



Ethernet Switch

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About Defaults

- Default IP address: 192.168.1.64
- Default user name (activation is required): admin

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Note	Provides additional information to emphasize or supplement important points of the main text.
 Caution	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Danger	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

TABLE OF CONTENTS

Chapter 1 Configuration Introduction	1
1.1 Product Introduction	1
1.2 Environment Configuration	1
Chapter 2 Activation and Login	2
2.1 Activate Device	2
2.2 Log In to Device	4
Chapter 3 Device Overview	6
Chapter 4 Device Monitoring	8
4.1 Configure Device Monitoring	8
4.2 View Port Details	11
Chapter 5 Device Configuration	12
5.1 Basic Configuration	12
5.1.1 Port Configuration	12
5.1.2 VLAN Configuration	23
5.1.3 MAC Address Configuration	27
5.1.4 ARP Configuration	31
5.1.5 IPv4 Configuration	32
5.1.6 IPv6 Configuration	38
5.1.7 DHCP Configuration	45
5.2 Advanced Configuration	57
5.2.1 STP Configuration	57
5.2.2 LLDP Configuration	67
5.2.3 IGMP Snooping Configuration	71
5.2.4 PoE Configuration	78
5.2.5 OSPF Configuration	79
5.2.6 Time Range Configuration	97
5.2.7 ERPS Configuration	98
5.2.8 SNMP Configuration	105
5.3 Security Configuration	117
5.3.1 ACL Configuration	117
5.3.2 QoS Configuration	137
5.3.3 AAA Configuration	152
5.3.4 802.1X Configuration	164
5.3.5 IP-MAC Binding Configuration	168
5.3.6 DHCP Snooping Configuration	172
5.3.7 Security Protection Configuration	177
5.3.8 IPSG Configuration	181
5.3.9 Port Security Configuration	185
Chapter 6 Device Diagnosis	191
6.1 Network Diagnosis	191

6.1.1 Configure Ping	191
6.1.2 Configure Trace	196
6.2 Cable Detection	199
Chapter 7 System Configuration	200
7.1 Time Configuration	200
7.1.1 Configure Time Synchronization	200
7.1.2 Configure Authentication Key	205
7.2 System Maintenance	206
7.2.1 Restart Device	206
7.2.2 Upgrade Device	207
7.2.3 Back Up Device	207
7.2.4 Reset Device	207
7.2.5 Export Diagnostic Info	208
7.3 Network Configuration	209
7.3.1 Configure Management Address	209
7.3.2 Configure Management Port	210
7.3.3 Configure DNS Server	212
7.3.4 Configure Cloud Service	214
7.3.5 Configure SADP	216
7.4 Remote Service	216
7.5 Security Service	218
7.6 Log Management	219
7.6.1 Query Security Audit Logs	219
7.6.2 Configure Log Server	219
7.6.3 Query Alarm Logs	220
7.7 User Management	221
7.8 Login Management	225

Chapter 1 Configuration Introduction

1.1 Product Introduction

This product is a full managed switch designed for enterprise and campus networks. It features a brand-new hardware architecture and an independently developed software platform, optimized specifically for high port density and enhanced security scenarios. In addition to delivering full-speed forwarding performance, it integrates a comprehensive set of functions including network topology management, link aggregation, VLAN assignment, MAC address binding, xSTP ring protection, and ACL/QoS policies. With its user-friendly web-based configuration interface and reliable performance, it significantly improves network management efficiency—making it an ideal solution for building highly reliable and intelligent networks.



Note

The actual supported functions may vary depending on the product model and software version.

1.2 Environment Configuration

The device supports web-based management through its Ethernet interface (used for service transmission). After connecting a PC to the switch via an Ethernet port, users can remotely access and configure the switch using a web browser. To get started, set your computer's IP address to be on the same network segment as the switch, then log in to the web management interface.

1. Use an Ethernet cable to connect any Ethernet interface (i.e., the RJ45 port) of the switch to the Ethernet port of a PC.
2. Configure the computer's IP address to be on the same network segment as the switch's IP address.



Note

The switch's default IP address is 192.0.0.64/24. You may set the computer's IP address to 192.0.0.XXX (where XXX ranges from 1 to 63 or 65 to 253). Alternatively, manually assign both the switch's and the computer's IP addresses within the same subnet to ensure the computer can ping the switch and access its web configuration page.

3. Open a browser, enter the switch's IP address in the address bar, and press **Enter** to access the switch's web login interface.



Note

We recommend that you use the following browsers to access the switch's web interface: Google Chrome 91.0, Firefox 88.0, Microsoft Edge 91.0, or Safari 13.0 and above.

Chapter 2 Activation and Login

2.1 Activate Device

To ensure the security and privacy of your personal account, as well as the protection of system and data, you should set a login password and activate the device before performing any function configurations via the web interface after initial startup.

Before You Start

- Ensure your computer is on the same network segment as the device.
- Use one of the following supported browsers: Google Chrome 91.0 or later, Firefox 88.0 or later, Microsoft Edge 91.0 or later, or Safari 13.0 or later.

1. Open your web browser.
2. Enter the IP address of the device in the address bar and press **Enter**.

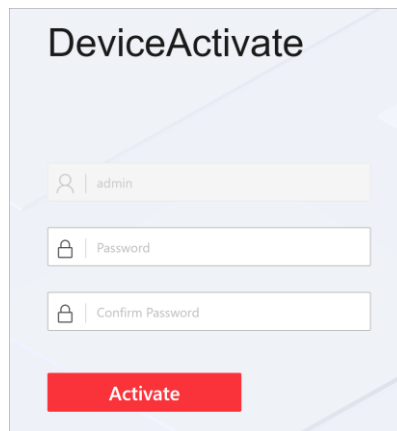


Figure 2-1 Activate Device

3. Set and confirm the new password.

Note

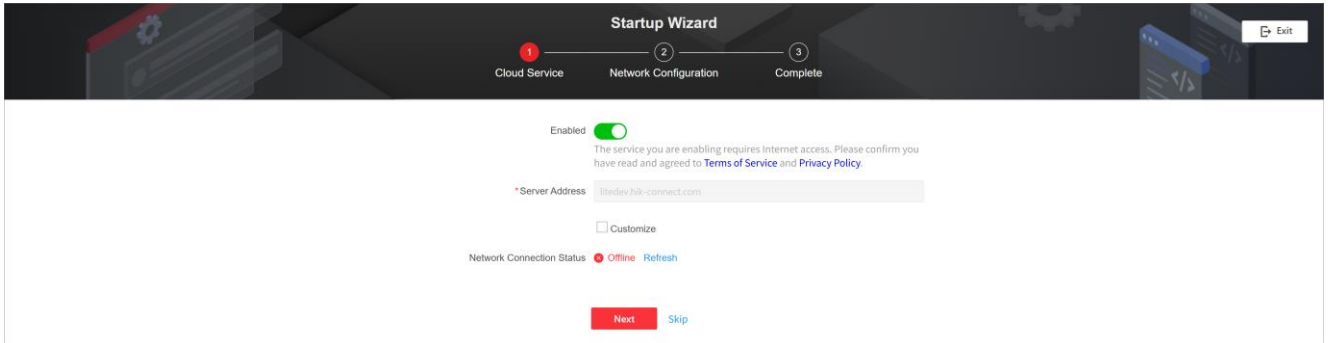
- The password should contain 8 to 16 characters and include at least two of the following character types: digits, uppercase letters, lowercase letters, and special characters.
- The password cannot contain the username, forbidden strings such as "123", "admin" (case-insensitive), "hik", "hkws", "hikvision", four or more consecutive ascending or descending digits (e.g., 1234, 4321), or four or more consecutive repeated characters (e.g., 1111, aaaa).
- The password cannot be a commonly used weak or risky password.

4. Click **Activate**.
5. After activation, follow the startup wizard to initialize and configure the device.

 Note

- If you do not want to perform the initial setup at this time, click **Exit** in the upper right corner to exit the wizard and log in directly.
- Once the device is activated, the startup wizard will appear during the first login. After completing the initial configuration, the wizard will no longer be accessible in subsequent logins.

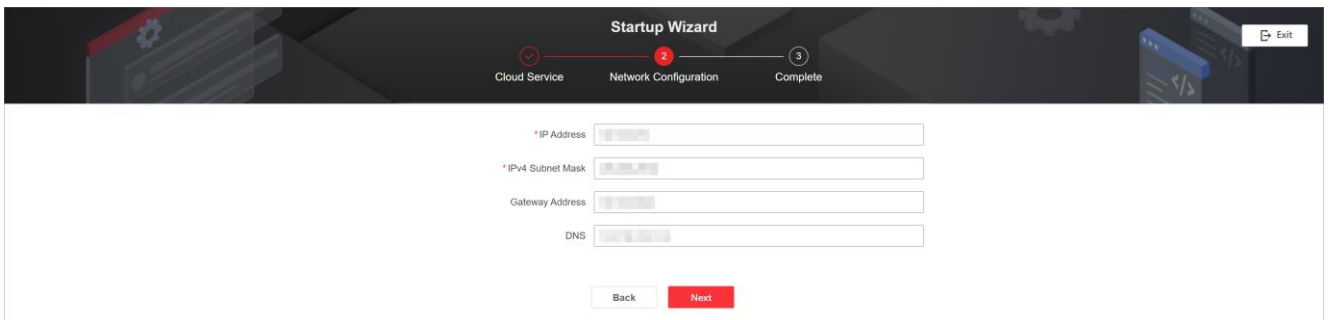
1) Configure cloud service.

**Figure 2-2** Configure Cloud Service

- Enable cloud service.
- Select **Customize** and enter the server IP address.
- Check if the network connection status is online. If it is offline now, please check your network connection and click **Refresh** to update the status.
- Click **Next**.

 Note

If no cloud service configuration is required, click **Skip** to skip the current step and proceed to the Network Configuration.

2) Configure network parameters: IP address, subnet mask, gateway address, and DNS server address as needed, and click **Next**.**Figure 2-3** Configure Network Parameters

- 3) Wait until the startup wizard configuration is complete and click **Complete** to automatically redirect to the new IP address.

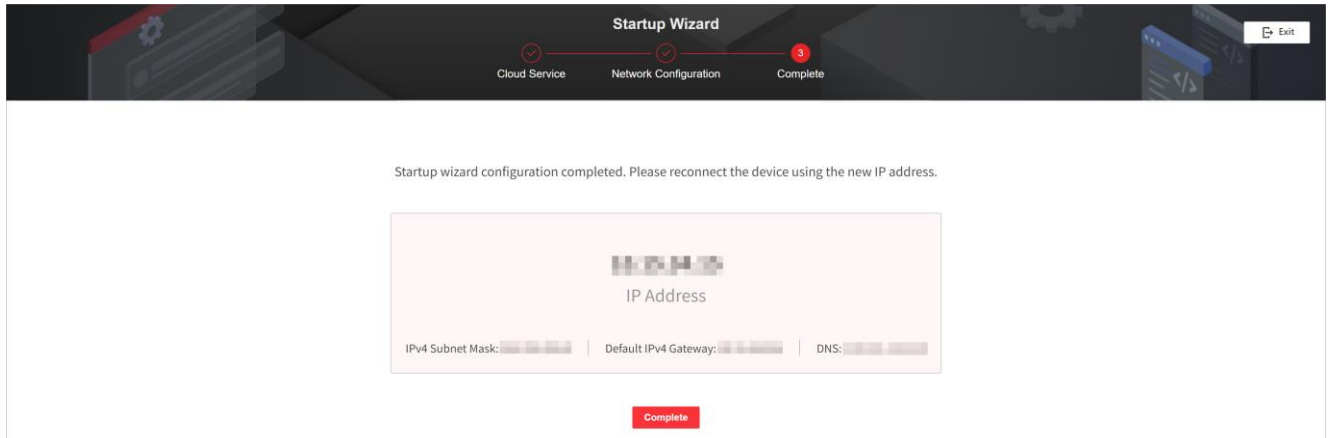


Figure 2-4 Complete Startup Configuration

Note

- If the switch's IP address is modified within the same subnet as the PC's IP address, no gateway configuration is required, and the web browser will automatically redirect to the new IP address.
- If the switch's IP address is changed to a different subnet than the PC's, the switch must be configured with a gateway address matching the PC's IP address to ensure successful redirection to the new IP address.

2.2 Log In to Device

After you log in to the device via a web browser, you can view device information and configure related functions.

Steps

1. Enter the device IP address in the address bar of your browser and press **Enter**.
2. Enter the user name and password.

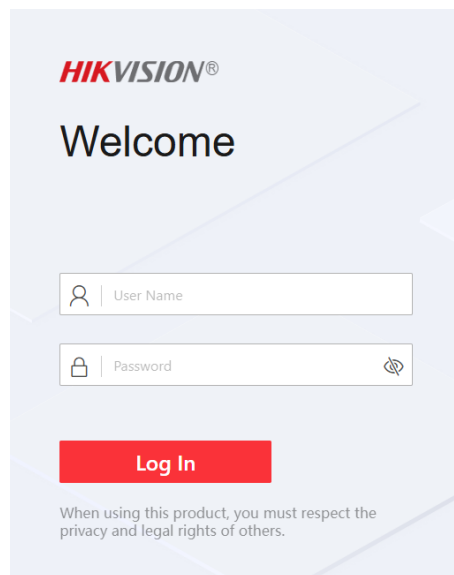


Figure 2-5 Log In to Device

 Note

- The device will be locked for 5 minutes after 5 consecutive failed password attempts.
- To enhance device security, it is recommended to change your password upon first login and update it periodically. To change the user password, go to **admin -> Change Password** in the upper-right corner.
- If you forget the device's IP address or password, you can restore it to factory settings by pressing and holding the Reset button on the device panel for more than 5 seconds while the device is powered on. After restoration, you can log in using the default IP address and reactivate the device. Please note that restoring factory settings will erase all existing configurations.

3. Click **Log In**.

Chapter 3 Device Overview

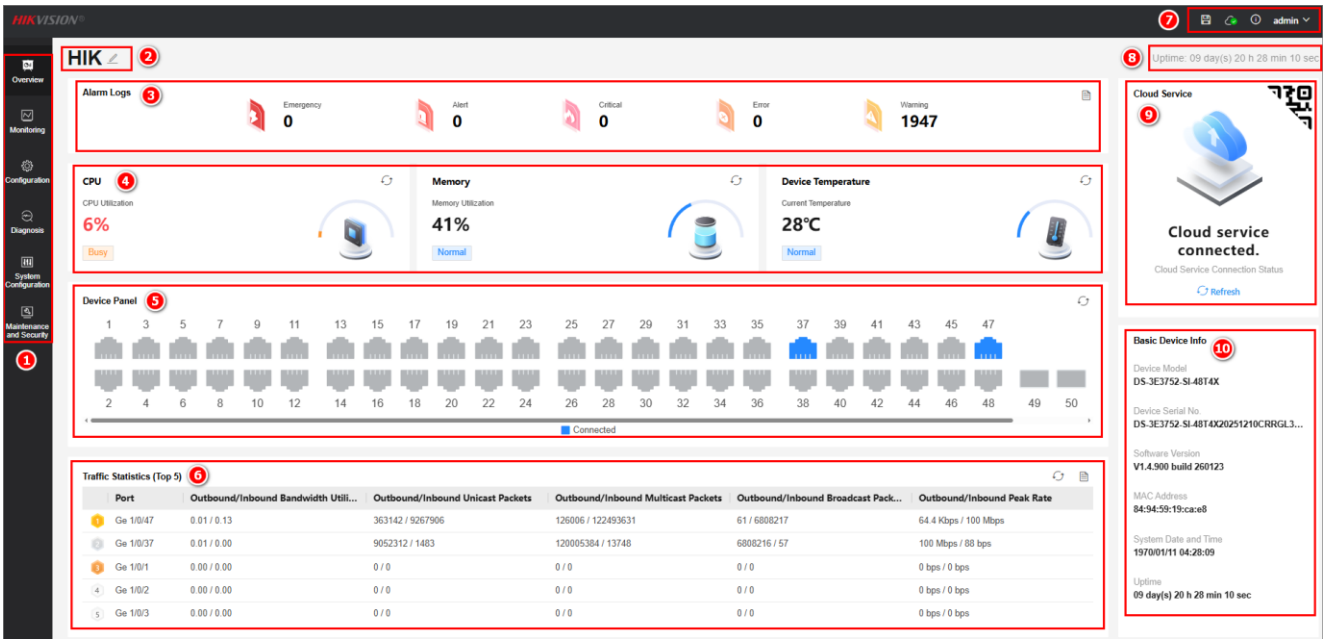


Figure 3-1 Home Page Overview

The Web home page of the full managed switch is mainly composed of the following modules:

No.	Module	Function Description
①	Navigation Menu	The navigation menu is used to switch between different configuration pages and configure corresponding functions.  Note Click  to always show or hide the sub-navigation menu.
②	Device Name Customization Module	Customize your device name to differentiate it from other devices.
③	Alarm Log Information Module	This module displays the number of alarm log entries recorded at each level for the device. Click on a specific alarm level to view its detailed logs, or click  on the right to view logs for all alarm levels.
④	Device Status Display Module	This module displays the device's CPU usage, memory usage, and current temperature.

⑤	Device Panel	The device panel displays the types and quantities of device ports and their connection status.
⑥	Traffic Statistics Module	This module displays the top 5 ports' traffic statistics for the device, including outbound/inbound bandwidth utilization (%), outbound/inbound unicast packets, outbound/inbound multicast packets, outbound/inbound broadcast packets, and outbound/inbound peak rate. Click  on the right to view traffic statistics for all ports of the device.
⑦	Tool Bar	Quick access to save configuration, view cloud service status, obtain online help, change password, and log out.
⑧	Device Uptime Module	This module displays the uptime of the current device.
⑨	Cloud Service Connection Status Display Module	Indicates the current cloud platform connection status of the device. • If the device is connected to the cloud platform, scan the QR code to add it to the Hik-Partner Pro app for remote management. • If the device is not connected to the cloud platform, you can click Diagnosis to diagnose the cause of connection failure or further click Configuration to go to the Cloud Service configuration page for configuration operations.
⑩	Basic Device Information Module	This module displays device model, serial No., software version, MAC address, system date and time, and device uptime.

 Note

- The device automatically refreshes its information and port data every 30 seconds.
- Users can also manually update device status, device panel, and top 5 ports' traffic statistics by clicking .

Chapter 4 Device Monitoring

4.1 Configure Device Monitoring

Click **Monitoring** -> **Device Details** to view the CPU, memory, temperature, and fan details of the switch, and perform relevant alarm settings.

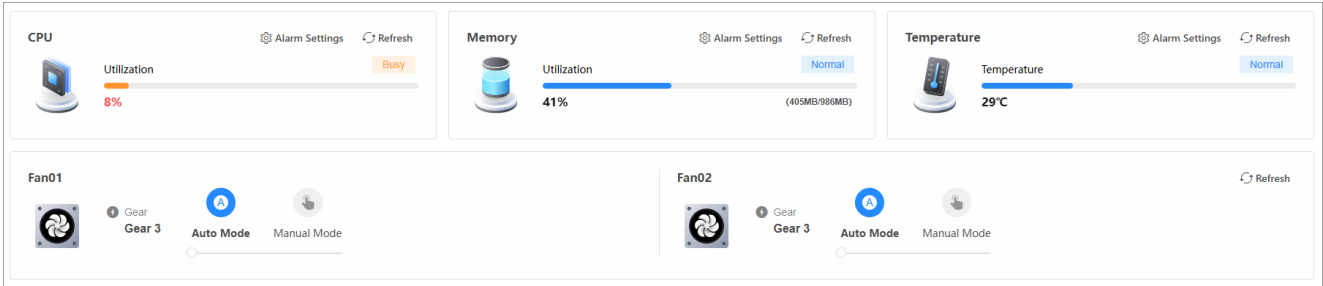


Figure 4-1 Device Details Alarm Settings

- CPU: This module allows you to monitor the device's CPU running status and current utilization rate, and configure CPU alarm settings.

