

Managed Switch

Web Operation Manual



V1.0.0






Foreword

General





This manual introduces operations on web interface of the RTL switch (hereinafter referred to as "the switch"). You can visit the switch on web browser, configure and manage the switch.

Safety Instructions

The following categorized signal words with defined meaning 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, lower performance, or unpredictable result.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Frequently Used Functions

Icon/Parameter	Description
	Edit an item.
 or Delete	Delete items one by one or in batches.
 or 	Enable or disable items one by one or in batches.
Refresh or Auto Refresh	Refresh or auto refresh the content.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	January 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: 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's 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 Switch.....	1
1.2 Logging in.....	2
2 Quick Configuration.....	4
2.1 Configuring General Information.....	4
2.2 Port Information.....	5
2.3 ONVIF.....	6
2.4 Viewing IPC and NVR.....	7
3 Maintenance.....	8
3.1 Configuring System Time.....	8
3.2 Viewing Legal Information.....	8
3.3 Changing Password.....	9
3.4 Configuring Firmware.....	9
3.5 File Management.....	10
3.6 Viewing Device Information.....	10
3.7 Viewing Log Information.....	11
3.8 Status Monitoring.....	12
3.9 Viewing Diagnosis.....	12
3.10 Configuring Mirroring.....	13
4 Network Settings.....	15
4.1 configuring Ports.....	15
4.2 Configuring EEE.....	16
4.3 Configuring VLAN.....	17
4.3.1 VLAN Definition.....	17
4.3.2 VLAN Function.....	17
4.3.3 Port-based VLAN.....	17
4.3.4 Adding VLAN.....	18
4.3.5 Configuring Port VLAN.....	19
4.4 Configuring VLANIF.....	20
4.5 Configuring IP and Routing.....	21
4.6 Configuring ERPS.....	22
4.6.1 ERPS Settings.....	22
4.6.2 MEP Settings.....	23
4.7 Configuring IGMP Snooping.....	24
4.8 Configuring STP.....	25

4.8.1 STP.....	25
4.8.2 Port Instance.....	26
4.9 Configuring Link Aggregation.....	27
4.10 Configuring SNMP Protocol.....	28
4.10.1 Configuring SNMP V1 and V2.....	28
4.10.2 Configuring SNMP V3.....	29
4.11 Configuring MAC Table.....	31
4.11.1 Adding MAC Table.....	31
4.11.2 Filtering Port MAC.....	32
4.12 Configuring LLDP.....	33
5 PoE Management.....	34
5.1 Configuring PoE Settings.....	34
5.2 Configuring Perpetual PoE.....	35
5.3 Configuring Long Distance PoE.....	35
5.4 Viewing PoE Event Statistics.....	36
5.5 Configuring Green PoE.....	36
5.6 Configuring Force PoE.....	37
5.7 Configuring PoE Watchdog.....	37
6 Security.....	39
6.1 Basic Services.....	39
6.1.1 Configuring Basic Services.....	39
6.1.2 Configuring HTTPS.....	39
6.2 Configuring CA Certificate.....	40
6.2.1 Installing Device Certificate.....	40
6.2.2 Installing Trusted CA Certificates.....	41
6.3 Configuring Attack Defense.....	42
6.3.1 Configuring Firewall.....	42
6.3.2 Configuring Anti-DoS Attack.....	44
6.4 Configuring Port Isolation.....	44
7 Control Policy.....	45
7.1 Configuring Port Priority.....	45
7.2 Configuring Priority Mapping Table.....	45
7.3 Configuring Queue Scheduling.....	46
7.4 Configuring Port Speed Limit.....	47
7.5 Configuring Storm Control.....	47
8 Authentication.....	49
8.1 Configuring 802.1x.....	49
8.2 Configuring Radius.....	50
Appendix 1 Cybersecurity Recommendations.....	51

1 Login

1.1 Initializing the Switch

Prerequisites

Before login, make sure that the switch and the configuration device are connected and powered on.

Procedure

- Step 1** Open the IE browser, 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** 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**.

Figure 1-1 Read policy



- Step 3** Set the password of the admin user.



The username is admin, and the password is custom.

Figure 1-2 Set password



- Step 4** Click **OK**.

1.2 Logging in

Prerequisites

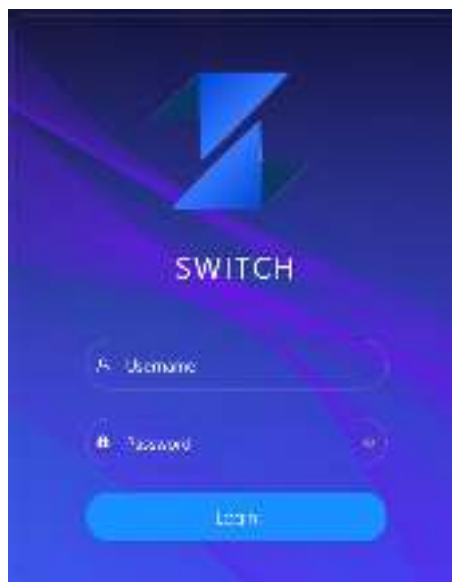
Before login, make sure:

- You have already configured the IP address of the switch. The IP address of VLAN 1 is 192.168.1.110 by default.
- The computer is connected to the network and can ping the switch.

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 username and password.
- Step 3 Click **Login**.

Figure 1-3 Login



- Change the password after the first login. The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
- For details on changing the password, see "3.3 Changing Password".

Figure 1-4 Home page

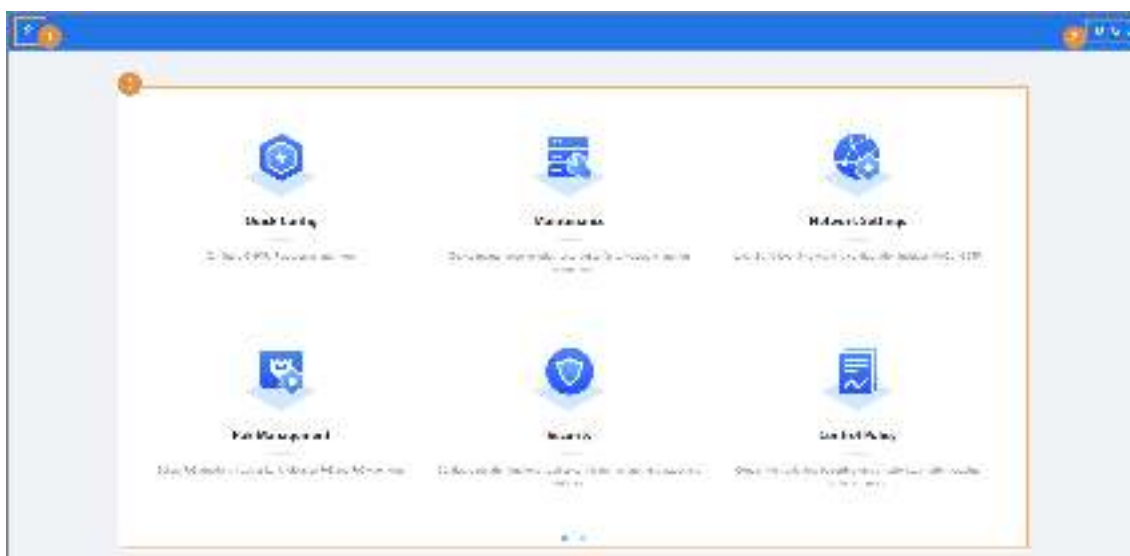






Table 1-1 Description of the homepage

No.	Name	Description
1		Go back to the home page.
2		Switch the system languages. Supports multiple languages.
		Logout the user, and then return to the login page.
		Full-screen displays the web page.
3	Status Display	Live view the current status of the switch.
	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.
	Security	Configure security settings, including certificate management, attack and defense.
	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 switch 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, subnet mask, and default gateway.

