn to **CA Certificate** page.

For details, see "6.3 Configuring CA Certificate".

Step 6 Click **OK**.

6.2 Enabling Telnet

Telnet is a basic remote management protocol used to access devices through command line for configuration and maintenance operations. Since it transmits data in plaintext, we recommend using SSH in environments with higher security requirements.

Select **Security** > **Telnet** to enable this protocol.

6.3 Configuring CA Certificate

6.3.1 Installing Device Certificate

A device certificate is a proof of device legal status. For example, when the browser is visiting device through HTTPS, the device certificate shall be verified.

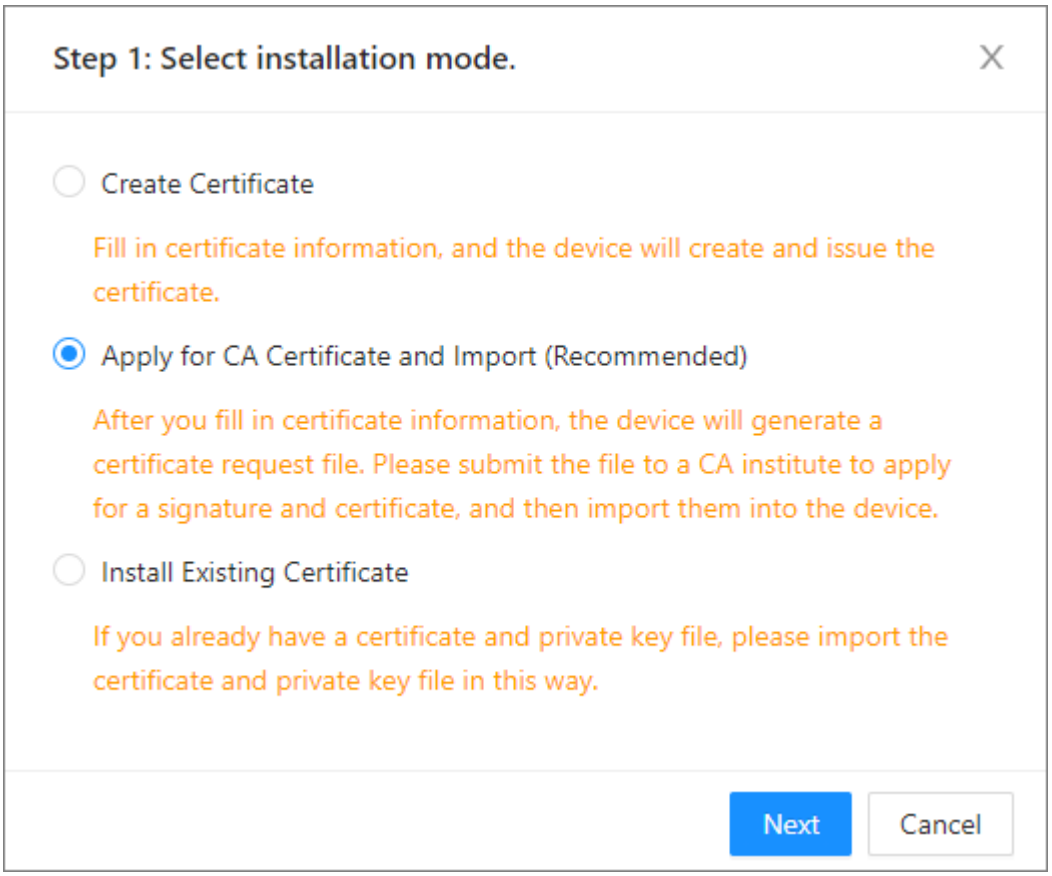
Procedure

Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 On the **Device Certificate** tab, click **Install Device Certificate**.

Step 3 Select an installation mode as needed.

Figure 6-1 Select installation mode



Step 4 Fill in certificate information, and then Click **Create and install certificate** , **Create and Download**, and **Import and Install**.

Step 5 (Optional) Click **Enter Edit Mode** to edit the **Custom Name**, and then click **Save Config**.

Figure 6-2 Edit certificate

Related Operations

- Download the certificate: Click .
- Delete the certificate: Click .

6.3.2 Installing Trusted CA Certificates

Background Information

A trusted CA certificate is used to verify the legal status of a host. For example, a switch CA certificate shall be installed for 802.1x authentication.

Only supports installing subordinate CA certificate.

Procedure

Step 1 Select **Security** > **CA Certificate**.

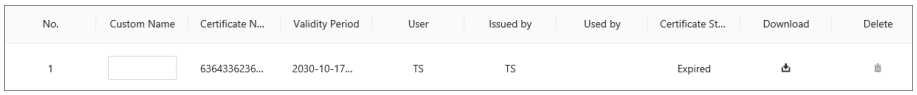
Step 2 On **Trusted CA Certificates** tab, click **Install Trusted Certificate**.

Step 3 Click **Browse** , and then click **OK**.

Figure 6-3 Install trusted certificate

Step 4 (Optional) Click **Enter Edit Mode** to edit the **Custom Name**, and then click **Save Config**.

Figure 6-4 Edit certificate



Related Operations

- Download the certificate: Click .
- Delete the certificate: Click .

6.4 Configuring Attack Defense

6.4.1 Configuring Firewall

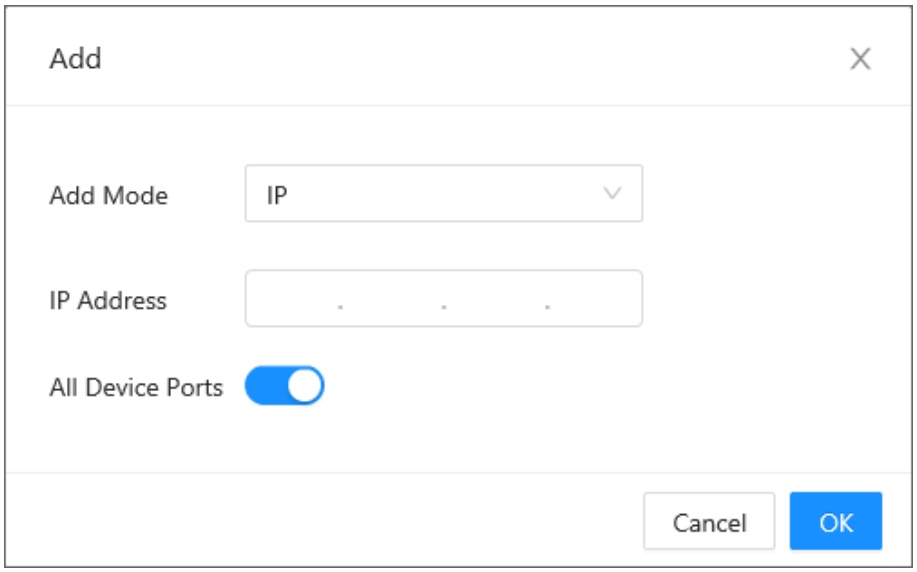
Procedure

Step 1 Select **Security** > **Attack Defense**.

Step 2 On the **Firewall** tab, click **All**, and all source hosts IP/MAC are allowed to access all the device ports.

Click **Allowlist** , and only source hosts whose IP/MAC are in the following list are allowed to access corresponding ports of the device, and then click **Add** to add hosts to allowlist.