1. Click **Alarm Settings**.

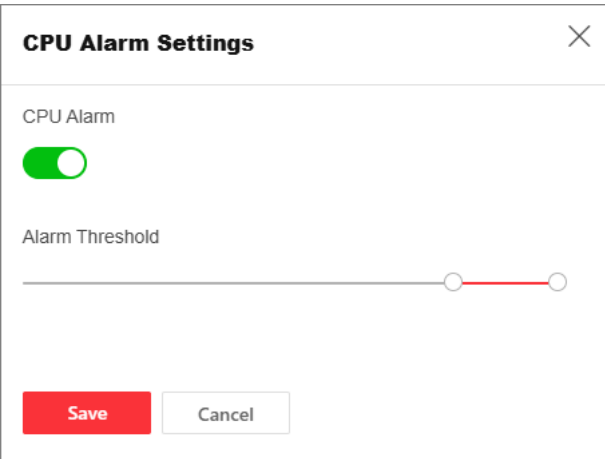


Figure 4-2 Configure CPU Alarm Settings

2. Enable **CPU Alarm**.
3. Drag the slider to manually set the low-level and high-level CPU usage thresholds for triggering alarms.

Note

The low-level alarm threshold can be set from 1% to 98%, and the high-level alarm threshold from 2% to 99%, with the high-level threshold required to be greater than the low-level threshold. Once CPU

alarm settings are configured, an alarm of the corresponding level will be triggered when the device's actual CPU usage falls below the low-level threshold or exceeds the high-level threshold.

4. Click **Save**.

- **Memory:** This module allows you to view the device's memory running status and current utilization rate, and configure memory alarm settings.

1. Click **Alarm Settings**.

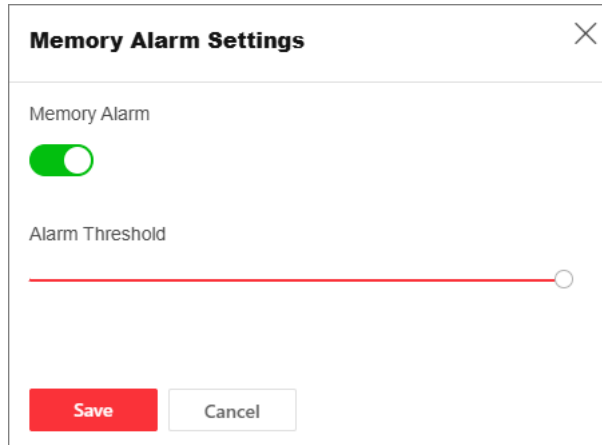
A screenshot of a web-based configuration window titled "Memory Alarm Settings". The window has a close button (X) in the top right corner. Inside, there is a section labeled "Memory Alarm" with a green toggle switch that is currently turned on. Below this is a section labeled "Alarm Threshold" with a horizontal slider bar. The slider bar is red and has a white circular handle positioned at the far right end, indicating 100%. At the bottom of the window, there are two buttons: a red "Save" button and a white "Cancel" button with a grey border.

Figure 4-3 Configure Memory Alarm Settings

2. Enable **Memory Alarm**.

3. Drag the slider to manually set the low-level and high-level memory usage thresholds for triggering alarms.

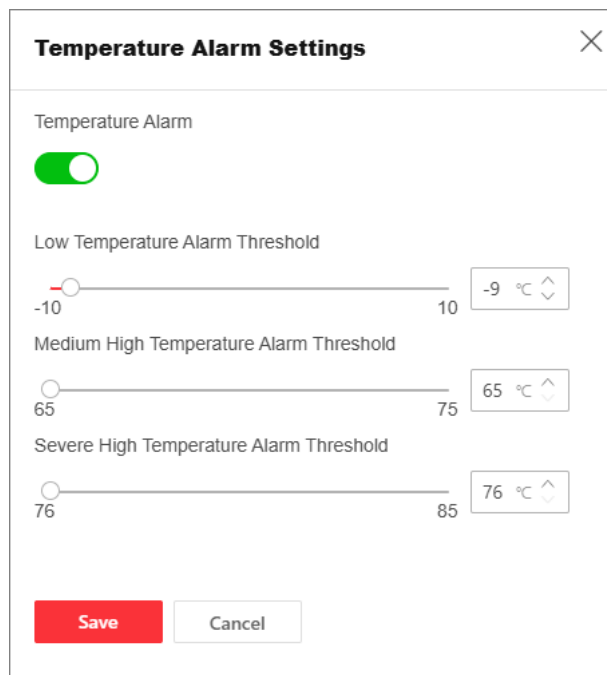
Note

The memory alarm threshold can be set from 0% to 100%. Once memory alarm settings are configured, an alarm will be triggered when the actual memory usage of the device exceeds this threshold.

4. Click **Save**.

- **Temperature:** This module allows you to view the device's temperature status and current temperature, and configure temperature alarm settings.

1. Click **Alarm Settings**.



The image shows a 'Temperature Alarm Settings' dialog box. At the top, there's a title bar with a close button (X). Below the title, the text 'Temperature Alarm' is followed by a green toggle switch that is turned on. Underneath, there are three temperature threshold settings, each with a slider and a numeric input box on the right. The first is 'Low Temperature Alarm Threshold' with a range from -10 to 10 and a value of -9. The second is 'Medium High Temperature Alarm Threshold' with a range from 65 to 75 and a value of 65. The third is 'Severe High Temperature Alarm Threshold' with a range from 76 to 85 and a value of 76. At the bottom, there are two buttons: 'Save' (red) and 'Cancel' (white).

Figure 4-4 Temperature Alarm Settings

2. Enable **Temperature Alarm**.
3. Drag the slider to manually set the following thresholds: Low Temperature Alarm, Medium High Temperature Alarm, and Severe High Temperature Alarm.

 Note

- You can also click the arrow on the right of the slider to manually adjust the temperature threshold. Each click on the up or down arrow will increase or decrease the threshold value by 1 °C.
 - The low, medium high, and severe high temperature alarm thresholds can be set within the ranges of -10 °C to 10 °C, 65 °C to 75 °C, and 76 °C to 85 °C, respectively. Once temperature alarm settings are configured, an alarm will be triggered when the actual temperature of the device falls below the low-temperature alarm threshold, rises above the medium high-temperature alarm threshold but does not exceed the severe high-temperature alarm threshold, or exceeds the severe high-temperature alarm threshold.
4. Click **Save**.
- Fan: This module enables you to monitor the fan speed level (gear) of the device and switch between automatic and manual modes.
 - In automatic mode, the fan speed level adjusts dynamically according to temperature changes.
 - In manual mode, you can adjust the fan speed level by dragging the slider.

4.2 View Port Details

Click **Monitoring** -> **Port Details** to view the outbound/inbound bandwidth utilization (%), unicast packets, broadcast packets, multicast packets, port rate, peak port rate, and error packets of each port.

You can select one or more ports, and then click **Clear** to clear the statistics of the selected ports, or directly click **Clear** to clear the statistics of all ports.

Clear Refresh								
☐	Port	Outbound/Inbound Bandwidth Utilization...	Outbound/Inbo...	Outbound/Inbo...	Outbound/Inbo...	Outbound/Inbound Port Rate	Outbound/Inbound Peak Rate	Outbound/Inbo...
☒	Ge 1/0/1	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☒	Ge 1/0/2	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/3	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/4	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/5	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/6	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/7	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/8	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/9	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/10	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/11	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/12	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/13	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/14	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/15	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/16	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/17	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/18	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/19	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0
☐	Ge 1/0/20	0.00 / 0.00	0 / 0	0 / 0	0 / 0	0 bps / 0 bps	0 bps / 0 bps	0 / 0

Figure 4-6 Port Details



Note

The outbound/inbound peak rate statistics of the port(s) will not be cleared.

Chapter 5 Device Configuration



Note

- The number and types of ports vary by device model, as do the supported features. Screenshots in this manual are for reference only. For actual supported functions, please refer to the device's product specifications.
- Settings configured via the **Save** button on individual pages take effect immediately but will be lost after a device reboot. To retain configurations after power-off or restart, click  in the upper right corner of the page. Saving global configuration also helps prevent accidental misconfiguration.

5.1 Basic Configuration

5.1.1 Port Configuration

Configure Port Attributes

If you need to configure the basic attributes such as the enable status, duplex mode, and rate of the selected port(s), or configure the advanced attributes such as description, flow control, traffic suppression, and bandwidth limit of the specified port, adjust relevant parameters in the port attribute settings. The configurable parameters vary depending on the port type. Please refer to the actual interface.

Steps

1. Click **Configuration** -> **Basic Configuration** -> **Port**.
2. In **Basic Configuration**, configure the basic attributes of the desired port(s) as needed.

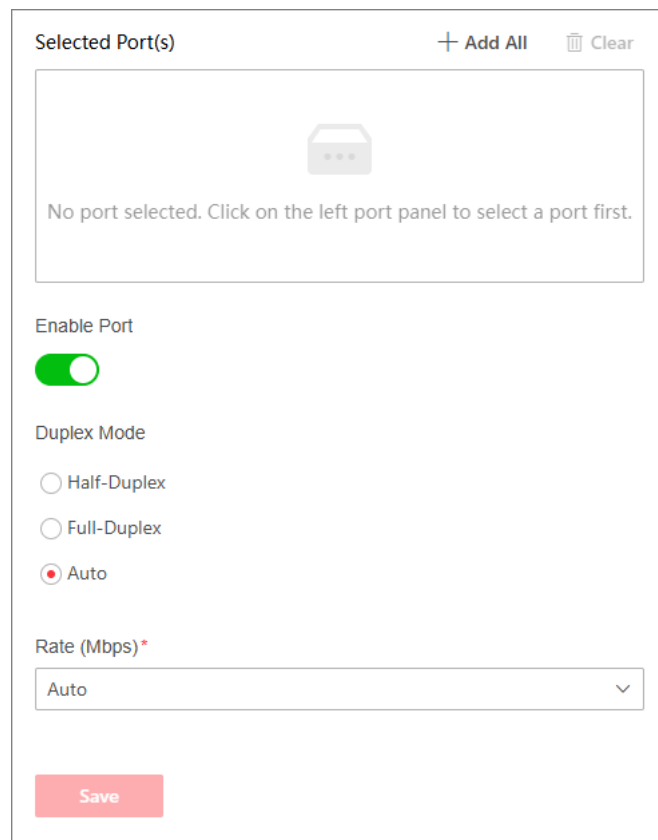


Figure 5-1 Configure Basic Attributes

- 1) Click to select one or more ports on the port panel, or click the aggregation group icon (for

example ) to select the corresponding aggregate interface above the port panel.

 Note

You can click **Add All** to batch select all Ethernet ports and aggregation groups, or click **Clear** to deselect the selected port(s).

- 2) Enable the selected port(s) as needed.

 Note

A port is enabled to allow data transmission, or disabled to block it.

- 3) Configure the duplex mode of the selected port(s).

Half-Duplex

Supports bidirectional data transmission but cannot transmit and receive data at the same time.

Full-Duplex

Supports bidirectional data transmission and can transmit and receive data at the same time.

Auto

The port automatically adjusts to the proper working mode according to the duplex mode of the peer device.

4) Configure the rate of the selected port(s).

5) Click **Save**.

3. Click **Advanced Configuration** to configure advanced attributes of the selected port as needed.

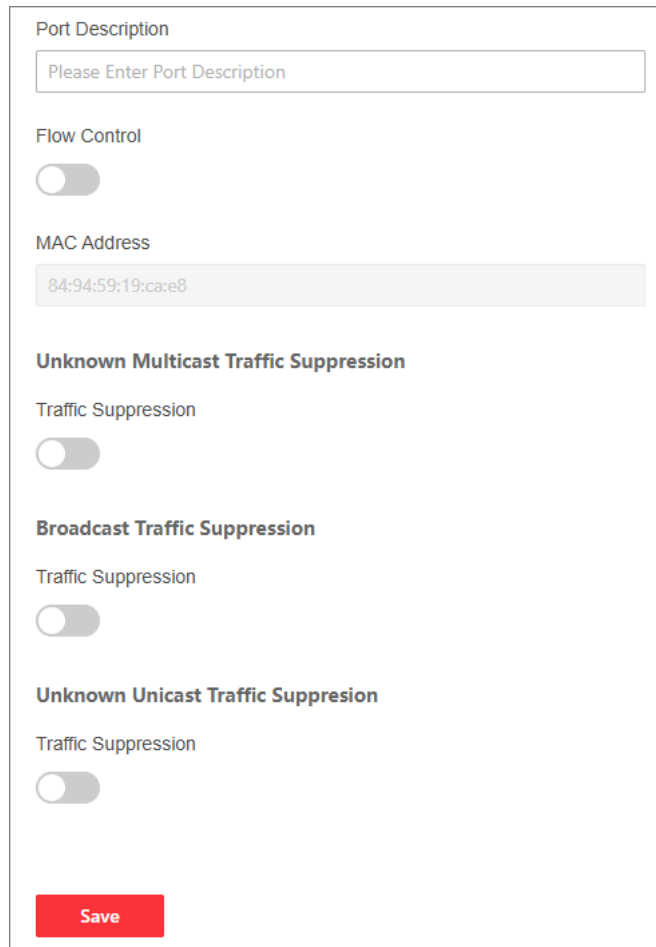
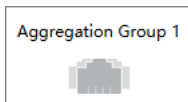


Figure 5-2 Configure Advanced Attributes

1) Click to select a port on the port panel, or click the aggregation group icon (for example



) to select the corresponding aggregate interface above the port panel.

2) Enter a description for the selected port.

Note

The port description cannot exceed 128 characters.

3) Enable flow control as needed.

 Note

- Enabling port flow control effectively prevents packet loss.
 - Flow control is not supported on aggregate interfaces.
- 4) Optional: Configure traffic suppression as needed to prevent broadcast storms and performance degradation resulting from the forwarding of unknown multicast, broadcast, or unicast packets to other VLAN interfaces when the egress port is undetermined.
1. Enable unknown multicast, broadcast, and unknown unicast traffic suppression as needed.

Unknown Multicast Traffic Suppression

Mitigates storms caused by unknown multicast packets by configuring the maximum receiving rate for multicast traffic. Packets exceeding this rate will be discarded.

Broadcast Traffic Suppression

Mitigates storms caused by broadcast packets by configuring the maximum receiving rate for broadcast traffic. Packets exceeding this rate will be discarded.

Unknown Unicast Traffic Suppression

Mitigates storms caused by unknown unicast packets by configuring the maximum receiving rate for unknown unicast traffic. Packets exceeding this rate will be discarded.

2. Configure the suppression unit and suppression threshold for unknown multicast, broadcast, or unknown unicast traffic.
 - If the unit is set to **ratio**, the valid range for the suppression threshold is 0 to 100.
 - If the unit is set to **pps**, the valid range for the suppression threshold is 0 to 1,488,100.
 - If the unit is set to **kpps**, the valid range for the suppression threshold is 0 to 1,000,000.
- 5) Optional: Adjust bandwidth limits as needed to prevent excessive consumption of network bandwidth resources.

Max. Inbound Bandwidth Rate (Kbps)

Specifies the maximum inbound bandwidth rate for the port. The value ranges from 16 to 1,000,000 kbps. It is recommended to configure the value as a multiple of 16; otherwise, inaccurate performance outcomes may result.

Max. Outbound Bandwidth Rate (Kbps)

Specifies the maximum outbound bandwidth rate for the port. The value ranges from 16 to 1,000,000 kbps. It is recommended to configure the value as a multiple of 16; otherwise, inaccurate performance outcomes may result.

 Note

Aggregate interfaces do not support traffic suppression or bandwidth limit configuration.

- 6) Set the maximum transmission unit (MTU).

 Note

By default, the MTU is set to 12000 bytes. When you need to ensure that large packets are not lost in the network, you can adjust the MTU of the port to set the size of packet fragmentation for large packets.

7) Click **Save**.

The **Port Details** list will display successfully configured information, including the actual connection status, enable status, actual and configured rate/duplex mode, as well as inbound and outbound bandwidth utilization for each port.

Port Details 					
Port	Connection St...	Enable Status	Actual Rate (Mbps)/Duplex M...	Configured Rate (Mbps)/Dupl...	Outbound/Inbound Bandwidt...
Ge 1/0/1	Disconnected	Enabled	1000 / Full-Duplex	Auto / Auto	0.00 / 0.00
Ge 1/0/2	Disconnected	Enabled	1000 / Full-Duplex	Auto / Auto	0.00 / 0.00
Ge 1/0/3	Disconnected	Enabled	10 / Half-Duplex	10 / Half-Duplex	0.00 / 0.00
Ge 1/0/4	Disconnected	Enabled	1000 / Full-Duplex	Auto / Auto	0.00 / 0.00
Ge 1/0/5	Disconnected	Enabled	1000 / Full-Duplex	Auto / Auto	0.00 / 0.00
Ge 1/0/6	Disconnected	Enabled	1000 / Full-Duplex	Auto / Auto	0.00 / 0.00
Ge 1/0/7	Disconnected	Enabled	1000 / Full-Duplex	Auto / Auto	0.00 / 0.00
Ge 1/0/8	Disconnected	Enabled	1000 / Full-Duplex	Auto / Auto	0.00 / 0.00

Figure 5-3 View Port Details

Configure Port Isolation

The port isolation function enables you to assign specified ports to an isolation group, preventing communication between ports within the same group.

1. Click **Configuration** -> **Security Configuration** -> **Port Isolation**.
2. Add an isolation group.

Figure 5-6 Configure Port Isolation

- 1) Select one or more ports to be added to the isolation group on the port panel, or click the aggregation group icon above the port panel to select the entire aggregate interface at once.

Note

- Member ports of an aggregation group do not support port isolation configuration.
- Currently, up to 8 isolation groups are supported.

- 2) Specify the isolation group No.
- 3) Click **Save**.

The **Isolation Group Info** list will display the successfully added isolation groups.

3. Optional: Delete an existing isolation group.

- 1) Select the isolation group you want to delete in the legend above the port panel.
- 2) Click **Delete Group** -> **OK**.

4. Optional: Edit an existing isolation group.

- 1) Select the isolation group you want to edit in the legend above the port panel.
- 2) Remove existing port(s) from the isolation group or add new ports to the isolation group.
- 3) Click **Save**.