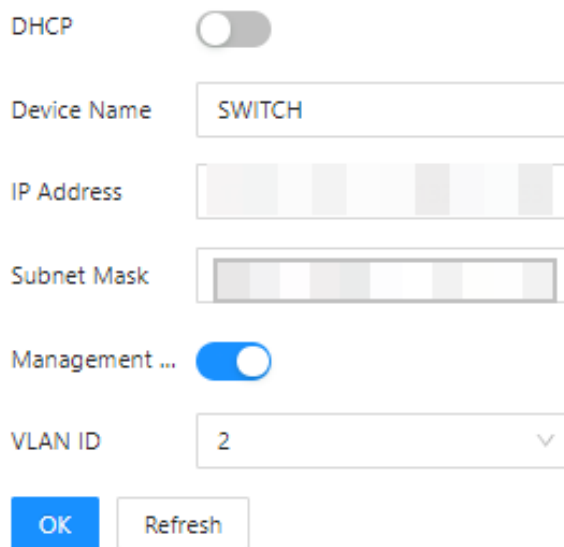
Procedure

- Step 1** Select **Quick Config > General**.
- Step 2** You can view and configure the general information of the switch.
- Step 3** (Optional) Click  to enable the DHCP function.



Please be advised of this function. 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.

Figure 2-1 General information



DHCP ☐

Device Name SWITCH

IP Address 192.168.1.110

Subnet Mask 255.255.255.0

Management ... ☒

VLAN ID 2

OK Refresh

Table 2-1 Description of general information

Parameter	Description
DHCP	Supports enabling DHCP. After enabling DHCP, new IP will be automatically acquired and assigned. Before new IP is assigned, the default IP 192.168.1.110 is adopted.
Device Name	Displays the current device name. Support changing the name.
IP Address	Displays the current IP address. Support manual configuration.
Subnet Mask	Supports entering the subnet mask.

Parameter	Description
Managed VLAN	After Managed VLAN is enabled, you can only access the webpage through the IP from managed VLAN.
VLAN ID	Displays the current the managed VLAN ID.

2.2 Port Information

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

Procedure

- Step 1** Select **Quick Config > Port Info**.
- Step 2** View the port information of the switch.

Figure 2-2 Port information

Port	Type	Link Status	Speed/Duplexing	VLAN	RX Usage	TX Usage	Media Type
1	Access	Down	Down	1	0	0	Copper
2	Access	Down	Down	1	0	0	Copper
3	Access	Down	Down	1	0	0	Copper
4	Access	Down	Down	1	0	0	Copper
5	Access	Down	Down	1	0	0	Fiber
6	Access	Down	Down	1	0	0	Fiber
7	Access	Down	Down	1	0	0	Fiber
8	Access	Down	Down	1	0	0	Fiber

Table 2-2 Description of port information

Parameter	Description
Port	Displays all ports of the switch.
Description	Set the port description. Support 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.
Type	Includes three types: Access , Hybrid , and Trunk .
Link status	Includes two statuses: Up and Down . <ul style="list-style-type: none"> Up: The port is connected. Down: The port is not connected or the connection fails.
Speed/Duplexing	<ul style="list-style-type: none"> Online: Displays the port rate and the duplex mode. Offline: Displays Down.
VLAN	VLAN port. VLAN 1 by default.
RX usage	Displays the receiving usage.

Parameter	Description
TX usage	Displays the sending usage.
Media type	Includes two types: Copper and Fiber . <ul style="list-style-type: none"> ● Copper: RJ-45 port. ● Fiber: Fiber port.

Related Operations

- Click **Refresh** to manually refresh the port information.
- Click ☐ next to **Auto Refresh** to enable the automatic refreshing.

2.3 ONVIF

Select **Quick Config** > **Port Info**, you can view the port information of the switch.

Click ☐ to enable the ONVIF display function. After enabling, the page displays all the ports and the connection status of the switch.

- Green port: Indicates successful connection.
- Light blue port: Indicates no connection or connection failure.



Different models are equipped with different numbers of ports. The following figure is only for reference. Please refer to the actual product.

Figure 2-3 ONVIF information

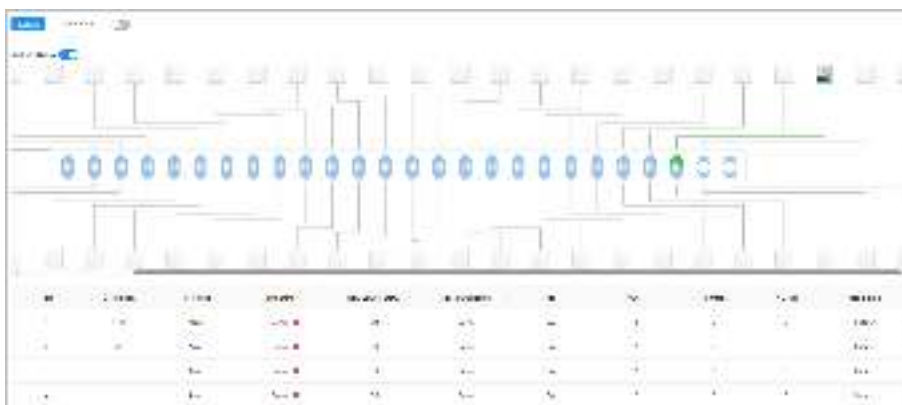



Table 2-3 Port descriptions

Name	Description
Port	Displays the port number.
Description	Displays port description.
Port Type	Includes three types: Access , Hybrid , and Trunk .
Link Status	Includes two statuses: Up and Down . <ul style="list-style-type: none"> ● Up: The port is connected. ● Down: The port is not connected or the connection fails.
Flow Control Status	Check the status of the flow control function.

Name	Description
Speed/Duplexing	<ul style="list-style-type: none"> ● Online: Displays the port rate and the duplex mode. ● Offline: Displays Down.
VLAN	VLAN port. VLAN 1 by default.
PoE	Displays the PoE power consumption.  <ul style="list-style-type: none"> ● Non-PoE switches do not support this function. ● Different models are equipped with different numbers of the PoE ports. Please refer to the actual product.
RX Usage	The current reception rate divided by the actual negotiated rate for a period of time(usually 5 minutes).
TX Usage	The current sending rate divided by the actual negotiated rate for a period of time(usually 5 minutes).
Media Type	Includes two types: Copper and Fiber . <ul style="list-style-type: none"> ● Copper: RJ-45 port. ● Fiber: Fiber port.

2.4 Viewing IPC and NVR

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

3 Maintenance

3.1 Configuring System Time

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

Procedure


- Step 1** Select **Maintenance** > **System Time**.
- Step 2** Configure the system time. There are 3 methods:
- Manually configure the **System Time** and **Time Zone**, and then click **OK**.
 - Click **Sync PC** to synchronize the switch time to the computer time.
 - Click  to synchronize the switch time to the server time, and then click **OK**.

Figure 3-1 Configure time



3.2 Viewing Legal Information

Select **Maintenance** > **Legal Info**, you can view **Open Source Software Notice**.

Figure 3-2 Legal information



3.3 Changing Password

Background Information



- To use the iLinkView function, the username and password of the iLinkView platform and the switch must be the same.
- The username is admin by default, and it cannot be changed.

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 two 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 **Restore Factory Default** to restore all the device parameters to the factory defaults.



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

Restore Factory Default

Click **Restore Now** to restore all the device parameters to the factory defaults.



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**.

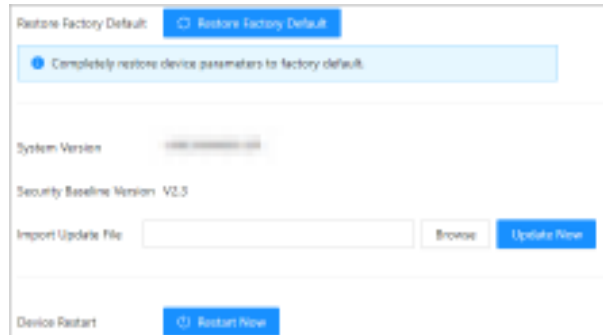


It might take 3 minutes to update the software. After the update, the system will automatically restart.