Figure 6-5 Add to allowlist



Click **Blocklist** , and the listed corresponding source host of IP addresses/MAC is prohibited from visiting the corresponding ports of the device by network connection. Click **Add** to add hosts to blocklist.

Figure 6-6 Add to blocklist

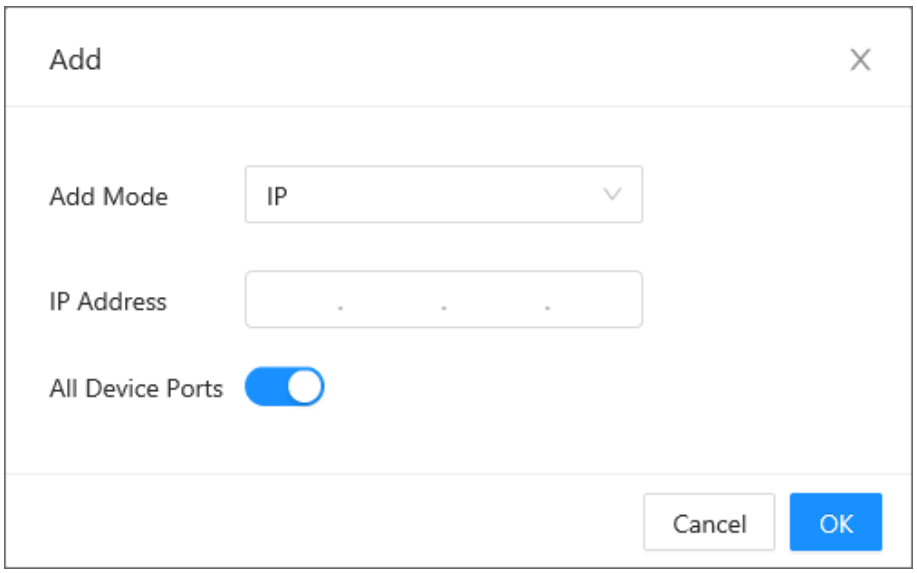


Table 6-1 Description of the firewall

Parameter	Description
All	All source hosts IP/MAC are allowed to access all the device ports.
Allowlist	Only source hosts whose IP/MAC are in the following list are allowed to access corresponding ports of the device.
Blocklist	The listed corresponding source host of IP addresses/MAC is prohibited from visiting the corresponding ports of the device.

Step 3 Click **OK**.

6.4.2 Configuring Anti-DoS Attack

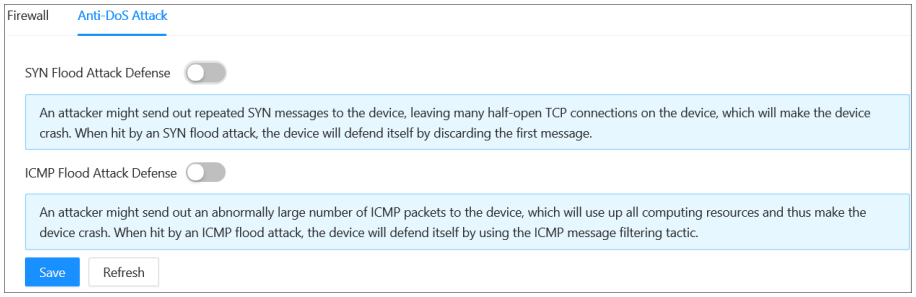
Procedure

Step 1 Select **Security** > **Attack Defense**.

Step 2 On the **Anti-DoS Attack** tab, click to enable different defense functions as needed.

Step 3 Click **Save**.

Figure 6-7 Anti-DoS attack



6.5 Configuring Port Isolation

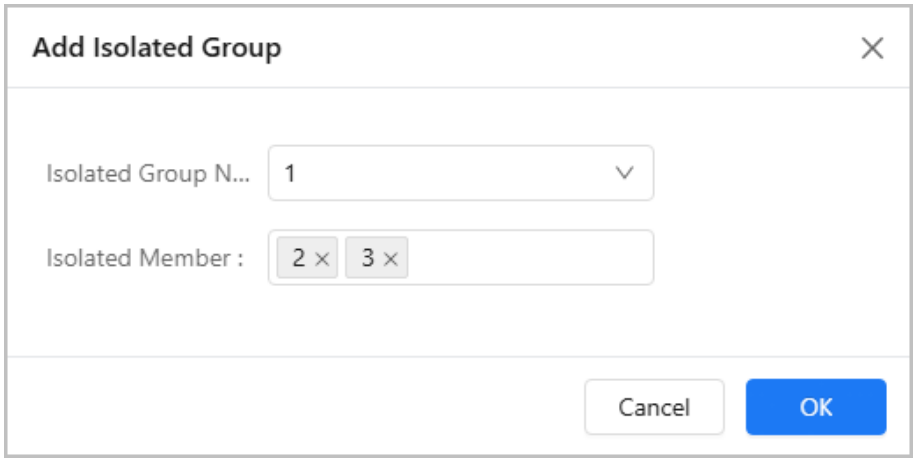
Port isolation is to achieve layer 2 isolation between messages. You only need to add the port to the isolation group to isolate the layer 2 data between the ports in the isolation group. The port isolation function provides users a safer and more flexible networking solution.

Procedure

Step 1 Select **Security** > **Port Isolation**.

Step 2 Click **Add**.

Figure 6-8 Add isolated group



Step 3 Select **Isolated Group No.** and **Isolated Member**, and then click **OK**.

Related Operations

- Edit isolated group: Click .
- Clear isolated group: Click .

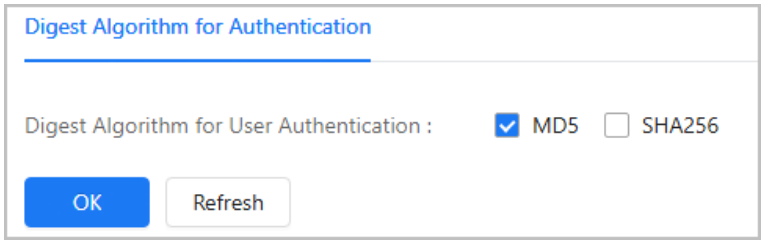
6.6 Configuring Security Authentication

This feature allows you to configure the authentication of user identity and the security algorithm for verification information.

Select **Security** > **Security Authentication**, select the user authentication digest algorithm, and then click **OK**.

MD5 or SHA256 uses the password provided by the user and other values to generate a digest, thereby increasing the difficulty of cracking and protecting information security.

Figure 6-9 Security Authentication



7 Control Policy

7.1 Configuring Port Priority

Background Information

By default, the 802.1p priority and DSCP priority for a voice VLAN are 6 and 46 respectively. You can dynamically configure 802.1p priority and DSCP priority to plan priorities for different voice services.

- The 802.1p priority is indicated by the value in the 3-bit PRI field in each 802.1Q VLAN frame. This field determines the transmission priority for data packets when a switching device is congested.
- The DSCP value is indicated by the 6 bits in the Type of Service (ToS) field in the IPv4 packet header. DSCP, as the signaling for DiffServ, is used for QoS guarantee on IP networks. The traffic controller on the network gateway takes actions merely based on the information carried by the 6 bits.

Procedure

Step 1 Select **Control Policy** > **Port Priority**.

Step 2 Select **Trust Mode**. Includes 3 types: Untrust, 802.1P, DSCP, and DSCP & 802.1P.

