

Ethernet Switch (Managed Switch)

Web Operation Manual








V1.0.0

Foreword

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.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	December 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 Initialization and Login.....	1
2 Status Display.....	3
2.1 Viewing the Device Information.....	3
2.2 Viewing the Port Information.....	3
2.3 Viewing the IPC and NVR Information.....	6
3 Quick Config.....	7
3.1 Configuring General Parameters.....	7
3.2 Configuring VLAN.....	8
3.3 Configuring Link Aggregation.....	10
3.3.1 Configuring Static Aggregation.....	10
3.3.2 Configuring Dynamic Aggregation.....	11
3.4 Viewing the IPC and NVR Information.....	12
3.5 Configuring the IP and Routing.....	13
4 Maintenance.....	15
4.1 Restarting the Device.....	15
4.2 Restoring to Factory Defaults.....	15
4.3 Managing Configuration Files.....	15
4.4 Updating the System.....	15
4.5 Managing the Logs.....	16
4.6 Managing the System Time.....	16
4.7 Configuring the Mirroring.....	17
4.8 Ping.....	18
4.9 iLinksView.....	19
4.9.1 Enabling iLinksView.....	19
4.9.2 Uploading Network Management Configuration Files.....	20
4.9.3 Exporting Network Management Configuration Files.....	20
4.10 Viewing Legal Information.....	20
5 Network Settings.....	21
5.1 Configuring Ports.....	21
5.2 Configuring VLANs.....	22
5.3 Configuring Link Aggregation.....	24
5.4 Configuring MAC.....	25
5.4.1 Adding the MAC Table.....	25
5.4.2 Filtering the Port MAC.....	26
5.5 Configuring STP.....	27
5.6 Configuring Long Distance PoE.....	28

5.7	Configuring PoE.....	28
5.7.1	Configuring PoE Settings.....	28
5.7.2	Configuring Green PoE.....	29
5.7.3	Configuring Force PoE.....	31
5.7.4	Configuring PoE Watchdog.....	31
5.7.5	Viewing PoE Event Statistics.....	32
5.8	Loopback Detection.....	32
5.9	Configuring ERPS.....	33
5.9.1	ERPS Settings.....	33
5.9.2	MEP Settings.....	34
5.9.3	Example of Single-Ring Configuration in ERPS.....	35
5.10	Configuring IGMP Snooping.....	40
5.11	Configuring IP and Routing.....	41
5.12	Configuring ARP.....	41
5.13	Configuring DHCP.....	42
5.14	Configuring DHCP Relay.....	45
5.15	Configuring LLDP.....	45
5.15.1	LLDP Settings.....	46
5.15.2	Viewing LLDP Remote Devices.....	46
5.16	Configuring RS-485 Pass-Through.....	47
5.17	Configuring SNMP Protocol.....	48
5.17.1	Configuring SNMP V1 and V2.....	48
5.17.2	Configuring SNMP V3.....	49
6	Security.....	51
6.1	Configuring Accounts.....	51
6.2	Configuring Login Mode.....	51
6.3	Configuring RADIUS.....	52
6.3.1	Configuring DNS.....	52
6.3.2	Adding RADIUS Servers.....	53
7	Control Policy.....	55
7.1	Managing ACL.....	55
7.1.1	Configuring ACL.....	55
7.1.2	Applying ACL Rules.....	56
7.2	Configuring QoS.....	57
7.2.1	Configuring Port Classification.....	57
7.2.2	Configuring Scheduling.....	58
7.2.3	Configuring Port Shaping.....	59
7.2.4	Configuring DSCP-Based.....	59
7.2.5	Configuring Storm Control.....	60
Appendix 1	Security Recommendation.....	62

1 Initialization and Login

When you turn on the device for the first time, you need to set the login password for the administrators.

Prerequisites

Make sure that the IP addresses of the computer and the device are on the same segment.

Procedure

- Step 1 Open the browser, enter the IP address of the device in the address bar, and then press the Enter key.



The default IP address is 192.168.1.110.

- Step 2 Enter the username and password.

- Step 3 Select the language and then click **Next**.

Figure 1-1 Language

- Step 4 Select the time zone and then click **Next**.

- Step 5 View the legal information and then click **Next**.

- Step 6 Set the password for the administrators and confirm the password, and then click **OK**.



The password must consist of 8 to 32 non-blank characters and contain at least 2 types of characters among numbers, letters, and special characters (except "'", '"', ";", ":", and "&"). Configure a high security password according to the prompt of password strength.

Figure 1-2 Configure the password

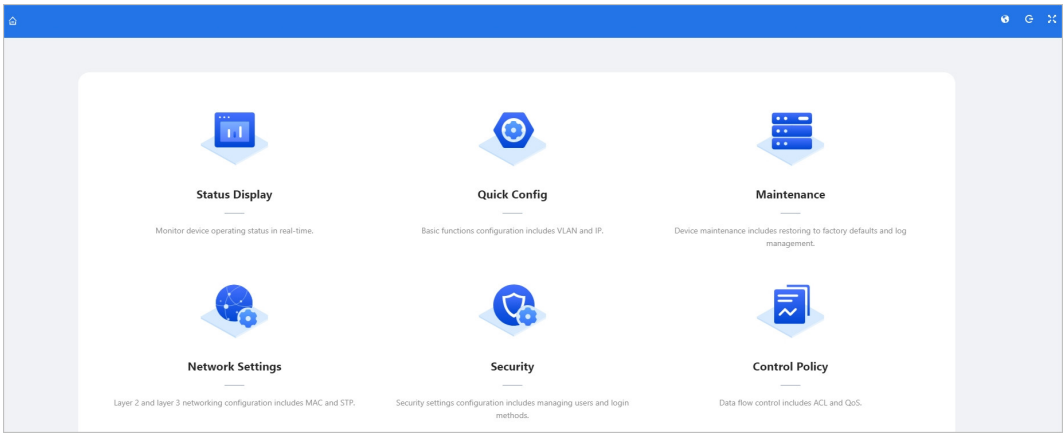
- Step 7 Enter the username and password, and then click **Login**.

The top of the page integrates quick operation functions, including returning to home

page , switching system language , logging out  and full screen . The center

of the home page includes 6 major sections. Click one of the icon to quickly go to the detailed configuration of each function.

Figure 1-3 Home page



2 Status Display

View the running status of the device, including the device information and the port information.

2.1 Viewing the Device Information

View the basic information about the device, including system, software, hardware, and time.

Procedure

Step 1 Select **Status Display** > **Device Info**.

Step 2 View the basic information about the device.

- System information includes the device name, the device model, the IP address and the mask length.
- Software information includes the software version and the complete date.
- Hardware information includes the MAC address and the SN.
- Time information includes the system time and operation time.

2.2 Viewing the Port Information

View the port information of the device, including port mode, link status, flow control status, speed/duplexing, VLAN, PoE, RX usage, TX usage, and media type.

Procedure

Step 1 Select **Status Display** > **Port Info**.

Step 2 View the port information of the device.

- The port graphic is displayed in green, indicating that the port has been successfully connected.
- The port graphic is displayed in grey, indicating that the port is not connected or the connection fails.



Hover over the port graphic to display the serial number of the port.






The total number of ports on different models of devices varies. Please refer to the actual situation.

Figure 2-1 Port information



Port	Port Mode	Link Status	Flow Control Status	Speed/Duplexing	VLAN	PoE	RX Usage	TX Usage	Media Type
1	Access	Up	Off	1G Full	1	0w	0.1%	0%	Copper
2	Access	Down	Off	Down	1	0w	0%	0%	Copper
3	Access	Down	Off	Down	1	0w	0%	0%	Copper
4	Access	Down	Off	Down	1	0w	0%	0%	Copper
5	Access	Down	Off	Down	1	0w	0%	0%	Copper
6	Access	Down	Off	Down	1	0w	0%	0%	Copper
7	Access	Down	Off	Down	1	0w	0%	0%	Fiber
8	Access	Down	Off	Down	1	0w	0%	0%	Fiber
9	Access	Down	Off	Down	1	0w	0%	0%	Fiber
10	Access	Down	Off	Down	1	0w	0%	0%	Fiber

Table 2-1 Port information

Name	Description
Port Mode	<p>Includes 3 types: Access , Hybrid, and Trunk.</p> <ul style="list-style-type: none"> ● Access : The port of the switch used to connect to the terminal device (such as the user host), generally connected to the access link. The access port can only belong to one VLAN. The access port sends and receives data frames without VLAN tags (Untagged). ● Trunk : The switch is used to connect to the ports of other switches, usually connected to intermediate interconnection links. Trunk ports can carry data streams from multiple VLANs and send data frames with VLAN tags (Tagged). ● Hybrid : The switch can be connected to both user hosts and the ports of other switches. A hybrid port can belong to multiple VLANs at the same time and can be configured to send data frames without VLAN tags (Untagged) on some VLANs and send data frames with VLAN tags (Tagged) on other VLANs. <p> The Hybrid mode is available on select models.</p>
Link Status	<p>View the connection status of each switch port and other devices.</p> <ul style="list-style-type: none"> ● Up: The port is connected. ● Down: The port is not connected or the connection fails.
Flow Control Status	<p>Displays the actual negotiation status of flow control.</p> <ul style="list-style-type: none"> ● On: Successfully negotiated. ● Off: Negotiation failed. <p> You can select Network Settings > Port, and then enable or disable the flow control function.</p>

Name	Description
Speed/Duplexing	<p>Displays the speed and duplex status of the port.</p> <ul style="list-style-type: none"> ● Down: The port is not connected. ● Displays rate: The port is connected. Full means full duplex, which can receive and send at the same time, and the maximum throughput can reach double the rate. Half means half duplex, which can only receive or send.  <p>You can select Network Settings > Port, and then you can set the speed and duplex mode.</p>
VLAN	<p>Displays the VLAN to which the port belongs. By default, it is VLAN 1.</p>  <p>You can select Quick Config > VLAN or Network Settings > VLAN > VLAN, and then set the VLAN to which the port belongs.</p>
PoE	<p>Displays the PoE power consumption.</p>  <ul style="list-style-type: none"> ● Non-PoE devices do not support this function. ● The total number of ports on different models of devices varies. Please refer to the actual situation.
RX Usage	The value of the RX rate divided by the actual negotiated rate over a period of time (usually in 5 minutes).
TX Usage	The value of the TX rate over a period of time (usually in 5 minutes) divided by the actual negotiated rate.
Media Type	Displays the port type, including the optical port and the Ethernet port.

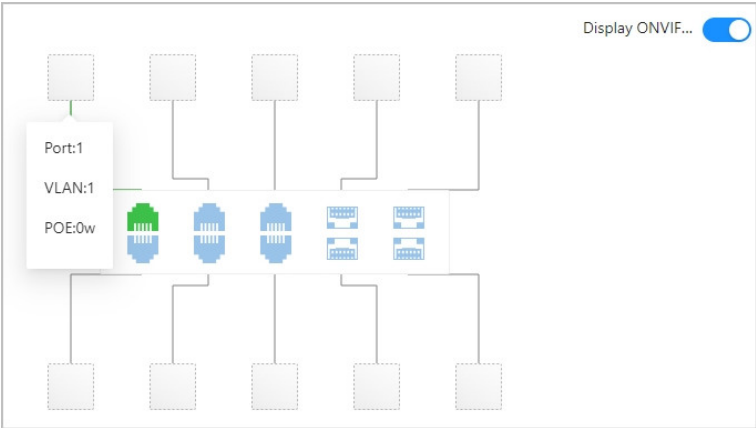
Related Operations

- Automatically refresh port information: Click  on the right of the **Auto Refresh**, enable automatic refresh function, and then the device updates the port information every 60 seconds.
- Display ONVIF devices: Click  on the right of the **Display ONVIF Devices**, and then the page displays devices connected to the switch through the ONVIF protocol. Move the mouse over the ONVIF device graphic to display its port, VLAN, and PoE power consumption information.



The function is available on select models. Please refer to the actual situation.

Figure 2-2 Display the ONVIF device



2.3 Viewing the IPC and NVR Information

Select **Status Display > IPC&NVR**, and then you can view the information of the front-end IPC, back-end NVR and other devices connected to the device.



The function is available on select models. Please refer to the actual situation.

Figure 2-3 View the information of IPC&NVR

IPC					
IP Address	MAC Address	Model	Port	VLAN	PoE
No Data					
NVR					
IP Address	MAC Address	Model	Port	VLAN	
No Data					
Other					
IP Address	MAC Address	Model	Port	VLAN	PoE

3 Quick Config

Quick Config integrates multiple basic functions, such as setting local information, VLAN, link aggregation and other functions.