Restart Device

Click **Restart Now** to restart the device.

Figure 3-3 Firmware configuration



3.5 File Management

You can configure the backup file and restore file.

Backup Configuration

We recommend backing up the logs for the future reference.

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

Restoration Configuration

We recommend backing up the logs for the future reference.

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 3-4 Device information

System	
Device Name	SWITCH
Device Model	4 Ports PoE Switch
IP Address	
Software	
Software Version	1.001.00000000.2.R
Compile Date	2022-03-31
Hardware	
MAC	
SN	000000000000000000
Time	
System Time	
Operation Time	18 Days 22 hr 13 min 53 sec

3.7 Viewing Log Information

You can view the log information on the switch operations.

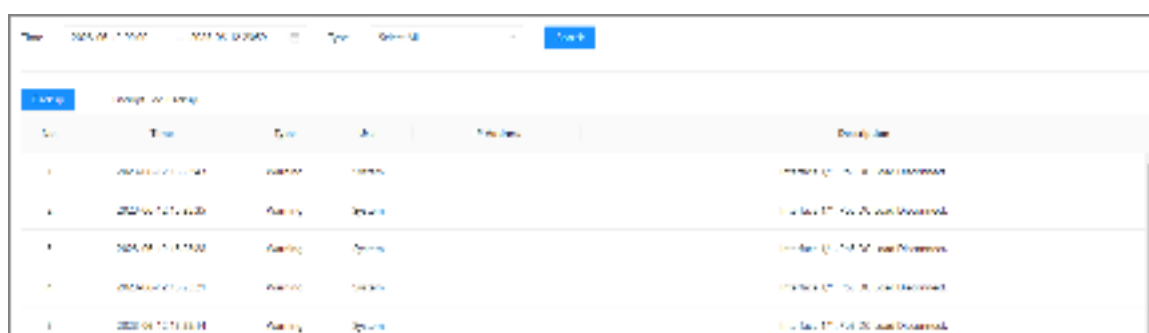
Background Information

We recommend enabling the log function to ensure that the key logs can be synchronized to the server for future reference.

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**.

Figure 3-5 Log information



Time	Type	Details
2025/04/10 10:00:00	Warning	Warning: CPU usage is high.
2025/04/10 10:00:00	Warning	Warning: Memory usage is high.
2025/04/10 10:00:00	Warning	Warning: Disk usage is high.
2025/04/10 10:00:00	Warning	Warning: Network usage is high.
2025/04/10 10:00:00	Warning	Warning: System load is high.

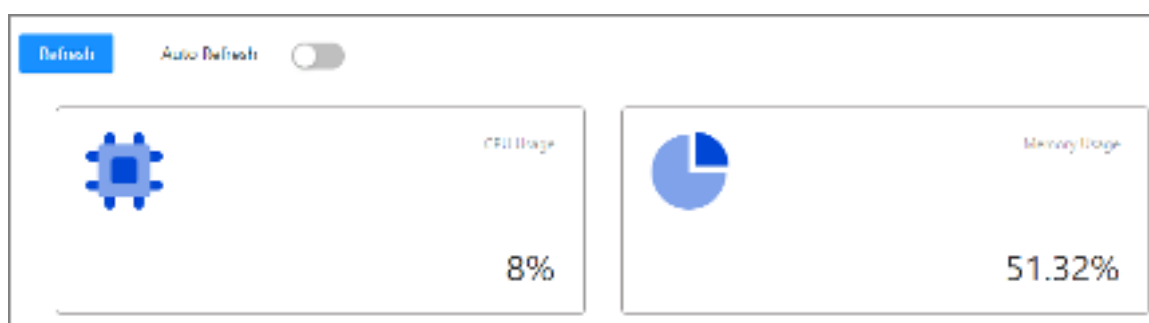
Table 3-1 Parameter description

Parameter	Description
Backup	Tap to backup the searched logs.
Encrypt Log Backup	Click the checkbox to encrypt the back-up logs.

3.8 Status Monitoring

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

Figure 3-6 Status monitoring



3.9 Viewing Diagnosis

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 3-7 Diagnosis

3.10 Configuring Mirroring

Background Information

Mirroring copies traffic received or sent or both on a specified source to a destination port for analysis. The specified source is called mirrored source, the destination port is called observing port, and the copied traffic is called mirrored traffic. Mirroring sends a copy of the traffic through an observing port on the switch to a monitoring device for service analysis.

Procedure



- Step 1 Select **Maintenance** > **Mirror**.
- Step 2 Click **Add**.
- Step 3 In **Add Mirroring Group** page, select **Mirroring Group No.**, **Mirroring Destination Port**, and then select from **TX Only**, **RX Only**, and **Both** according to the actual situation.
- Step 4 Click **OK**.

Figure 3-8 Add Mirroring Group

Table 3-2 Source port description

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

Related Operations

- Click  to edit the information of mirroring group.
- Click  or **Delete** to delete the mirroring group.

4 Network Settings

4.1 configuring Ports

Background Information

You can configure the port parameters, including speed/duplexing, flow control, and other parameters. The port parameters will directly affect the working mode of the port. Make configurations according to the practical requirements.



The webpage might differ from different devices. Refer to the actual pages.

Procedure

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

Step 2 You can view and configure the parameters.

Figure 4-1 Port settings



Port	Description	Type	Link Stat.	Speed/Duplex	Speed/Duplexing	Flow Co.	RX Usage	TX Usage	Details
1	<input type="text"/>	Ethernet...	Down	Down	Auto	<input type="checkbox"/>	0	0	
2	<input type="text"/>	Ethernet...	Down	Down	Auto	<input type="checkbox"/>	0	0	
3	<input type="text"/>	Ethernet...	Down	Down	Auto	<input type="checkbox"/>	0	0	
4	<input type="text"/>	Ethernet...	UP	100M Full	Auto	<input type="checkbox"/>	0	0	
5	<input type="text"/>	Optical...	Down	Down	Auto	<input type="checkbox"/>	0	0	
6	<input type="text"/>	Optical...	Down	Down	Auto	<input type="checkbox"/>	0	0	
7	<input type="text"/>	Optical...	Down	Down	Auto	<input type="checkbox"/>	0	0	

OK

Refresh

Table 4-1 Description of the port parameters

Parameter	Description
Port	Displays all ports of the switch.
Description	Enter the description of the port. The description cannot exceed 16 characters. Only numbers, letters and the following special characters are allowed: . _ -. The first character must be a letter and the last character must not be a special character.
Media Type	Displays two kinds of media type, includes two types: Copper and Fiber . <ul style="list-style-type: none">● Copper: Ethernet port.● Fiber: Optical port.

Parameter	Description
Link status	Includes two statuses: Up and Down . <ul style="list-style-type: none"> Up: The port is connected. Down: The port is not connected or the connection fails.
Speed/Duplexing status	<ul style="list-style-type: none"> 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.
Details	<ul style="list-style-type: none"> View the total RX and total TX of each port. You can refresh or clear the detailed information of each port. View the number of error bytes.

Step 3 Click **OK**.