- **Untrust** : Untrust packets carry priority.
- **802.1P** : Determines packet forwarding priority based on 802.1P priority carried in the packet.
- **DSCP** : Determines packet forwarding priority based on DSCP priority carried in the packet.

When the trust mode is set to 802.1P, DSCP, and DSCP & 802.1P, you need to configure the priority mapping table. For details, see "7.3 Configuring Priority Mapping Table".

Step 3 (Optional) Configure the priority for each corresponding port.

When the mode is set to **Untrust**, you need to manually set the priority for each port. A higher priority value indicates a higher priority level.

Step 4 Click **OK**.

7.2 ACL

ACL (Access Control List) is used to implement traffic identification. To filter packets, network devices need to configure a series of matching conditions to classify packets. These conditions can include the source address, destination address, port number, and more.

When a port receives a packet, it analyzes the packet fields based on the ACL rules applied to that port. After identifying specific packets, the device allows or blocks them according to predefined policies.

7.2.1 Configuring ACL

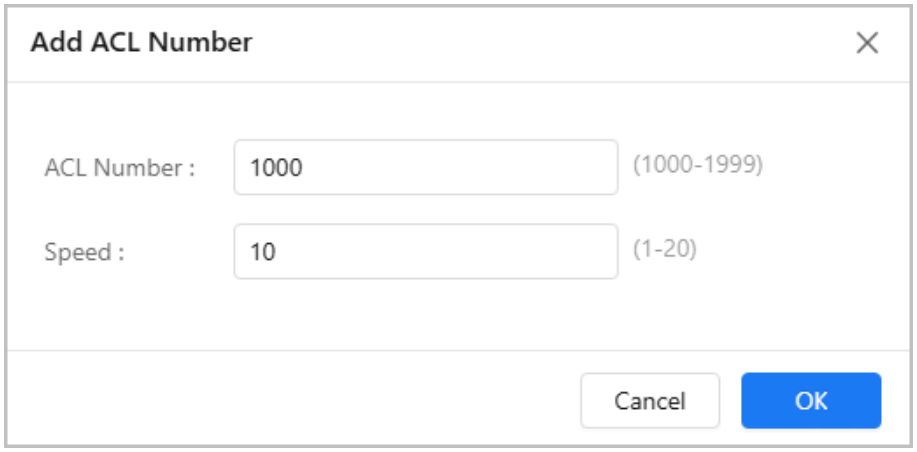
7.2.1.1 MAC ACL

Procedure

Step 1 Select **Control Policy** > **ACL** > **ACL Config** > **MAC ACL**.

Step 2 In the **MAC ACL List** area, click **Add**, set the parameters, and then click **OK**.

Figure 7-1 Add MAC ACL number



- **ACL Number** : Used to identify and distinguish ACL rules. The valid range for MAL ACL rules is **1000-1999**.
- **Speed** : Controls the increment for automatically assigned rules IDs when adding the new rules. This reserves numbering space for future rule insertion and management.

Step 3 In the **MAC ACL Rule List** area, click **Add**, and then set the parameters.

Figure 7-2 Add MAC ACL rule

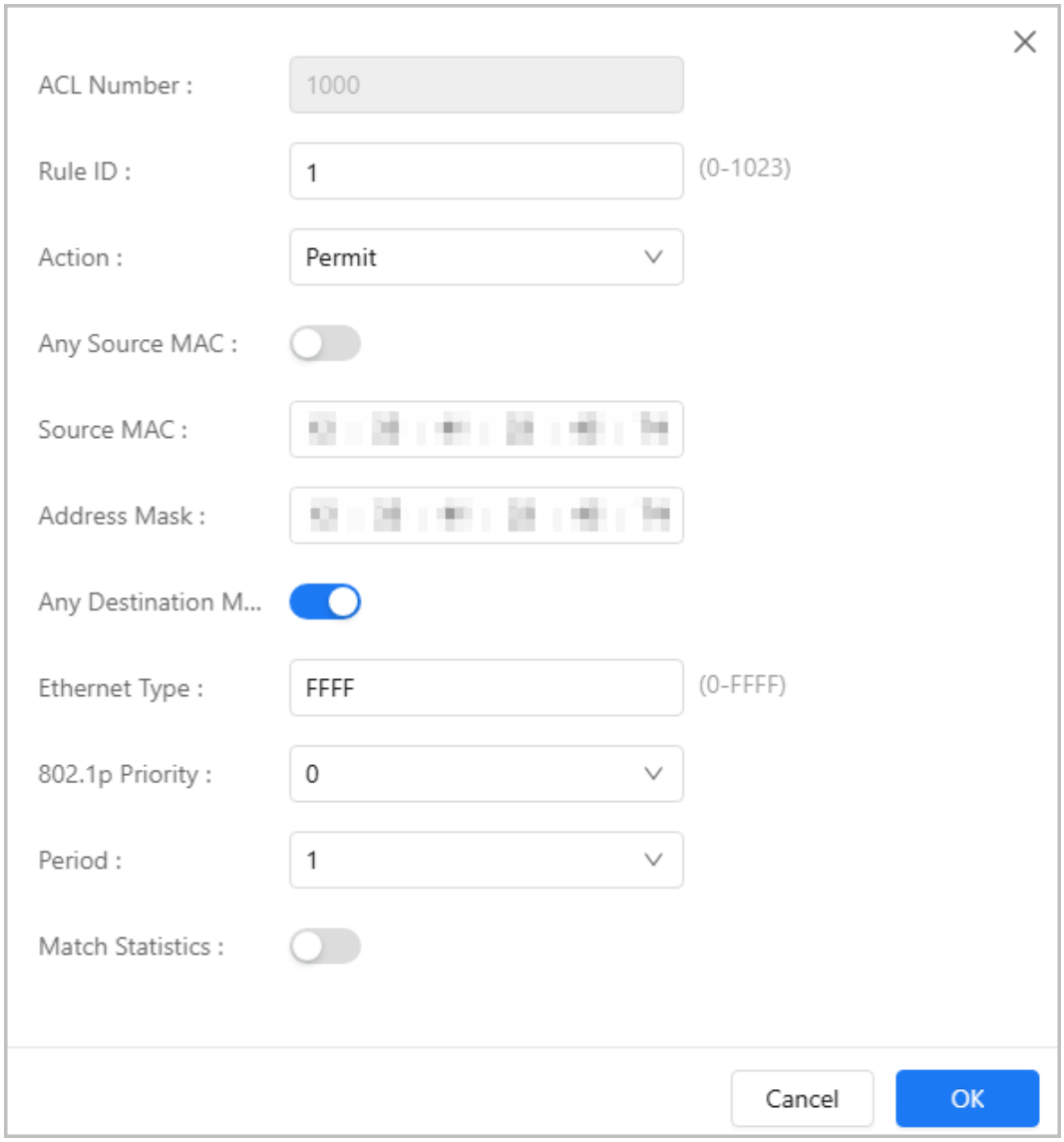


Table 7-1 Description of MAC ACL parameters

Parameter	Description
ACL Number	Set the unique identifier for the MAC ACL rule.
Rule ID	(Optional) Set the order of this MAC ACL rule for easier management.
Action	• Permit: The source MAC address can access the destination MAC address. • Deny: The source MAC address is blocked from accessing the destination MAC address.
Any Source MAC	• Click next to **Any Source MAC** to enable and match all source MAC addresses. • Click next to **Any Source MAC** to specify the source MAC and address mask.
Source MAC	
Address Mask	

Parameter	Description
Any Destination MAC	• Click next to **Any Destination MAC** to enable and match all destination MAC addresses. • Click next to **Any Destination MAC** to specify the destination MAC and address mask.
Destination MAC	
Address Mask	
Ethernet Type	Set the Ethernet type (range: **0-FFFF**), used to identify protocols. FFFF is the maximum value in hexadecimal.
802.1p Priority	Set the priority level to classify traffic. Include an unrestricted or 0-7 priority field.
Period	Set the time range to control when this rule is active. Include an unrestricted or predefined periods.
Match Statistics	Click next to **Match Statistics**. The device will record the hit count for this rule.