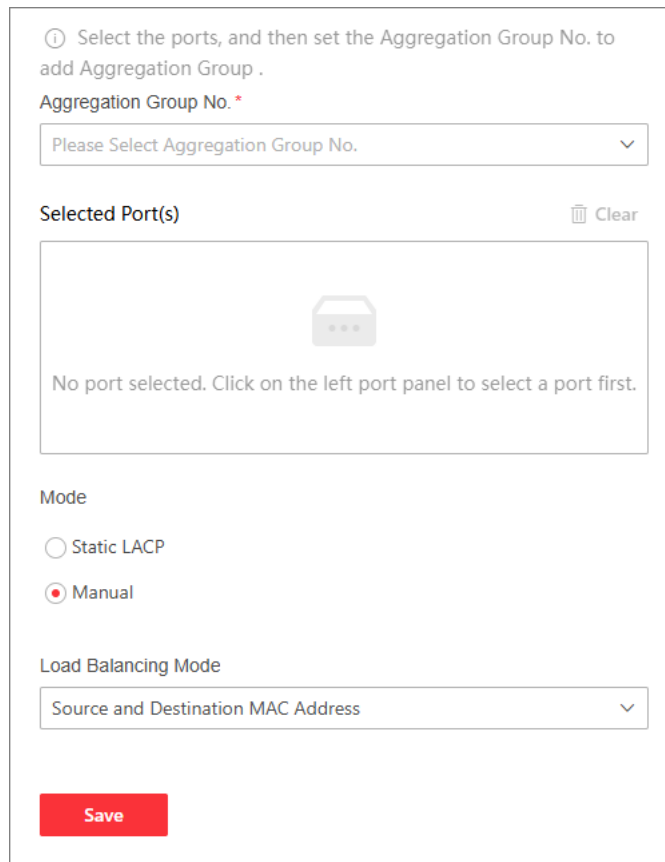
Configure Port Aggregation

Port aggregation combines multiple Ethernet ports into a single logical interface to enable load balancing and increase bandwidth for data streams across member ports. In the event of a link failure on one member port, traffic is automatically redirected to an available link to ensure reliable transmission.

Steps

1. Click **Configuration** -> **Basic Configuration** -> **Port Aggregation**.

2. Add an aggregation group.



① Select the ports, and then set the Aggregation Group No. to add Aggregation Group .

Aggregation Group No. *

Please Select Aggregation Group No. ▼

Selected Port(s) Clear

No port selected. Click on the left port panel to select a port first.

Mode

☐ Static LACP

☒ Manual

Load Balancing Mode

Source and Destination MAC Address ▼

Save

Figure 5-7 Configuration Port Aggregation

1) Select multiple ports on the port panel to add them to the aggregation group.

Note

- Currently, up to 8 ports can be added to the same aggregation group. Please refer to the actual interface for specific limits.
- The maximum number of configurable aggregation groups varies by device model. Please refer to the actual interface for details.
- The rate, duplex mode, and VLAN configurations of all ports in the same aggregation group should be consistent.

2) Select the aggregation group No.

3) Set the aggregation mode.

Static LACP

In static LACP mode, the selection of active ports is managed by Link Aggregation Control Protocol (LACP) packets. LACP dynamically adjusts the active/inactive status of member ports based on information exchanged between the local and peer devices. This mode provides both load balancing and link redundancy.

Manual

In manual mode, the aggregate interface and its member ports are configured manually, without LACP participation. All active ports in this mode participate in data forwarding and share the traffic load. If an active link fails, the aggregation group automatically redistributes the traffic evenly among the remaining active links. Manual mode is suitable when a high-bandwidth link is needed between two directly connected devices, and one or both ends do not support LACP.

4) Set the load balancing mode.

Source MAC Address

Distributes traffic based on the source MAC address of packets.

Destination MAC Address

Distributes traffic based on the destination MAC address of packets.

Source IP Address

Distributes traffic based on the source IP address of packets.

Destination IP Address

Distributes traffic based on the destination IP address of packets.

Source and Destination MAC Address

Distributes traffic based on both the source and destination MAC addresses of packets.

Source and Destination IP Address

Distributes traffic based on both the source and destination IP addresses of packets.



Note

The available load balancing modes for aggregation groups vary by device model. Please refer to the actual interface for supported options. The default load balancing mode for aggregation groups on the current device is **Source and Destination MAC Address**.

5) Click **Save**.

The **Port Status** list will display successfully added aggregation groups.

3. Optional: Delete an existing aggregation group.

1) Select the aggregation group you want to delete in the legend above the port panel.

2) Click **Delete Group** -> **OK**.

4. Optional: Edit an existing aggregation group.

1) Select the aggregation group you want to edit in the legend above the port panel.

2) Remove existing port(s) from the aggregation group or add new ports to the aggregation group.

- 3) Edit the aggregation mode and load balancing mode of the aggregation group as needed.
- 4) Click **Save**.

Configure Port Mirroring

Port Mirroring copies traffic from a designated source port (also referred to as a mirror port) to a destination port (also referred to as a monitoring port), allowing real-time monitoring and analysis of network data flows. This function is commonly used for troubleshooting, performance monitoring, and security auditing, enabling observation of network communications without impacting normal traffic.

Mirror Source

The mirror source refers to the object being monitored, known as the source port or mirror port. The device where the source port resides is called the source device.

Mirror Destination

The mirror destination refers to the target where mirrored packets are sent, known as the destination port or monitoring port. The device where the destination port resides is called the destination device.

Mirroring Direction

Mirroring direction defines which types of traffic are copied from the mirror source.

- Inbound: Only copies packets received by the mirror source.
- Outbound: Only copies packets sent by the mirror source.
- Bidirectional: Copies both received and sent packets from the mirror source.

Steps

1. Click **Configuration -> Advanced Configuration -> Mirroring**.
2. Add a mirroring group.

① Set the mirroring group No., type, and member ports to add a mirroring group.

Mirroring Group No. *

Please Select Mirroring Group No. ▼

Mirroring Group Type *

Local Mirroring Group ▼

Selected Bidirectional Source Port(s) Clear

No port selected. Click on the left port panel to select a port first.

Selected Inbound Source Port(s) Clear

No port selected. Click on the left port panel to select a port first.

Selected Outbound Source Port(s) Clear

No port selected. Click on the left port panel to select a port first.

Destination Port

Please select Destination Port ▼

Save

Figure 5-8 Configuration Port Mirroring

- 1) Select the mirroring group No.

 Note

Currently, up to 4 mirroring groups are allowed.

- 2) Set the mirroring group type based on your network setup.

Local Mirroring Group

A mirroring group where both the mirror source and mirror destination reside on the same device.

Remote Source Mirroring Group / Remote Destination Mirroring Group

Mirroring groups where the mirror source and mirror destination are located on different devices. The group containing the mirror source is referred to as the remote source mirroring Group, while the group containing the mirror destination is called the remote destination mirroring group.

 Note

Supported mirroring group types and configurable parameters vary by device model. Refer to the actual interface for available options.

- For a local mirroring group, you can configure bidirectional, inbound, or outbound source ports, as well as a destination port. Multiple source ports (including aggregation groups) are supported. The destination port can be a CPU or a single physical port.
- For a remote source mirroring group, you can configure bidirectional, inbound, or outbound source ports, an egress port, and a remote mirroring VLAN. Multiple source ports (including aggregation groups) are supported, while the egress port must be a single physical port.
- For a remote destination mirroring group, you can configure a destination port and a remote mirroring VLAN. The destination port must be a single physical port.

3) Configure parameters of the mirroring group.

Source Port(s)

When the mirroring group type is **Local Mirroring Group** or **Remote Source Mirroring Group**, select the mirroring direction and source port(s). Choose a direction ( **Bidirectional**,  **Inbound**, or  **Outbound**), then select port(s) from the port panel to add them to the corresponding **Selected Bidirectional Source Port(s)**, **Selected Inbound Source Port(s)**, or **Selected Outbound Source Port(s)** list on the right.

 Note

Select the mirroring direction before choosing port(s). You may select one or multiple ports, or click the aggregation group icon to select an entire group at once. To configure source port(s) for another direction, switch to that direction first.

Destination Port / Egress Port

- For local mirroring or remote destination mirroring groups, configure a destination port. In local mirroring groups, the destination port can be a CPU or a physical port.
 - Mirror to CPU: Copies network traffic to the CPU for processing.
 - Mirror to Port: Copies traffic from one or more source ports to a specified destination port.
- For remote source mirroring groups, configure an egress port.

Remote Mirroring VLAN

Required for remote source mirroring or remote destination mirroring groups. This dedicated VLAN (ID range: 1 to 4094) transports mirrored traffic from the source to the destination device. It must be a pre-configured static VLAN and cannot be used for any other purpose once assigned.

**Note**

The source port and destination/egress port cannot be the same.

4) Click **Save**.

The **Port Mirroring Status** list will display successfully added mirroring groups.

3. Optional: Delete an existing mirroring group.

1) Select the mirroring group you want to delete in the legend above the port panel.

2) Click **Delete Group** -> **OK**.

4. Optional: Edit an existing mirroring group.

1) Select the mirroring group you want to edit in the legend above the port panel.

2) Modify the available parameters as needed and click **Save**.

5.1.2 VLAN Configuration

VLAN (Virtual Local Area Network) is a technology that logically—rather than physically—partitions devices within a LAN into separate network segments, enabling broadcast domain isolation within a single physical network.

Add/Edit VLAN

You can add a single VLAN or batch add multiple VLANs, and delete or edit existing VLANs.

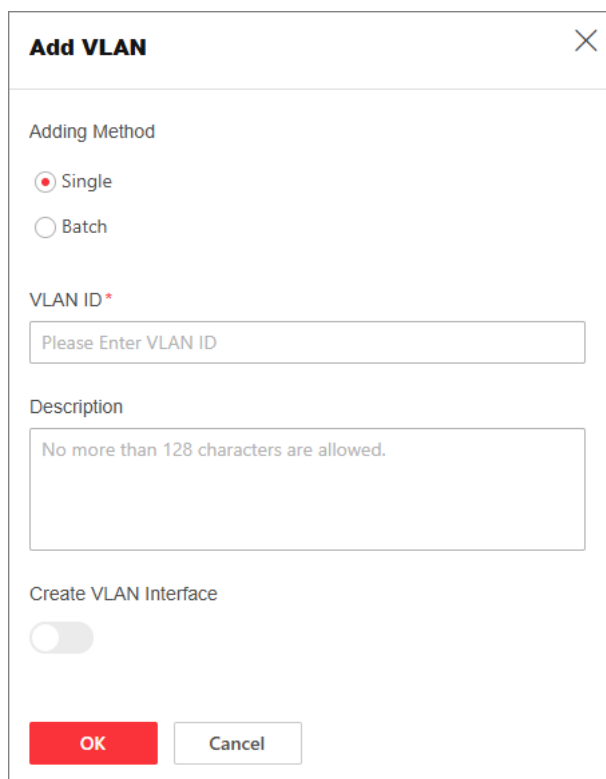
Steps

1. Click **Configuration** -> **Basic Configuration** -> **VLAN**.

2. Add VLAN(s).

- **Add a Single VLAN:**

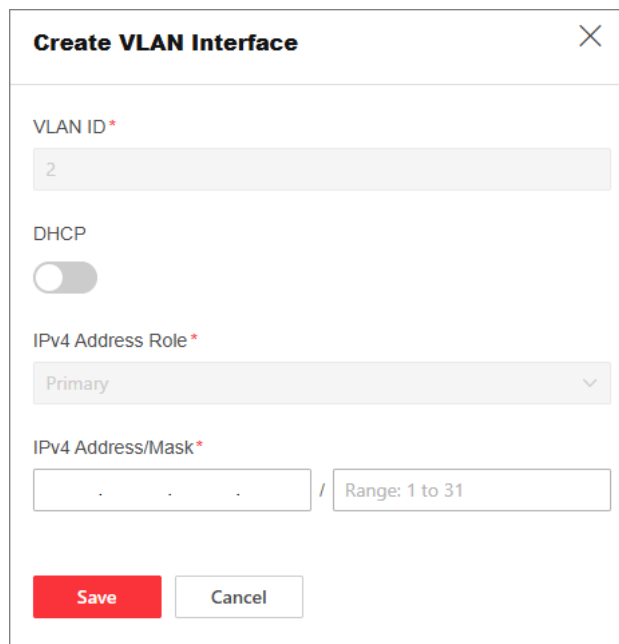
- a. In **Global VLAN Configuration**, click **Edit** -> **Add** or simply click **Add** (if the device has no configured VLANs except the default VLAN 1).



The image shows a web-based dialog box titled "Add VLAN" with a close button (X) in the top right corner. The dialog is divided into several sections. The first section, "Adding Method", contains two radio buttons: "Single" (which is selected) and "Batch". The second section, "VLAN ID *", features a text input field with the placeholder text "Please Enter VLAN ID". The third section, "Description", has a larger text area with the instruction "No more than 128 characters are allowed." The fourth section, "Create VLAN Interface", includes a toggle switch that is currently turned off. At the bottom of the dialog are two buttons: a red "OK" button and a grey "Cancel" button.

Figure 5-9 Add a Single VLAN

- b. Set the adding method to **Single**.
- c. Enter the VLAN ID.
- d. Enter the description for the VLAN.
- e. (Optional) Create the corresponding VLAN interface as needed. If layer-3 communication is required for the VLAN, create its VLAN interface (e.g., interface VLANIF 10), then either enable DHCP for automatic IP assignment, or manually assign a static IPv4 address and subnet mask.



The 'Create VLAN Interface' dialog box contains the following fields and controls:

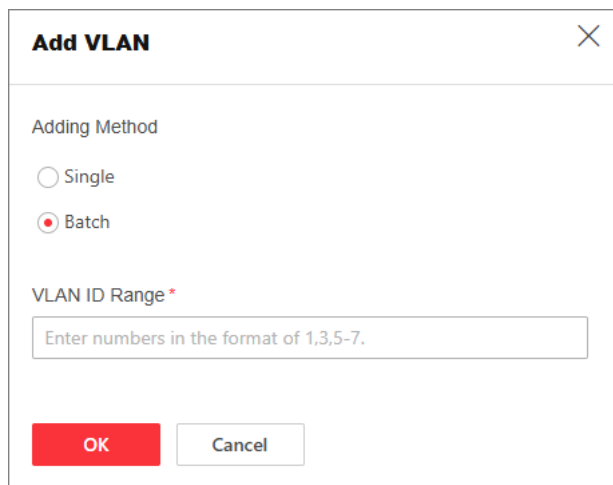
- VLAN ID ***: A text input field containing the value '2'.
- DHCP**: A toggle switch currently in the 'off' position.
- IPv4 Address Role ***: A dropdown menu with 'Primary' selected.
- IPv4 Address/Mask ***: Two adjacent input fields. The first field contains three dots, and the second field contains the text 'Range: 1 to 31'.
- Buttons**: A red 'Save' button and a grey 'Cancel' button.

Figure 5-9 Create VLAN Interface

f. Click **OK**.

- **Batch Add VLANs:**

a. In **Global VLAN Configuration**, click **Edit** -> **Add** or simply click **Add** (if the device has no configured VLANs except the default VLAN 1).



The 'Add VLAN' dialog box contains the following fields and controls:

- Adding Method**: Two radio button options: 'Single' and 'Batch'. The 'Batch' option is selected.
- VLAN ID Range ***: A text input field containing the placeholder text 'Enter numbers in the format of 1,3,5-7.'.
- Buttons**: A red 'OK' button and a grey 'Cancel' button.

Figure 5-10 Batch Add VLANs

- Set the adding method to **Batch**.
- Enter the VLAN ID range, for example, 1,3,5-7.
- Click **OK**.

The **Port VLAN Details** list will display successfully added VLANs.

3. Optional: Delete existing VLAN(s).

- a) Click **Edit** in **Global VLAN Configuration** or simply click **VLAN Management**.
- b) Select a VLAN and click , or select multiple VLANs and click **Delete** to batch delete them.

Note

VLAN 1 cannot be deleted.

4. Optional: Edit an existing VLAN.

- a) Click **Edit** in **Global VLAN Configuration** or simply click **VLAN Management**.
- b) Select a VLAN and click .
- c) Modify the available parameters as needed.
- d) Click **OK**.

5. Optional: In the **Port VLAN Details** list, you can view the enable status, type, and tagged and untagged ports of the newly added VLAN(s).

Configure Port VLAN

You can add specific ports to the created VLAN as needed.

Steps

1. Click **Configuration** -> **Basic Configuration** -> **VLAN**.
2. Select one or more ports on the port panel, or click the aggregation group icon above the port panel to select all ports in the group.
3. Configure the link type.

ACCESS

Transmits traffic only for a single specified VLAN (Default value: VLAN 1). A PVID (range: 1 to 4094) must also be configured.

TRUNK

Carries traffic for multiple VLANs. You must configure a PVID and specify the allowed VLANs (e.g., 3,5,10-100).

HYBRID

Carries traffic for multiple VLANs, supporting both tagged and untagged frames. A PVID must be set, and allowed VLANs should be designated as either tagged or untagged.

DOT1Q-TUNNEL

Adds a double VLAN tag to frames by inserting an outer tag over the original tag, enabling support for up to 4094 × 4094 VLANs. A PVID is also required.

Note

The PVID must be an existing VLAN ID.

4. Click **Save.**

The **Port VLAN Info** list will display successfully configured port VLAN information.

5. Optional: To edit the port VLAN information, repeat the above steps.

5.1.3 MAC Address Configuration

The MAC (Media Access Control) address table records mappings between MAC addresses and interfaces, along with information such as the VLAN to which each interface belongs.

When forwarding a packet, the device looks up the destination MAC address in its MAC address table:

- If an entry matching the destination MAC address exists, the packet is forwarded directly through the corresponding outgoing interface.
- If no matching entry is found, the device broadcasts the packet to all interfaces except the receiving interface.

MAC address entries mainly include: static entries, dynamic entries, and blackhole entries.

Static entries: Manually configured to forward frames with a specific destination MAC address through the associated interface. These entries never age out and take precedence over dynamically learned entries.

Dynamic entries: Automatically learned to forward frames with a specific destination MAC address. These entries may age out over time.

Blackhole entries: Manually configured to discard frames with a specific source or destination MAC address. These entries never age out and are commonly used for security purposes, such as blocking traffic from or to a specific user. Blackhole entries have higher priority than dynamically learned entries.

Users can view the device's MAC address table as needed, manually add static or blackhole MAC entries, and configure the global aging time for dynamic MAC entries.

Configure MAC Address Aging Time

Each dynamic MAC address entry has an aging time. Once the aging time expires, the entry is automatically deleted. You can configure the aging time according to your actual network conditions.

Steps

1. Click **Configuration -> **Basic Configuration** -> **MAC Address** -> **Global Configuration**.**

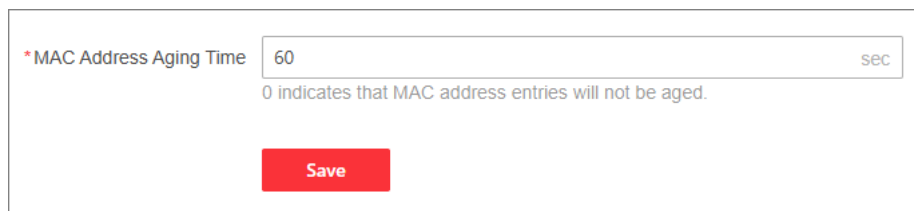


Figure 5-11 Configure MAC Address Aging Time

2. Set the aging time of dynamic MAC address entries.

Note

The aging time for MAC addresses can be configured within the range of 60 to 1,000,000 seconds or 0 seconds. A value of 0 seconds indicates that dynamic MAC address entries do not age.

3. Click **Save**.

Add MAC Address Entry

You can manually add static or blackhole MAC address entries as needed.