4.2 Configuring EEE

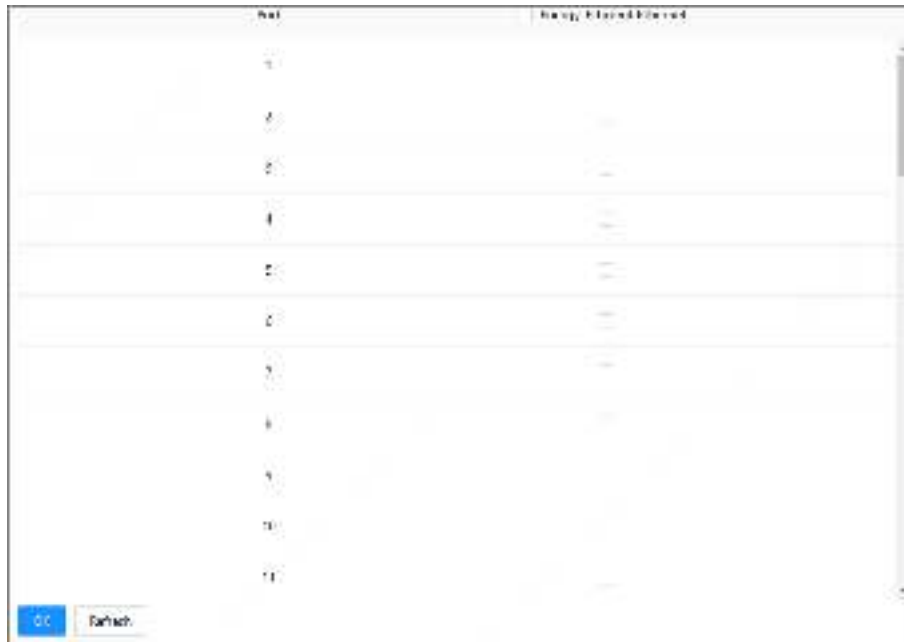
Enable the EEE (Energy-Efficient Ethernet) function.

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 4-2 EEE function



4.3 Configuring VLAN

4.3.1 VLAN Definition

Logically, one LAN (Local Area Network) can be divided into many subsets. Each subset has its own broadcast area: virtual LAN (VLAN). A VLAN is divided from a LAN on a logical basis rather than on a physical basis, to realize the isolated broadcast area in the VLAN.

4.3.2 VLAN Function

- Enhance the network performance. The broadcast packets are in the VLAN, which can effectively control the network broadcast storm, reduce network bandwidth and enhance network processing ability.
- Enhance the network security. The switches in different VLANs cannot access each other, and the hosts in different VLAN cannot communicate with each other. They need a router or the three-layer switch to forward the message.
- Simplify the network management. The host of the same virtual working group is not limited in one physical area, which can simplify the network management and facilitate to establish working groups for users in different areas.

4.3.3 Port-based VLAN

The port types include **Access**, **Trunk** and **Hybrid**.

- Access: The port belongs to one VLAN, and is used to connect to the computer port.
- Trunk: The port allows multiple VLANs to pass, to receive and send messages of multiple VLANs, and is used to connect between the switches.
- Hybrid: The port allows multiple VLANs to pass, to receive and send messages of multiple VLANs, and is used to connect between the switches, and connect the computer.

4.3.4 Adding VLAN

Background Information

You can add the port to the VLAN. The VLAN is VLAN1 by default.

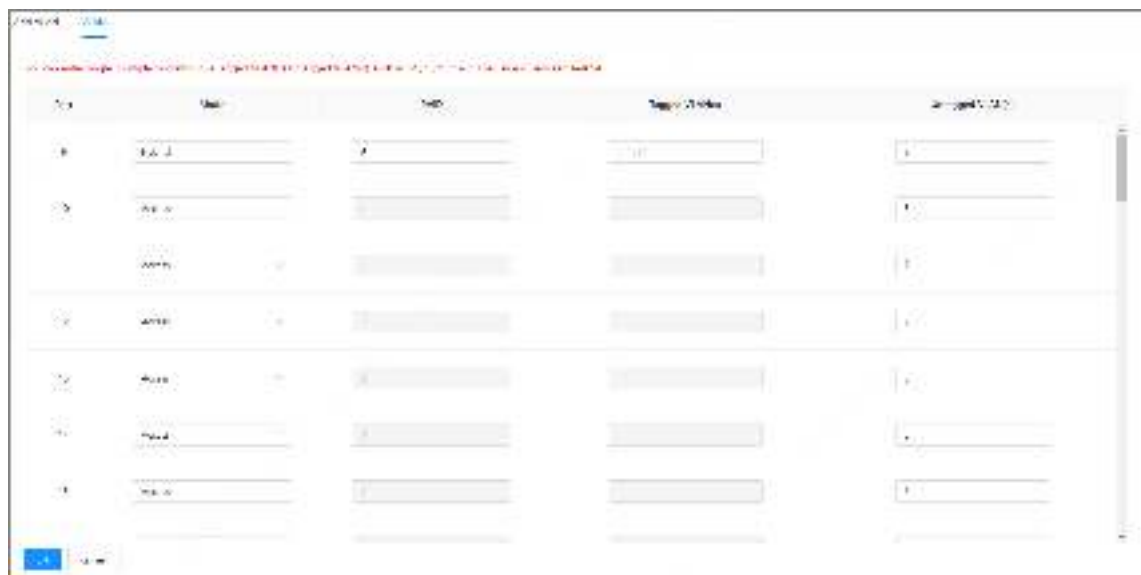


Port isolation and VLAN cannot be enabled at the same time. If one of them is enabled, the other one will be automatically disabled. Please be advised.

Procedure

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

Figure 4-3 VLAN setting



Step 2 On the **Add VLAN** page, click **Add**, enter the **VLAN ID** and **Description**.

Figure 4-4 Add VLAN

Add VLAN

VLAN ID

(1-4094)

Description

It can contain up to 64 characters, and can only consist of numbers, letters and underscores.

Cancel

OK

Step 3 Click **OK**.



VLAN1 cannot be deleted.

Related Operations

- Click to edit VLAN.
- Click to delete VLAN.

4.3.5 Configuring Port VLAN

You can configure the port VLAN parameters.