Step 4 Click **OK**.

Related Operations

After adding, you can view all MAC ACL rule information on the current page.

- **Clear Hits** or : Select the MAC ACL rule, and then click **Clear Hits** or to reset this hit count to zero.
- : Click next to a specific MAC ACL rule to open the details page.

Figure 7-3 View MAC ACL rule

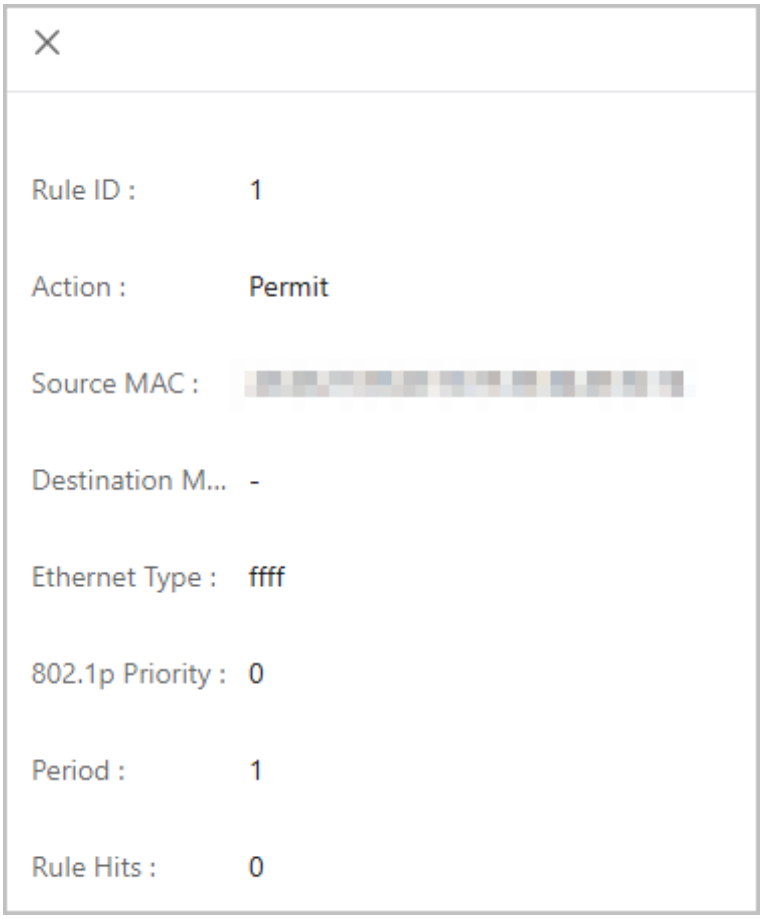
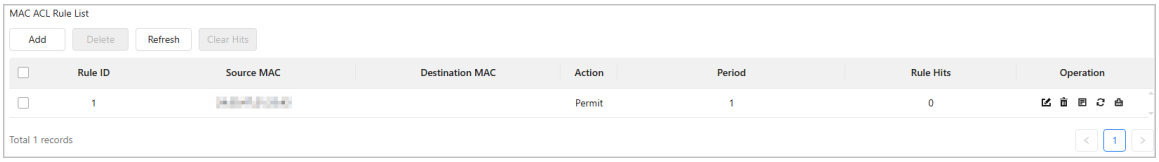


Figure 7-4 MAC ACL rule list



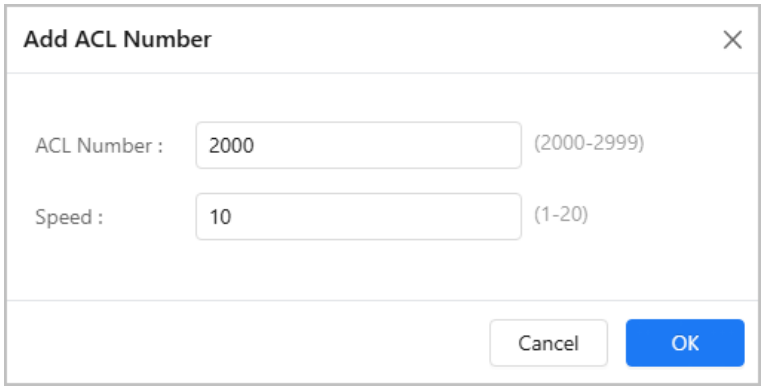
7.2.1.2 Basic IP ACL

Procedure

Step 1 Select **Control Policy** > **ACL** > **ACL Config** > **Basic IP ACL**.

Step 2 In the **Basic IP ACL List** area, click **Add**, set the parameters, and then click **OK**.

Figure 7-5 Add basic IP ACL number



- **ACL Number** : Used to identify and distinguish ACL rules. The valid range for basic IP ACL rules is **2000-2999**.
- **Speed** : Controls the increment for automatically assigned rules IDs when adding the new rules. This reserves numbering space for future rule insertion and management.

Step 3 In the **Basic IP ACL Rule List** area, click **Add**, and then set the parameters.