Steps

1. Click **Configuration** -> **Basic Configuration** -> **MAC Address** -> **MAC Address**.

2. Add a MAC address entry.

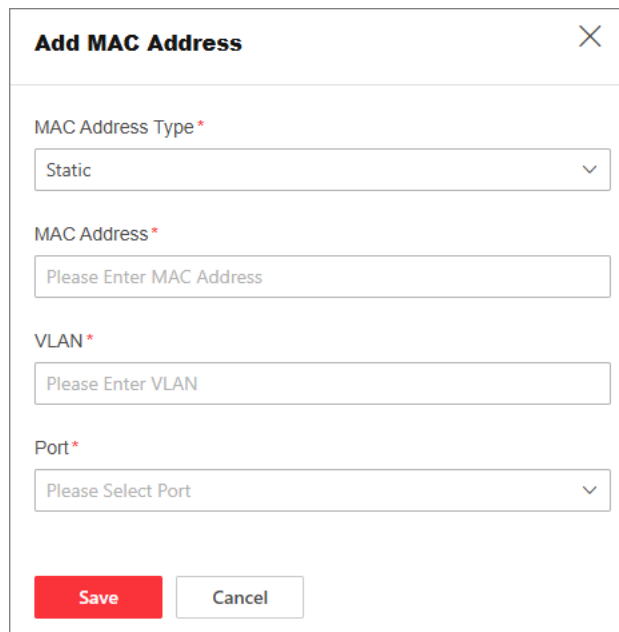


Figure 5-13 Add MAC Address Entry

1) Click **Add**.

2) Set the MAC address type.

Static

Add a static MAC address entry.

Blackhole

Add a blackhole MAC address entry.

3) Enter the MAC address.

4) Enter the VLAN ID and select a physical port or aggregation group.

**Note**

If the MAC address type is configured as blackhole, port configuration is not required.

5) Click **Save**.

The added MAC address entries will be displayed in the list below.

3. Optional: Delete one or more existing MAC address entries.

Single Deletion:

a. Select the MAC address entry to be deleted in the list.

b. Click  -> **OK**.

Batch Deletion:

a. Click **Clear Static MAC Addresses**, **Clear Dynamic MAC Addresses**, or **Clear Blackhole MAC Addresses** to delete all static, dynamic, or blackhole MAC address entries.

b. Click **OK**.

4. Optional: Search for specified MAC address entries.

1) Enter the VLAN ID, or select port/MAC address type to filter.

MAC Address Type**All**

Includes entries of all MAC address types.

Static

Manually configured by users and do not age out.

Dynamic

Automatically learned by the device based on source MAC addresses and age out after a specified time.

Blackhole

Manually configured by users to discard packets with a specified source or destination MAC address and do not age out.

2) Click **Search**.

Configure MAC Address Learning

You can also configure the MAC address learning status, maximum number of learnable MAC addresses, and whether to forward packets with unknown source MAC addresses for each port.

Steps

1. Click **Configuration -> Basic Configuration -> MAC Address -> MAC Address Learning**.

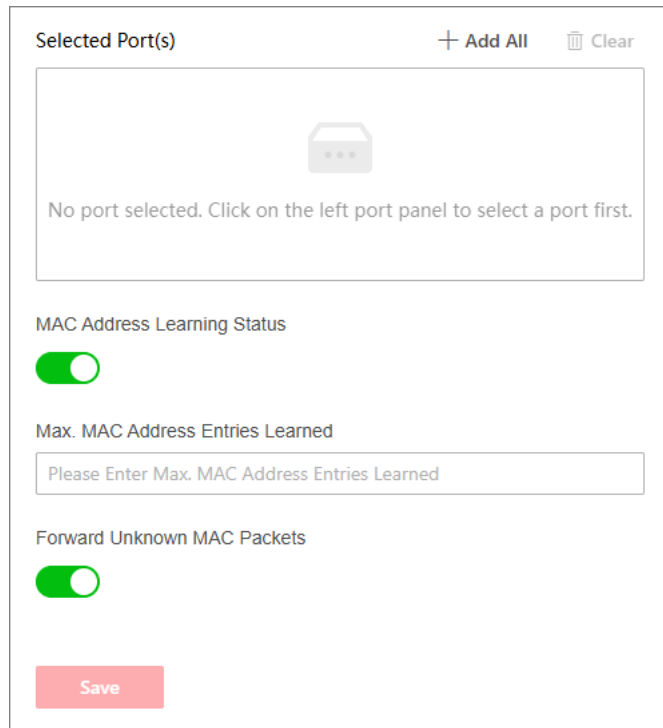


Figure 5-14 Configure MAC Address Learning

2. Select one or more ports on the port panel, or click the aggregation group icon above the port panel to select an aggregation group.

Note

- You can click **Add All** to batch select all Ethernet ports and aggregation groups, or click **Clear** to deselect the selected port(s).
 - Member ports of an aggregation group do not support MAC address learning configuration.
3. Enable or disable MAC address learning as needed.
 4. Set the maximum number of MAC addresses that can be learned on the port, with a valid range of 0 to 4,096.
 5. Enable or disable **Forward Unknown MAC Packets** as needed to configure whether the port is allowed to forward packets with unknown source MAC addresses after the learning limit is reached.
 6. Click **Save**.

- The **MAC Address Learning Status** list will display successfully configured ports.
- The MAC address learning status of the port(s) will be displayed on the port panel.

7. Optional: To modify MAC address learning configuration for a port, repeat the above steps.

5.1.4 ARP Configuration

Address Resolution Protocol (ARP) is used to map an IP address to a corresponding Ethernet MAC address (physical address). Once a device resolves the destination MAC address using ARP, it adds an entry containing the IP-to-MAC mapping to its ARP table. This entry is then used to forward subsequent packets to the same destination. ARP entries can be either dynamic or static.

Steps

1. Click **Configuration** -> **Basic Configuration** -> **ARP**.
2. Add a static ARP entry.
 - 1) Click **Add**.

Figure 5-16 Add Static ARP Entry

- 2) Configure ARP entry parameters.

Destination IPv4 Address

The IPv4 address of the destination device whose MAC address is being resolved.

Destination MAC Address

The MAC address corresponding to the destination IPv4 address, used to construct Ethernet frames for packet forwarding.

Outbound Interface

The network interface used to transmit packets toward the destination IP address.

VLAN

The VLAN that specifies the broadcast domain and Layer-2 forwarding scope for the ARP entry, ranging from 1 to 4094.

3) Click **Save**.

The information of successfully added ARP entries will be displayed in the list.

5. Optional: Delete one or more existing ARP entries.

Single Deletion:

a. Select an ARP entry to be deleted in the list.

b. Click  -> **OK**.

Batch Deletion:

Method 1

a. Select multiple ARP entries to be deleted in the list.

b. Click  **Delete** -> **OK**.

Method 2

a. Click **Clear Static ARP Entries**, **Clear Dynamic ARP Entries**, or **Clear All** to delete all static ARP entries, all dynamic ARP entries, or both static and dynamic ARP entries.

b. Click **OK**.

3. Optional: Search for specified ARP entries.

1) Select port or ARP type, or enter the VLAN ID, IPv4 address, or MAC address to filter.

All

Both dynamic and static ARP entries.

Dynamic

Automatically generated and maintained by the ARP protocol via ARP packets. Entries can age out and may be overwritten by static ARP entries.

Static

Manually configured with a fixed mapping between an IP address and a MAC address.

2) Click **Search**.

5.1.5 IPv4 Configuration

An IPv4 (Internet Protocol version 4) address comprises two components: the network address and the host address.

Configure IPv4 Address

You can add, delete, or edit IPv4 address manually according to your actual needs.

Steps

1. Click **Configuration** -> **Basic Configuration** -> **IPv4 Address**.
2. Add an IPv4 address.

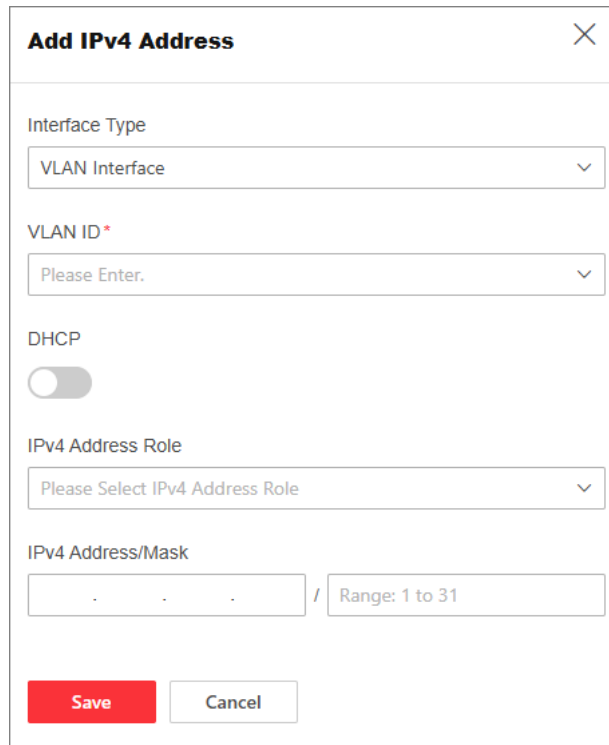


Figure 5-18 Add IPv4 Address

Note

The available interface types vary by device model, and the configurable parameters depend on the selected interface type. Please refer to the actual interface for details.

VLAN Interface

- a. Click **Add**.
- b. Select **VLAN Interface** as the interface type.
- c. Enter the VLAN ID (1 to 4094) and select the corresponding VLAN.

Note

If the VLAN does not appear in the dropdown list, it indicates that the corresponding VLAN has not been created. Click **Add VLAN** to add VLAN(s) in batch first.

- d. Configure the IP address:

- Manual configuration: Select an IPv4 address role and set the IPv4 address/mask.

**Note**

A primary IPv4 address serves as the main address for an interface, while a secondary address provides additional aliases on the same interface.

- Automatic assignment: Enable **DHCP** for automatic IP address assignment.

- e. Click **Save**.

Loopback Port

- a. Click **Add**.
- b. Select **Loopback Port** as the interface type.
- c. Enter the Loopback ID (1 to 15).
- d. Select an IPv4 address role and set the IPv4 address/mask.
- e. Click **Save**.

Tunnel Interface

- a. Click **Add**.
- b. Select **Tunnel Interface** as the interface type.
- c. Enter the tunnel ID (1 to 5).

**Note**

The Tunnel ID uniquely identifies a tunnel and distinguishes multiple tunnels on the device.

- d. Configure the tunnel mode:
 - **ipv4-ipv6**: IPv6 over IPv4 tunnel, transmitting IPv6 traffic over an IPv4 network.
 - **ipv4-ipv4**: IPv4 over IPv4 tunnel, encapsulating an IPv4 packet within another IPv4 packet (dual IPv4 encapsulation) for transmission over an IPv4 network.
 - **gre ipv4-ipv4**: GRE over IPv4-to-IPv4 tunnel, using the Generic Routing Encapsulation (GRE) protocol to encapsulate any network protocol (including IPv4) and transmitting the encapsulated packet over an IPv4 network.
 - **gre ipv4-ipv6**: GRE over IPv4-to-IPv6 tunnel, using the GRE protocol to encapsulate any network protocol and transmitting the encapsulated packet over an IPv6 network.
- e. Select an IPv4 address role and set the IPv4 address/mask.
- f. Click **Save**.

The successfully added IPv4 addresses will be displayed in the list.

3. Optional: Select the IPv4 address and click  to delete it.

4. Optional: Select the IPv4 address and click  to edit it as needed.

**Note**

- The interface type of an IPv4 address cannot be modified.
- Only static IPv4 address can be deleted or edited.

5. Optional: Search for specified IPv4 addresses.

- a. Select interface, IPv4 address role, or IPv4 address type, or enter the IPv4 address to filter.

IPv4 Address Type**All**

All IPv4 addresses.

Static

Manually configured IPv4 address.

Auto

IPv4 address automatically generated by the device's algorithm.

DHCP

IPv4 address assigned through DHCP (Dynamic Host Configuration Protocol).

VRRP

IPv4 address acquired via VRRP (Virtual Router Redundancy Protocol).

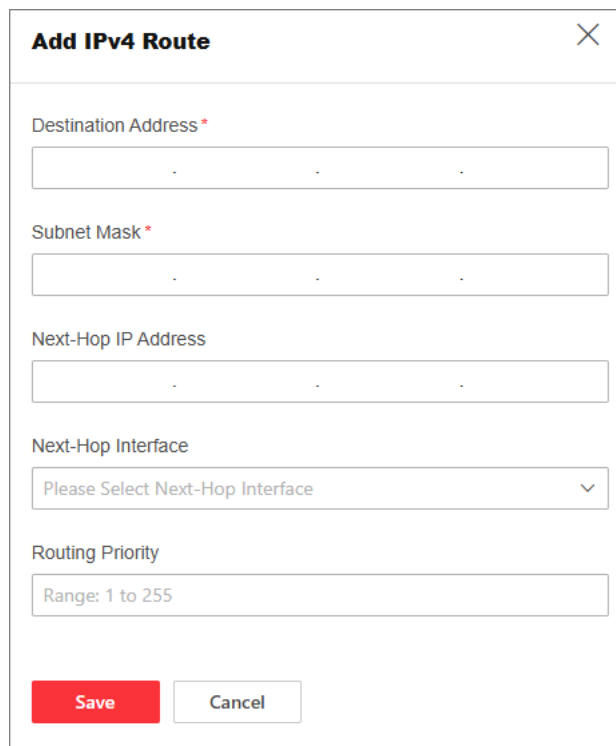
- b. Click **Search**.

Configure IPv4 Route

The routing table contains route entries that devices learn through various methods. Network devices (such as Layer 3 switches) can obtain route entries through static or dynamic means and maintain their own routing tables. A device searches its routing table based on the destination IP address. Upon finding a matching route entry, it forwards the data packet according to the egress interface or next-hop IP address specified by the entry. Users can manually add or delete static IPv4 routes based on actual requirements.

Steps

1. Click **Configuration** -> **Basic Configuration** -> **IPv4 Route** -> **IPv4 Static Route Configuration**.
2. Add a static IPv4 route.



The image shows a web-based dialog box titled "Add IPv4 Route" with a close button (X) in the top right corner. The dialog contains five input fields: "Destination Address *" (with a red asterisk), "Subnet Mask *" (with a red asterisk), "Next-Hop IP Address", "Next-Hop Interface" (a dropdown menu showing "Please Select Next-Hop Interface"), and "Routing Priority" (with a hint "Range: 1 to 255"). At the bottom, there are two buttons: a red "Save" button and a white "Cancel" button with a grey border.

Figure 5-20 Add Static IPv4 Route

Add a Single Static IPv4 Route

- a. Click **Add**.
- b. Configure static IPv4 route parameters.

Destination Address

Specifies the destination IPv4 address for this static route.

Subnet Mask

Specifies the subnet mask corresponding to the destination address.

Next-Hop IP Address

Specifies the IPv4 address of the next hop for this static route.

Next-Hop Interface

Specifies the interface through which the traffic will be forwarded.

Routing Priority

Defines the priority of this static route. When multiple routes exist, the route with the smallest priority value (highest priority) is preferred.

Note

Either the next-hop IP address or the next-hop interface must be configured.

- c. Click **Save**.

Batch Add Static IPv4 Routes

- a. Click **Import**.
- b. Download the import template.
- c. Enter the required parameters and save the file to the specified path.
- d. Click  to import the routing information configuration file saved in the specified path.
- e. Click **OK**.

The successfully added static IPv4 route entries will be displayed in the list.

3. Optional: Click **Export All Routes** to export all static IPv4 routes in batch.

4. Optional: Delete one or multiple static IPv4 routes.

- Select a static IPv4 route, click  -> **OK**.
- Select multiple static IPv4 routes, click  **Delete** -> **OK**.

5. Optional: Enter the outbound interface or destination address to filter and click **Search** to search for specified static IPv4 routes.

6. Optional: Click **Configuration** -> **Basic Configuration** -> **IPv4 Route** -> **IPv4 Routing Table** to view all types of existing IPv4 routes, or perform related operations as needed.

- Click **Export All Routes** to export all types of existing IPv4 routes in batch.
- Select route protocol type or enter the outbound interface or destination address, and then click **Search** to search for specified IPv4 routes.

All

Displays all IPv4 routes, regardless of the routing protocol.

Direct

Displays directly connected routes discovered via the link-layer protocol, which are automatically obtained by the device.

Static

Displays static routes manually configured by the network administrator.

OSPF

Displays routes discovered through OSPF (Open Shortest Path First).

BGP

Displays routes discovered through BGP.

IS-IS

Displays routes discovered through IS-IS (Intermediate System to Intermediate System).

RIP

Displays routes discovered through RIP (Routing Information Protocol).

5.1.6 IPv6 Configuration

IPv6 (Internet Protocol Version 6), also known as IPng (IP Next Generation), is the upgraded version of IPv4. The most significant change compared to IPv4 is the expansion of the address length from 32 bits to 128 bits.

Users can add, delete, or edit IPv6 addresses according to actual requirements.

Configure IPv6 Address

Steps

1. Click **Configuration** -> **Basic Configuration** -> **IPv6 Address**.
2. Add an IPv6 address.

Figure 5-22 Add IPv6 Address

Note

The available interface types vary by device model, and the configurable parameters depend on the selected interface type. Please refer to the actual interface for details.

VLAN Interface

- a. Click **Add**.
- b. Select **VLAN Interface** as the interface type.
- c. Enter the VLAN ID (1 to 4094) and select the corresponding VLAN.

 Note

If the VLAN does not appear in the dropdown list, it indicates that the corresponding VLAN has not been created. Click **Add VLAN** to add VLAN(s) in batch first.

- d. Enable IPv6.
- e. Configure the IP address:
 - Manual configuration: Select an IPv6 address role and set the IPv6 address/mask.

 Note

A primary IPv6 address serves as the main address for an interface, while a secondary address provides additional aliases on the same interface.

- Automatic assignment: Enable **DHCP** for automatic IP address assignment.
- f. (Optional) Enable **IPv6 Address in EUI-64 Format** to allow nodes to automatically generate IPv6 addresses using the EUI-64 format when no DHCP server is available on the network.
 - g. (Optional) Disable **Auto-Generate Link-Local Address** to prevent automatic generation of IPv6 link-local addresses via EUI-64.
 - h. Click **Save**.

Loopback Port

- a. Click **Add**.
- b. Select **Loopback Port** as the interface type.
- c. Enter the Loopback ID (1 to 15).
- d. Enable IPv6.
- e. Select an IPv6 address role and set the IPv4 address/mask.
- f. (Optional) Enable **IPv6 Address in EUI-64 Format** to allow nodes to automatically generate IPv6 addresses using the EUI-64 format when no DHCP server is available on the network.
- g. (Optional) Disable **Auto-Generate Link-Local Address** to prevent automatic generation of IPv6 link-local addresses via EUI-64.
- h. Click **Save**.

Tunnel Interface

- a. Click **Add**.
- b. Select **Tunnel Interface** as the interface type.
- c. Enter the tunnel ID (1 to 5).

 Note

The Tunnel ID uniquely identifies a tunnel and distinguishes multiple tunnels on the device.