Figure 4-5 Configure VLAN

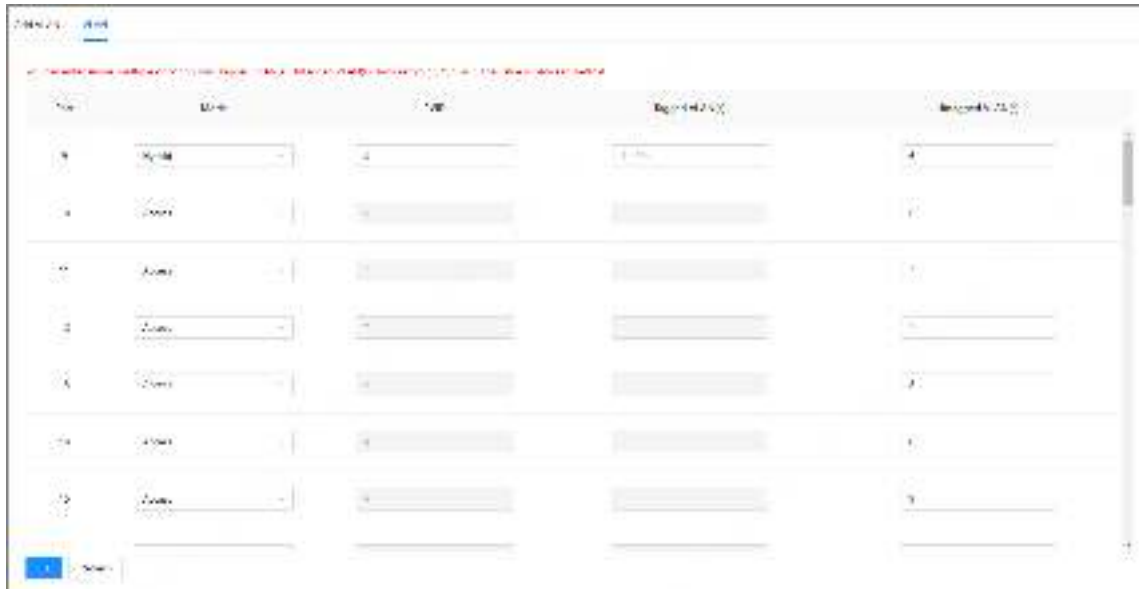


Table 4-2 Port VLAN configuration parameter

Parameter	Description
Port	Displays all ports of the switch.
Mode	Includes three modes: Access , Hybrid , and Trunk . <ul style="list-style-type: none">● Access: Belongs to one VLAN. Commonly used to connect computer ports.● Trunk: Allows multiple VLANs through. Receives and sends multiple VLAN packets. Typically used for connection between switches.● Hybrid: Allow multiple VLANs through. Receives and sends multiple VLAN packets. Used for connection between switches, or switch and computer.
Tagged VLAN(s)	Set the VLAN ID for the port that is allowed to be tagged when sending packets.
Untagged VLAN(s)	Set the VLAN ID for the port that is allowed to be untagged when sending 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.	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Adds a tag with the default VLAN ID to an untagged frame and accepts the frame if the interface permits the default VLAN ID. Adds a tag with the default VLAN ID to an untagged frame and discards the frame if the interface denies the default VLAN ID. 	<ul style="list-style-type: none"> Accepts a tagged frame if the VLAN ID carried in the frame is permitted by the interface. Discards a tagged frame if the VLAN ID carried in the frame is denied by the interface. 	<ul style="list-style-type: none"> If the frame's VLAN ID matches the default VLAN ID and the VLAN ID is permitted by the interface, 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 interface, the frame is transmitted. The interface can be configured whether to transmit frames with tags.

4.4 Configuring VLANIF

Background Information

A VLANIF interface is a Layer 3 logical interface most commonly used to implement Layer 3 communication between hosts in different VLANs across different network segments.

Each VLANIF interface corresponds to a VLAN. After an IP address is configured for a VLANIF interface, the VLANIF interface becomes the gateway of the user hosts within that VLAN and forwards packets across network segments at Layer 3.

Procedure

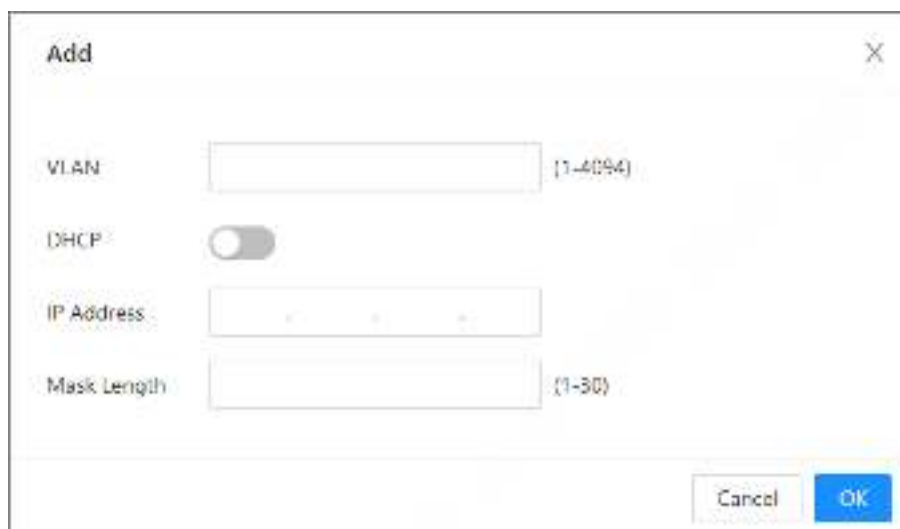
Step 1 Select **Network Settings > VLANIF**.

Step 2 Click **Add**, input **VLAN** number, and then enable **DHCP** for the port with **Mode** as **Dynamic**.



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

Figure 4-6 Add VLANIF

A dialog box titled "Add" with a close button (X) in the top right corner. It contains four input fields: "VLAN" with a range of (1-4094), "DHCP" with a toggle switch, "IP Address" with a dotted separator, and "Mask Length" with a range of (1-30). At the bottom right are "Cancel" and "OK" buttons.

Add

VLAN (1-4094)

DHCP ☐

IP Address . . .

Mask Length (1-30)

Cancel OK

Related Operations

- Delete the VLANIF: Select the VLAN, and then click **Delete** or .
- Refresh the parameter: Click **Refresh** to refresh the VLAN parameters.

4.5 Configuring IP and Routing

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

Procedure

- Step 1 Select **Network Settings** > **IP & Routing**.
- Step 2 On the **Routing Settings** tab, click **Add**, and then configure the parameters.



Some models only support default routing. Refer to the actual product.

Figure 4-7 Routing settings

A dialog box titled "Add" with a close button (X) in the top right corner. It contains three input fields: "Network" with a dotted separator, "Mask Length" with a range of (1-30), and "Next Hop" with a dotted separator. At the bottom right are "Cancel" and "OK" buttons.

Add

Network . . .

Mask Length (1-30)


Next Hop . . .

Cancel OK

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 segment to identify the destination switch or router with the destination address.
Next Hop	Set the next hop address of the router.

Related Operations

- Delete the routing: Select the VLAN and routing, and then click **Delete** or .
- Refresh the parameter: Click **Refresh** to refresh the parameters of the routing.

4.6 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, may produce loops, causing broadcast storms and rendering the MAC address table unstable. As a result, communication quality deteriorates, and communication services may 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.

4.6.1 ERPS Settings

Procedure

- Step 1 Select **Network Settings** > **ERPS**.
- Step 2 On the **ERPS** tab, click **Add** to add ERPS.
- Step 3 Configure the parameters, and then click **OK**.

Figure 4-8 Add ERPS

Table 4-5 Parameter description

Parameter	Description
ERPS ID	The ID number of the ERPS.
Port 0	Two ports of the switch to be added into the ERPS.
Port 1	
Port 0 APS MEP	<ul style="list-style-type: none"> • BPDU MEP of the ERPS port. • Link monitoring MEP of the ERPS port. Port 0 APS MEP keeps the same as Port 0 SF MEP. Port 1 APS MEP keeps the same as Port 1 SF MEP.
Port 1 APS MEP	
Port 0 SF MEP	
Port 1 SF MEP	

4.6.2 MEP Settings

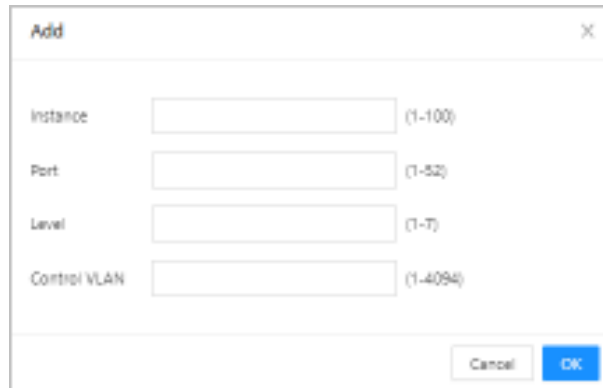
Background Information

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 two ports on each node can be added to the same ERPS ring.

Procedure

- Step 1 Select **Network Settings** > **ERPS**.
- Step 2 On the **MEP** tab, click **Add** to add MEP.
- Step 3 Configure MEP parameters.
- Step 4 Click **ok**.

Figure 4-9 Add MEP



The 'Add' dialog box contains four input fields with their respective ranges:

- Instance: [] (1-100)
- Port: [] (1-52)
- Level: [] (1-7)
- Control VLAN: [] (1-4094)

At the bottom right, there are 'Cancel' and 'OK' buttons.

Table 4-6 MEP parameter description

Parameter	Description
Instance	The number of the MEP instance.
Port	The port number of MEP.
Level	Maintenance level. We recommend setting as 0.
Control VLAN	The ID of the control VLAN in a SEP segment.