Figure 7-6 Add basic IP ACL rule

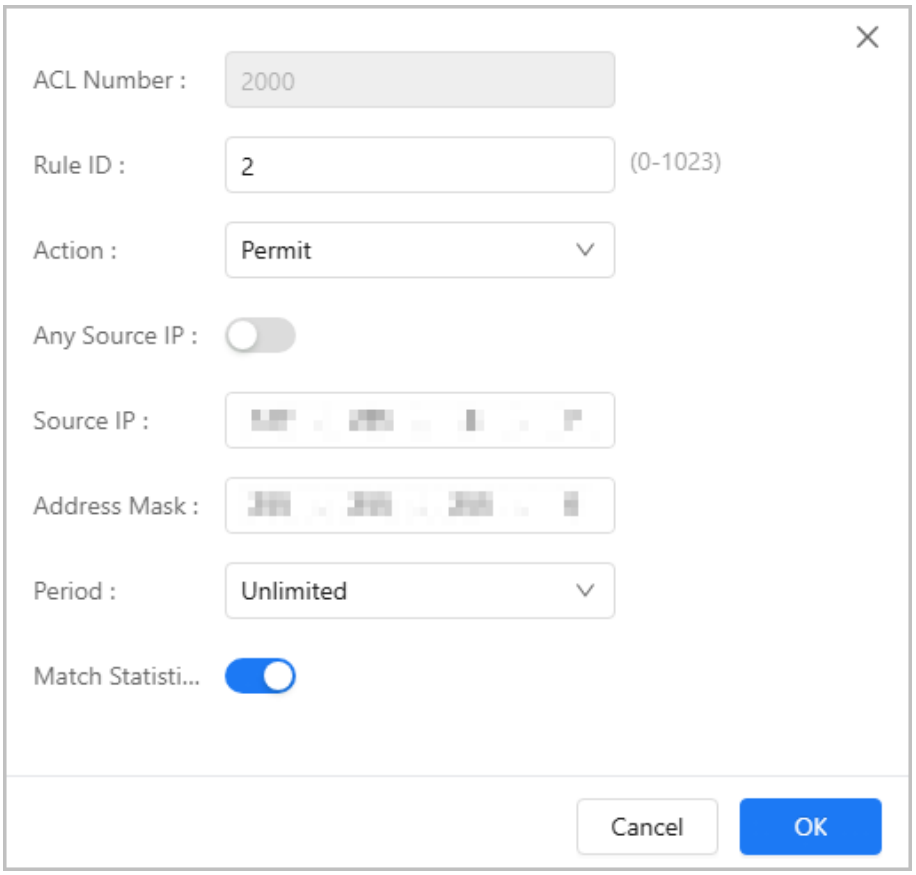


Table 7-2 Description of basic IP ACL parameters

Parameter	Description
ACL Number	Set the unique identifier for the basic IP ACL rule.

Parameter	Description
Rule ID	(Optional) Set the order of this basic IP ACL rule for easier management.
Action	• Permit: The source basic IP address can access the destination address. • Deny: The source basic IP address is blocked from accessing the destination address.
Any Source IP	• Click next to **Any Source Basic IP** to enable and match all source basic IP addresses. • Click next to **Any Source Basic IP** to specify the source basic IP and address mask.
Source IP	
Address Mask	
Period	Set the time range to control when this rule is active. Include an unrestricted or predefined periods.
Match Statistics	Click next to **Match Statistics**. The device will record the hit count for this rule.

Step 4 Click **OK**.

Related Operations

After adding, you can view all basic IP ACL rule information on the current page.

- **Clear Hits** or : Select the basic IP ACL rule, and then click **Clear Hits** or to reset this hit count to zero.
- : Click next to a specific basic IP ACL rule to open the details page.

Figure 7-7 View basic IP ACL rule

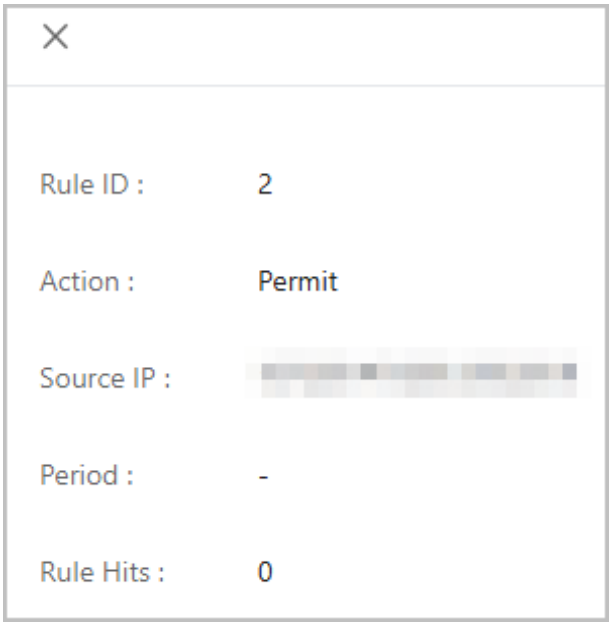
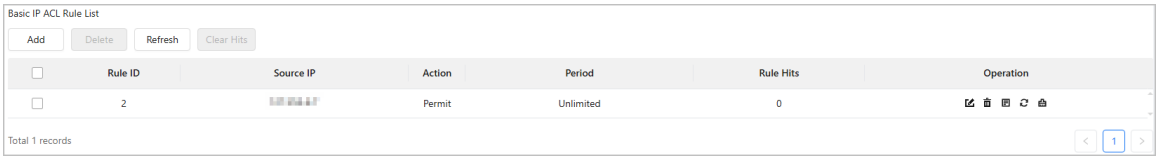


Figure 7-8 Basic IP ACL rule list



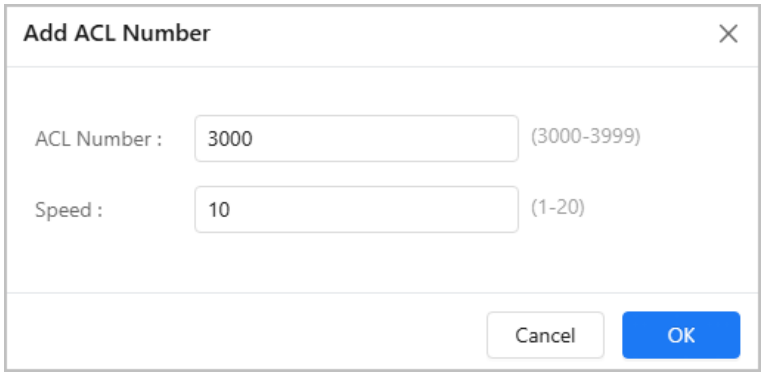
7.2.1.3 Advanced IP ACL

Procedure

Step 1 Select **Control Policy** > **ACL** > **ACL Config** > **Advanced IP ACL**.

Step 2 In the **Advanced IP ACL List** area, click **Add**, set the parameters, and then click **OK**.

Figure 7-9 Add advanced IP ACL number



- **ACL Number** : Used to identify and distinguish ACL rules. The valid range for advanced IP ACL rules is **3000-3999**.
- **Speed** : Controls the increment for automatically assigned rules IDs when adding the new rules. This reserves numbering space for future rule insertion and management.

Step 3 In the **Advanced IP ACL Rule List** area, click **Add**, and then set the parameters.