- VLAN, link aggregation, IP and routing functions can also be configured through the **Network Settings**.
- The information of IPC&NVR can also be viewed through the **Display Status**.



The quick configuration page of different device models might be different. Please refer to the actual situation.


3.1 Configuring General Parameters

You can configure the device name, IP address and mask length of the device.

Procedure

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

Step 2 Configure the IP address.

- Manual Settings: Enter the IP address and mask length of the device.
- Auto Obtain: Click  on the right of the **DHCP**, enable the DHCP function, and then the device obtains an IP address from a DHCP server or router in the network.



- ◇ Please be advised that you can enable the DHCP function. Enabling this function will make it impossible to access the webpage using the manually set IP address.
- ◇ During the acquisition process, you cannot log in to the webpage. If the automatic acquisition fails to obtain an IP address within 60 seconds, the manually set IP address will continue to be used.

Figure 3-1 Configure the parameters

The screenshot shows a configuration form for a switch. At the top, there is a 'DHCP' toggle switch which is currently turned off. Below it is a 'Device Name' text input field containing the text 'SWITCH'. The next row contains an 'IP' address input field showing '192.168.1.1'. Below that is a 'Mask Length' input field with '24' and a range '(1-30)' to its right. The 'Manage VLAN' section has a blue toggle switch turned on. Below this is a 'VLAN' input field with '1' and a range '(1-4094)' to its right. At the bottom of the form are two buttons: a blue 'Save' button and a white 'Refresh' button with a grey border.

Step 3 Enter the device name.

Step 4 Enable **Manage VLAN** and set the VLAN number.



- **Manage VLAN** is enabled by default. The default management VLAN is VLAN1. You cannot log in to the webpage through ports other than the management VLAN. Modify the management VLAN if necessary.
- Disable **Manage VLAN**, and then the device will not be accessible through ConfigTool or iLinkview.

Step 5 Click **Save**.

3.2 Configuring VLAN

You can set the port mode, add the port to a VLAN, and set the allowed VLAN.

Procedure

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


Step 2 Configure the **Mode**, **Port to VLAN** and **Allowed VLAN**.


Figure 3-2 Configure the VLAN

Port	Mode	Port to VLAN	Allowed VLAN
1	Access	1	1
2	Access	1	1
3	Access	1	1
4	Access	1	1
5	Access	1	1
6	Access	1	1
7	Access	1	1

Save Refresh

Table 3-1 VLAN parameter description

Parameter	Description
Port	Displays all ports of the device.
Mode	<p>Configure port type, including 3 types: Access , Hybrid and Trunk.</p> <ul style="list-style-type: none"> ● Access : The port of the switch used to connect to the terminal device (such as the user host), generally connected to the access link. The access port can only belong to one VLAN. The access port sends and receives data frames without VLAN tags (Untagged). ● Hybrid : The switch can be connected both user hosts and the ports of other switches. A hybrid port can belong to multiple VLANs at the same time and can be configured to send data frames without VLAN tags (Untagged) on some VLANs and send data frames with VLAN tags (Tagged) on other VLANs. ● Trunk : The switch is used to connect to the ports of other switches, usually connected to intermediate interconnection links. Trunk ports can carry data streams from multiple VLANs and send data frames with VLAN tags (Tagged). <p> The Hybrid mode is available on select models.</p>
Port to VLAN	Add ports to the VLAN, and all ports belong to VLAN 1 by default. The range is from 1 through 4094.

Parameter	Description
Allowed VLAN	<p>Configure the allowed VLAN.</p> <p>Supports entering single digits, multiple consecutive or non-consecutive digits. For example:</p> <ul style="list-style-type: none"> • When you enter 2, it means creating VLAN2. • When you enter 2,5, it means creating VLAN2 and VLAN5. • When you enter 2-5, it means creating VLAN2, VLAN3, VLAN4 and VLAN5.  <p>When the mode is Trunk or Hybrid, it supports setting the allowed VLAN.</p>

Step 3 Click **Save**.

3.3 Configuring Link Aggregation

After setting the link aggregation, each member port in the same aggregation group can dynamically share communication traffic, improving bandwidth utilization and network performance. At the same time, ports in the same aggregation group back up each other, thereby enhancing link reliability.

Link aggregation includes static aggregation and dynamic aggregation.

- **Static Aggregation:** The administrator manually adds multiple ports to the same aggregation group. All member ports are in forwarding state, working together to share the load flow.
- **Dynamic Aggregation:** The connected devices exchange messages through LACPDU (Link Aggregation Control Protocol Data Unit) to exchange aggregation information. Based on the coordination results, ports that meet the criteria will be automatically aggregated for data transmission and reception. In this mode, the addition and deletion of ports in the aggregation group are automatically completed by the protocol, providing higher flexibility and effective load balancing capabilities.

3.3.1 Configuring Static Aggregation

Procedure

Step 1 Select **Quick Config** > **Link Aggregation**.

Step 2 Click **Add**, select **Aggregation Group No.** and **Aggregation Group Mode**, and then click **OK**.

Selection of aggregation group mode is **Static**.



Different models of devices support different numbers of static aggregation groups. Please refer to the actual situation.

Figure 3-3 Add the static aggregation

Step 3 Select ports to be added from above, and then click **OK**.

Figure 3-4 Select the port

<input type="checkbox"/>	Aggregation Group No.	Aggregation Group Mode	Port ID	Operation
<input type="checkbox"/>	2	Static	4,6	
<input type="checkbox"/>	1	Static		

Buttons: Add, Delete, Refresh

3.3.2 Configuring Dynamic Aggregation

Procedure

Step 1 Select **Quick Config** > **Link Aggregation**.

Step 2 Click **Add**, select **Aggregation Group No.** and **Aggregation Group Mode**, and then click **OK**.

- **Active** : This type of port sends LACPDU's periodically to discover and maintain aggregated links.
- **Passive** : This type of port does not actively initiate an aggregation request, but decides whether to participate in link aggregation based on the received LACPDU.

Figure 3-5 Add the dynamic aggregation (active)

The 'Add' dialog box contains two dropdown menus. The first dropdown, labeled 'Aggregation ...', has the value '1' selected. The second dropdown, also labeled 'Aggregation ...', has the value 'Active' selected. At the bottom right of the dialog are 'Cancel' and 'OK' buttons.

Step 3 Select ports to be added from above, and then click **OK**.

Figure 3-6 Select the port

The interface shows a selection area at the top with icons for different port types. Below this is a red instruction text: "Select ports to be added from above and click 'OK' to save." followed by 'OK' and 'Cancel' buttons. Below the instruction are 'Add' and 'Delete' buttons. A table lists aggregation groups:

<input type="checkbox"/>	Aggregation Group No.	Aggregation Group Mode	Port ID	Operation
<input type="checkbox"/>	2	Static	4,6	
<input type="checkbox"/>	1	Active		
<input type="checkbox"/>	1	Active		

At the bottom left is a 'Refresh' button.

3.4 Viewing the IPC and NVR Information

Select **Status Display** > **IPC&NVR**, and then you can view the information of the front-end IPC, back-end NVR and other devices connected to the device.



The function is available on select models. Please refer to the actual situation.

Figure 3-7 View the information of IPC&NVR

IPC					
IP Address	MAC Address	Model	Port	VLAN	PoE
No Data					
NVR					
IP Address	MAC Address	Model	Port	VLAN	
No Data					
Other					
IP Address	MAC Address	Model	Port	VLAN	PoE

3.5 Configuring the IP and Routing

Add the IP address of the VLAN and the route of the device.

Procedure

- Step 1 Select **Quick Config > IP & Routing**.
- Step 2 Click **Add** on the **IP Settings** tab, configure related parameters, and then click **OK**.

Figure 3-8 Add IP address of VLAN

Add

VLAN

(1-4094)

You can only access the webpage through the management VLAN. It is VLAN 1 by default. You can change the management VLAN if necessary.

IP Address

-

-

-


Mask Length

(1-30)

Cancel

OK

Table 3-2 Description of VLAN IP address parameters

Parameter	Description
VLAN	<p>Enter the number of VLAN.</p>  <p>The management VLAN is VLAN 1 by default. Except for the management VLAN, ports in other VLANs cannot log in to the WEB. If necessary, modify the management VLAN.</p>
IP Address	Configure the IP address and mask length of the VLAN.
Mask Length	

Step 3 Click **Add** on the **Routing Settings** tab, configure related parameters, and then click **OK**.



Different devices support different numbers of routes to be added. Please refer to the actual number.

Figure 3-9 Add the route



Table 3-3 Routing setting parameter description

Parameter	Description
Network	Enter the destination address or destination network used to identify the IP packet.
Mask Length	Set the mask length. Perform a "logical AND" operation on the destination address and mask/prefix length to get the address of the network segment where the destination host or router is located.
Next Hop	Set the next hop IP address of this route.

4 Maintenance

4.1 Restarting the Device

Procedure

Step 1 Select **Maintenance** > **Device Restart**.

Step 2 Click **Reboot Now**.

Step 3 Click **OK** in the pop-up window.

The device starts restarting.

4.2 Restoring to Factory Defaults

You can restore the Switch to its default settings.

Procedure

Step 1 Select **Maintenance** > **Restore Factory Default**.

Step 2 Click **Restore Factory Default**.

Step 3 Click **OK** in the pop-up prompt box.

The device starts restoring.

4.3 Managing Configuration Files

Save the configuration files which can be used for subsequent quick import to complete the configuration.

Export Configuration Files

1. Select **Maintenance** > **Configuration**.
2. Click **Export** in the **Export** tab to export the files.

Upload Configuration Files

1. Select **Maintenance** > **Configuration**.
2. Click **Browse** in the **Upload** tab.
3. Select the upload files, click **Upload**, and then upload the files.

4.4 Updating the System

Procedure

Step 1 Select **Maintenance** > **Update**.

Step 2 Click **Browse**, select the update file, and then click **Update now** to update the system.

4.5 Managing the Logs

Supports querying and exporting logs.

Procedure

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

Step 2 Select **Time** and **Log level**.



The log levels include **All**, **Error**, **Warning**, **Notice** and **Informational**.

Step 3 Click **Query** to view the log information.

Step 4 (Optional) Click **Export** to export the log. Click **Clear** to clear the log records.

4.6 Managing the System Time

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

Procedure

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

Step 2 Set the system time. There are 3 methods:

- Manually set: Set system time and time zone, and then click **Save**.



The time zone is configured when the device is initialized, and you can modify the time zone.

- Synchronize computer time: Click **Sync PC** to modify the device time according to the local computer time.
- Synchronize the server time.



This function requires that an NTP server has been deployed on the network.


1. Click  on the right of the **NTP**, click **OK** in the pop-up window, and then enable NTP.
2. Set the IP address of the NTP server.
3. Click **Save**.

Figure 4-1 Set the time

The screenshot shows a configuration window titled 'Set the time'. It contains the following elements:

- System Time:** A text field displaying '2000-01-23 07:41:45' with a calendar icon to its right.
- Time Zone:** A dropdown menu showing '(UTC) Coordinated Univers...'.
- NTP:** A toggle switch currently turned off.
- Server IP1:** A text field with three dots, indicating an IP address.
- Server IP2:** A text field with three dots, indicating an IP address.
- Buttons:** A blue 'Sync PC' button at the top right, and 'Save' and 'Refresh' buttons at the bottom left.

4.7 Configuring the Mirroring

Port mirroring also known as port monitoring, is a packet capture technology. By configuring the mirroring function, the device can copy packets from one or more source ports (mirroring source ports) to a specified destination port (mirroring destination port). Connect a host with packet analysis software installed to the mirroring destination port to analyze the collected packets. This technology effectively implements network monitoring and helps identify and troubleshoot network faults.

Procedure

- Step 1 Select **Maintenance** > **Mirror**.
- Step 2 Enable **Mode**.
- Step 3 Select the **Destination** column of the port to set it as the mirror destination port.
- Step 4 Select a specific mode in the **Source** column of the port to set it as a mirror source port.
 - Disabled: This port is not mirrored.
 - Both: Both send and receive type packets are copied.
 - Tx only: Only packets sent by this port are copied.
 - Rx only: Only packets received on this port are copied.