4.7 Configuring IGMP Snooping

Background Information

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 the forwarding rate will be decreased.



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

- Step 4** Click **OK** .

4.8 Configuring STP

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

STP, RSTP, and MSTP 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.
- MSTP: A virtual VLAN mapping table in which VLAN IDs are associated with spanning tree instances. Not only this, MSTP divides a switching network into multiple regions, each of which has multiple spanning tree instances that are mutually independent. Unlike STP and RSTP, MSTP provides multiple redundant paths for data forwarding. In addition, it implements load balancing among VLANs.

4.8.1 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 Working Mode.
- Step 4** Click **Advanced**, and then configure the advanced parameters.

Figure 4-10 Configure STP

STP Part Instance

STP ☒

Working Mode: RSTP

Max Aging Time: 20 (1-100)

Forwarding Delay Time: 15 (4-30)

Bridge Priority: 0 (0-65535)

OK Refresh

Table 4-7 Description of the advanced parameters

Parameter	Description
STP	The basic spanning tree protocol.
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.

4.8.2 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 4-11 Port instance



Table 4-8 Parameter 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.

4.9 Configuring Link Aggregation

Background Information

Link aggregation is to form a multiple physical ports of the switch 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.



- The link aggregation is mutually exclusive with STP mode, IGMP Snooping, and 802.1x mode. When STP mode is enabled, link aggregation cannot be configured. You must disable STP mode before configuring link aggregation.
- We do not recommend implementing configuration and advanced functions for the ports which are used for link aggregation.
- Link aggregation can be divided into static aggregation and LACP. Generally, the peer devices with the switch link aggregation are switch and network adapter.
- Only the ports with the same speed rate, duplex, long distance and VLAN configuration can be in the one aggregation group.

Procedure

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

Step 2 Click **Add**.

Step 3 Select the **Aggregation Group No.**.

Step 4 Select the **Aggregation Group Mode**, and then click **OK**.

Aggregation group mode includes static, LACP active, and LACP passive.

- Static: Static is also known as manual mode. The Eth-Trunk interface must be manually created and member interfaces need to be manually added. The LACP protocol is disabled.
- LACP active: The Eth-Trunk interface must be manually created and member interfaces need to be manually added. Compared with static, the selection of interface is configured by LACP protocol. This mode places an interface in an active negotiating state. In this mode, the interface initiates negotiations with other interfaces by sending LACPDU.
- LACP passive: The Eth-Trunk interfaces are created and member interfaces are added by LACP protocol. This mode places an interface in a passive negotiating state. In this mode, the interface responds to the LACPDUs that it receives but does not initiate LACPDU negotiation.

Step 5 Select ports to be added, and then click **OK**.

Step 6 Set the **Operational Key**.



- You can only configure link aggregation when the **Aggregation Group Mode** is set as LACP.
- The value ranges from 1 to 65535.

Step 7 Select the **Timeout** from **Long Timeout** or **Short Timeout**.

Step 8 Click **OK**.

Figure 4-12 Link aggregation



4.10 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.

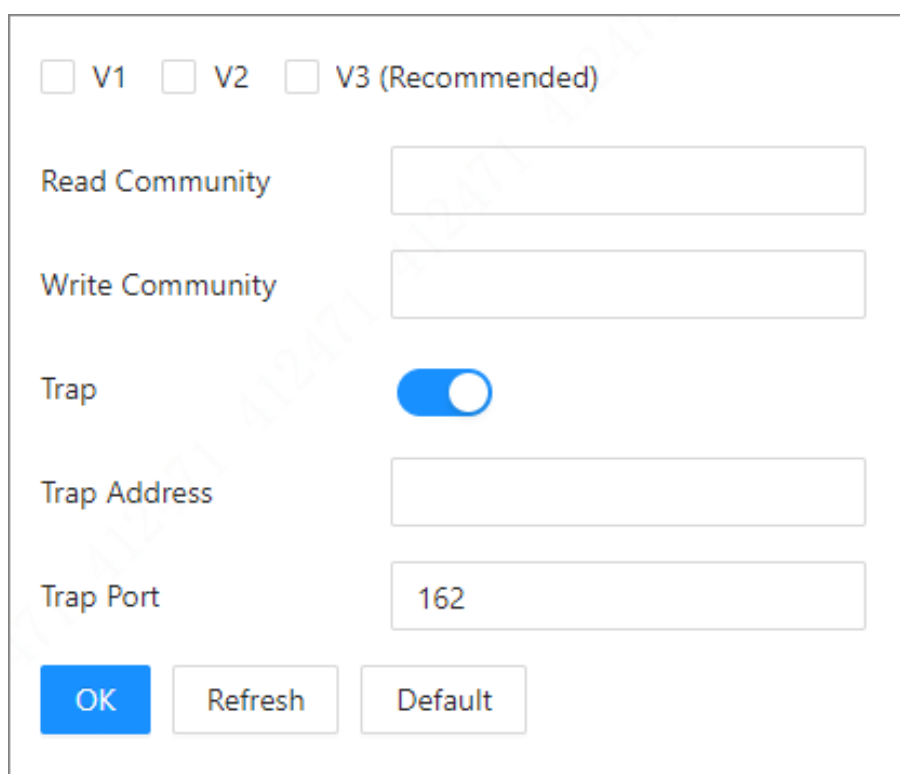
- NMS (Network Management System) is the manager in SNMP network, and it provides friendly human-machine interface to help the network administrator to finish most of the network management work.
- Agent is the managed role in SNMP network, and it receives and handles the request packet from NMS. In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

4.10.1 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 4-13 SNMP



The image shows a configuration window for SNMP. At the top, there are three radio buttons: ☐ V1, ☐ V2, and ☐ V3 (Recommended). Below these are two text input fields: 'Read Community' and 'Write Community'. The 'Trap' option is a toggle switch that is currently turned on (blue). Below the toggle is a 'Trap Address' text input field. At the bottom, there is a 'Trap Port' text input field containing the value '162'. At the very bottom of the window are three buttons: 'OK' (highlighted in blue), 'Refresh', and 'Default'.

Step 4 Click **OK**.

4.10.2 Configuring SNMP V3

Procedure

- Step 1 Select **Network Settings > SNMP**.
- Step 2 Select **V3**.
- Step 3 Configure parameters.

Figure 4-14 SNMP V3

The image shows a configuration window for SNMP V3. At the top, there are three radio buttons: V1, V2, and V3 (Recommended), with V3 selected. Below this, there are several configuration options:

- Read Community**: A text input field.
- Write Community**: A text input field.
- Trap**: A toggle switch, currently turned off.
- Read-Only Username**: A text input field containing the value "public".
- Authentication Type**: Two radio buttons, MD5 (selected) and SHA.
- Authentication Password**: A password input field with masked characters.
- Encryption Type**: Two radio buttons, CBC-DES (selected) and CFB-AES.
- Encryption Password**: A password input field with masked characters.
- Read/Write Username**: A text input field containing the value "private".
- Authentication Type**: Two radio buttons, MD5 (selected) and SHA.
- Authentication Password**: A password input field with masked characters.
- Encryption Type**: Two radio buttons, CBC-DES (selected) and CFB-AES.
- Encryption Password**: A password input field with masked characters.

At the bottom of the window, there are three buttons: OK, Refresh, and Default.

Table 4-9 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.

Parameter	Description
Encryption type	Set encryption mode when the authentication mode is Authentication and encryption .
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**.

4.11 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.

4.11.1 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 4-15 Add MAC table

Related Operations

Figure 4-16 related operations



- Delete static MAC address: Select a MAC, and then click **Delete**.
- Refresh the MAC address list: Click **Refresh** or enable **Auto Refresh**.
- 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**.