Figure 7-10 Add advanced IP ACL rule

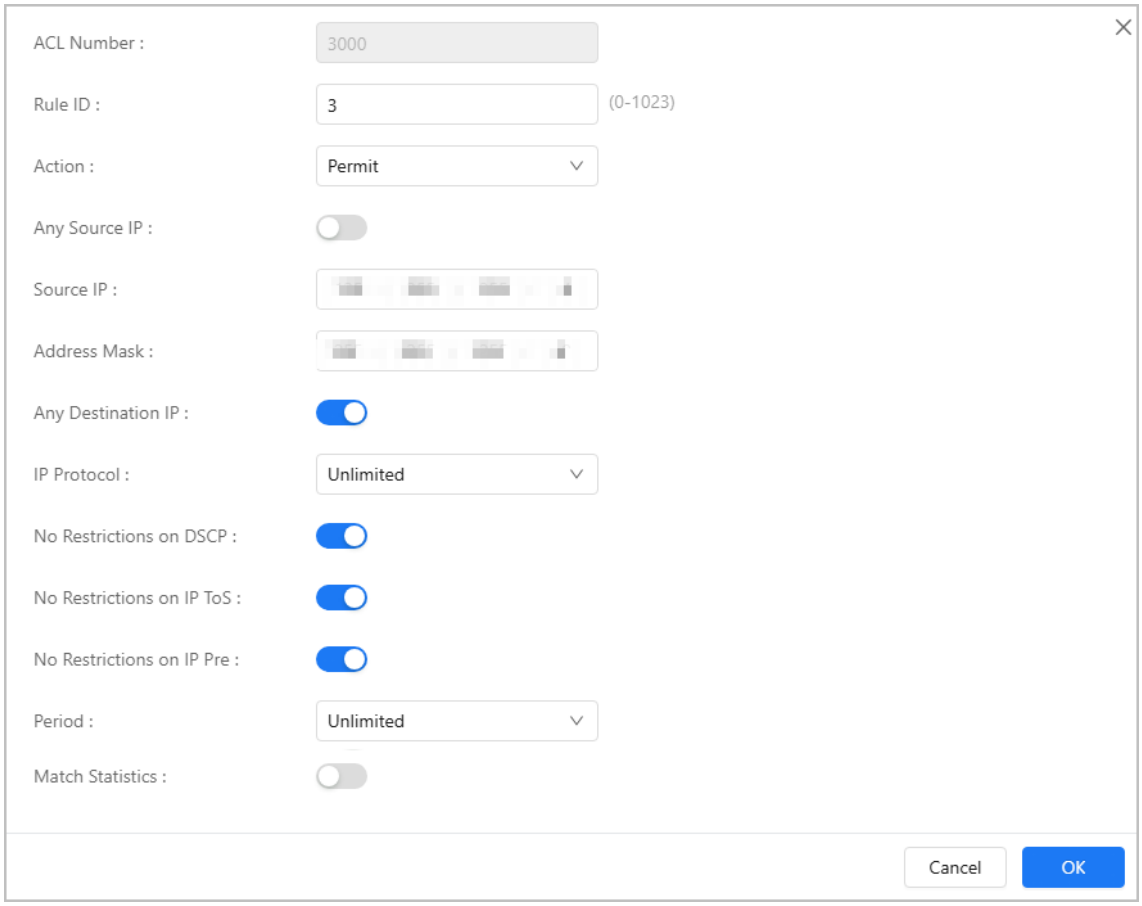
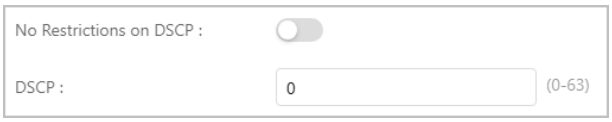


Table 7-3 Description of advanced ACL parameters

Parameter	Description
ACL Number	Set the unique identifier for the advanced ACL rule.
Rule ID	(Optional) Set the order of this advanced ACL rule for easier management.
Action	• Permit: The source address can access the destination address. • Deny: The source address is blocked from accessing the destination address.
Any Source IP Source IP Address Mask	• Click next to **Any Source IP** to enable and match all source IP addresses. • Click next to **Any Source IP** to specify the source IP and address mask.
Any Destination IP Destination IP Address Mask	• Click next to **Any Destination IP** to enable and match all destination IP addresses. • Click next to **Any Destination IP** to specify the destination IP and address mask.

Parameter	Description
IP Protocol	Select the IP protocol for this rule, including **unrestricted** or specific types.
No Restrictions on DSCP	• Click next to **No Restrictions on DSCP** to allow all DSCP-marked traffic. • Click next to **No Restrictions on DSCP** to permit only traffic with designed DSCP markings. 
No Restrictions on ToS	• Click next to **No Restrictions on ToS** to allow all IP ToS-marked traffic. • Click next to **No Restrictions on ToS** to permit only traffic with designed IP ToS markings. 
No Restrictions on Pre	• Click next to **No Restrictions on Pre** to allow all IP Pre-marked traffic. • Click next to **No Restrictions on Pre** to permit only traffic with designed IP Pre-markings. 
Period	Set the time range to control when this rule is active. Include an unrestricted or predefined periods.
Match Statistics	Click next to **Match Statistics**. The device will record the hit count for this rule.

Step 4 Click **OK**.

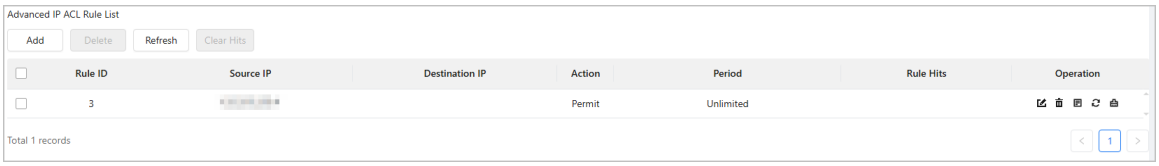
Related Operations

After adding, you can view all advanced IP ACL rule information on the current page.

- **Clear Hits** or : Select the advanced IP ACL rule, and then click **Clear Hits** or to reset this hit count to zero.
- : Click next to a specific advanced IP ACL rule to open the details page.

Figure 7-11 View advanced IP ACL rule

Figure 7-12 Advanced IP ACL rule list



7.2.2 Configuring Period

Procedure

Step 1 Select **Control Policy** > **ACL** > **Period**.

Step 2 Click **Add**.

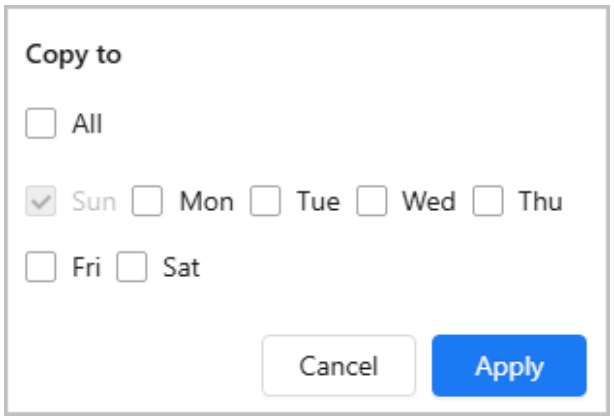
Step 3 Set the name of this time period (user-defined).

Step 4 Set the time period.

- Set the periodic time range.

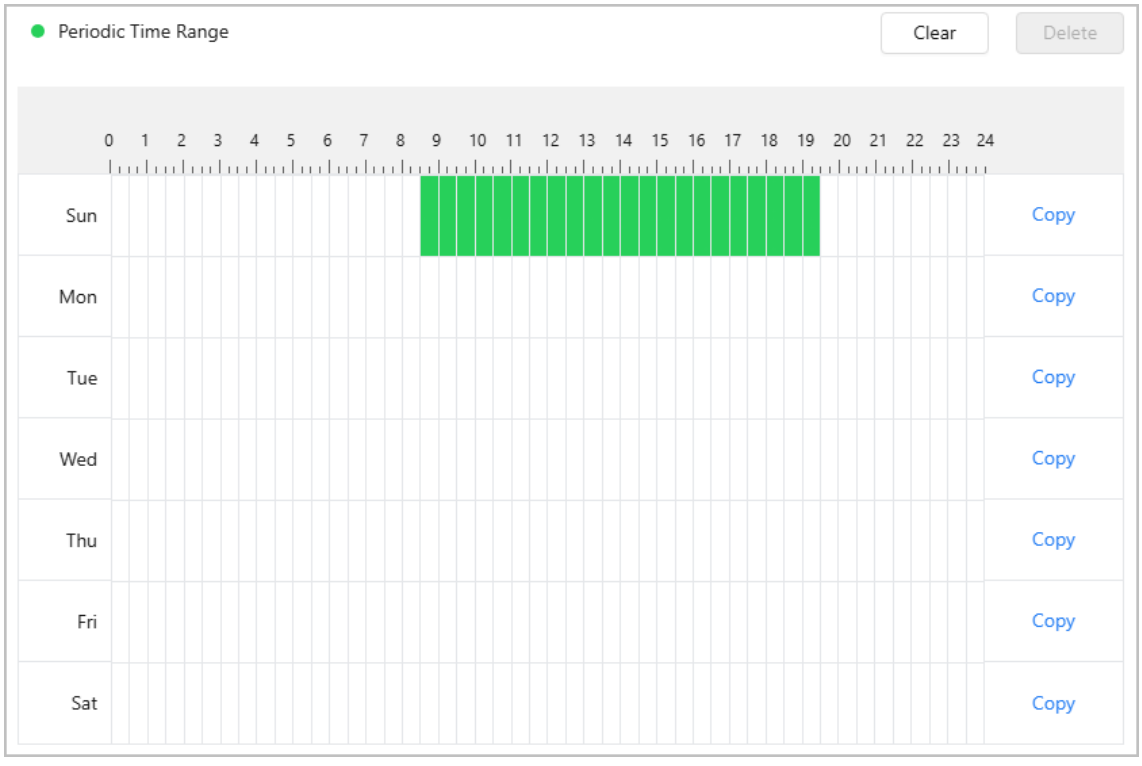
1. In the **Periodic Time Range** area, drag the slider to select the desired time range.
2. (Optional) Click **Copy** , select the target time, and then click **Apply** to duplicate the same time period.