Figure 4-2 Mirror configuration

The image shows a 'Global Config' window with a 'Mode' toggle switch turned on. Below it is the 'Port Config' section, which contains a table with three rows. The first row is a header with 'Port' and 'Destination' columns. The second row has '3' in the 'Port' column and a dropdown menu in the 'Destination' column. The dropdown menu is open, showing options: 'Disabled' (highlighted), 'Both', 'Tx only', and 'Rx only'. The third row has '4' in the 'Port' column and a 'Disabled' dropdown in the 'Destination' column. The fourth row has '5' in the 'Port' column and a 'Disabled' dropdown in the 'Destination' column.

Port	Destination
3	Disabled
4	Disabled
5	Disabled

Step 5 Click **Save**.

4.8 Ping

You can use the Ping tool to check whether the device with the specified IP address is reachable and test whether the network connection is faulty.

Procedure

Step 1 Select **Maintenance** > **Ping**.

Step 2 Enter the IP address, Ping size, Ping times and Ping interval of the device whose network connection status needs to be detected.

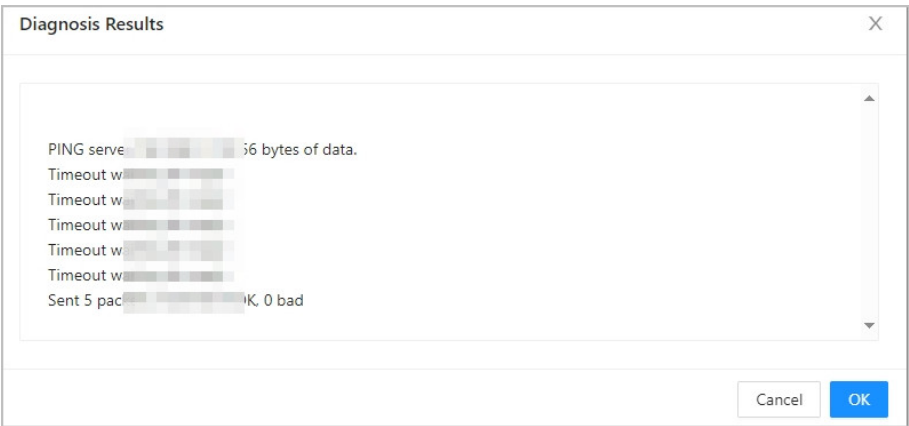
Figure 4-3 Ping

The image shows a 'Ping' configuration window. It has four input fields: 'IP Address' (with a placeholder 'x.x.x.x'), 'Ping Size' (with the value '56'), 'Ping Times' (with the value '5'), and 'Ping Interval' (with the value '1'). Below these fields is a blue button labeled 'Ping'.

Step 3 Click **Ping**.

Check whether the network is connected in the pop-up **Diagnosis Results** page.

Figure 4-4 Diagnosis results



4.9 iLinksView

4.9.1 Enabling iLinksView

The network management supporting function is used in conjunction with the iLinksView network management platform.

Procedure

- Step 1 Select **Maintenance** > **iLinksView** > **iLinksView**.
- Step 2 Enable the network management supporting function and enter the username and password of the network management platform.



The default username is admin and the password is lt_91_il_02_nmp.

Figure 4-5 iLinksView

A screenshot of the iLinksView configuration form. It contains an 'Enable' toggle switch which is currently turned on (blue). Below it are two input fields: 'Username' with the value 'admin' and 'Password' which is empty. At the bottom, there are two buttons: 'Save' (blue) and 'Refresh' (grey).

- Step 3 Click **Save**.

4.9.2 Uploading Network Management Configuration Files

Procedure

- Step 1 Select **Maintenance** > **iLinksView** > **Upload**.
- Step 2 Click **Browse** , select upload files, and then click **Upload**.

4.9.3 Exporting Network Management Configuration Files

Procedure

- Step 1 Select **Maintenance** > **iLinksView** > **Export**.
- Step 2 Click **Export** to export the files.

4.10 Viewing Legal Information

Click **Maintenance** > **Legal Info**, and then you can view the **Open Source Software Notice**.

5 Network Settings

Describes the network settings of the device, including MAC and spanning tree configurations.

5.1 Configuring Ports

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.

Procedure


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




Step 2 Set the parameters.

Figure 5-1 Port settings

Port	Description	Type	Link Status	Speed/Duplexing Status	Speed/Duplexing	Flow Control Status	Flow Control	In	Ingress Limit(kbps)	Out	Egress Limit(kbps)	RX Usage
1	<input type="text"/>	Copper	Up	1G Full	Auto	Off	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="500"/>	<input checked="" type="checkbox"/>	<input type="text" value="500"/>	0.1%
2	<input type="text"/>	Copper	Down	Down	Auto	Off	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="checkbox"/>	<input type="text" value="500"/>	0%
3	<input type="text"/>	Copper	Down	Down	Auto	Off	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="checkbox"/>	<input type="text" value="500"/>	0%
4	<input type="text"/>	Copper	Down	Down	Auto	Off	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="checkbox"/>	<input type="text" value="500"/>	0%
5	<input type="text"/>	Copper	Down	Down	Auto	Off	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="checkbox"/>	<input type="text" value="500"/>	0%
6	<input type="text"/>	Copper	Down	Down	Auto	Off	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="checkbox"/>	<input type="text" value="500"/>	0%
7	<input type="text"/>	Fiber	Down	Down	Auto	Off	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="checkbox"/>	<input type="text" value="500"/>	0%

Table 5-1 Port setting parameter descriptions

Parameter	Description
Port	Displays all ports of the device.
Description	<div>Enter the description of the port.</div> <div></div> <div>The description cannot exceed 64 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.</div>
Type	<div>Displays 2 kinds of media type, includes 2 types: Copper and Fiber.</div> <ul style="list-style-type: none">● Copper: Ethernet port.● Fiber: Optical port.
Link Status	<div>Includes 2 status: Up and Down.</div> <ul style="list-style-type: none">● Up: The port is connected.● Down: The port is not connected or the connection fails.

Parameter	Description
Speed/Duplexing Status	<p>Displays the speed and duplex status of the port.</p> <ul style="list-style-type: none"> ● Down: The port is not connected. ● Displays rate: Full means full-duplex which can receive and send at the same time, and the maximum throughput can reach double the rate. Half means half-duplex which means only receiving or sending.
Speed/Duplexing	<p>Select the speed and duplex mode.</p>  <p>The combo port rate and duplex mode are fixed to Auto.</p>
Flow Control Status	<ul style="list-style-type: none"> ● On: Successfully negotiated. ● Off: Negotiation failed.
Flow Control	Click  to enable or disable the function.
In	Enable inbound rate limiting and set the rate limit for inbound data.
Ingress Limit (kbps)	
Out	Enable outbound rate limiting and set the rate limit for outbound data.
Egress Limit (kbps)	
RX Usage	The value of the received rate divided by the actual negotiated rate over a period of time (usually in 5 minutes).
TX Usage	The value of the sending rate over a period of time (usually in 5 minutes) divided by the actual negotiated rate.
Details	Click  , and then you can refresh or clear the detailed information of each port.

Step 3 Click **Save**.

5.2 Configuring VLANs

You can add the port to the VLAN and configure the parameters of the VLAN.

Procedure

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

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

Step 3 Click **OK**.

Supports entering single digits, multiple consecutive or non-consecutive digits. For example:

- When you enter **2**, it means creating VLAN2.
- When you enter **2,5**, it means creating VLAN2 and VLAN5.
- When you enter **2-5**, it means creating VLAN2, VLAN3, VLAN4 and VLAN5.



Step 4 Configure the parameters of the VLAN on the **VLAN** page.


Figure 5-2 Configure the VLAN

Port	Mode	Port to VLAN	Ingress Acceptance	Egress Tagging	Allowed VLAN
1	Access	1	Tagged and Untagged	Untag All	1
2	Access	1	Tagged and Untagged	Untag All	1
3	Access	1	Tagged and Untagged	Untag All	1
4	Access	1	Tagged and Untagged	Untag All	1
5	Access	1	Tagged and Untagged	Untag All	1
6	Access	1	Tagged and Untagged	Untag All	1
7	Access	1	Tagged and Untagged	Untag All	1

Save Refresh

Table 5-2 Port VLAN configuration parameter

Parameter	Description
Port	Displays all ports of the device.
Mode	<p>Configure port type, including 3 types: Access , Hybrid and Trunk.</p> <ul style="list-style-type: none"> ● Access : The port of the switch used to connect to the terminal device (such as the user host), generally connected to the access link. The access port can only belong to one VLAN. The access port sends and receives data frames without VLAN tags (Untagged). ● Hybrid : The switch can be connected both user hosts and the ports of other switches. A hybrid port can belong to multiple VLANs at the same time and can be configured to send data frames without VLAN tags (Untagged) on some VLANs and send data frames with VLAN tags (Tagged) on other VLANs. ● Trunk : The switch is used to connect to the ports of other switches, usually connected to intermediate interconnection links. Trunk ports can carry data streams from multiple VLANs and send data frames with VLAN tags (Tagged). <p> The Hybrid mode is available on select models.</p>
Port to VLAN	Add ports to the VLAN, all ports belong to VLAN 1 by default. The range is from 1 through 4094.
Ingress Acceptance	<p>Set the type of data that can flow into the device port, including the following 3 situations.</p> <ul style="list-style-type: none"> ● Tagged and Untagged: All data can flow into this port. ● Tagged only: Only tagged data can flow into this port. ● Untagged only: Only untagged data can flow into this port. <p> Only the Hybrid port needs to be configured. In other modes, all data flows into the port by default.</p>

Parameter	Description
Egress Tagging	<p>Set whether to add a tag to the data of the given port, including the following 3 situations.</p> <ul style="list-style-type: none"> • Untag Port VLAN: If the data flow tag is the same as the PVID (the VLAN ID to which the port belongs), the tag will be stripped. • Tag All: All data are labeled. • Untag All: All data are unlabeled.
Allowed VLAN	<p>Configure the allowed VLAN.</p> <p>Supports entering single digits, multiple consecutive or non-consecutive digits. For example:</p> <ul style="list-style-type: none"> • When you enter 2, it means creating VLAN2. • When you enter 2,5, it means creating VLAN2 and VLAN5. • When you enter 2-5, it means creating VLAN2, VLAN3, VLAN4 and VLAN5. <p></p> <p>When the mode is Trunk or Hybrid, it supports setting the allowed VLAN.</p>

Step 5 Click **Save**.

5.3 Configuring Link Aggregation

Procedure

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

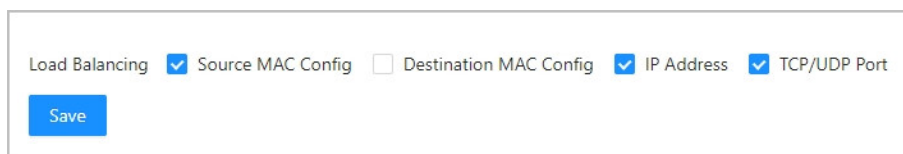
Step 2 Select a load balancing algorithm mode.

Includes the following 4 modes.

- **Source MAC Config** : Based on source MAC addresses of packets.
- **Destination MAC Config** : Based on destination MAC addresses of packets.
- **IP Address** : Based on source IP address, destination IP address of packets.
- **TCP/UDP Port** : Based on source TCP/UDP port number, and destination TCP/UDP port number of packets.

For example, if you select **Source MAC Config**, when different source MACs of data are detected, they are assigned to different ports for processing.

Figure 5-3 Link aggregation mode



Load Balancing ☒ Source MAC Config ☐ Destination MAC Config ☒ IP Address ☒ TCP/UDP Port

Save

Step 3 Refer to "3.3 Configuring Link Aggregation" to set up link aggregation.

5.4 Configuring MAC

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.
- 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.

5.4.1 Adding the MAC Table

Procedure

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

View the MAC table information, including port ID, MAC address, type, and VLAN.




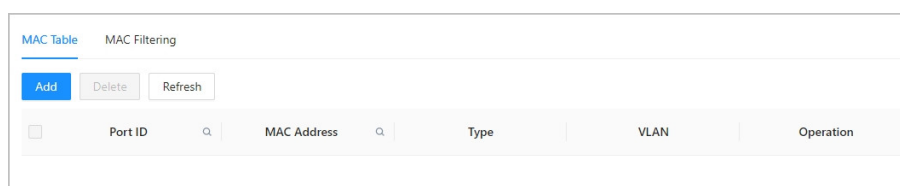
Click  of the port ID or MAC address table header to enter keywords to quickly query MAC address information.