- d. Configure the tunnel mode:

- **ipv6-ipv6**: IPv6 over IPv6 tunnel, encapsulating and transmitting IPv6 packets over an IPv6-based tunnel, typically used to traverse intermediate networks that lack native IPv6 support.
 - **ipv6-ipv4**: IPv6 over IPv4 tunnel, carrying IPv6 traffic across an IPv4 infrastructure by encapsulating IPv6 packets within IPv4.
 - **gre ipv6-ipv4**: GRE over IPv6-to-IPv4 tunnel, using the GRE protocol to transport IPv6 packets over an IPv4 network.
 - **gre ipv6-ipv6**: GRE over IPv6-to-IPv6 tunnel, using the GRE protocol to encapsulate IPv6 packets within GRE headers for transmission over an IPv6 network.
- e. Enable IPv6.
 - f. Select an IPv6 address role and set the IPv6 address/mask.
 - g. (Optional) Enable **IPv6 Address in EUI-64 Format** to allow nodes to automatically generate IPv6 addresses using the EUI-64 format when no DHCP server is available on the network.
 - h. (Optional) Disable **Auto-Generate Link-Local Address** to prevent automatic generation of IPv6 link-local addresses via EUI-64.
 - i. Click **Save**.
- The successfully added IPv6 addresses will be displayed in the list.

6. Optional: Select the IPv6 address and click  to delete it.

7. Optional: Select the IPv6 address and click  to edit it as needed.

Note

- The interface type of an IPv6 address cannot be modified.
- Only static IPv6 address can be deleted or edited.

8. Optional: Search for specified IPv6 addresses.

- a. Select interface, IPv6 address role, or IPv6 address type, or enter the IPv6 address to filter.

IPv6 Address Type

All

All IPv6 addresses.

Static

Manually configured IPv6 address.

Auto

IPv6 address automatically generated by the device's algorithm.

DHCP

IPv6 address assigned through DHCP.

VRRP

IPv6 address acquired via VRRP.

Other

All IPv6 addresses except those obtained through manual static configuration, algorithmic auto-generation, VRRP protocol negotiation, or DHCP protocol assignment.

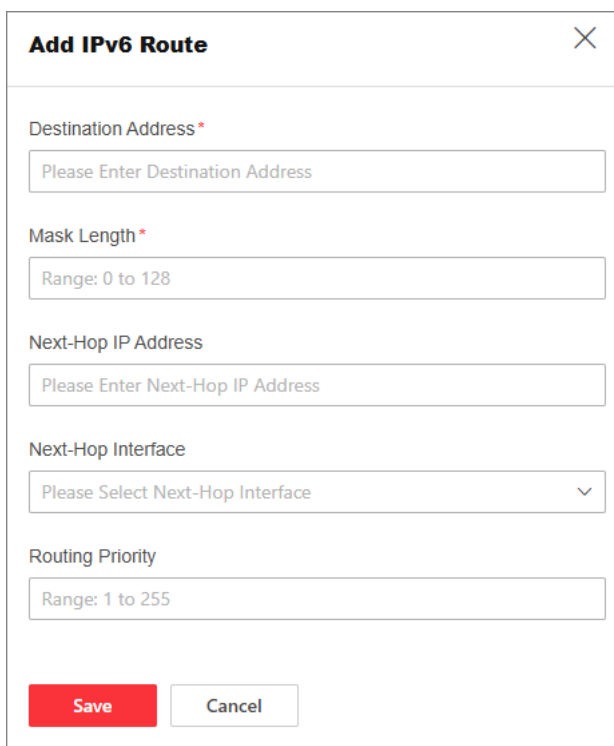
- b. Click **Search**.

Configure IPv6 Route

The routing table stores route entries acquired by network devices (such as Layer 3 switches) through static or dynamic methods. When forwarding data packets, devices search the routing table using the destination IP address and, upon finding a matching entry, direct the packet according to the specified egress interface or next-hop IP address. Users can also manually add or delete static IPv6 routes as needed.

Steps

1. Click **Configuration** -> **Basic Configuration** -> **IPv4 Route** -> **IPv6 Static Route Configuration**.
2. Add a static IPv6 route.



The screenshot shows a web-based configuration dialog titled "Add IPv6 Route" with a close button (X) in the top right corner. The dialog contains several input fields and buttons:

- Destination Address ***: A text input field with the placeholder text "Please Enter Destination Address".
- Mask Length ***: A text input field with the placeholder text "Range: 0 to 128".
- Next-Hop IP Address**: A text input field with the placeholder text "Please Enter Next-Hop IP Address".
- Next-Hop Interface**: A dropdown menu with the placeholder text "Please Select Next-Hop Interface" and a downward arrow icon.
- Routing Priority**: A text input field with the placeholder text "Range: 1 to 255".
- At the bottom, there are two buttons: a red "Save" button and a white "Cancel" button with a grey border.

Figure 5-20 Add Static IPv6 Route

Add a Single Static IPv6 Route

- a. Click **Add**.
- b. Configure static IPv6 route parameters.

Destination Address

Specifies the destination IPv6 address for this static route.

Mask Length

Specifies the subnet mask length corresponding to the destination IP address.

Next-Hop IP Address

Specifies the IPv6 address of the next hop for this static route.

Next-Hop Interface

Specifies the interface through which the traffic will be forwarded.

Routing Priority

Defines the priority of this static route. When multiple routes exist, the route with the smallest priority value (highest priority) is preferred.

**Note**

Either the next-hop IP address or the next-hop interface must be configured.

- c. Click **Save**.

Batch Add Static IPv6 Routes

- a. Click **Import**.
- b. Download the import template.
- c. Enter the required parameters and save the file to the specified path.
- d. Click  to import the routing information configuration file saved in the specified path.
- e. Click **OK**.

The successfully added static IPv6 route entries will be displayed in the list.

3. Optional: Click **Export All Routes** to export all static IPv6 routes in batch.

4. Optional: Delete one or multiple static IPv6 routes.

- Select a static IPv6 route, click  -> **OK**.
- Select multiple static IPv6 routes, click  **Delete** -> **OK**.

5. Optional: Enter the outbound interface or destination address to filter and click **Search** to search for specified static IPv6 routes.

6. Optional: Click **Configuration** -> **Basic Configuration** -> **IPv6 Route** -> **IPv6 Routing Table** to view all types of existing IPv6 routes, or perform related operations as needed.

- Click **Export All Routes** to export all types of existing IPv6 routes in batch.
- Select route protocol type or enter the outbound interface or destination address, and then click **Search** to search for specified IPv6 routes.

All

Displays all IPv6 routes, regardless of the routing protocol.

Direct

Displays directly connected routes discovered via the link-layer protocol, which are automatically obtained by the device.

Static

Displays static routes manually configured by the network administrator.

OSPF

Displays routes discovered through OSPF (Open Shortest Path First).

BGP

Displays routes discovered through BGP.

IS-IS

Displays routes discovered through IS-IS (Intermediate System to Intermediate System).

RIP

Displays routes discovered through RIP (Routing Information Protocol).

Configure IPv6 Neighbor

IPv6 Neighbor Discovery Protocol (NDP) is a fundamental IPv6 protocol that uses five ICMPv6 message types—Neighbor Advertisement (NA), Neighbor Solicitation (NS), Router Advertisement (RA), Router Solicitation (RS), and Redirect—to determine relationships and address information between neighboring nodes. It supports key functions such as address resolution, neighbor reachability detection, duplicate address detection, router/prefix discovery, automatic address configuration, and redirection. Users can also manually configure IPv6 neighbor entries based on actual requirements.

Steps

1. Click **Configuration** -> **Basic Configuration** -> **IPv6 Neighbor**.
2. Add a static IPv6 neighbor.

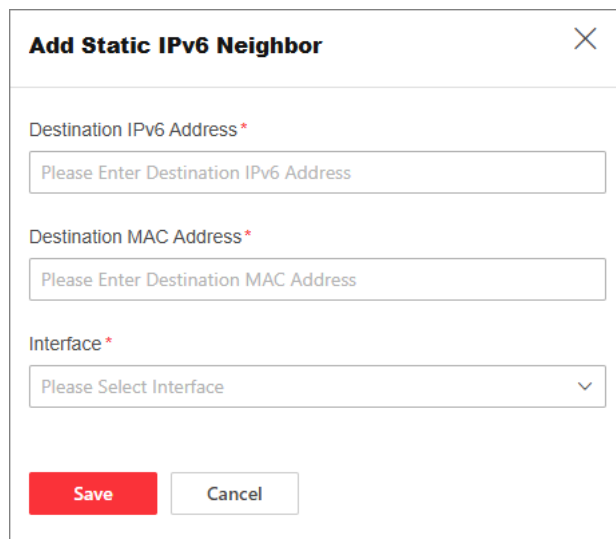


Figure 5-21 Add Static IPv6 Neighbor

1) Click **Add**.

2) Configure IPv6 neighbor parameters.

Destination IPv6 Address

Specifies the IPv6 address of the neighbor.

Destination MAC Address

Specifies the MAC address corresponding to the destination IPv6 address.

Interface

Specifies the VLAN interface associated with the neighbor.

3) Click **Save**.

The successfully added IPv6 neighbor entries will be displayed in the list.

3. Optional: View IPv6 neighbor information in the list, including the destination IPv6 address of the neighbor, MAC address corresponding to the destination IPv6 address, outbound interface for message forwarding, protocol type, aging time, etc.

4. Optional: Delete one or more static IPv6 neighbors.

- Select a static IPv6 neighbor, click  -> **OK**.
- Click **Clear Static Neighbors** or **Clear Dynamic Neighbors** to delete all existing IPv6 static or dynamic neighbors.

5. Optional: Search specified IPv6 neighbors.

1) Select outbound interface or protocol type, or enter the destination IPv6 address, destination MAC address, or VLAN interface to filter.

2) Click **Search**.

5.1.7 DHCP Configuration

DHCP is a network management protocol designed for centralized IP address configuration and management. It operates on a client-server (C/S) model, in which a client (DHCP Client) sends configuration requests to a server (DHCP Server), which dynamically assigns IP addresses and other network settings to devices. In essence, the server manages a predefined IP address pool and automatically provides clients with essential configuration parameters—such as IP address, subnet mask, default gateway, and DNS server addresses—upon client login.

DHCP Server

The DHCP server receives DHCP requests from clients and centrally manages IP network configurations within the LAN.

It maintains an address pool containing available IP addresses and associated network parameters, from which it dynamically assigns an appropriate IP address and corresponding settings to each requesting client.

DHCP Client

In general, a DHCP client is typically an individual PC within the LAN. The DHCP protocol is initiated when the client sends a DHCP DISCOVER message. Most DHCP operations—such as lease renewal, address discovery, and address release—are proactively initiated by the DHCP client. For ease of configuration and centralized management, you can also configure a device interface to act as a DHCP client, allowing it to dynamically obtain an IP address and other parameters from a DHCP server.

DHCP Relay

In a typical DHCP setup, one DHCP server serves multiple DHCP clients (such as PCs).

The DHCP server must be within the same network segment as the client to directly receive the DHCP DISCOVER message broadcast by the client.

If the DHCP client and server are on different network segments, the client can still obtain an IP address and configuration parameters by communicating with the server via a DHCP relay agent.

Configure DHCP Server

The DHCP server maintains an address pool containing IP addresses and associated network parameters, from which it allocates appropriate settings to requesting clients.

An address pool comprises all IP addresses available for assignment by the DHCP server. Besides IP addresses, it can be configured with additional parameters such as lease duration, subnet mask, and default gateway.

Address management within the pool operates in two modes: static binding and dynamic allocation.

- Static binding involves associating a specific client's MAC address or client ID with a fixed IP address to ensure consistent assignment.

- Dynamic allocation defines a range of available IP addresses in the pool, allowing the DHCP server to automatically assign an unused address from this range upon receiving a client request.

Steps

1. Click **Configuration -> Basic Configuration -> DHCP -> Global Configuration**.

The screenshot shows the DHCP configuration page. At the top, there is a 'DHCP' toggle switch that is turned on (green). Below this is the 'Global DHCP Server Configuration' section, which includes a 'Trust Option82' toggle switch (turned on), a 'Ping Timeout' input field with the value '500' and a unit of 'ms', and a 'Ping Packets' input field with the value '1'. The 'Global DHCP Relay Configuration' section follows, containing three toggle switches: 'Fake Server Detection' (turned off), 'Relay User Table Record' (turned off), and 'Refresh Relay User Table' (turned on). Below these is a 'Refresh Interval' input field with the value '60' and a unit of 'sec'. At the bottom of the form is a red 'Save' button.

Figure 5-25 Configure DHCP Server Global Parameters

2. Enable DHCP.
3. Configure the global function of DHCP server.
 - 1) Enable or disable **Trust Option82** according to your needs.

Note

To mitigate attacks exploiting DHCP messages containing the Option 82 field—which may result in excessive CPU usage and degrade system performance—the DHCP server can be configured to disable the trust Option 82 function. When a DHCP message lacks the Giaddr field, this configuration causes the server to discard any message carrying the Option 82 option.

- 2) Configure the parameters of the function that detects conflicts in IP address allocation.

Note

The IP address allocation conflict detection mechanism is designed to prevent IP address conflicts resulting from duplicate assignments.

- If no response is received within the detection period (number of attempts × waiting time per session), it indicates that no device is currently using the IP address, and the address is assigned to the requesting client.
- If a response is received during the detection period, it signifies that the IP address is already in use by another terminal. In this case, the address is marked as conflicting, and the server awaits a new request to select an available IP address for allocation.

Ping Timeout

Specifies the ping timeout time, which determines the waiting period for IP address conflict detection during IP address assignment to a device. The value ranges from 20 ms to 10,000 ms and is 500 ms by default.

Ping Packets

Specifies the maximum number of ping packets to be sent for conflict detection. The value should be between 0 and 10.

4. Click **Save**.

5. Click **Configuration** -> **Basic Configuration** -> **DHCP** -> **Address Pool Configuration**.

6. Add a DHCP address pool.

1) Click **Add**.

2) Configure the basic parameters of the address pool.

The screenshot shows a web form for configuring a DHCP address pool. The fields are as follows:

- * Address Pool Name:** A text input field with the placeholder "Please Enter Address Pool Name".
- Address Pool IP Address:** A text input field with the placeholder "Please Enter Address Pool IP Address".
- IP Address Range:** Two text input fields labeled "Start IP Address" and "End IP Address" separated by a hyphen.
- Subnet Mask:** A text input field with the placeholder "Please Enter Subnet Mask".
- Allowed Internet Access Duration:** Four numeric input fields for "day(s)", "h", "min", and "sec", followed by a checkbox labeled "Permanent".
- DNS Server:** A text input field with the placeholder "Please Enter DNS Server.", accompanied by a trash icon and a plus sign.
- Gateway:** A text input field with the placeholder "Please Enter Gateway.", accompanied by a trash icon and a plus sign.

Figure 5-26 Configure Address Pool Basic Parameters

Address Pool Name

Specifies the name of the DHCP address pool to be added. The name length must not exceed 63 characters.

Address Pool IP Address

Specifies the IP addresses dynamically allocated within the DHCP address pool when used with the subnet mask.

IP Address Range

Defines the IP address range of the address pool by setting start IP address and end IP address.

Subnet Mask

Specifies the subnet mask corresponding to the dynamically allocated IP addresses in the DHCP address pool. The assignable IP address range is determined by configuring both the IP address and subnet mask. If no subnet mask is specified, the natural mask is applied by default.

**Note**

To avoid assigning incorrect IP addresses, it is recommended to ensure that this IP address range matches the subnet of the DHCP server interface or DHCP relay interface.

Allowed Internet Access Duration

Specifies the lease duration, which is the validity period of dynamically allocated IP addresses in the DHCP address pool. The value can be set from 0 to 365 days, 23 hours, 59 minutes, and 59 seconds. Alternatively, select **Permanent** to impose no time restriction.

DNS Server

Specifies the DNS server address assigned by the DHCP address pool to DHCP clients. You can click  to add multiple DNS server addresses so as to enable load balancing and enhance network reliability.

Gateway

Specifies the gateway address assigned by the DHCP address pool to DHCP clients. You can click  to add multiple gateway addresses so as to enable load balancing and improve network reliability.

- 2) Optional: Click **Advanced Configuration** and configure the advanced parameters of the address pool as needed.

The screenshot shows a web interface titled "Advanced Configuration" with a list of configuration fields for a DHCP address pool. The fields are: Domain Name, TFTP Server Domain Name, TFTP Server Address, Next Server Address, NBNS Server Type (a dropdown menu), NBNS Server Address (a text field with a plus icon and a trash icon), Startup File Name, Option43 Format (a dropdown menu), and Option138 Format (a dropdown menu). Each field has a placeholder text indicating what to enter.

Figure 5-27 Configure Address Pool Advanced Parameters

Domain Name

Specifies the domain name suffix assigned by the DHCP address pool to DHCP clients. Once a domain name is configured for the address pool, it will be sent to the client along with the assigned IP address.

TFTP Server Domain Name

Specifies the domain name of the TFTP server assigned by the DHCP address pool to DHCP clients. This allows clients to resolve and access the TFTP server using a domain name (instead of an IP address) after startup, facilitating the retrieval of device configuration files or boot files.

TFTP Server Address

Specifies the IP address of the TFTP server assigned by the DHCP address pool to DHCP clients. This enables clients to access the server after startup and retrieve device configuration files.

Next Server Address

Specifies the IP address of the next server assigned by the DHCP address pool to DHCP clients. This allows clients to connect to the server after startup to obtain necessary information.

NBNS Server Type

Specifies the NetBIOS Name Server (NBNS) type assigned by the DHCP address pool to DHCP clients. Options include: b-node (broadcast node), p-node (peer-to-peer node), h-node (hybrid node), or m-node (mixed node).

NBNS Server Address

Specifies the IP address of the NetBIOS Name Server assigned by the DHCP address pool to DHCP clients.

Startup File Name

Specifies the boot file name assigned by the DHCP address pool to DHCP clients when the boot file is located on the TFTP server.

Option43 Format

The format used for DHCP Option 43, which carries vendor-specific configuration information assigned by the DHCP address pool to DHCP clients. This enables devices (such as IP phones or access points) to obtain customized settings directly from the DHCP server, simplifying centralized management and deployment. Once the Option 43 format is selected, you need to enter the Option 43 value accordingly. Ensure the value complies with the vendor's specified format (e.g., hex, string, or IP list) to avoid configuration errors.

Option138 Format

The format used for DHCP Option 138, which specifies the IP address of the wireless access controller (AC) assigned by the DHCP address pool to wireless clients. This allows clients (e.g., APs) to automatically discover and connect to the designated AC during startup, streamlining large-scale wireless network configuration. Once the Option 138 format is selected, you need to enter the Option 138 value accordingly. Ensure the value follows the vendor-defined format (e.g., hex, string, or IP list) to guarantee correct configuration and avoid deployment issues.

3) Configure the IP address(es) excluded from dynamic allocation.

The screenshot displays the 'Forbidden Address' configuration page. At the top, there are buttons for '+ Add', 'Delete', and 'Refresh'. A modal dialog is open for adding a new IP address, featuring two input fields: 'IP Address*' and 'End IP Address'. The 'IP Address*' field has a placeholder 'Please enter an IP address.' and the 'End IP Address' field has a placeholder 'Please Enter End IP Address.'. Below these fields are 'Save' and 'Cancel' buttons. The table below the dialog is empty, showing 'No data.' and a pagination bar at the bottom indicating 'Total 0' and '20 /page'.

Figure 5-28 Configure IP Address Excluded from Dynamic Assignment

a. Click **Add**.

Note

Before configuring IP addresses to be excluded from assignment, first click **Add** > **OK** to save the address pool configuration. Once the configuration is saved, the IP address range assigned by the address pool will be displayed in the **Available Address** list.