Figure 7-13 Copy the periodic time



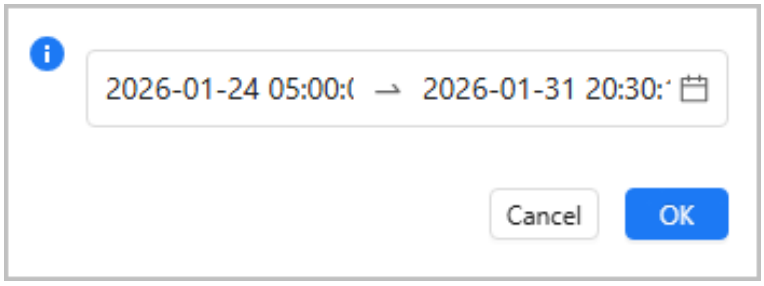
3. (Optional) Click **Clear** to reset the configured recurring time period.
4. Click ⊙ to confirm the time period.

Figure 7-14 Set the periodic time range



- Set the absolute time range.
  1. In the **Absolute Time Range** area, click **Add**.
  2. Set the start time and end time, and then click **OK**.

Figure 7-15 Set the absolute time range



Step 5 Click **OK**.

7.2.3 ACL Binding

Apply the configured MAC ACL, standard IP ACL, or advanced IP ACL to a specific port.

Procedure

Step 1 Select **Control Policy** > **ACL** > **ACL Binding**.

Step 2 Click **Add**.

Step 3 Configure ACL binding rules.

- In the **ACL Number** list, select the corresponding number.
- Click the port icon on which the ACL should be applied.

Figure 7-16 Add ACL binding

Step 4 Click **OK**.

Related Operations

After the configuration is completed, you can view all ACL binding rule information on the current page.

- ACL number: Display the bound ACL rule number.
- Port: Displays the corresponding port where the ACL rule takes effect.
- Direction: Displays at which traffic stage the ACL rule is applied.
  - In: Allows or denies traffic entering the device through the port.
  - Out: Allows or denies traffic leaving the device through the port.

Figure 7-17 ACL binding list

7.3 Configuring Priority Mapping Table

Procedure

Step 1 Select **Control Policy** > **Priority Mapping Table**.

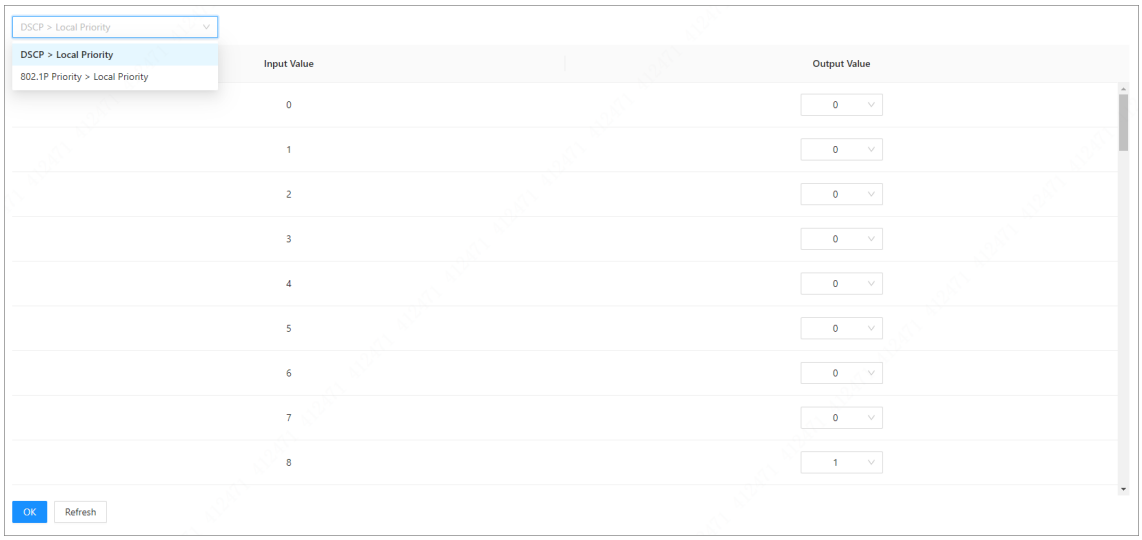
Step 2 Select **DSCP > Local Priority** or **802.1p > Local Priority**.

Step 3 Select **Output Value**.

The input value and the output value vary from different modes.

Step 4 Click **OK**.

Figure 7-18 Priority mapping



7.4 Configuring Queue Scheduling

Background Information

- PQ: Priority queuing. PQ schedules packets in descending order of priority. Packets in queues with a lower priority can be scheduled only after all packets in queues with a higher priority have been scheduled.
- WRR: Weighted Round Robin. In WRR scheduling, the device schedules packets in queues in a polling manner based on the queue weight. After one round of scheduling, the weights of all queues are decreased by 1. The queue whose weight is decreased to 0 cannot be scheduled.