Figure 5-4 MAC table



Step 2 Click **Add**, and then bind the MAC address to a port belonging to a certain VLAN.

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

Figure 5-5 Add the MAC

Step 3 Click **OK**.

5.4.2 Filtering the Port MAC

Background Information

After enabling port MAC filtering, the following 2 MAC devices can communicate with the port.

- Devices in MAC allowlist.
- The static MAC devices changing from the dynamic MAC devices.

Procedure

- Step 1** Select **Network Settings** > **MAC Table** > **MAC Filtering**.
- Step 2** Select the port of the device, and then click ☐ to enable the filtering function.
- Step 3** Configure the MAC filtering of the port.
- Create the MAC allowlist.
 1. Click **Add**.
 2. Set MAC address and VLAN.
 3. Click **OK**.

Figure 5-6 Add the MAC

The 'Add' dialog box contains the following elements:

- MAC Table:** A text input field containing '00 : 00 : 00 : 00 : 00 : 01'. Below it, a hint text says 'For example: 90:02:A9:2C:44:11'.
- VLAN:** A text input field with a range '(1-4094)' to its right.
- Buttons:** 'Cancel' and 'OK' buttons at the bottom right.

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

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

Static MAC devices can communicate with the port normally.

Figure 5-7 Change from dynamic to static

The MAC Filtering configuration page includes the following components:

- Port 4:** A toggle switch is turned on.
- Table:** A table with columns: No., Port ID, MAC Address, Type, VLAN, Reserved Status, and Reserved. It contains one record with No. 1, Port ID 4, MAC Address 00:00:00:00:00:01, Type Static, VLAN 12, and Reserved Status Reserved. The 'Reserved' column has a toggle switch.
- Buttons:** 'Add' and 'Save' buttons.
- Footer:** 'Total 1 records' and pagination controls.

5.5 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.

Background Information

- 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.



Generally, the spanning tree function needs to be configured in conjunction with the overall network planning.

Procedure

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

Step 2 Select the STP mode, and then click **Save**.

STP mode includes **STP**, **RSTP** and **MSTP**.

Step 3 Enable the spanning tree function on the corresponding port.

Figure 5-8 STP mode

STP Mode	STP						
<input type="checkbox"/> Enable	Port	Priority	Root Path Cost	Status	Port Status	Designated Bridge	Designated Port
<input checked="" type="checkbox"/>	1	128	20000	RootPort	Forwarding	20-23-06-12-16-15	40
<input type="checkbox"/>	2	128	-	Non-STP	Discarding	-	-
<input checked="" type="checkbox"/>	3	128	-	Disabled	Discarding	-	-
<input type="checkbox"/>	4	128	-	Non-STP	Discarding	-	-
<input type="checkbox"/>	5	128	-	Non-STP	Discarding	-	-
<input type="checkbox"/>	6	128	-	Non-STP	Discarding	-	-
<input type="checkbox"/>	7	128	-	Non-STP	Discarding	-	-
<input type="checkbox"/>	8	128	-	Non-STP	Discarding	-	-
<input type="checkbox"/>	9	128	-	Non-STP	Discarding	-	-
<input type="checkbox"/>	10	128	-	Non-STP	Discarding	-	-
<input type="button" value="Save"/> <input type="button" value="Refresh"/>							

Step 4 Click **Save**.

5.6 Configuring Long Distance PoE

After enabling the long-distance PoE function, the maximum transmission distance of the device increases from 100 meters to 250 meters, but the transmission speed decreases from 1 Gbps to 10 Mbps.

Background Information



- In long-distance power supply mode, the transmission rate drops to 10 Mbps. The actual transmission distance is strongly related to the PoE power and cable quality. The advertised distance is only the laboratory distance.
- Non-PoE devices do not support this function.

Procedure

- Step 1** Select **Network Settings** > **Long Distance PoE**.
- Step 2** Enable the long-distance PoE function of the corresponding port as needed.

Figure 5-9 Long distance PoE

Enabling Long Distance will extend the max transmission distance from 100 m to 250 m, but the transmission speed will be reduced from 1 Gbps to 10 Mbps.

Port	Enable
1	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>

[Save](#)

- Step 3** Click **Save**.

5.7 Configuring PoE

PoE means that the device uses the Ethernet port and the network cable to remotely power the external PD (Powered Device). The PoE function allows centralized power supply and convenient backup. The network terminal does not need an external power supply, and only needs a network cable for power supply. It complies with IEEE 802.3af, IEEE 802.3at and IEEE 802.3bt standards and uses a globally unified power interface. It can be used for IP phones, wireless APs (Access Points), portable device chargers, card readers, network cameras, etc.



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

5.7.1 Configuring PoE Settings

Enable the PoE function and set the available power, overload power and other parameters.

Procedure

- Step 1** Select **Network Settings** > **PoE** > **PoE Settings**.
- Step 2** Configure PoE power and view the power status.

- In **Power Settings**, you can view the total power of the ports and configure available power and overload power.
 - ◇ **Available Power** : Refers to the maximum power that can be provided to the powered device. When the total power consumed is less than the available power, the newly connected powered device is allowed to power on.
 - ◇ **Overload Power** : When the total power consumption exceeds the overload power, the device will be powered off (in descending order of port numbers).
- In **Power Status**, you can view consumed power, remaining power and reserved power. The reserved power is the unavailable PoE power. The reserve power is equal to the total power minus the overload power.

Step 3 In **Port Status and Control**, enable the PoE power supply function of the corresponding port as needed.

Figure 5-10 PoE parameters

PoE Settings

Total PoE Power 120W

Available Power 108 W (Available Power must not be greater than Overload Power.)

Overload Power 110 W (Overload Power must not be greater than Total Power.)

Power Status

Power Consumed 0W

Remaining Power 120W

Reserved Power 10W

Port Status and Control

Port	Power Consumed	Enable	PD Class	Port Status
1	0	<input checked="" type="checkbox"/>	-	PoE turned OFF
2	0	<input type="checkbox"/>	-	PoE turned OFF
3	0	<input type="checkbox"/>	-	PoE turned OFF
4	0	<input checked="" type="checkbox"/>	-	PoE turned OFF
5	0	<input checked="" type="checkbox"/>	-	PoE turned OFF
6	0	<input checked="" type="checkbox"/>	-	PoE turned OFF

Save Refresh


Step 4 Click **Save**.

5.7.2 Configuring Green PoE


Green PoE can reduce power consumption while retaining full compatibility with existing equipment. When the specified time expires, the port automatically resumes PoE power supply.


Procedure

Step 1 Select **Network Settings** > **PoE** > **Green PoE**.

Step 2 Click  of the corresponding energy saving plan, set the start time and end time of green PoE, enable weekly cycle as needed, and then click **OK**.

For example, if the start time is set to 1 o'clock on Sunday, the corresponding **On/Off**

setting is , and the end time is set to 3 o'clock on Sunday, the corresponding

On/Off setting is , then green PoE is turned on at 1 o'clock on Sunday and turned off at 3 o'clock on Sunday. If weekly cycle is enabled, this setting will be executed every week.





- The start time and end time must be set to on/off.
- If the start time is set to  and the end time is set to , and then Green PoE is turned off between the start time and the end time.

Figure 5-11 Edit the time

Edit

Start Time

Sun

01:00

On/Off

End Time

Sun

03:00

On/Off

Weekly Cycle

Cancel

OK

Step 3 Select ☐, and the port will be executed according to the energy-saving plan.

- Only one energy saving plan can be enabled on each port at the same time.
- Click **Enable** under an energy-saving plan to enable this plan on all ports.

Click **Disable** to cancel the energy-saving plan for all ports that have enabled the energy saving plan.

Figure 5-12 Enable the green PoE

Add

Port	Energy Saving Plan 1					Operation	Energy Saving Plan					Operation
	Start Time	On/Off	End Time	On/Off	Weekly Cycle		Start Time	On/Off	End Time	On/Off	Weekly Cycle	
-	Sun01:00	On	Sun03:00	Off	Yes		-	-	-	-	-	
All	<div>EnableDisable</div>						<div>EnableDisable</div>					
1	<input type="checkbox"/>						<input type="checkbox"/>					
2	<input type="checkbox"/>						<input type="checkbox"/>					
3	<input type="checkbox"/>						<input type="checkbox"/>					
4	<input type="checkbox"/>						<input type="checkbox"/>					
5	<input type="checkbox"/>						<input type="checkbox"/>					
6	<input type="checkbox"/>						<input type="checkbox"/>					

Save

Refresh

Step 4 Click **Save**.

Related Operations

The page displays 2 energy-saving plans by default. If you need to configure more energy-saving plans, you can click **Add** to add a new energy-saving plan. A maximum of 5 energy-saving plans can be configured.

5.7.3 Configuring Force PoE

When the powered device connected to the port is a non-standard device, this function can be used to force PoE power supply.

Background Information



- After force PoE is enabled, the port will force supply power to the powered device, whether or not the device connected to the port meets the requirements. Please be advised.
- Force PoE power supply and PoE watchdog conflict with each other. Only one can be configured at the same time.

Procedure

Step 1 Select **Network Settings** > **PoE** > **Force PoE**.

Step 2 Enable the force PoE power supply function of the port as needed.

Figure 5-13 Enable force PoE

After force PoE is enabled, the port will force supply power 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.

Port	<input type="checkbox"/> Enable
1	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>

Step 3 Click **Save**.

5.7.4 Configuring PoE Watchdog

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

Background Information



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

Procedure

Step 1 Select **Network Settings** > **PoE** > **PoE Watchdog**.

Step 2 Enable the PoE watchdog function of the port as needed.

Figure 5-14 Enable PoE watchdog

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

Port	<input type="checkbox"/> Enable
1	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>

[Save](#)

Step 3 Click **Save**.

5.7.5 Viewing PoE Event Statistics

View the number of abnormal events that occur on the PoE port, such as overcurrent, current limiting, DC power failure, startup failure, and overheating.

Procedure

Step 1 Select **Network Settings** > **PoE** > **PoE Event Statistics**.

Step 2 View the number of times various events occur on the PoE port.

Figure 5-15 PoE event statistics

Port	Overcurrent	Limited Current	DC Disconnection	Start Failure	Overheating
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0

5.8 Loopback Detection

LBDT periodically sends detection packets on an interface to check whether the packets return to the local device, and determines whether a loop occurs on the interface, on the downstream network or device, or between 2 device interfaces.

Background Information



It is not recommended to enable the spanning tree function and ERPS function at the same time. It might cause network errors.

Procedure

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

Step 2 Click  to enable the function.

Step 3 Click **OK**.

5.9 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.



- Generally, the ERPS function is configured when building a ring network.
- ERPS is available on select models. Please refer to the actual model.

5.9.1 ERPS Settings

Procedure

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


Step 2 Click **Add**.

Step 3 Configure the parameters.

Figure 5-16 Add the ERPS

Parameter	Value	Range
ERPS ID	1	(1-64)
Port 0	1	(1-10)
Port 1	1	(1-10)
Port 0 APS MEP	1	(1-100)
Port 1 APS MEP	1	(1-100)
Port 0 SF MEP	1	(1-100)
Port 1 SF MEP	1	(1-100)

Table 5-3 ERPS parameter description

Parameter	Description
ERPS ID	The ID number of the ERPS.
Port 0	2 ports of the device 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.  <p>Port 0 APS MEP keeps the same as Port 0 SF MEP. Port 1 APS MEP keeps the same as Port 1 SF MEP.</p>
Port 1 APS MEP	
Port 0 SF MEP	
Port 1 SF MEP	

Step 4 Click **OK**.

5.9.2 MEP Settings

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** > **MEP**.
- Step 2 Click **Add**.
- Step 3 Configure the parameters.

Figure 5-17 Add the MEP

Table 5-4 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.

Step 4 Click **OK**.

5.9.3 Example of Single-Ring Configuration in ERPS

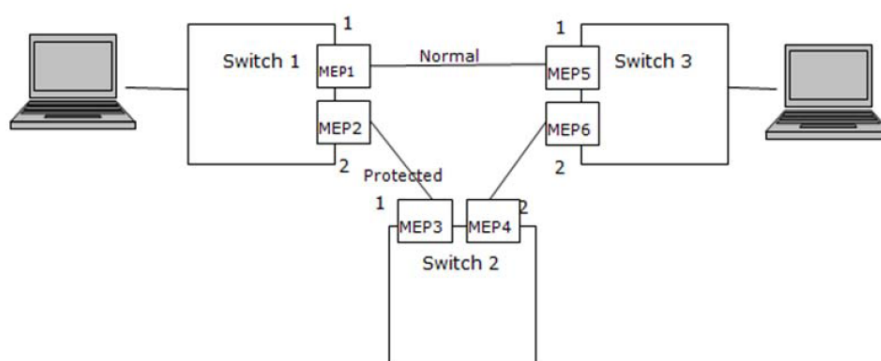
Prerequisites

Before configuration, ensure that the mutually exclusive functions on the port, such as the spanning tree function and LLDP function, are disabled.