- b. Click **Add** again.
- b. Enter the start IP address (and end IP address) to specify the address range of IP addresses excluded from dynamic assignment.
- c. Click **Save**.

Note

- Excluded IP addresses will be displayed in the **Forbidden Address** list.
- You can repeat the steps above to add multiple IP addresses or ranges to be excluded from assignment, or click **Delete** to remove a specific IP address or range. Once deleted, the IP address or range will reappear in the **Available Address** list.
- Each delete operation removes only one IP address. If a range of excluded IP addresses is configured by specifying a start IP address and an end IP address, each delete operation will remove only the start IP address of that range.

- 4) Configure static IP address binding to assign a specific IP address to a particular client by binding the client's MAC address or client ID to an IP address.

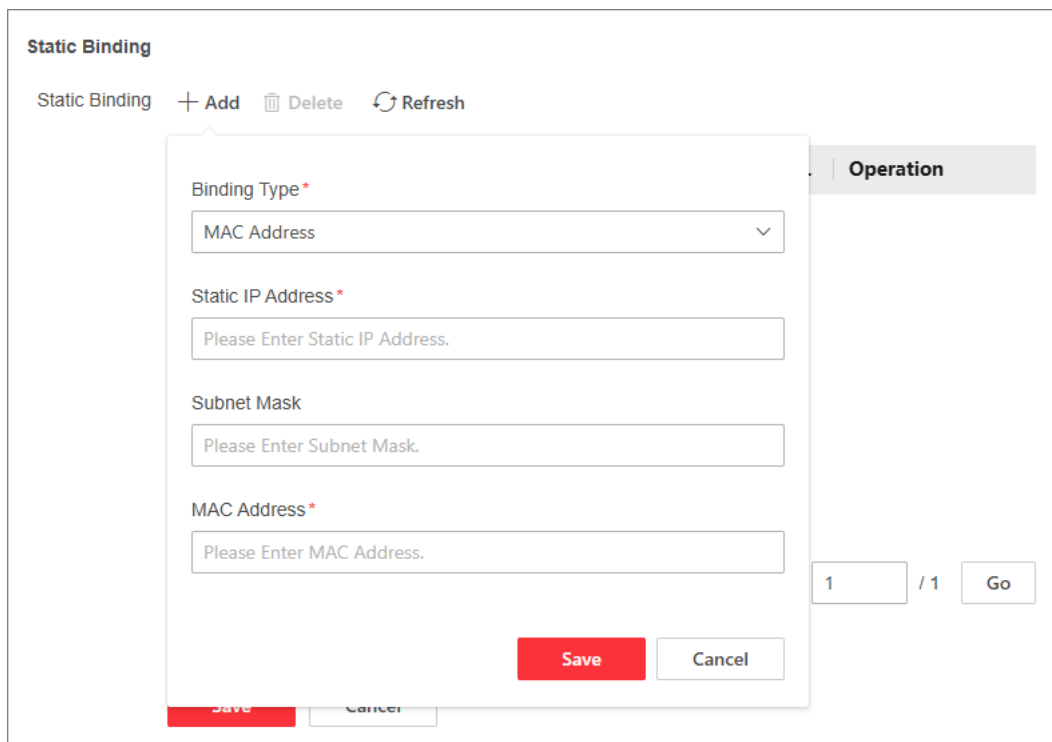


Figure 5-29 Configure Static IP Address Binding

- a. Click **Add**.
- b. Set **Binding Type** to **MAC Address** or **Client ID**.
- c. Set static IP address, subnet mask, and MAC address or static IP address, subnet mask, and client ID.
- d. Click **Save**.

8. Click **Save.**

The information of successfully added address pools will be displayed in the list.

9. Optional: To add multiple address pools, repeat the above steps.

10. Optional: Select the address pool and click -> **OK to delete a single address pool; or select multiple address pools, click **Delete** -> **OK** to delete multiple address pools in batch.**

11. Optional: Select an address pool and click to edit the address pool as needed.

12. Optional: View the details of IP address allocation for the configured address pool or delete allocated IP address(es).

1) Click **Configuration** -> **Basic Configuration** -> **DHCP** -> **Address Pool Allocation Details**.

2) Select address type or enter the IP address to filter.

All

All types of IP addresses.

Conflicted

IP addresses that are already in use by other clients.

Expired

IP addresses whose lease period has expired.

Static and Dynamic

All statically and dynamically assigned IP addresses.

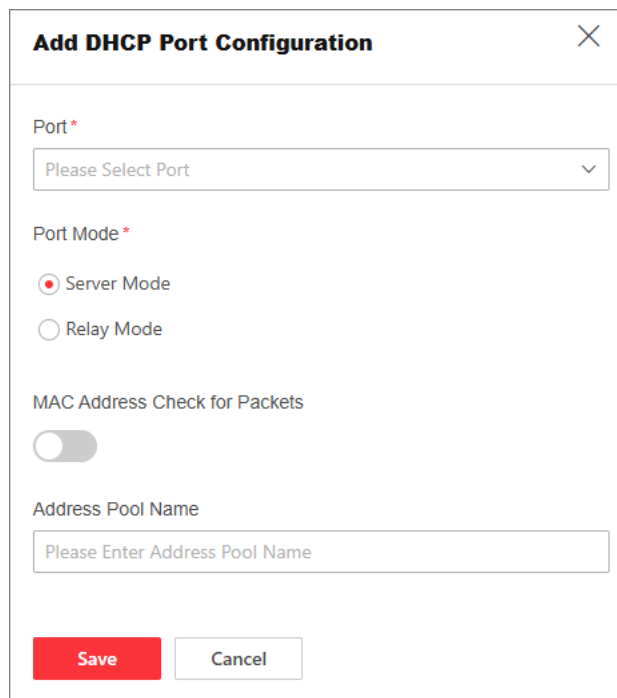
3) Click **Search**.

4) Optional: Select an assigned IP address and click  -> **OK** to delete a single IP address; or select multiple assigned IP addresses and click **Delete** -> **OK** to batch delete multiple IP addresses.

13. Configure the usage port for the address pool so that users connecting through this port can obtain IP addresses and other configuration details from the address pool.

1) Click **Configuration** -> **Basic Configuration** -> **DHCP** -> **DHCP Port Configuration**.

2) Click **Add**.



The dialog box titled "Add DHCP Port Configuration" contains the following fields and controls:

- Port ***: A dropdown menu with the placeholder text "Please Select Port".
- Port Mode ***: Two radio buttons, "Server Mode" (selected) and "Relay Mode".
- MAC Address Check for Packets**: A toggle switch currently in the "off" position.
- Address Pool Name**: A text input field with the placeholder text "Please Enter Address Pool Name".
- Buttons**: "Save" (red) and "Cancel" (white) buttons at the bottom.

Figure 5-31 Configure Address Pool Usage Port

- 3) Select the usage port.
- 4) Set the port mode to **Server Mode**.

 Note

In this mode, when the port receives DHCP messages from a DHCP client, it will assign addresses from the DHCP server's address pool.

- 5) Enable or disable **MAC Address Check for Packets** as needed.

 Note

If you enable this function, the DHCP server checks whether the chaddr field in the received DHCP request matches the source MAC address in the data frame. If they match, the packet is considered valid and processed further; otherwise, it is discarded.

- 6) Enter the name of the address pool to be bound.
- 7) Click **Save**.

The port information of the successfully added address pools will be displayed in the list.
- 8) Optional: To add multiple address pool usage ports, repeat the above steps.
- 9) Optional: Select a port and click  -> **OK** to delete a single address pool usage port; or select multiple ports and click **Delete** -> **OK** to delete multiple address pool usage ports in batch.
- 10) Optional: Select a port and click  to edit the address pool usage port as needed.

Configure DHCP Relay

The working principle of DHCP relay can be summarized as follows:

- 1) When a network device equipped with DHCP relay functionality receives a DHCP DISCOVER or DHCP REQUEST broadcast message from a DHCP client, it fills the giaddr field in the message with the IP address of the DHCP relay. The message is then unicast to the designated DHCP server based on the configuration.
- 2) The DHCP server uses the giaddr field to determine the appropriate address pool and assigns configuration parameters (such as an IP address) for the client. The server then sends the configuration information back to the DHCP relay, which forwards it to the client to complete the dynamic configuration process.

Steps

1. Click **Configuration -> Basic Configuration -> DHCP -> Global Configuration**.

The screenshot shows the 'Global DHCP Relay Configuration' web interface. At the top, there is a 'DHCP' toggle switch that is turned on (green). Below this, the 'Global DHCP Server Configuration' section contains a 'Trust Option82' toggle switch (turned on), a 'Ping Timeout' input field with the value '500' and a unit of 'ms', and a 'Ping Packets' input field with the value '1'. The 'Global DHCP Relay Configuration' section below it includes a 'Fake Server Detection' toggle switch (turned off), a 'Relay User Table Record' toggle switch (turned off), a 'Refresh Relay User Table' toggle switch (turned on), and a 'Refresh Interval' input field with the value '60' and a unit of 'sec'. At the bottom of the configuration area is a red 'Save' button.

Figure 5-32 Configure DHCP Relay Global Parameters

2. Enable DHCP.
3. Configure the global function of DHCP Relay.
 - 1) Enable or disable **Fake Server Detection** as needed.

 Note

When a rogue DHCP server exists in the network, it may interact with DHCP clients during IP address requests and assign incorrect IP addresses. Such unauthorized DHCP servers are referred to as pseudo-DHCP servers. After enabling the pseudo-DHCP server detection feature, relevant information about these servers can be retrieved from the system logs for further action.

2) Enable or disable **Relay User Table Record** as needed.

 Note

After enabling the DHCP relay user address entry recording feature, when a client obtains an IP address from a DHCP server via the DHCP relay, the relay automatically records the binding relationship between the client's IP address and its MAC address, generating a user address entry. This mechanism helps prevent unauthorized hosts from accessing external networks by statically configuring an IP address.

3) Enable or disable **Refresh Relay User Table** as needed.

 Note

- When a DHCP client sends a DHCP RELEASE message to release its dynamically assigned IP address, the DHCP relay does not process the content of this message. As a result, if the relay has previously recorded the IP-MAC binding relationship, the corresponding user address entry will not be updated in real time. Enabling the periodic refresh feature for dynamic user address entries in the DHCP relay resolves this issue.
- If you enable **Refresh Relay User Table**, you need to configure the refresh interval, which ranges from 10 to 180 seconds and defaults to 60 seconds.

4) Click **Save**.

4. Configure the usage port for the DHCP relay.

1) Click **Configuration** -> **Basic Configuration** -> **DHCP** -> **DHCP Port Configuration**.

2) Click **Add**.

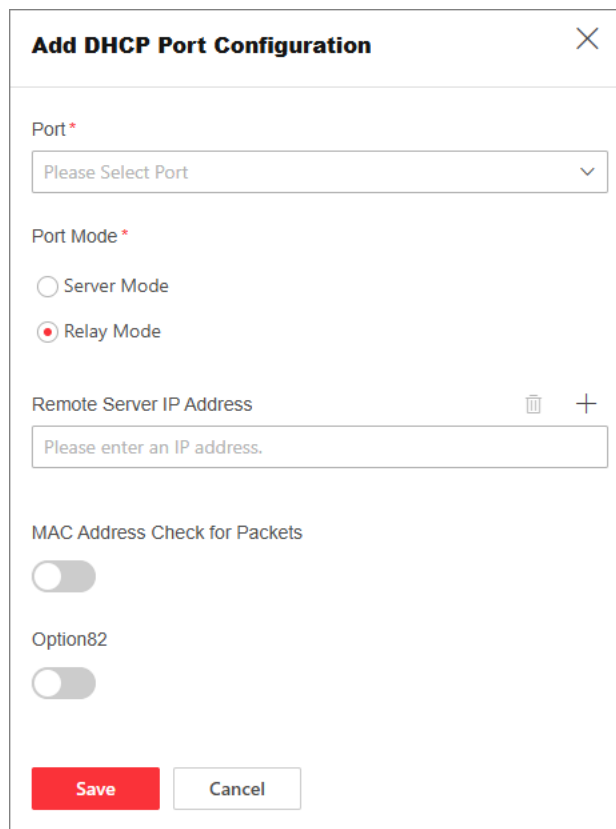


Figure 5-33 Configure DHCP Relay Usage Port

- 3) Select the usage port.
- 4) Set the port mode to **Relay Mode**.

 Note

In this mode, when a port receives a DHCP packet from a DHCP client, it forwards the packet to the DHCP server for address assignment.

- 5) Configure the remote server IP address.

 Note

The DHCP relay enables a remote DHCP server to dynamically assign IP addresses to local DHCP clients across different network segments. You can click  to add multiple remote server IP addresses so as to improve network reliability. When multiple DHCP servers are configured on the DHCP relay, it forwards DHCP packets from clients to all servers.

- 6) Enable or disable **MAC Address Check for Packets** as needed.

 Note

If you enable this function, the DHCP relay checks whether the chaddr field in the received DHCP request matches the source MAC address in the data frame. If they match, the packet is considered valid and processed further; otherwise, it is discarded.

7) Enable or disable **Option82** as needed.

 Note

- By inserting the Option 82 field into DHCP request packets, the DHCP relay provides the DHCP server with precise location information about the client. This allows the server to assign appropriate IP addresses and configuration parameters, enhancing security control over DHCP clients.
- After enabling Option 82, configure the following:
 - **Option 82 Strategy**: Determines how the DHCP relay handles Option 82—discard (**Drop**), replace with the DHCP relay's own Option 82 (**Replace**), or retain the original (**Keep**).
 - **Option82 Circuit ID**: Identifies the client's VLAN or interface (no less than 3 characters).
 - **Option82 Remote ID**: Identifies the device the client is connected to (usually the device's MAC address).

Only after configuring Option 82 processing can the DHCP relay accept, process, and forward DHCP packets containing Option 82.

8) Optional: Enable or disable **Sub-option 9** as needed, and configure its value to be inserted into the Option 82 field.

 Note

Option 82 must be configured before setting Sub-option 9.

9) Click **Save**.

The successfully added DHCP relay usage ports will be displayed in the list.

10) Optional: To add multiple DHCP relay usage ports, repeat the above steps.

11) Optional: Select a port and click  -> **OK** to delete a single DHCP relay usage port; or select multiple ports and click **Delete** -> **OK** to delete multiple DHCP relay usage ports in batch.

12) Optional: Select a port and click  to edit the DHCP relay usage port as needed.

5.2 Advanced Configuration

5.2.1 STP Configuration

Spanning Tree Protocol (STP) is a layer-2 link management protocol that can not only eliminate redundant loops but also realize link backup and path optimization. STP uses the spanning tree algorithm to select one switch as the root of the spanning tree, and determines the topology by transmitting BPDU (Bridge Protocol Data Unit) data packets between devices. Configuring spanning tree can improve network stability.

 Note

- After enabling the STP globally, you can configure STP settings. By default, interfaces have STP enabled once it is activated globally. The STP feature only takes effect when it is enabled both globally and on the interface.
- The STP feature cannot be configured simultaneously with the ERPS feature.

Configure Global STP

Steps

1. Click **Configuration -> Advanced Configuration -> STP -> Global Configuration**.
2. Configure the basic parameters of STP.

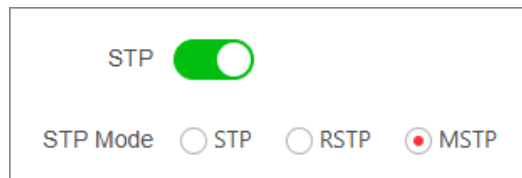


Figure 5-34 Configure STP Basic Parameters

- 1) Enable STP.

 Note

Enabling STP globally is a prerequisite for other configurations to take effect.

- 2) Select the STP mode.

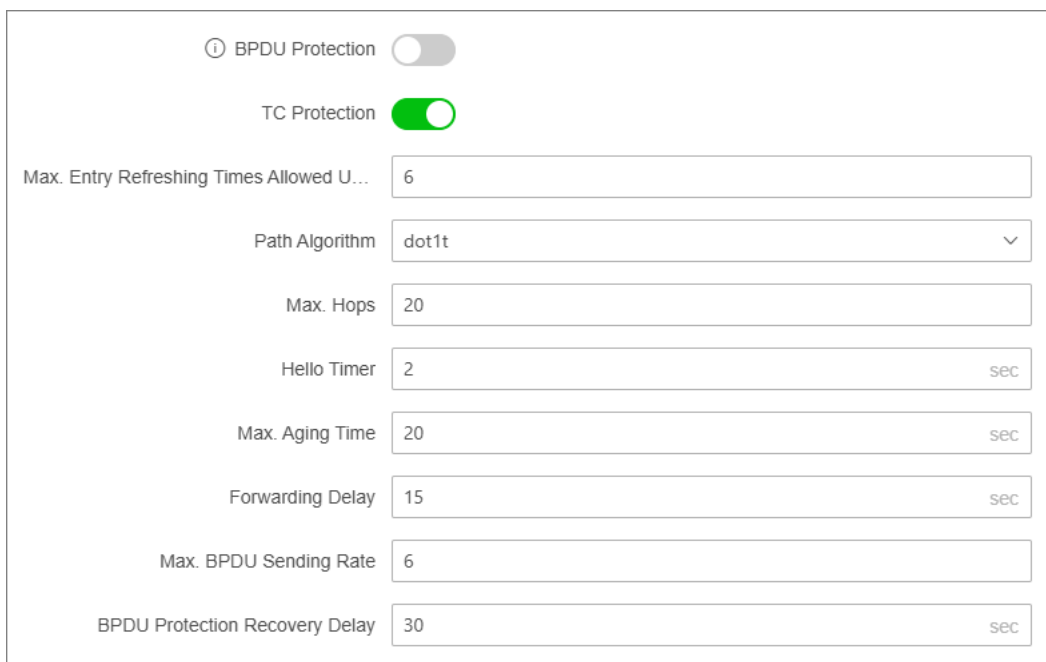
- STP** STP (Spanning Tree Protocol) is used to eliminate physical loops at the data link layer of a LAN. In STP mode, all device ports transmit STP BPDUs. Select this mode when the port's peer device supports only STP.
- RSTP** Rapid Spanning Tree Protocol (RSTP) is a protocol designed to achieve rapid convergence of network topology. In RSTP mode, all device ports send RSTP BPDUs externally. When a port receives an STP BPDU from a peer device, it automatically switches to STP mode; if it receives BPDUs from other protocols, the port transitions to the corresponding mode accordingly. However, if the received BPDU is not from the target root bridge, the switch will not change the port mode.
- MSTP** Multiple Spanning Tree Protocol (MSTP) enables fast convergence and isolates broadcast storms. VLAN traffic is forwarded along dedicated paths, offering improved load balancing across redundant links. In MSTP mode, all device ports send MSTP BPDUs externally. When a port receives an MSTP BPDU from a peer device, it remains

in MSTP mode. However, if it receives an RSTP or STP BPDU, the port automatically switches to RSTP or STP mode accordingly.

Note

- The device supports three STP modes: STP, RSTP, and MSTP.
 - In a ring network running only STP, the switch can operate in STP mode.
 - In a ring network running only RSTP, the switch can operate in RSTP mode.
 - In a ring network running only MSTP, the switch can operate in MSTP mode.
 By default, the device operates in MSTP mode.
- STP and RSTP modes do not support the creation of additional instances; only Instance 0 exists, which serves as the Common and Internal Spanning Tree (CIST) and cannot be deleted. In STP and RSTP modes, you can configure the device's bridge priority for Instance 0. In MSTP mode, multiple instances can be created, and the device's bridge priority can be configured for each instance.