Procedure

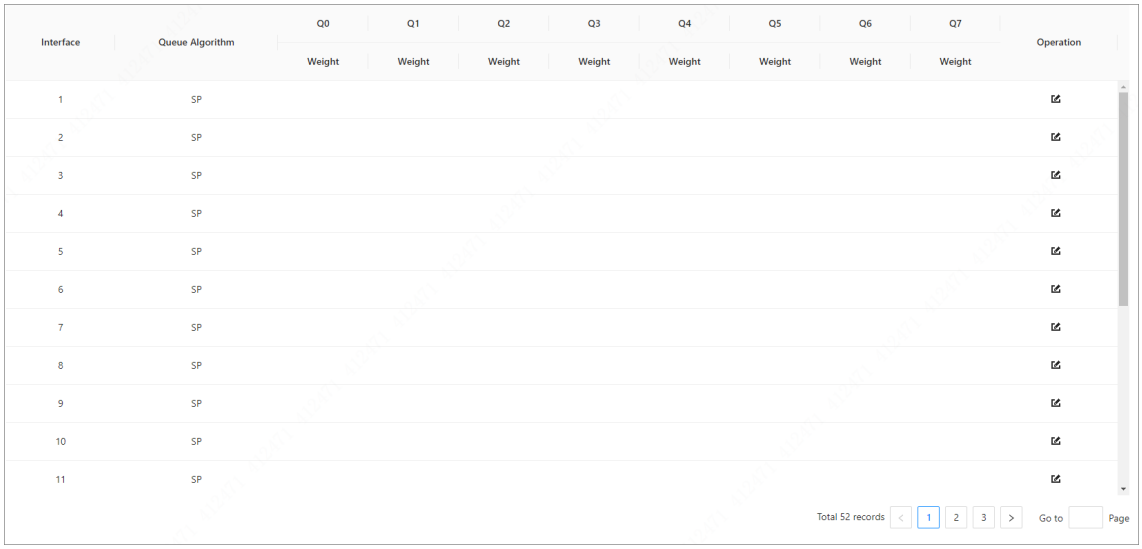
Step 1 Select **Control Policy** > **Queue Scheduling**.

Step 2 Select from the **Queue Algorithm**.

In WRR mode, the weight ratio of the priority queue is Queue0:Queue1:Queue2:Queue3=1:2:4:8.

Step 3 Click **OK**.

Figure 7-19 Queue scheduling



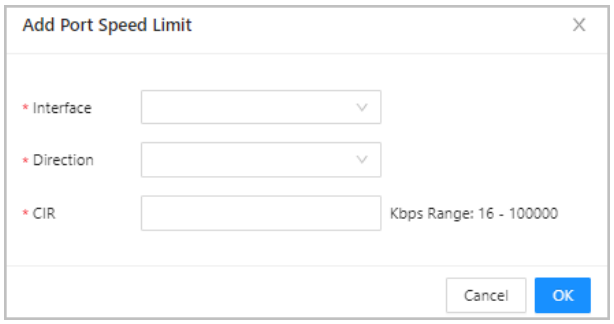
7.5 Configuring Port Speed Limit

Procedure

Step 1 Select **Control Policy** > **Port Speed Limit**.

Step 2 Click **Add**.

Figure 7-20 Add port speed limit



Step 3 Enter the **Interface** , **Direction**, and **CIR**.

- The values of **Direction** include **In** and **Out**.
- The input rule for CIR: Range from 16 to 100000, and must be an integer multiple of 16.

Step 4 Click **OK**.

7.6 Configuring Storm Control

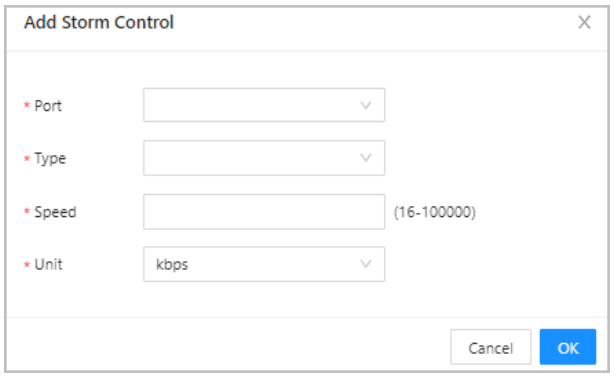
The broadcast frames on the network are forwarded continuously, which affects the proper communications, and greatly reduces the network performance. The storm control can limit the broadcast flows of the port and discard the broadcast frames once the flow exceeds the specified threshold, which can reduce the risk of the broadcast storm and ensure the network proper operation.

Procedure

Step 1 Select **Control Policy** > **Storm Control**.

Step 2 Click **Add**.

Figure 7-21 Add storm control



Step 3 Enter the **Port** , **Type**, and **Speed**.

Step 4 Click **OK**.

8 Authentication

8.1 Configuring 802.1x

802.1x is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network.

Procedure

Step 1 Click next to the **Enable** to enable NAS (Network Attached Storage).

Step 2 Select from **Port Status**.

The status includes **Auto** , **Force unAuthorized**, and **Force Authorized**.

Figure 8-1 Configure 802.1x

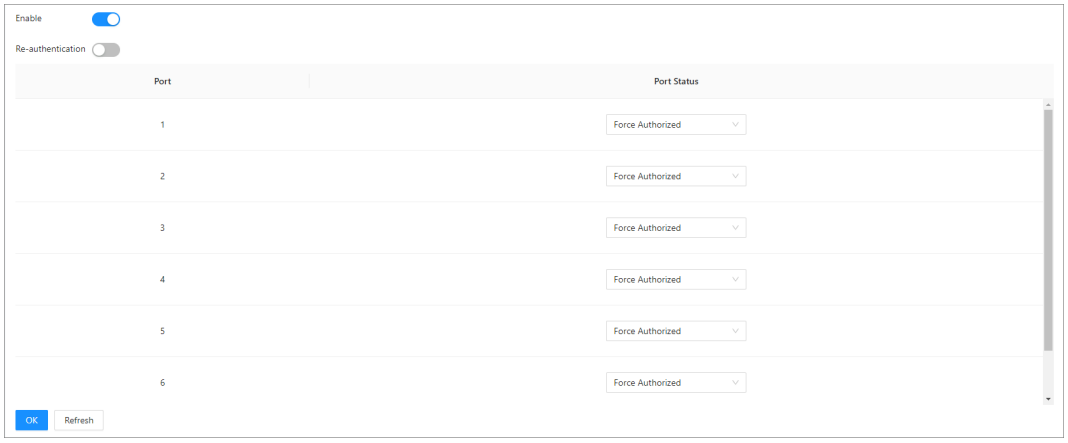


Table 8-1 Description of 802.1x

Parameter	Description
Auto	The port automatically configure status according to the authentication results.
Force UnAuthorized	• The port is always in an unauthorized status, and users are not allowed to authenticate. • The device does not provide authentication services for users that access through this port.
Force Authorized	The port is always in the authorized status, and users are allowed to access network resources without authentication.

Step 3 Click **OK**.

8.2 Configuring Radius

Background Information

RADIUS (Remote Authentication Dial-In User Service) is a common protocol to realize AAA (Authentication, Authorization and Accounting).

RADIUS is an information interaction protocol of distributed and C/S construction. It can protect the network from unauthorized visits. It is used in the network that allows remote visits but requests the higher security. It defines the RADIUS packet format and the message transmission mechanism. It stipulates that using UDP as transport layer protocol to encapsulate the RADIUS packet.

At the beginning, RADIUS is the AAA protocol for the dial-up users only. With the development of the user accesses, RADIUS adapts to various access, including Ethernet access and ADSL access. It accesses server through authentication and authorization, and collects records the usage of network source through accounting.

Procedure

Step 1 Select **Authentication** > **RADIUS**.

Figure 8-2 RADIUS

Step 2 Click **Add**.

Figure 8-3 Add RADIUS

Step 3 Set the **IP Address** , **port**, and **Secret key**.

Step 4 Click **OK**.

Appendix 1 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use repeating characters, such as 111, aaa, etc.

2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. **Set and update password reset information in a timely manner**

   Dahua device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access Web services through secure channels.
2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, we recommend you to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

   If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allowlist**

   It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

   Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

   We recommend you to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188