Background Information

The networking requirements are as follows: Ports 1 and 2 of the 3 switches are required to form an ERPS ring. Switch 1 corresponds to MEP1 and MEP2, switch 2 corresponds to MEP3 and MEP4, and switch 3 corresponds to MEP5 and MEP6.

Figure 5-18 The single-ring configuration in ERPS



The configuration roadmap is as follows:

1. Determine the topology, plan the protection VLAN and protocol VLAN, and determine the RPL owner port.
2. Make sure the muted functionality on the port is turned off.
3. Configure the VLAN.
4. Add the MEP.
5. Add an ERPS ring and configure the control VLAN and protection instance.
6. View the status.

The following example takes the planning of protection VLAN and protocol VLAN as 2 and 3 respectively, and setting port 2 of switch 1 as the RPL owner port.

Procedure

- Step 1** Configure the protection VLAN and protocol VLAN as VLAN2 and VLAN3 respectively.
1. Select **Network Settings > VLAN > VLAN**.
 2. Set the mode of the port 1 and port 2 to **Trunk**, the port to VLAN is **1** and the allowed VLANs are **2 and 3**.
 3. Click **Save**.

Figure 5-19 Configuration examples

Add VLAN **VLAN**

Port	Mode	Port to VLAN	Ingress Acceptance	Egress Tagging	Allowed VLAN
1	Trunk	1	Tagged and Untagged	Untag Port VLAN	2,3
2	Trunk	1	Tagged and Untagged	Untag Port VLAN	2,3
3	Access	1	Tagged and Untagged	Untag All	1
4	Access	1	Tagged and Untagged	Untag All	1
5	Access	1	Tagged and Untagged	Untag All	1
6	Access	1	Tagged and Untagged	Untag All	1
7	Access	1	Tagged and Untagged	Untag All	1

Save Refresh

Step 2 Add MEP1 and MEP2.

1. Select **Network Settings** > **ERPS** > **ERPS**.
2. Click **Add**, configure the parameters, and then click **OK**.
 - MEP1: Set the instance to 1, port to 1, level to 1, and control VLAN to 3.
 - MEP2: Set the instance to 2, port to 2, level to 1, and control VLAN to 3.

Figure 5-20 Add the MEP

Add [X]

Instance: 1 (1-100)

Port: 1 (1-10)

Level: 1 (1-7)

Control VLAN: 3 (1-4094)

[Cancel] [OK]


3. Click  in the **Operation** column to modify the MEP detailed configuration.
 - a. Modify the MEP ID.
 - b. Click **Add**, add peer IDs, set the peer ID of MEP 1 to 5 and the peer ID of MEP 2 to 3, and then click **OK**.

Figure 5-21 Set the peer ID of MEP1

MEP Config [X]


Instance Info

Instance	Domain	MEP Mode	Direction	Port	Port MAC	Operational State
1	Port	MEP	In	1	74-C9-29-05-53-13	●

Instance Config

Level: 1 MEP ID: 1 Control VLAN: 3

Peer MEP Config [Add]

Peer MEP Config Id	Peer MAC	Operation
2	00 : 00 : 00 : 00 : 00 : 00	

[Cancel] [OK]

Figure 5-22 Set the peer ID of MEP2

The MEP Config window displays the following configuration:

Instance	Domain	MEP Mode	Direction	Port	Port MAC	Operational State
2	Port	MEP	In	3	74-C9-29-05-53-15	●

Level	MEP ID	Control VLAN
4	1	5

Peer MEP Config Add

Peer MEP Config Id	Peer MAC	Operation
5	00 : 00 : 00 : 00 : 00 : 00	

Cancel OK

c. Click **OK**.

Step 3 Add the ERPS.

1. Select **Network Settings > ERPS > ERPS**.
2. Click **Add**, configure the parameter, and then click **OK**.

Figure 5-23 Add the ERPS

The Add ERPS configuration window contains the following fields:

ERPS ID	1	(1-64)
Port 0	1	(1-10)
Port 1	2	(1-10)
Port 0 APS MEP	1	(1-100)
Port 1 APS MEP	2	(1-100)
Port 0 SF MEP	1	(1-100)
Port 1 SF MEP	2	(1-100)

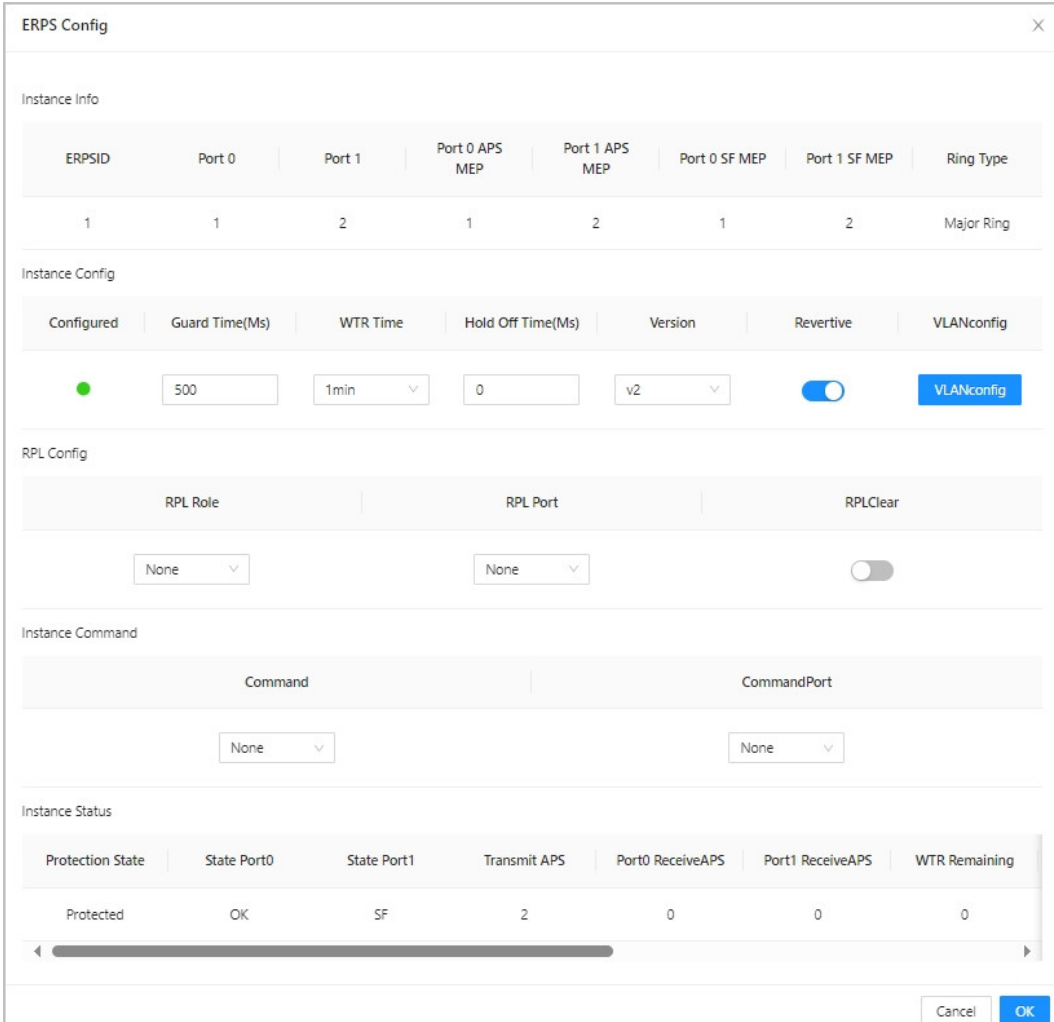
Cancel OK

Table 5-5 ERPS parameter description

Parameter	Description
ERPS ID	Set the ERPS ID to 1.
Port 0	Set Port 0 and Port 1 to 1 and 2 respectively.
Port 1	
Port 0 APS MEP	Set the APS MEP values of Port 0 and Port 1 to 1 and 2 respectively.
Port 1 APS MEP	
Port 0 SF MEP	Set Port 0 SF MEP and Port 1 SF MEP to 1 and 2 respectively.
Port 1 SF MEP	

3. Click  in the **Operation** column to configure the ERPS.

Figure 5-24 Configure the ERPS



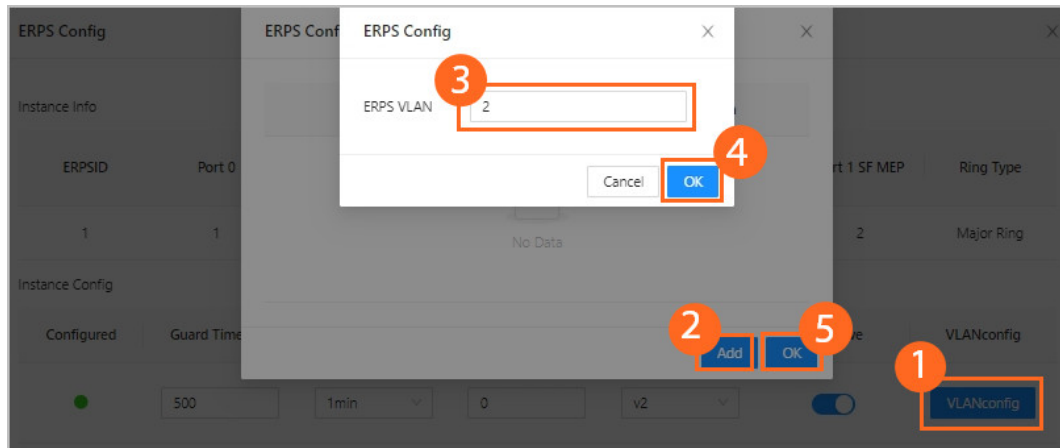
The ERPS Config window is divided into several sections:

- Instance Info:** A table showing configuration for ERPSID (1), Port 0 (1), Port 1 (2), Port 0 APS MEP (1), Port 1 APS MEP (2), Port 0 SF MEP (1), Port 1 SF MEP (2), and Ring Type (Major Ring).
- Instance Config:** Fields for Configured (green dot), Guard Time(Ms) (500), WTR Time (1min), Hold Off Time(Ms) (0), Version (v2), Revertive (toggle on), and a blue **VLANconfig** button.
- RPL Config:** Fields for RPL Role (None), RPL Port (None), and RPLClear (toggle off).
- Instance Command:** Fields for Command (None) and CommandPort (None).
- Instance Status:** A table showing Protection State (Protected), State Port0 (OK), State Port1 (SF), Transmit APS (2), Port0 ReceiveAPS (0), Port1 ReceiveAPS (0), and WTR Remaining (0).

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

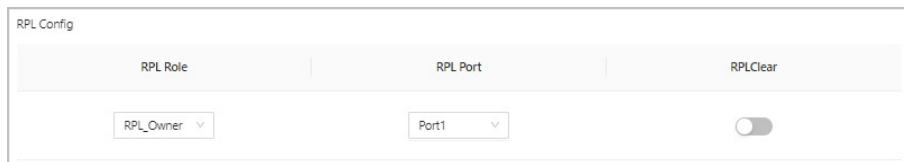
- Click **VLANconfig**, and then click **Add**.
- Set the ERPS VLAN to 2, and then click **OK**.

Figure 5-25 Set the ERPS VLAN




- c. Click **OK** in the **ERPS Config** page.
- d. In the **RPL Config** area, select the RPL role as **RPL_Owner**, select the RPL port as **Port1**, and then click **OK**.

Figure 5-26 Set owner port



Step 4 Configure the switch 2 and the switch 3 in the same way.

Step 5 Select **Network Settings** > **ERPS** > **ERPS**.

Click  in the **Operation** column to view the configuration status.

5.10 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 the **IGMP Snooping** to enable the function.

Step 3 Enable **Drop Unknown Multicast Messages** as needed.

The function of dropping unknown multicast messages is disabled by default.

- 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.