4.11.2 Filtering Port MAC

Background Information

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

- Devices in 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 4-17 MAC filtering



4.12 Configuring LLDP

Background Information

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 4-18 LLDP remote device



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 switches do not support this function.
- Only some models of PoE switches 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

Select **PoE Management** > **PoE Settings**. You can configure power settings, power status, port status and control.

Procedure


- Step 1 In **Power Settings**, you can view the total power of the 4 ports, and configure reserved power and alert power.
- Step 2 In **Power Status**, you can view consumed power, remaining power and reserved power.
- Step 3 In **Port Status and Control**, select from the list below the **PoE Management** to enable or disable PoE of the corresponding port.
- Step 4 Click **OK**.

Figure 5-1 PoE settings




Table 5-1 Description of PoE parameters

Parameter		Description
Power settings	Total power	Displays the total PoE power.
	Reserved power	Configure the reserved PoE power.
	Alert Power	Configures the alert PoE power.
Power status	Consumed power	Displays the current PoE power consumed by all ports.
	Remaining power	Displays the current remaining PoE power.
	Reserved power	Unusable PoE power. Reserved power = total power – overload 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	<p>Select from Enable and Disable.</p> <ul style="list-style-type: none"> When selecting the Disable, the system does not supply power to the PD or reserve power for the PD. When selecting the Enable, the PoE port will not result in PoE power overload. Otherwise, you are not allowed to enable PoE for the PoE port.  <ul style="list-style-type: none"> 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.

5.2 Configuring Perpetual PoE

Procedure

- Step 1 Select **PoE Management** > **Perpetual PoE**.
- Step 2 Click  to enable **Global Enable**.
- Step 3 Click **OK** to save the configuration.

5.3 Configuring Long Distance PoE

Background Information

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 100 Mbps to 10 Mbps.



In Extend Mode, the transmission distance of the PoE port is up to 250 m but the transmission rate drops to 10 Mbps. The actual transmission distance might vary due to power consumption of connected devices or the cable type and status.

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 disconnect	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

Background Information

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

Procedure

- Step 1 Select **PoE Management** > **Green PoE**.
- Step 2 Add **Start Time** and **End Time**.
- Step 3 Select the port, and then click ☐ to enable the green PoE.
- Step 4 Click **OK**.

Figure 5-3 Green PoE

5.6 Configuring Force PoE

Background Information



After force PoE is enabled, the port will force power supply to the powered device, whether or not the device connected to the port meets the requirements. Please be advised.

Procedure

- Step 1 Select **PoE Management** > **Force PoE**.
- Step 2 Click ☐ of the corresponding port to enable force PoE.
- Step 3 Click **OK**.

Figure 5-4 Force PoE



5.7 Configuring PoE Watchdog

Background Information

With PoE watchdog enabled, you can monitor PD and keep it online, and check the status of PD devices every 60 s. If there is no data transmission, the PoE port will be automatically powered off and restarted.



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.

Step 3 Click **OK**.

Figure 5-5 PoE watchdog



Type	PoE Watchdog
1	...
2	...
3	...
4	...

6 Security

6.1 Basic Services

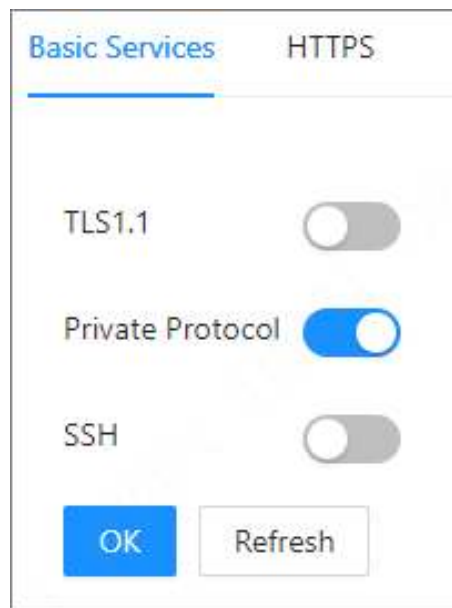
6.1.1 Configuring Basic Services

The secure transport layer protocol (TLS) is used to guarantee confidentiality and data integrity between two communication applications. This protocol consists of two layers: TLS Record and TLS Handshake. TLS1.1 uses a weak encryption algorithm. We recommend you disable it.

A private protocol is an unpublished protocol. We recommend you disable it.

SSH and Secure Shell are security protocols based on the application layer. 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.

Figure 6-1 Basic services




6.1.2 Configuring HTTPS

Background Information

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 must use TLS1.1, you must enable TLS1.1 on the webpage. Please be advised that TLS1.1 poses security risks. We recommend you disable TLS1.1 to avoid unexpected risks.

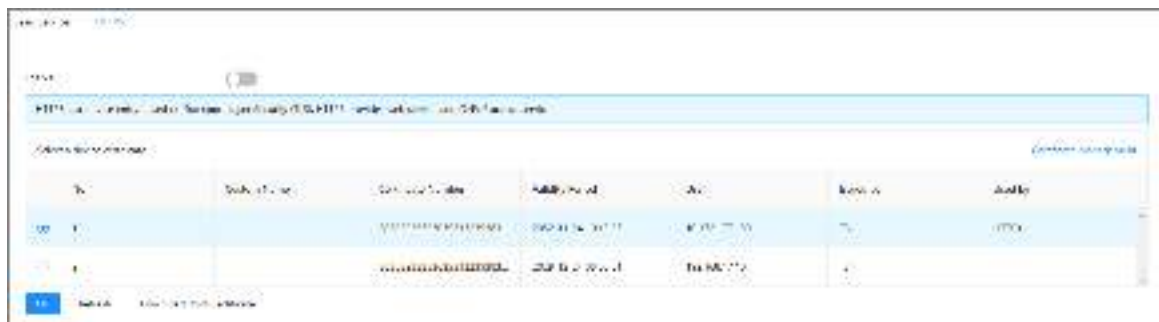
- Step 3 On the **HTTPS** tab, click ☐ to enable HTTPS.
- Step 4 Select a device certificate.
- Step 5 Select **Certificate Management** and the page will turn to **CA Certificate** page.



For details, see "6.2 Configuring CA Certificate".

- Step 6 Click **OK**.

Figure 6-2 Configure HTTPS



6.2 Configuring CA Certificate

6.2.1 Installing Device Certificate

Background Information

A device certificate is a proof of device legal status. For example, when the browser is visiting device via 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 6-3 Select installation mode

Step 1: Select installation mode.

☐ Create Certificate

Fill in certificate information, and the device will create and issue the certificate.

☒ Apply for CA Certificate and Import (Recommended)

After you fill in certificate information, the device will generate a certificate request file. Please submit the file to a CA institute to apply for a signature and certificate, and then import them into the device.

☐ Install Existing Certificate

If you already have a certificate and private key file, please import the certificate and private key file in this way.

Next **Cancel**



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 6-4 Edit certificate

ID	Custom Name	Certificate Name	Serial Number	Issued	Revoked	Validity	Authority	Private Key File	Public Key File	View
1		XXXXXXXXXX	2014/12/01	2014/12/05	0	10	HTTP	Private	Public	View

Related Operations

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

6.2.2 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 support installing subordinate CA certificate.