3. Click **Advanced Configuration** to configure the advanced parameters of STP.



BPDU Protection	☐
TC Protection	☒
Max. Entry Refreshing Times Allowed U...	6
Path Algorithm	dot1t
Max. Hops	20
Hello Timer	2 sec
Max. Aging Time	20 sec
Forwarding Delay	15 sec
Max. BPDU Sending Rate	6
BPDU Protection Recovery Delay	30 sec

Figure 5-35 Configure STP Advanced Parameters

BPDU Protection

Enable or disable the BPDU protection function.

When BPDU protection is enabled, if an edge port receives a BPDU packet, the system will automatically disable the port and notify the NMS that the port has been shut

down by the STP protocol. After the configured recovery time elapses, the port will automatically restart and return to the Up state, while retaining its edge port attribute.

TC Protection

Enable or disable protection against TC-BPDU packet attacks.

When the device receives a TC-BPDU packet, it refreshes the MAC address table and ARP table. If an attacker forges TC-BPDU packets to maliciously flood the device, frequent table refreshes may overload the system. Enabling TC-BPDU attack protection prevents excessive refreshing of the MAC and ARP tables.



Note

It is recommended to enable this function.

Max. Entry Refreshing Times Allowed Upon Receiving TC Messages

Sets the maximum number of times the device is allowed to immediately refresh the MAC and ARP tables within each 10-second interval after receiving TC-BPDU packets. The value ranges from 1 to 255 and defaults to 6.



Note

This setting takes effect only when TC Protection is enabled.

Path Algorithm

Specifies the algorithm used to calculate the default path cost for a port, which is dot1t by default.

- **legacy**: Uses a proprietary standard to calculate the default path cost.
- **dot1d-1998**: Uses the IEEE 802.1D-1998 standard to calculate the default path cost.
- **dot1t**: Uses the IEEE 802.1t standard to calculate the default path cost.

Max. Hops

Sets the maximum number of hops in an MST region, which determines the scale of the region. The value ranges from 1 to 40 and defaults to 20.

Hello Timer

Sets the interval for sending BPDU packets. The value ranges from 1 to 10 seconds and defaults to 2 seconds.

The Hello Timer is used to detect link failures. STP sends BPDUs at each Hello Time interval to verify link status.

Max. Aging Time

Sets the maximum time a BPDU packet is stored in the device. The value ranges from 6 to 40 seconds, and defaults to 20 seconds

If the value is set too large, the device may not detect link failures promptly, reducing network adaptability. If the value is set too small, frequent spanning tree recalculations may occur, potentially misinterpreting network congestion as a link failure.

Forwarding Delay

Sets the delay time for port state transitions. The value ranges from 4 to 30 seconds and defaults to 15 seconds.

To prevent temporary loops, STP introduces the Learning state as an intermediate step when transitioning from Discarding to Forwarding. The forwarding delay ensures synchronization with peer devices during state transitions.

Max. BPDU Sending Rate

Sets the maximum number of BPDU packets that can be sent per second. The value ranges from 1 to 255 and defaults to 6.

BPDU Protection Recovery Delay

Sets the time before a BPDU-protected port is restored to the Up state after being shut down. The value ranges from 10 to 300 seconds and defaults to 30 seconds.

**Note**

On the root bridge, the following relationship must be maintained: $2 \times (\text{Forwarding Delay} + 1) \geq \text{Max. Aging Time} \geq 2 \times (\text{Hello Timer} + 1)$

4. Click **Save**.

Configure STP Instance

MSTP divides a switched network into multiple regions. Within each region, multiple spanning trees are established, each operating independently and mapped to corresponding VLANs. Each such spanning tree is referred to as a multiple spanning tree instance (MSTI).

Steps

1. Click **Configuration** -> **Advanced Configuration** -> **STP** -> **Global Configuration** -> **Domain Configuration**.

Domain Configuration

Domain Name

MSTP Revision Level

0

Configuration Digest

MSTP Multi-Instance and VLAN

Mapping Relationship

+ Add

↺ Refresh

MSTP Multi-Inst...	VLAN ID	Bridging Type	Priority	Operation
0	1-4094	Normal	32768	

Figure 5-36 Configure MSTP Region

2. Set the MST region parameters.

Domain Name

The MST region name can contain 1 to 32 characters. By default, the region name is the device's MAC address.

MSTP Revision Level

Set the revision level of the MST domain. The range ranges from 0 to 65535 and defaults to 0.

Configuration Digest

A hash value derived from key MST region parameters, including the VLAN-to-instance mapping table, to verify switch configuration consistency.

3. Click **Add** in **MSTP Multi-Instance and VLAN**.

Add Mapping Relationship

MSTP Multi-Instance ID *

Please Enter MSTP Multi-Instance ID

VLAN ID *

Please Enter VLAN ID

Save

Cancel

Figure 5-37 Add MSTP Instance

4. Configure the mapping relation between the spanning tree instance ID and VLAN ID.

MSTP Multi-Instance ID

Set the ID of the spanning tree instance to be configured, which should be an integer ranging from 1 to 63.

VLAN ID

Specify the VLAN ID to be mapped to the MSTP instance. The value ranges from 1 to 4094.

5. Click **Save**.

6. In the MSTP instance list, you can view information about the MSTP instance, including instance ID, VLAN ID, bridging type, and priority, or perform relevant operations.

- Click  to edit the MSTP instance.
- Click  to delete the MSTP instance.

Note

- You can edit parameters such as VLAN ID (except for instance 0), bridging type, and device priority in the MSTP instance. Actual available parameters may vary based on the actual interface.
- Only when the bridging type is normal, modifying the device's priority in the MSTP instance is supported. The priority of the switch device in the instance affects whether the switch can be elected as the root bridge. The priority ranges from 0 to 61440, with a step size of 4096, meaning the selectable values from insignificant to severe are 0, 4096, 8192, and so on. For example, setting the device priority to 0 can make the switch device the root bridge, while setting another switch device's priority to 4096 can serve as a backup root bridge.
- Instance 0 can be edited but cannot be deleted.
- If the VLAN in instance 0 is assigned to other instances, it will be automatically deleted from instance 0.

7. Click **Save** to save the MSTP region and instance configurations.

8. View the information about the STP instance.

- 1) Click **Configuration -> Advanced Configuration -> STP -> STP Port Instance Configuration**.
- 2) Click **STP Instance** on the right.

Refresh								
Instan...	Bridge ID	Common Root Bridge ID	External P...	Regional Root Bridge ID	Internal Pa...	Specified Bridge ID	Designat...	Root P...
0	32768.8494-5919-cae8	32768.8494-5919-cae8	0	32768.8494-5919-cae8	0	32768.8494-5919-cae8	--	--

Figure 5-38 View STP Instance Information

- 3) View the information about instance 0 and the configured MSTIs, including bridge ID, common root bridge ID, external path cost, etc.

Configure STP Port

Steps

1. Click **Configuration -> Advanced Configuration -> STP -> STP Port Instance Configuration**.

2. Click **STP Port Configuration** on the right.
3. Select one or more ports on the port panel.

Port Name	STP Status	Edge Port	Actual Edge Port	Link Type	Actual Effective Lin...	Loop Pro...	Root Prot...	Port-based BPD...
Ge 1/0/1	Enable	Disable	Disable	Point-to-Point	Point-to-Point	Disable	Disable	Disable
Ge 1/0/2	Enable	Disable	Disable	Point-to-Point	Point-to-Point	Disable	Disable	Disable
Ge 1/0/3	Enable	Disable	Disable	Point-to-Point	Point-to-Point	Disable	Disable	Disable
Ge 1/0/4	Enable	Disable	Disable	Point-to-Point	Point-to-Point	Disable	Disable	Disable
Ge 1/0/5	Enable	Disable	Disable	Point-to-Point	Point-to-Point	Disable	Disable	Disable
Ge 1/0/6	Enable	Disable	Disable	Point-to-Point	Point-to-Point	Disable	Disable	Disable
Ge 1/0/7	Enable	Disable	Disable	Point-to-Point	Point-to-Point	Disable	Disable	Disable

Figure 5-40 Edit STP Port Configuration

4. Edit the parameters of a STP port.

STP Status

Enable or disable the STP function on a port. The STP function is enabled on all ports by default.

Edge Port

Set whether the port is an edge port. By default, all ports are not configured as edge ports. A port that is connected to user terminal devices directly and not to other devices or network segments is called an edge port. When the network topology changes, the edge port will not generate a temporary loop, so it can skip two forwarding delay periods and enter Forwarding state directly without any delay.

Link Type

Set the link type of the port, which is point-to-point by default.

- **Point-to-Point:** The port is connected to the point-to-point link.
- **Non-Point-to-Point:** The port is not connected to a point-to-point link.
- **Auto:** The system will automatically detect if the port is connected to a point-to-point link.

A point-to-point link is a direct connection between two devices. If the ports at both ends of this link are configured as root ports or designated ports, they can rapidly transition to the forwarding state by exchanging synchronization messages (proposal and agreement). This mechanism minimizes unnecessary forwarding delays.

Loop Protection

Configures whether to enable loop protection on the port. By default, this feature is disabled.

The device maintains the state of the root port and other ports by continuously receiving BPDUs from the upstream device. Due to link congestion or unidirectional link failure, a port may fail to receive BPDUs from the upstream device. In such cases, the device will reselect the root port, and blocked ports may transition to the forwarding state, potentially creating a loop in the network. Loop protection prevents such loops from forming.

Root Protection

Configures whether to enable root protection on the port. By default, this feature is disabled.

Due to misconfiguration by maintenance personnel or malicious attacks in the network, higher-priority BPDUs may appear, leading to a recalculation of the spanning tree and incorrect changes in the network topology. Root protection prevents such situations from occurring.

Port-based BPDU Filtering

Configures whether to enable BPDU filtering on the port. By default, this feature is disabled.

Even when configured as an edge port, the port may still send BPDU packets, which could propagate to other networks and cause instability. Enabling BPDU filtering on edge ports prevents them from processing or sending BPDU packets.



Note

- It is recommended to configure both the edge port and BPDU protection features simultaneously to prevent network instability caused by edge ports receiving BPDUs.
 - Loop protection cannot be configured simultaneously with either edge port or root protection.
5. Optional: Click **Port Check** to manually switch the port packet sending mode back to the device configuration mode.

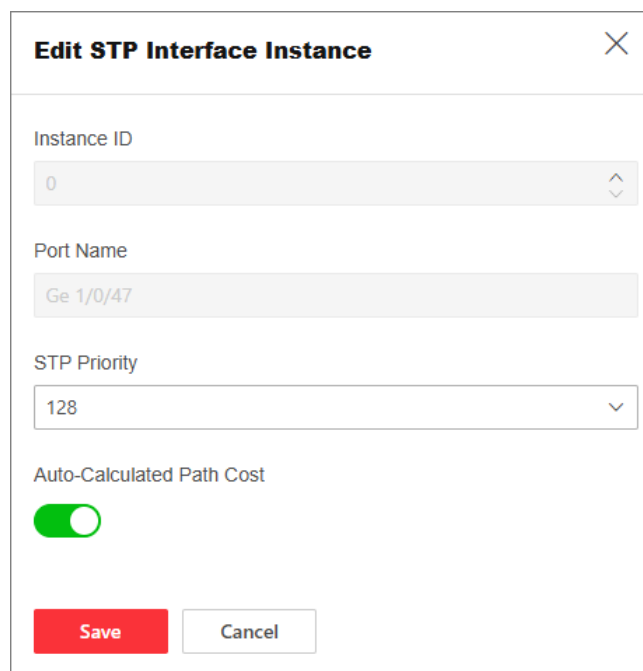
6. Click **Save**.

The edited STP port configuration information will be displayed in the **Port Configuration Info** list.

Configure STP Port Instance

Steps

1. Click **Configuration** -> **Advanced Configuration** -> **STP** -> **STP Port Instance Configuration**.
2. Edit the STP port instance.
 - 1) Select an STP port instance in the list, and click  in the **Operation** column.



Edit STP Interface Instance

Instance ID
0

Port Name
Ge 1/0/47

STP Priority
128

Auto-Calculated Path Cost
☒

Save Cancel

Figure 5-41 Edit STP Port Instance

- 2) Edit the STP port instance parameters, including port STP priority and settings for enabling automatic calculation of path cost.

STP Priority

Configures the STP priority for a port. The value ranges from 0 to 240, with a step size of 16 (i.e., valid values are 0, 16, 32, etc.). A lower value indicates a higher priority.

Port priority is a key factor in determining whether a port is elected as the root port. Under equal conditions, the port with the highest priority (lowest numerical value) will be selected. On devices supporting STP, a port can have different priorities across multiple spanning tree instances, allowing it to assume different roles in different trees. This enables traffic from different VLANs to traverse distinct physical paths, achieving per-VLAN load balancing. Users can set port priorities based on network requirements.

Auto-Calculated Path Cost

Configures whether to enable or disable automatic calculation of the default path cost for a port. If **Auto-Calculated Path Cost** is disabled, the path cost must be configured manually.

- When the path cost mode is set to **legacy**, The value ranges from 1 to 200,000.
- When the path cost mode is set to **dot1t**, The value ranges from 1 to 200,000,000.
- When the path cost mode is set to **dot1d-1998**, The value ranges from 1 to 65,535.

Path cost is a parameter associated with the link speed of a port. On STP-supported devices, a port can have different path costs in different MSTP instances. Configuring appropriate path costs allows traffic from different VLANs to be forwarded along separate physical links, enabling VLAN-based load balancing.

- 3) Click **Save**.
3. Optional: View port instance information in the STP port instance list, including the port bound to the instance, port STP priority, port role, port status, etc.
4. Optional: Click  next to the port name to view the detailed STP configuration information of the port.

Ge 1/0/37

Instance ID

0

Priority

128

Actual Path Cost

20000

Role

Designated Port

Status

FORWARDING

Remaining Hops

20

Bridge ID

Root Bridge ID

External Path Cost

0

Regional Root Bridge ID

Internal Path Cost

0

Specified Bridge ID

Designated Port No.

128.37

Figure 5-42 View Detailed STP Port Configuration Information

5.2.2 LLDP Configuration

LLDP (Link Layer Discovery Protocol) is a protocol that enables network devices to discover each other and exchange status and information. The LLDP function collects and advertises local device details—such as management addresses, device identifiers, and interface identifiers—to neighboring devices. Upon receiving this information, neighboring devices store it in a standard MIB (Management Information Base) format, allowing a NMS to query the data and assess link connectivity.

Configure Global LLDP

Steps

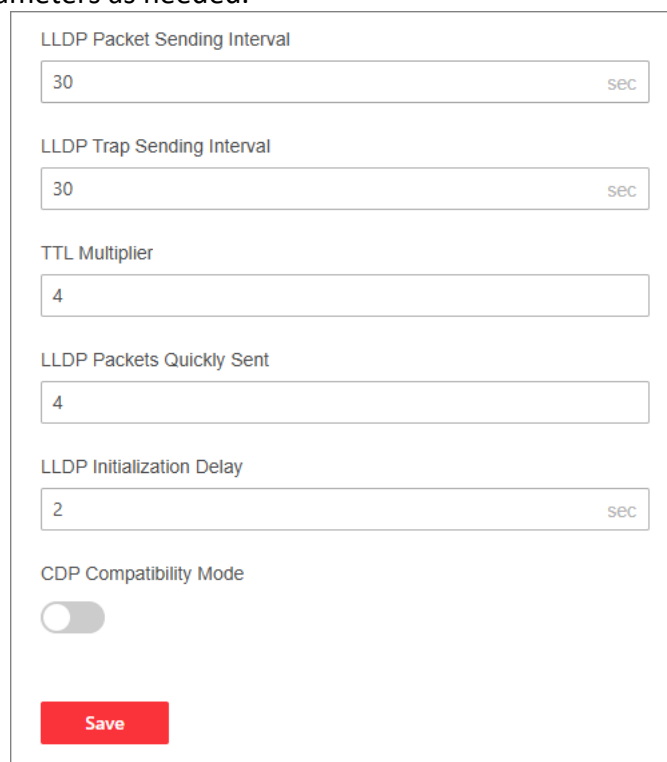
1. Click **Configuration** -> **Advanced Configuration** -> **LLDP** -> **Global LLDP Configuration**.
2. Enable LLDP globally.



The screenshot shows the 'Global LLDP Configuration' page. At the top, there are two tabs: 'Global LLDP Config...' (active) and 'LLDP Port Configura...'. Below the tabs, the text 'Enabled' is displayed above a green toggle switch that is turned on. Underneath the toggle, there is a blue link labeled 'Advanced Configuration' with a downward arrow. At the bottom of the page, there is a red 'Save' button.

Figure 5-43 Enable LLDP Globally

3. Configure LLDP advanced parameters.
 - 1) Click **Advanced Configuration**.
 - 2) Configure the parameters as needed.



The screenshot shows the 'LLDP Advanced Configuration' page. It contains several input fields and a toggle switch. The 'LLDP Packet Sending Interval' is set to 30 sec. The 'LLDP Trap Sending Interval' is set to 30 sec. The 'TTL Multiplier' is set to 4. The 'LLDP Packets Quickly Sent' is set to 4. The 'LLDP Initialization Delay' is set to 2 sec. The 'CDP Compatibility Mode' is a toggle switch that is currently turned off. At the bottom, there is a red 'Save' button.

Figure 5-44 Configure LLDP Advanced Parameters

LLDP Packet Sending Interval

Sets the interval at which the device sends LLDP packets. The value ranges from 5 to 32,768 seconds.

This interval defines the periodic cycle for transmitting LLDP packets to neighbor devices when no status changes occur.

LLDP Trap Sending Interval

Configures the minimum interval for sending LLDP Trap messages to the NMS. The value ranges from 5 to 3,600 seconds.

Adjusting this interval helps avoid frequent Trap transmissions caused by rapid changes in neighbor information.

TTL Multiplier

Sets the TTL multiplier, with a valid range of 2 to 10.

This value controls how long the local device's information is retained by neighbor devices before aging out.

LLDP Packets Quickly Sent

Defines the number of LLDP packets sent rapidly to neighbors. The value ranges from 1 to 10. This applies when the local device discovers a new neighbor, re-enables LLDP, or when a port transitions from Down to Up. Rapid transmission ensures neighbors quickly obtain the local device's information.

LLDP Initialization Delay

Sets the initialization delay for LLDP on a port, ranging from 1 to 10 seconds.

This delay occurs when re-enabling the LLDP module on a port, helping to prevent topology oscillation caused by frequent LLDP state changes.

CDP Compatibility Mode

Configures whether to enable or disable LLDP compatibility with Cisco Discovery Protocol (CDP).

CDP is Cisco's proprietary link-layer discovery protocol. When **CDP Compatibility Mode** is enabled, the device can receive and interpret CDP packets from other vendors' devices to obtain their status information.

**Note**

This configuration is only supported on certain devices. Refer to the device interface for availability.