Be cautious when enabling the function of dropping unknown multicast messages. Enabling it might cause some multicast applications to fail.

- Step 4 Click **Add**, set the VLAN number and search address, enable the **Querier**, and then click **OK**.

Figure 5-27 IGMP Snooping

The screenshot shows a dialog box titled 'Add' with a close button (X) in the top right corner. It contains three fields: 'VLAN' with a text input box and a range '(1-4094)' to its right; 'Querier' with a toggle switch currently turned off; and 'Search Address' with a text input box containing three dots. At the bottom right, there are 'Cancel' and 'OK' buttons.

- Step 5 Click **Save**.

5.11 Configuring IP and Routing

For more information, see "3.5 Configuring the IP and Routing".

5.12 Configuring ARP

Address Resolution Protocol (ARP) is a protocol used to map IP addresses to MAC addresses. It is therefore necessary for hosts or Layer 3 network devices to maintain an ARP table for storing the mapping information of IP and MAC addresses. There are generally 2 types of ARP entries: Static and dynamic.

Background Information



ARP is available on select models. Please refer to the actual situation.

Procedure

- Step 1 Select **Network Settings** > **ARP**, and then you can view the IP address, the MAC address, the type and the VLAN.
- Step 2 Click **Add**, enter the IP address, the MAC address and the VLAN.
Add a static MAC address.

Figure 5-28 Add a static MAC address

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains three input fields: "IP Address" with the value "192 . 168 . 10 . 110", "MAC Table" with the value "00 : 00 : 00 : 00 : 00 : 01" and a hint "For example: 90:02:A9:2C:44:11", and "VLAN" with the value "2" and a range "(1-4094)". At the bottom right, there are "Cancel" and "OK" buttons.

Step 3 Click **OK**.

5.13 Configuring DHCP

Dynamic Host Configuration Protocol (DHCP) is a network management protocol for dynamic and centralized IP address allocation and management. DHCP Server is the server for managing DHCP standard in the specific network. DHCP Server is to allocate IP address for the workstation and make sure that the IP address for every workstation is different. DHCP Server simplifies the network management task which should be done manually before.

Background Information

Generally, in the following scenes, DHCP Server is adopted to allocate IP address.

- The network scale is large. The workload is too heavy if manually configured, and centralized management for network will be difficult.
- The quantity of PC is larger than the quantity of IP address in the network, and it is impossible to allocate a static IP address for every PC. For example, the user quantity that can access network at the same time is limited by ISP, and the user needs to acquire the IP address dynamically.
- Only a small number of PC need the static IP address, and most of the PC do not need the static IP address.

Procedure

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

Step 2 Enable **Global Enable**.

Figure 5-29 DHCP server

Step 3 Add a new DHCP address pool.

1. Click **Add** on the **Address Pool** area.
2. Configure the parameter.

Figure 5-30 Add the address pool

Table 5-6 Address pool parameter description

Parameter	Description
Name	<p>DHCP address pool name, such as pool1.</p> <p> Only numbers or letters can be entered, and the length of the string is limited to 1–32.</p>

Parameter	Description
Type	<p>Includes 2 types: Network and Host.</p> <ul style="list-style-type: none"> • Network: The DHCP server provides IP address allocation and other network configurations for hosts within the entire network or subnet range, and is suitable for large network environments. • Host: The DHCP server allocates IP addresses to specific hosts, usually by assigning a fixed IP address to a single device based on a specific physical address (MAC address).
IP Address	The IP address of the host or the network.
Subnet Mask	The subnet mask of the host or the network.
Lease Time	The DHCP server sets a lease term for the IP address assigned to the client. When the lease expires, the client must request a renewal from the DHCP server or obtain a new IP address.
Gateway	Set the gateway address (usually the IP address of the router). The DHCP server will provide the gateway address when assigning an IP address to the client to ensure that the client can correctly access the network and interact with other network devices.
Client ID	<p>When the type is selected as Host, you need to set the client ID of the client. The DHCP server assigns the IP address to the corresponding client based on this information.</p> <ul style="list-style-type: none"> • Client ID is Name, and then the host name needs to be set. • Client ID is MAC, and then the MAC address of the host needs to be set.

3. Click **OK**.

Step 4 Configure the reserved IP.



Reserved IP refers to the IP reserved for the server and will not be assigned to the client.

1. Click **Add** on the **Reserved IP** area.
2. Enter an IP address range, such as **192.168.100.2-192.168.100.50**.

Figure 5-31 Add the IP

3. Click **OK**.

Step 5 (Optional) Configure the VLAN mode.

1. Click **Add** on the **VLAN Mode** area.
2. Enter the VLAN range, such as **1-3**.

IP addresses are allocated only to devices in the added VLAN.

Figure 5-32 Add the VLAN

A dialog box titled "Add VLAN" with a close button (X) in the top right corner. It contains a label "VLAN" followed by two input fields separated by a hyphen. The first input field contains the number "1" and the second contains the number "3". At the bottom right, there are two buttons: "Cancel" and "OK".

3. Click **OK**.

5.14 Configuring DHCP Relay

The DHCP relay function enables message exchanges between a DHCP server and a client on different network segments. When DHCP clients and a server are on different network segments, the DHCP relay agent transparently transmits DHCP messages to the destination DHCP server. In this way, DHCP clients on different network segments can communicate with one DHCP server.

Background Information

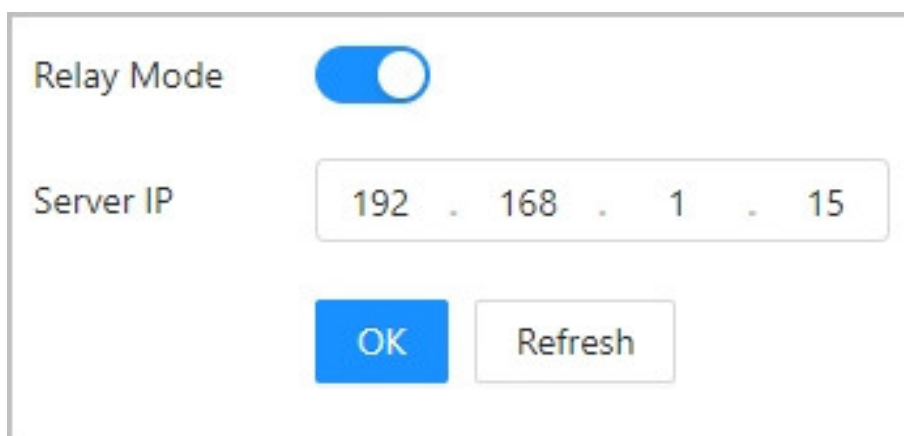


DHCP relay is available on select models. Please refer to the actual situation.

Procedure

- Step 1 Select **Network Settings > DHCP Relay**.
- Step 2 Click ☐ to enable **Relay Mode**.
Enable relay mode to use the device as a DHCP relay.
- Step 3 Enter the IP address of the DHCP server.

Figure 5-33 DHCP relay

A configuration interface for DHCP relay. It features a "Relay Mode" label next to a blue toggle switch that is currently turned on. Below this, there is a "Server IP" label followed by a text input field containing the IP address "192 . 168 . 1 . 15". At the bottom, there are two buttons: a blue "OK" button and a grey "Refresh" button.

Step 4 Click **OK**.

5.15 Configuring LLDP

LLDP (Link Layer Discovery Protocol) is a standard link layer discovery way. It can form its main capabilities, management address, device No. and port No. 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.

5.15.1 LLDP Settings

Procedure

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

Step 2 Configure the LLDP.

- Enable: Both send and receive LLDP packets.
- Disable: Neither send nor receive LLDP packets.
- Rx only: Only receive LLDP packets.
- Tx only: Only send LLDP packets.

Figure 5-34 LLDP settings

Port	Mode
1	Enable
2	Enable
3	Enable
4	Enable
5	Enable
6	Enable
7	Enable
8	Enable
9	Enable

Save Refresh

Step 3 Click **Save**.

5.15.2 Viewing LLDP Remote Devices

Procedure

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

Step 2 View the information of the remote devices.

- Enable **Auto Refresh**, the device will refresh remote device information every 60 seconds.
- In the **Address Management** column, you can click the address to go to the webpage of the device.

Figure 5-35 View LLDP remote devices

Local Port	Port ID	Port Description	System Name	System Capacity	Address Management
GigabitEthernet 1/5	GigabitEthernet1/0/40	GigabitEthernet1/0/40	SWITCH	Bridge(+)	1 (4)

5.16 Configuring RS-485 Pass-Through

The data of the asynchronous serial port RS-232/485 is transparently transmitted through the Ethernet network.

Background Information



RS-485 pass-through is available on select models. Please refer to the actual situation.

Procedure


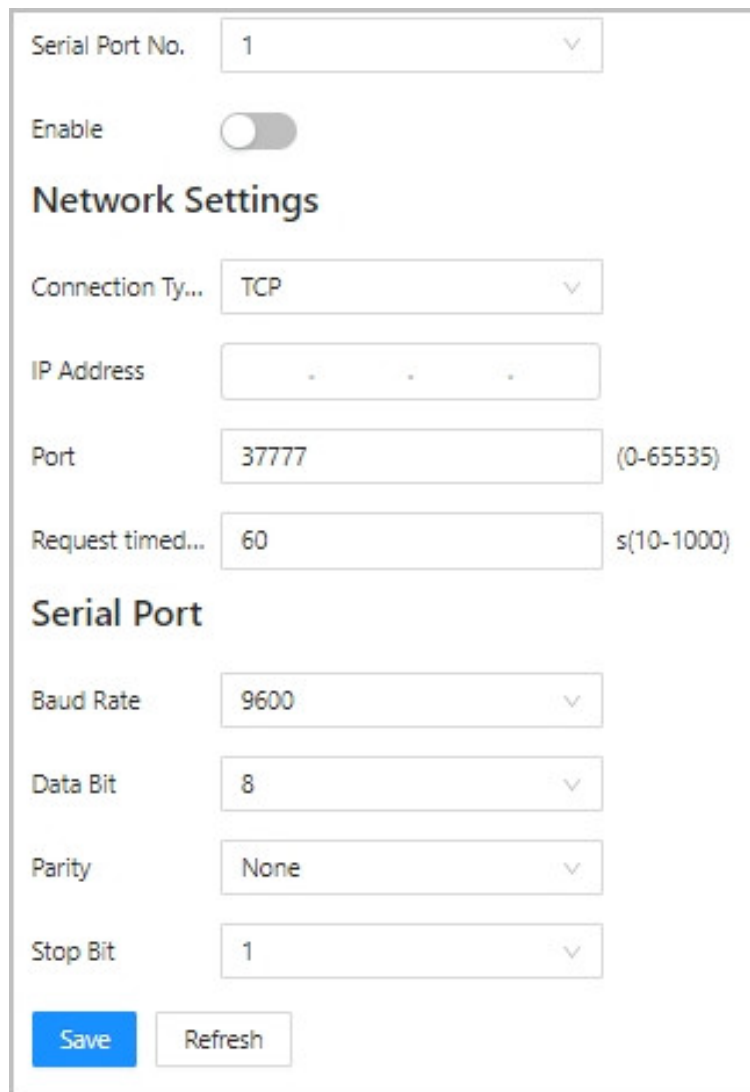
- Step 1 Select **Network Settings** > **RS-485 Pass-through**.
- Step 2 Select the serial port number, and then click .
- Step 3 Select the connection type and fill in the **IP address**, **Port** and **Request timed out** of the device that needs data transparent transmission.
- Step 4 Configure the serial ports such as baud rate, data bit, parity and stop bit.

Figure 5-36 RS-485 pass-through



The screenshot shows a configuration window for RS-485 Pass-through. It contains the following fields and controls:

- Serial Port No.:** A dropdown menu with the value '1' selected.
- Enable:** A toggle switch that is currently turned off.
- Network Settings:**
 - Connection Ty...:** A dropdown menu with 'TCP' selected.
 - IP Address:** A text input field with three dots, indicating a placeholder for an IP address.
 - Port:** A text input field with the value '37777' and a range '(0-65535)' to its right.
 - Request timed...:** A text input field with the value '60' and a range 's(10-1000)' to its right.
- Serial Port:**
 - Baud Rate:** A dropdown menu with '9600' selected.
 - Data Bit:** A dropdown menu with '8' selected.
 - Parity:** A dropdown menu with 'None' selected.
 - Stop Bit:** A dropdown menu with '1' selected.
- Buttons:** A blue 'Save' button and a white 'Refresh' button.