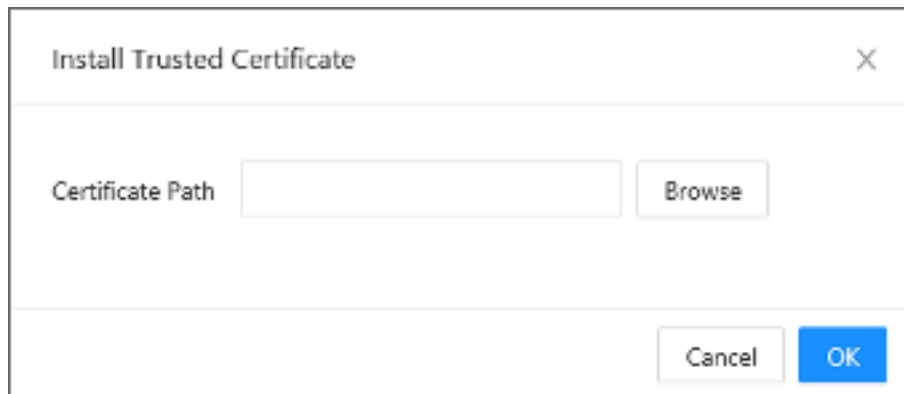
Procedure

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 6-5 Install Trusted Certificate





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

Figure 6-6 Edit certificate

Pos	System Name	Localhost Name	Public Name	Unit	Interface	Availib	Localhost IP	Availib IP	Version
		192.168.1.1	192.168.1.1	1	1		192.168.1.1	192.168.1.1	1.0

Related Operations

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

6.3 Configuring Attack Defense

6.3.1 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 6-7 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 6-8 Add to blocklist

Table 6-1 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.

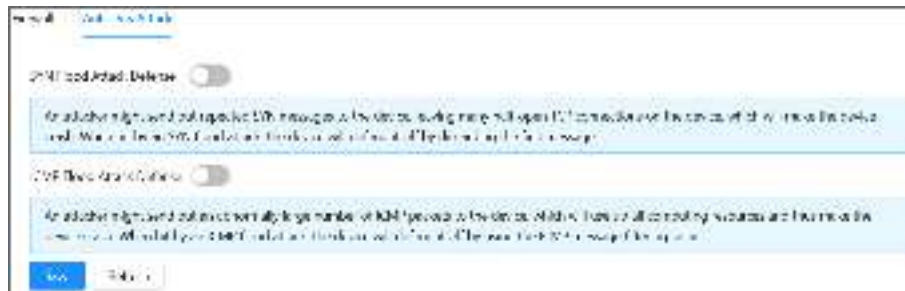
Step 3 Click **OK**.

6.3.2 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 6-9 Anti-DoS attack



6.4 Configuring Port Isolation

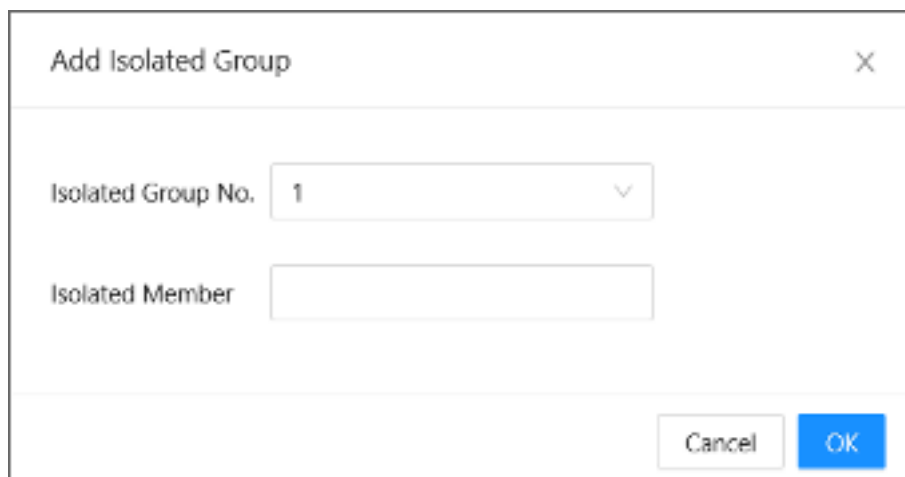
Background Information

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 6-10 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 .

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 from the **Priority** and **Trust Mode**.



Trust mode includes 4 types of **Untrust**, **802.1P**, **DSCP**, and **DSCP & 802.1P**.

Step 3 Click **OK**.

Figure 7-1 Configure port priority

Port	Priority	Trust Mode
1	3	Untrust
2	3	Untrust
3	3	Untrust
4	3	Untrust
5	3	Untrust
6	3	Untrust
7	3	Untrust

7.2 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 7-2 Priority mapping



7.3 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**.

Location	Station 2 (left)	ST	SL	SO	SE	SH	SH	SH	SH	SH	Open Line
		ST	SL	SO	SE	SH	SH	SH	SH	SH	
1	ST										Y
2	ST										Z
3	ST										Z
4	ST										X
5	ST										Y
6	ST										Y
7	ST										Z
8	ST										X
9	ST										X
10	ST										Y
11	ST										Z

10 of 10 rows

Procedure

- Figure 7-4 Add port speed limit

Add Port Speed Limit

Interface

Direction

QoS Kbps Range: 1K - 100000

Cancel OK

-

-

- The input rule for CIR: Range from 16 to 100000, and must be an integer multiple of 16.

- ## Background Information

47

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 7-5 Add storm control

A screenshot of a Windows-style dialog box titled "Add Storm Control". The dialog box contains four labeled input fields: "Port", "Type", "Speed", and "Limit". The "Speed" field has a value of "1000000" and a unit selector showing "(10-1000000)". The "Limit" field has a value of "kbits". At the bottom right of the dialog box are two buttons: "Cancel" and "OK".

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

Step 4 Click **OK**.

8 Authentication

8.1 Configuring 802.1x

Background Information

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

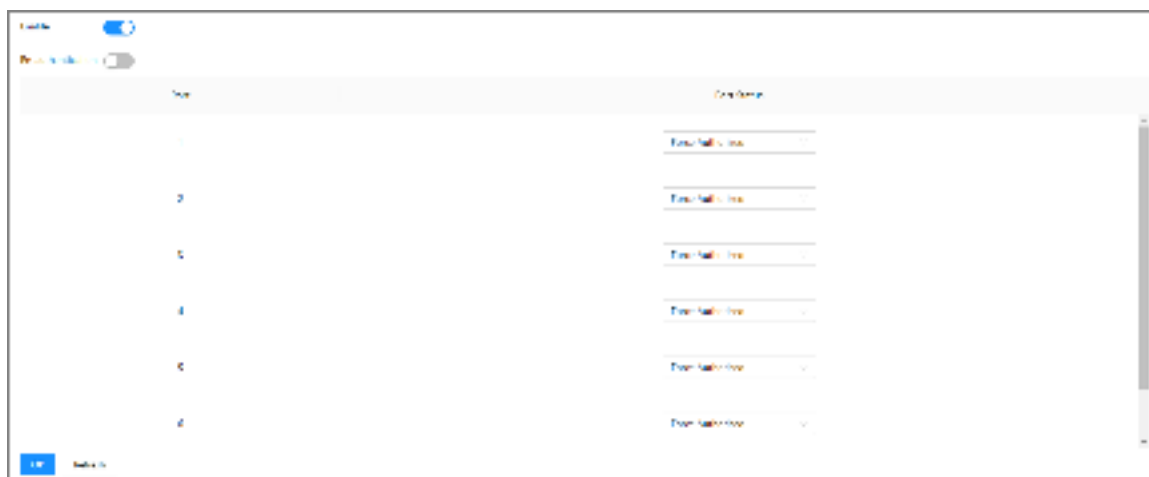


Table 8-1 Description of 802.1x

Parameter	Description
Auto	The port automatically configure status according to the authentication results.
Force unAuthorized	<ul style="list-style-type: none">• 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).

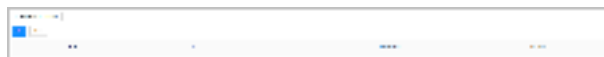
RADIUS is an information interaction protocol of distributed and C/S construction. It can protect the network from unauthorized visits. It is used in the network that allows remote visits but requests the higher security. It defines the RADIUS packet format and the message transmission mechanism. It 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 **key**.

Step 4 Click **OK**.

Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. Use Strong 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; character types include 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 overlapped characters, such as 111, aaa, etc.

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. Physical Protection

We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

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

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.