- Step 5 Click **Save**.

5.17 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 two 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.

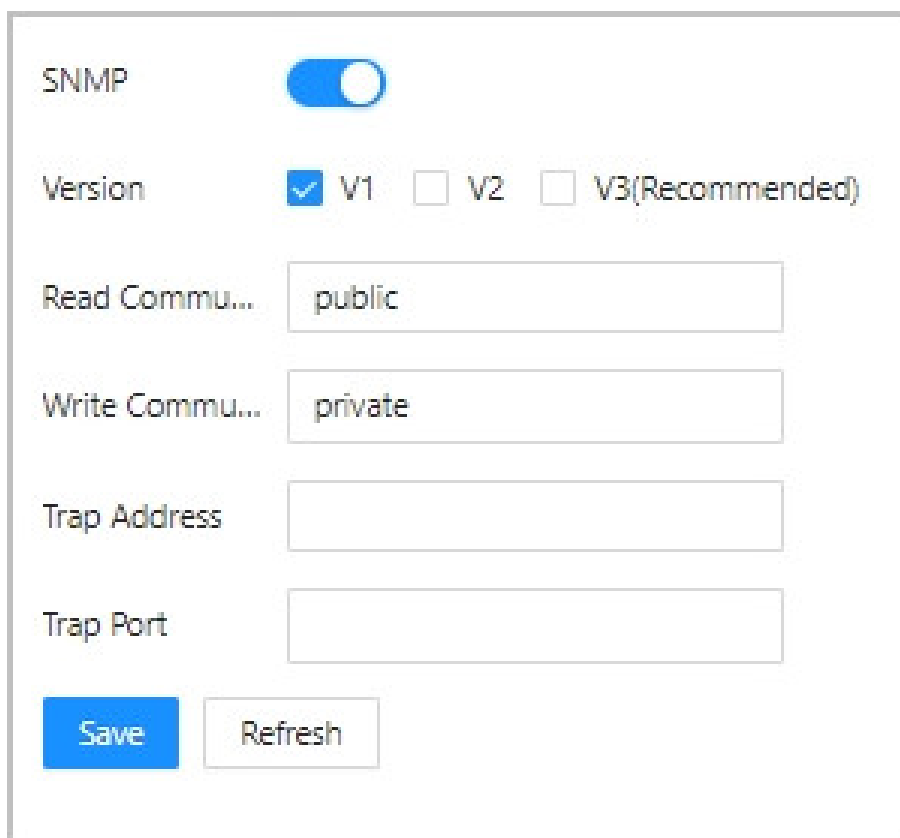
5.17.1 Configuring SNMP V1 and V2

Procedure

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

Step 2 Click  to enable the function.

Figure 5-37 SNMP

The image shows a web-based configuration interface for SNMP. At the top, there is a toggle switch labeled 'SNMP' which is currently turned on (blue). Below this, there are three radio buttons for 'Version': 'V1' is selected with a blue checkmark, 'V2' is unselected, and 'V3(Recommended)' is unselected. Further down, there are two text input fields: 'Read Commu...' containing the text 'public' and 'Write Commu...' containing the text 'private'. Below these are two more empty text input fields labeled 'Trap Address' and 'Trap Port'. At the bottom of the form, there are two buttons: a blue 'Save' button and a grey 'Refresh' button.

Step 3 Select **Version** as **V1** or **V2**.

Step 4 Configure **Read Community** , **Write Community**, **Trap Address** and **Trap Port**.

Step 5 Click **Save**.

5.17.2 Configuring SNMP V3

Procedure

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

Step 2 Click  to enable the function.



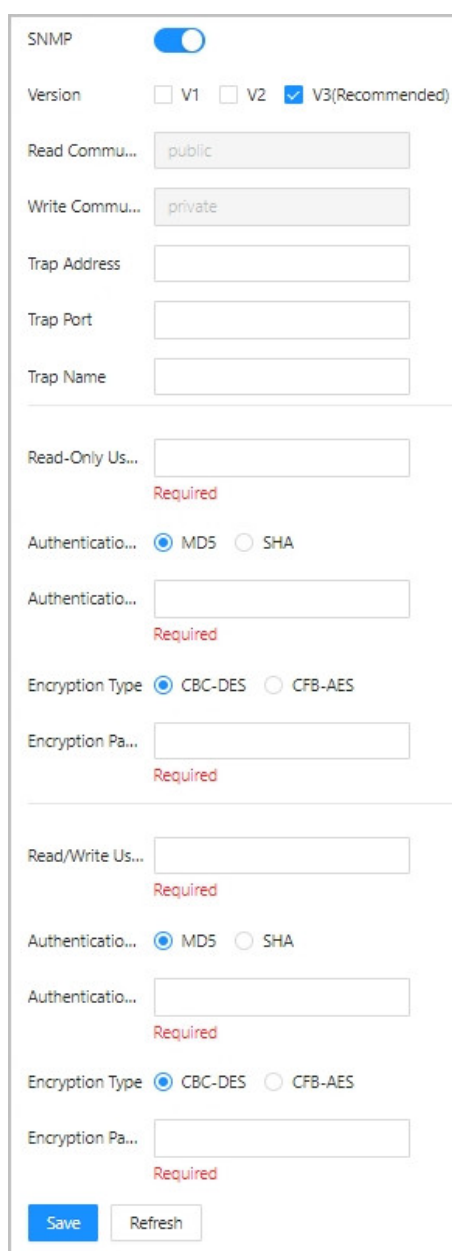
In SNMP version 3, each agent (a small program on a network device) has a unique identification code (engine ID) that is used to distinguish and identify each agent.

Step 3 Select **Version** as **V3**.

Step 4 Configure **Trap Address** , **Trap Port** and **Trap Name**.

Step 5 Configure **Read-Only Username** , **Authentication Type**, **Authentication Password**, **Encryption Type** and **Encryption Password**.

Figure 5-38 SNMP V3



The image shows a web-based configuration form for SNMP V3. At the top, there is a toggle switch for 'SNMP' which is turned on. Below this, the 'Version' section has three radio buttons: 'V1', 'V2', and 'V3(Recommended)', with 'V3(Recommended)' being selected. The 'Read Commu...' field contains the text 'public'. The 'Write Commu...' field contains the text 'private'. There are empty input fields for 'Trap Address', 'Trap Port', and 'Trap Name'. A horizontal line separates the top section from the bottom section. The bottom section has a 'Read-Only Us...' field with a red 'Required' label below it. Below this are radio buttons for 'Authenticatio...' with 'MD5' selected and 'SHA' unselected, followed by an empty 'Authenticatio...' field with a red 'Required' label. Then are radio buttons for 'Encryption Type' with 'CBC-DES' selected and 'CFB-AES' unselected, followed by an empty 'Encryption Pa...' field with a red 'Required' label. Another horizontal line separates this from the final section. The final section has a 'Read/Write Us...' field with a red 'Required' label, followed by radio buttons for 'Authenticatio...' with 'MD5' selected and 'SHA' unselected, an empty 'Authenticatio...' field with a red 'Required' label, radio buttons for 'Encryption Type' with 'CBC-DES' selected and 'CFB-AES' unselected, and an empty 'Encryption Pa...' field with a red 'Required' label. At the bottom are two buttons: 'Save' (blue) and 'Refresh' (grey).

Step 6 Configure **Read/Write Username** , **Authentication Type**, **Authentication Password**, **Encryption Type** and **Encryption Password**.

Step 7 Click **Save**.

6 Security

6.1 Configuring Accounts

Procedure

- Step 1 Select **Security** > **Account**, and then you can view the account list.
- Step 2 Click **Add** to add new users by entering username, password, confirming password, and then configuring permission level.

You can log in to the device webpage with the username and password to complete the configuration. The higher the permission level, the greater the permission and the more configuration functions it supports.



Password must be 8 to 32 characters, including at least 2 of the following categories: numbers, uppercase letters, lowercase letters and special characters (characters like ' " ; : & cannot be included in).

Figure 6-1 Add the account

- Step 3 Click **OK**.

6.2 Configuring Login Mode

Procedure

- Step 1 Select **Security** > **Login Mode**.
- Step 2 Click ☐ next to **SSH** to enable SSH function.

SSH (Secure Shell) is a security protocol based on the application layer. SSH is a relatively reliable protocol designed to provide security for remote login sessions and other network services. Enabling SSH allows you to remotely log in to the device through the background, effectively preventing information leakage during remote management.

Step 3 Click  next to **HTTPS** to enable HTTPS function.

HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer) is a secure HTTP channel that ensures the security of the transmission process through transmission encryption and identity authentication based on HTTP. After enabling HTTPS, you need to use the https://IP address format to access the device webpage.

Step 4 Click **Save**.

6.3 Configuring RADIUS

RADIUS (Remote Authentication Dial-In User Service) is a protocol specifically used for user authentication, authorization, and accounting information exchange between NAS (Network Access Server) servers and RADIUS servers. This protocol enables network administrators to flexibly set access control policies for different users or user groups, and provides accounting functions, thereby effectively managing the use of network resources. By applying RADIUS, network security is enhanced, effectively preventing illegal access, and realizing functions such as user identity authentication, permission management, and audit tracking.

Work Mode

When you attempt to connect to the network, the NAS sends its authentication information to the RADIUS server. The RADIUS server processes the authentication request and decides whether to allow the connection, thus ensuring that only authorized users can securely access the network.

Applicable scenarios

RADIUS is widely used in network environments that require high security and allow remote access, such as enterprise networks, campus networks, and Internet Service Provider (ISP) networks.

6.3.1 Configuring DNS

Use this device as a NAS server. When the end user accessing the device initiates a network connection application, this device forwards the user information to the RADIUS server for authentication.

Procedure

Step 1 Select **Security** > **RADIUS** > **NAS**.

Step 2 Click  next to **Mode** to enable NAS function.

Step 3 Click  next to **Re-authentication** to enable re-authentication function.

After passing authentication, they will need to re-authenticate at regular intervals.

Step 4 Select the management status corresponding to the port.

- **Force-authorized:** NAS requires that all users be authorized. Users must be authenticated and authorized by the RADIUS server before they can access network resources.
- **Force-unauthorized:** NAS does not require users to be authenticated and authorized by a RADIUS server, allowing users to directly access network resources.
- **Port-based 802.1X:** Control user rights based on the access port, which is applicable to 802.1X network. When a user has passed the authentication and authorization on the port, other users do not need to authenticate and authorize again.

- **MAC-based Auth:** The NAS determines whether a user is allowed to access the network based on the device's MAC address.

Figure 6-2 NAS settings

Port	Authorization Method	Port Status
1	Force-authorized	Globally Disabled
2	Force-unauthorized	Globally Disabled
3	Port-based 802.1X	Globally Disabled
4	MAC-based Auth	Globally Disabled
5	Force-authorized	Globally Disabled
6	Force-authorized	Globally Disabled

Step 5 Click **OK**.

6.3.2 Adding RADIUS Servers

Prerequisites

- The NAS function has been enabled.
- The RADIUS server information has been obtained.

Procedure

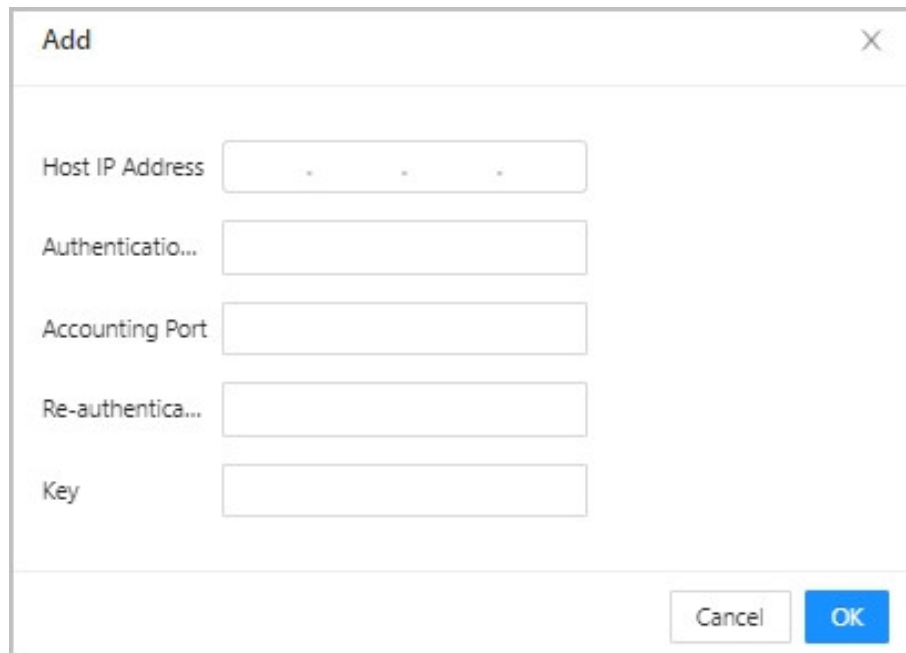
Step 1 Select **Security** > **RADIUS** > **RADIUS**.

Step 2 Click **Add**.

Step 3 Configure the host IP address, authentication port, accounting port, re-authentication times and key of the RADIUS server.

Since the RADIUS protocol uses UDP packets to carry data, its communication process is not reliable. After setting the number of re-authentication times, if the device does not receive a response from the RADIUS server within the time specified by the response timeout timer, the device will retransmit the RADIUS request packet to the RADIUS server.

Figure 6-3 Add the RADIUS



The image shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains five input fields, each with a label to its left: "Host IP Address" (with a placeholder "x . x . x"), "Authenticatio...", "Accounting Port", "Re-authentica...", and "Key". At the bottom right of the dialog are two buttons: "Cancel" and "OK".

Field Label	Input Type
Host IP Address	Text (with placeholder "x . x . x")
Authenticatio...	Text
Accounting Port	Text
Re-authentica...	Text
Key	Text

Buttons: Cancel, OK

Step 4 Click **OK**.

7 Control Policy

7.1 Managing ACL

ACL (Access Control List) is used to implement flow identification. In order to filter messages, network devices need to configure a series of matching conditions to classify messages. These conditions can be the source address, destination address, port number and other messages.

When the port of the device receives a message, it analyzes the fields of the message according to the ACL rules applied on the current port. After identifying a specific message, it allows or prohibits the message from passing according to the pre-set policy.

7.1.1 Configuring ACL

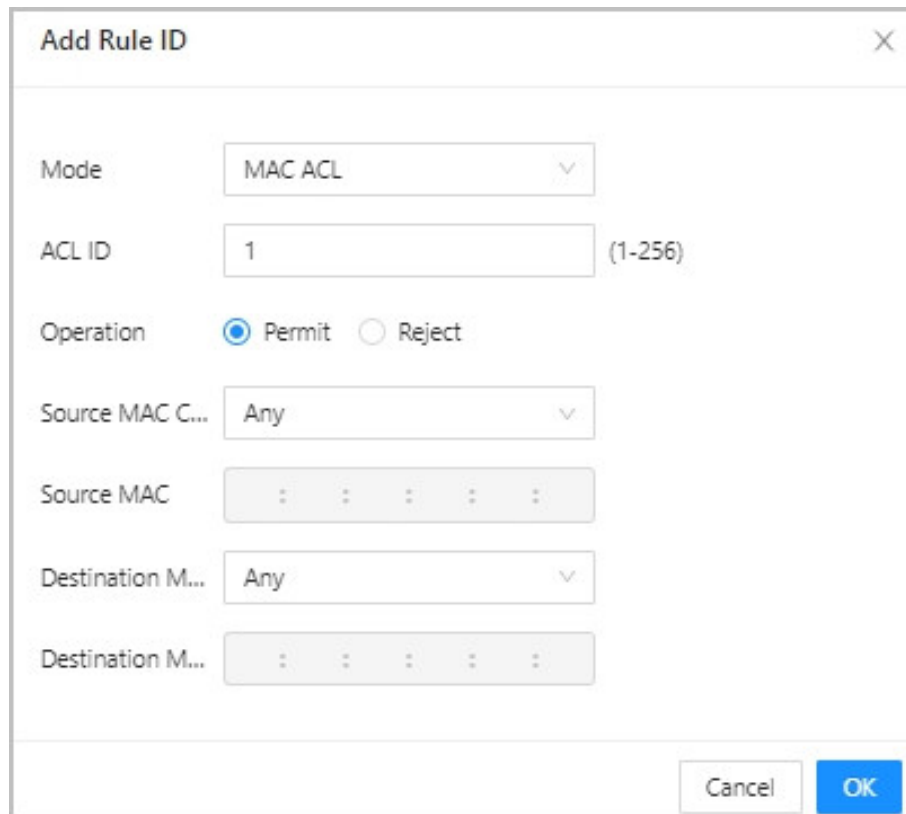
Procedure

- Step 1 Select **Control Policy** > **ACL** > **ACL**.
- Step 2 Click **Add**.
- Step 3 Select the mode and configure the ACL ID.
- Step 4 Select **Permit** or **Reject** and enter the detailed MAC address or IP address.
 - When you select **MAC ACL**, you need to set the source MAC address and destination MAC address.
 - When you select **IP ACL**, you need to set the protocol type (TCP, UDP), source IP address, and destination IP address.



- Example 1: Select **MAC ACL** for mode, **Permit** for operation, **Any** for source MAC, **Designate** for destination MAC, and set the destination MAC to 00:00:00:00:00:01, which means that any device with any MAC address can access the specified MAC (00:00:00:00:00:01).
- Example 2: Select **MAC ACL** for mode, **Reject** for operation, **Any** for source MAC, **Designate** for destination MAC, and set destination MAC to 00:00:00:00:00:01, which means that devices with any MAC address cannot access the specified MAC (00:00:00:00:00:01).

Figure 7-1 Add the rule ID

A screenshot of a web-based configuration window titled "Add Rule ID" with a close button (X) in the top right corner. The window contains several input fields: "Mode" is a dropdown menu set to "MAC ACL"; "ACL ID" is a text box containing "1" with a range "(1-256)" to its right; "Operation" has two radio buttons, "Permit" (selected) and "Reject"; "Source MAC C..." is a dropdown menu set to "Any"; "Source MAC" is a text box with five colons ":"; "Destination M..." is a dropdown menu set to "Any"; and "Destination M..." is a text box with five colons ":". At the bottom right are "Cancel" and "OK" buttons.

Add Rule ID

Mode: MAC ACL

ACL ID: 1 (1-256)

Operation: ☒ Permit ☐ Reject

Source MAC C...: Any

Source MAC: : : : : :

Destination M...: Any

Destination M...: : : : : :

Cancel OK

Step 5 Click **OK**.

7.1.2 Applying ACL Rules

Apply the added MAC ACL or IP ACL to a specific port.

Prerequisites

The ACL ID has been added to the ACL.

Procedure

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

Step 2 Enter the ACL ID in the **ACL ID** column corresponding to the port.

When you need to enter multiple ACL IDs, you can use commas to separate them.

Figure 7-2 Configure the port

Port	ACL ID
1	<input type="text" value="1,2"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>

Step 3 Click **Save**.

7.2 Configuring QoS

QoS(Quality of Service) improves network resource utilization and allows different types of traffic to compete for network resources based on their priorities, so that important data applications are preferentially processed on network devices.

7.2.1 Configuring Port Classification

By setting different CoS values for ports, the priority of packets passing through the device's outbound port is determined. When the outbound port is congested, after the packet passes through the inbound port, the device will assign a CoS value to the packet passing through the port. The larger the CoS value, the higher the priority, and the packet will pass through the port first.

Procedure

Step 1 Select **Control Policy > QoS > Port Classification**.

Step 2 Set the port CoS value.

For example, set the CoS value of port1 to 1, and set the CoS value of port2 to 2. Ports 1 and 2 are input ports, port3 is the output port, and the CoS value of port2 is greater than the CoS value of port1, and then the data of port2 will be sent out through port3 first.

Figure 7-3 Port classification

Port	CoS	DSCP
1	1	<input type="checkbox"/>
2	2	<input type="checkbox"/>
3	0	<input type="checkbox"/>
4	0	<input type="checkbox"/>
5	0	<input type="checkbox"/>
6	0	<input type="checkbox"/>
7	0	<input type="checkbox"/>
8	0	<input type="checkbox"/>

Step 3 Select the **DSCP** corresponding to the port to enable the function.

After enabling **DSCP**, support setting the corresponding priority for different DSCP through **DSCP-Based** page.



Port classification manages the priority of different data by recognizing data sources, and DSCP provides a clear priority tag for each data packet.

Step 4 Click **Save**.

7.2.2 Configuring Scheduling

Background Information

The port scheduling modes are divided into **Strict Priority** and **n Queues Weighted**. N is an integer variable. The value of n varies on different devices. Please refer to the actual interface for details.

- **Strict Priority**: In the case of congestion, the CoS value of the port classification determines the priority of the message passing through the egress port.
- **n Queues Weighted**: In the case of congestion, the priority of the message passing through the egress port is determined according to the proportion of the total rate.

Procedure

Step 1 Select **Control Policy > QoS > Port Scheduling**.

Step 2 Click  in the **Details** column to enter the editing page.


Step 3 Select **Scheduling Mode**.

Step 4 Configure the port shaping,



The settings here take effect simultaneously on the port shaping page.

1. In the **Ingress Shaping per Queue** area, enable the queue and set the rate at which data enters the queue.

- When **Strict Priority** is selected for the scheduling mode, select the enable box  of the queue and set the speed, unit, and rate type.

- When the scheduling mode is **n Queues Weighted**, select the enable box ☒ of the queue, set the speed, unit, rate type, weight and the percentage.

Figure 7-4 Set ingress shaping per queue

QPort	Enable	Speed	Unit	Rate type	Weight	Percentage
Q0	<input checked="" type="checkbox"/>	500	kbps	Line	17	33%
Q1	<input checked="" type="checkbox"/>	500	kbps	Line	17	33%
Q2	<input checked="" type="checkbox"/>	500	kbps	Line	17	33%
Q3	<input checked="" type="checkbox"/>	500	kbps	Line		
Q4	<input type="checkbox"/>	500	kbps	Line		

2. In the **Egress Shaping per Queue** area, select the enable box ☒ and set the speed and unit for when data leaves the queue.

Step 5 Click **OK**.

7.2.3 Configuring Port Shaping

Select **Control Policy > QoS > Port Shaping** to view the port speed. Click in the **Details** column to enter the editing page. For the configuration of port shaping, see "7.2.2 Configuring Scheduling".

7.2.4 Configuring DSCP-Based

DSCP is a field in the IP packet header that identifies the priority and service level of different types of data flows in the network. By setting the CoS value of the DSCP value, the device can classify, schedule and process data packets, thereby achieving priority allocation for different traffic flows.

Prerequisites

The DSCP function has been enabled for port classification.

Procedure

Step 1 Select **Control Policy > QoS > DSCP-Based**.

Step 2 Configure the DSCP function.

For example, when the DSCP value is set to 4 and 8, the CoS value are set to 2 and 1 respectively.

1. Select the ☒ in the **Trust** column for DSCP values 4 and 8.
2. Set the CoS value of the DSCP value of 4 to 2.

3. Set the CoS value of the DSCP value of 8 to 1.

The larger the CoS value corresponding to the DSCP value, the higher the priority. The corresponding ingress port message will be preferentially transmitted through the egress port.

Figure 7-5 DSCP-Based

Port Classification	Port Scheduling	Port Shaping	DSCP-Based	Storm Control
DSCP		<input type="checkbox"/> Trust		CoS
3		<input type="checkbox"/>		0
4		<input checked="" type="checkbox"/>		2
5		<input type="checkbox"/>		0
6		<input type="checkbox"/>		0
7		<input type="checkbox"/>		0
8		<input checked="" type="checkbox"/>		1
9		<input type="checkbox"/>		0
10		<input type="checkbox"/>		0

Step 3 Click **Save**.

7.2.5 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 > QoS > Storm Control**.

Step 2 Enable the storm suppression function for the corresponding frame type (such as unicast) and set the port receive speed and unit.

For example, as shown in the figure below, the maximum receiving speed is set to 10 fps.



Different devices support different rates. Please refer to the page prompts to set the accurate rate value.

Figure 7-6 Configure storm control

Speed must be a multiple of 10 fps or 25 Kbps.

Frame Type	Enable	Speed	Unit
Unicast	<input checked="" type="checkbox"/>	10	fps
Multicast	<input type="checkbox"/>	10	fps
Broadcast	<input type="checkbox"/>	10	fps

Save

Refresh

Step 3 Click **Save**.

Appendix 1 Security Recommendation

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

The 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, it is recommended 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 Allow list**

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

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;
- Establish 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**

It is recommended 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).