4. Click **Save**.

Configure LLDP Port

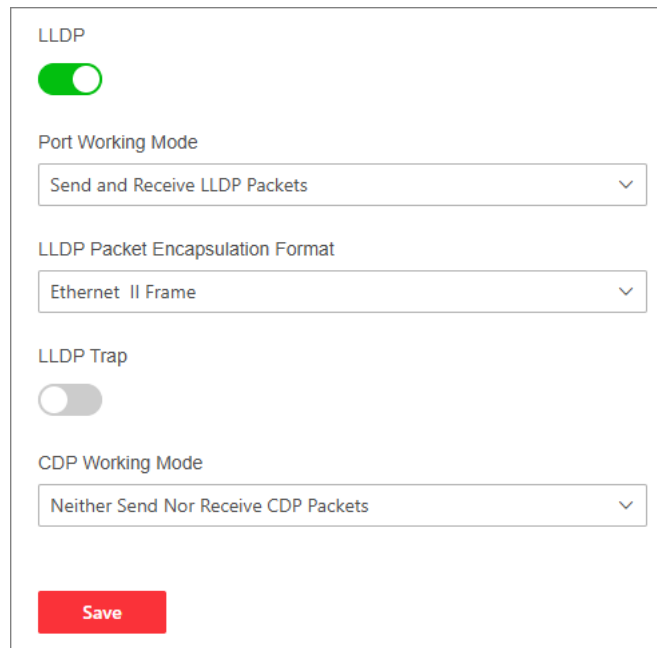
Steps

1. Click **Configuration** -> **Advanced Configuration** -> **LLDP** -> **LLDP Port Configuration**.
2. Select one or more ports on the port panel.

**Note**

You can click **Add All** to batch select all Ethernet ports, or click **Clear** to deselect the selected port(s).

3. Set the parameters.



LLDP

☒

Port Working Mode

Send and Receive LLDP Packets

LLDP Packet Encapsulation Format

Ethernet II Frame

LLDP Trap

☐

CDP Working Mode

Neither Send Nor Receive CDP Packets

Save

Figure 5-45 Configure LLDP Port

LLDP

Configures whether to enable or disable the LLDP function of the selected port(s).

Port Working Mode

You can choose among **Send and Receive LLDP Packets**, **Send LLDP Packets Only**, **Receive LLDP Packets Only**, or **Neither Send Nor Receive LLDP Packets** according to your needs.

LLDP Packet Encapsulation Format

Specifies the encapsulation format for LLDP frames within Ethernet frames to enable transmission and ensure interoperability between devices from different vendors. You can choose between **Ethernet II Frame** or **Subnet Access Protocol (SNAP)**.

LLDP Trap

Configures whether to enable or disable the LLDP Trap function for the selected port(s). After the LLDP Trap function is enabled, the device can send Trap information to the NMS to announce important events such as the discovery of new LLDP neighbors or a fault in the communication link with the original neighbor.

CDP Working Mode

Specifies the LLDP port's operating mode when CDP compatibility is enabled. You can configure the port to send and/or receive CDP packets, with options including **Send and Receive CDP Packets**, **Receive CDP Packets Only**, or **Neither Send Nor Receive CDP Packets**.

5. Click **Save**.

The successfully configured LLDP port information will be displayed in the **LLDP Port Status** List.

6. Optional: Click **Neighbor Info** to view the information about neighbor devices.

 Refresh	 Delete					
☐	Port	System Name	Device ID Type	Device ID	Neighbor Port ID Type	Neighbor Port No.
☐	Ge 1/0/37	HIK	MAC Address		Interface Name	Ge 1/0/24
☐	Ge 1/0/47	WH-	MAC Address		Interface Name	Ge 1/0/34

Figure 5-46 View LLDP Neighbor Information

5.2.3 IGMP Snooping Configuration

IGMP Snooping (Internet Group Management Protocol Snooping) is a Layer 2 IPv4 multicast protocol that builds an IGMP Snooping forwarding table by monitoring IGMP messages exchanged between Layer 3 multicast devices and user hosts, and uses this table to guide the forwarding of multicast data.

To enable IGMP Snooping, you must first configure the VLAN where the feature is activated. Then, depending on specific requirements, you can configure multicast group entries (including multicast group addresses and multicast source addresses) and router port entries as needed.

Note

A router port refers to a port on a Layer 2 device that faces toward an upstream Layer 3 multicast device.

Enable IGMP Snooping Globally

Steps

1. Click **Configuration -> Advanced Configuration -> IGMP Snooping -> Global Configuration**.
2. Enable IGMP Snooping globally.

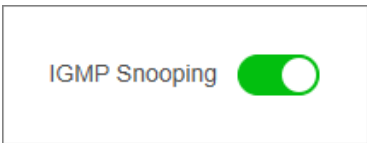


Figure 5-47 Enable IGMP Snooping Globally

Configure VLAN

Steps

1. Click **Configuration** -> **Advanced Configuration** -> **IGMP Snooping** -> **Global VLAN Configuration**.
2. Click **Add**.
3. Set the parameters as needed.

Add VLAN ✕

VLAN ID *

Unknown Multicast Handling Mode

Flooding ▼

Fast Leave
☐

Report Packet Suppression
☐

Multicast Querier
☐

Interval for Sending Group-Specific Query Messages

1 sec

Interval for Sending IGMP General Query Messages

125 sec

Max. Query Response Time

10 sec

Robustness Coefficient

2

Save

Cancel

Figure 5-48 Configure IGMP Snooping VLAN

VLAN ID

Sets the VLAN ID based on which the IGMP snooping function is enabled. The value ranges from 1 to 4094.

Unknown Multicast Handling Mode

Sets the handling method for unknown multicast packets. The default mode is flooding.

- **Flooding:** When an unknown multicast data packet is received on a port, it will be forwarded out of all ports in the same VLAN that are in the Up state.
- **Drop:** Unknown multicast data packets are dropped.

Fast Leave

Configures whether to enable or disable the Fast Leave feature on a port. By default, it is disabled.

Fast Leave allows a port to be immediately removed from the corresponding forwarding entry's output port list when an IGMP Leave message for a specific multicast group is received from a host. Afterward, the Layer 2 device will not send or forward IGMP Group-Specific Query messages for that multicast group to that port.

Report Suppression

Configures whether to enable or disable IGMP Membership Report Suppression. By default, it is disabled.

When this feature is enabled, within one query interval, the switch will forward only a number of Report/Leave messages equal to the "Robustness Coefficient" for the same multicast group, reducing the volume of packets in the network.

Multicast Querier

Configures whether to enable or disable the IGMP Multicast Querier. By default, it is disabled.

When IGMP Snooping is enabled, a Layer 2 device can dynamically build multicast forwarding entries by monitoring IGMP messages exchanged between an IGMP Querier and hosts. However, if the upstream Layer 3 multicast device does not run IGMP (e.g., uses static multicast configuration) or if multicast sources and hosts are within the same Layer 2 network without a Layer 3 multicast device, the Layer 2 device may fail to build multicast entries due to the absence of IGMP messages. In such cases, configuring an IGMP Snooping Querier on the Layer 2 device allows it to send IGMP Query messages to hosts on behalf of the Layer 3 device.

Querier IP Address

Required if **Multicast Querier** is enabled. Format: A.B.C.D. Valid range: 0.0.0.0 to 255.255.255.255. Default value: 192.168.0.1.

Interval for Sending Group-Specific Query Messages

Sets the interval (in seconds) at which the Querier sends Group-Specific Query messages. Valid range: 1 to 5 seconds. Default value: 1 second.

When the Querier receives a Leave message for a multicast group, it sends Group-Specific Query messages to check whether any members remain in that group.

Interval for Sending IGMP General Query Messages

Sets the interval (in seconds) at which the Querier sends General Query messages. Valid range: 1 to 18000 seconds. Default value: 125 seconds.

The Querier periodically sends General Query messages to maintain group membership information on the interface.

Max. Query Response Time

Sets the maximum response time (in seconds) for IGMP General and Group-Specific Query messages. Valid range: 1 to 25 seconds. Default value: 10 seconds.

Upon receiving a query, multicast group members must send a Report within this time limit.

Robustness Coefficient

Sets the robustness coefficient for the IGMP Querier. Valid range: 2 to 5. Default value: 2.

This value determines the number of retransmissions to compensate for possible packet loss.

- When the Querier starts, it sends General Query messages "Robustness Coefficient" times.
- When a Leave message is received, the Querier sends Group-Specific Query messages "Robustness Coefficient" times to confirm whether the group has any remaining members.

4. Click **Save**.

5. In the IGMP Snooping VLAN configuration information list, you can view the VLAN configuration information of IGMP Snooping or perform relevant operations.

VLAN ID	Unknown Multicast Handling ...	Fast Leave	Port Status Info	Report Packet Suppression	Multicast Querier	Operation
2	Flooding	Disable	Packet Statistics >	Disable	Disable	 
3	Flooding	Enabled	Packet Statistics >	Enabled	Disable	 

Figure 5-49 View IGMP Snooping VLAN Configuration Information

- Click  to edit IGMP Snooping VLAN configuration information.

- Click  to delete IGMP Snooping VLAN configuration information.
- Click  in the **Port Status Info** column to view statistics such as the number of IGMP Report/Leave/Query messages received.
- Enter the VLAN ID and click **Search** to search for a specific IGMP Snooping VLAN configuration entry.

Configure Multicast Group Entry

When a Layer 2 multicast device receives a multicast data packet, it searches the Layer 2 multicast forwarding table for the corresponding outgoing interface information based on the packet's VLAN and destination address (i.e., multicast group address). If a matching entry exists, the packet is forwarded to the member ports and router ports associated with that multicast group. If no entry is found, the packet is either discarded or flooded within the VLAN.

If a host connected to a port requires multicast data for a specific multicast group or multicast source group, the port can be configured as a static member port for that group. Static member ports do not respond to IGMP queries from the querier. Additionally, when a port is configured or unconfigured as a static member, it does not send IGMP Membership Report or Leave messages proactively.

Steps

1. Click **Configuration** -> Advanced **Configuration** -> **IGMP Snooping** -> **Multicast Group Table**.
2. Click **Add**.
3. Configure relevant parameters to add a static multicast group entry.

Add Static Multicast Group Entry

VLAN ID *

Please Enter VLAN ID

Port Name *

Please Select Port Name

Multicast Group Address *

Multicast Source Address

Save

Cancel

Figure 5-50 Add Static Multicast Group Entry

VLAN ID Sets the VLAN ID of the static multicast group. The value ranges from 1 to 4094.

Configures the static multicast group member port. You can select an Ethernet port or aggregate interface.



Note

Port Name Aggregation group member ports are not supported.

Multicast Group Address Configures the IPv4 address of the multicast group that the port statically joins. The configurable multicast group address range is 224.0.1.0 to 239.255.255.255.

Optional configuration item. After setting the multicast source address, you can add the port to the multicast group of the specified multicast source.

Multicast Source Address



Note

Please configure a valid unicast address.

4. Click **Save**.
5. Optional: View multicast group entries in the multicast group list, including manually configured multicast group entries (static entry type) and dynamically generated multicast group entries (dynamic entry type), or perform related operations.
- Click to delete the desired static multicast group entry. Dynamic multicast group entries cannot be deleted and can only be aged out.
 - Enter the VLAN ID or select port, and click **Search** to search for the specified multicast group entry.

Configure Router Port Entry

Dynamic router ports age out periodically. If a dynamic router port does not receive an IGMP Query or PIM Hello message before its aging timer expires, the device will remove the interface from the router port list. To ensure stable and long-term forwarding of IGMP Report/Leave messages to the upstream IGMP querier, configure the interface as a static router port.

Steps

1. Click **Configuration** -> **Advanced Configuration** -> **IGMP Snooping** -> **Router Port List**.
2. Click **Add**.
3. Configure relevant parameters as needed to add a static router port entry.

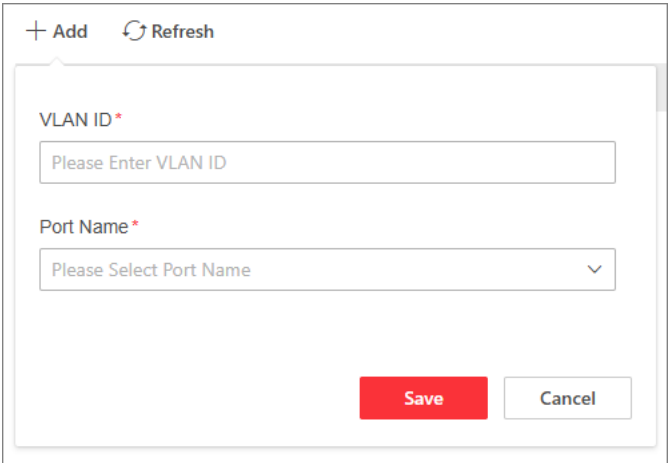


Figure 5-51 Add Static Router Port Entry

VLAN ID

Sets the VLAN ID for the static router port. The value ranges from 1 to 4094.

Port Name

Selects the port to be configured as a static router port. You may choose from the device's Ethernet ports or aggregate interfaces, but member ports of an aggregation group are not supported.

4. Click **Save**.
5. Optional: View the router port information in the router port list, or perform relevant operations.

VLAN ID	Port Name	Other Querier Address(es)	Aging Time (s)	Port Type	Operation
2	Ge 1/0/2		Never	Static	

Figure 5-52 View IGMP Snooping Router Port Information

- Click  to delete the desired static router port entry. Dynamic router port entries cannot be deleted and can only be aged out.

- Enter the VLAN ID or select port, and click **Search** to search for the specified router port entry.

5.2.4 PoE Configuration

PoE (Power over Ethernet) is a technology that enables the transmission of both data and DC power over standard Ethernet cables, without requiring modifications to the existing network infrastructure. It allows IP-based devices—such as IP phones, wireless access points (APs), and network cameras (IPCs)—to receive power directly through their Ethernet connections. For devices equipped with PoE functionality, this feature can be enabled to supply power to compatible powered devices (PDs).

Steps

1. Click **Configuration** -> **Advanced Configuration** -> **PoE** -> **Port PoE Configuration**.

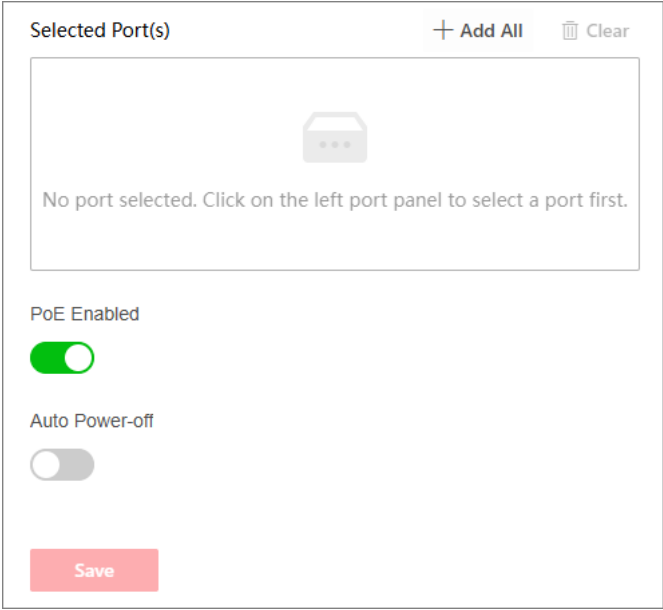


Figure 5-53 Configure Port PoE

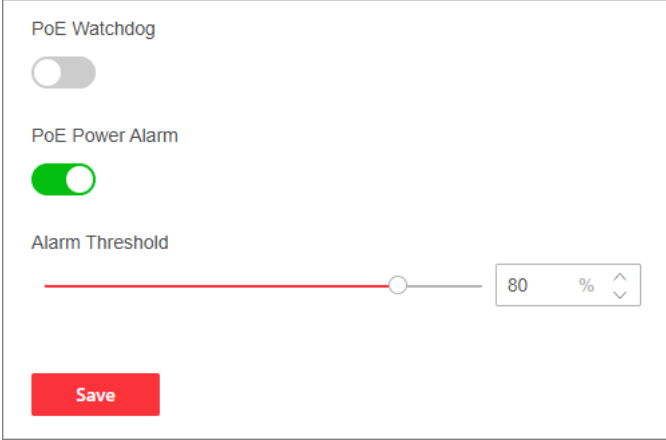
2. Select one or more PoE ports on the port panel.

Note

You can click **Add All** to batch select all PoE ports, or click **Clear** to deselect the selected port(s).

3. Enable PoE to activate PoE on the selected port(s), allowing the port(s) to deliver both data and electrical power to connected PDs over a single Ethernet cable.
4. Optional: Enable **Auto Power-off** to automatically cut off power to PoE ports during specified time periods. If this feature is enabled, you need to specify the power-off time period for the selected PoE port(s). Select an existing time period, or click  to add a time period.
5. Click **Save**.

6. Optional: Configure advanced parameters for the PoE feature.



PoE Watchdog

PoE Power Alarm

Alarm Threshold

80 %

Save

Figure 5-53 Configure Advanced PoE Parameters

- Click **Advanced Configuration**.
- (Optional) Enable **PoE Watchdog** to automatically detect and restart ports.
- (Optional) Enable **PoE Power Alarm** and set the alarm threshold accordingly.

Note

This feature monitors the real-time power consumption of PoE ports and triggers alarms when usage exceeds the configured threshold.

- Click **Save**.

7. Optional: View the PoE power supply status and power information for each PoE port in either a list or bar chart format.

5.2.5 OSPF Configuration

OSPF (Open Shortest Path First) is an interior gateway protocol that uses the SPF (Shortest Path First) algorithm to find the shortest path between two points in the network.

OSPF is a kind of dynamic routing protocol widely used in computer networks. It describes network topology via LSA (Link State Advertisement) and generates a SPT (Shortest Path Tree) based on the network topology to calculate the shortest path to all destinations in the network for exchanging routing information. OSPF converges fast and can be applied to medium-sized enterprise networks with extended network support via area division.

Create OSPF Process

To enable OSPF on a switch, you must first create an OSPF process, specify the area associated with the process, and define the network segments included in that area. If an interface's IP address on a

switch falls within the network segment of a specific area, the interface will belong to that area and have OSPF enabled. OSPF will then advertise the directly connected route of that interface.

Steps

1. Click **Configuration** -> **Advanced Configuration** -> **OSPF** -> **Basic Configuration**.
2. Add an OSPF process.
 - 1) Click **Add**.

Add Process

Process ID *

Please Enter Process ID

Router ID

IP Address Range: 0.0.0.1 to 255.255.255.255

Internal Priority

10

External Priority

150

Advertise Default Route

☐ Enable

☒ Disable

☐ Always Advertise

SPF Initial Delay

500ms

Min. SPF Delay

500ms

Max. SPF Delay

10000ms

BFD

☐

Save

Cancel

Figure 5-54 Add OSPF Process

2) Set the OSPF process parameters.

Process ID

A unique identifier used by the router to distinguish between different OSPF instances, which ranges from 1 to 65,535.

Router ID

A unique identifier (Router ID, or RID) assigned to each OSPF router for identification within the OSPF network.

Internal Priority

The priority value assigned to routes that are generated internally by the OSPF protocol, which ranges from 1 to 255, with a default value of 10. A lower numerical value indicates a higher priority. When multiple routes to the same destination are available, the OSPF internal route with the highest priority (lowest value) is selected.

External Priority

The priority value assigned to routes that are imported into the OSPF domain from external routing protocols, which ranges from 1 to 255, with a default value of 150. A lower value corresponds to a higher priority. If the external priority is configured lower than the internal priority, OSPF will prefer internal routes during route selection and only resort to external routes when internal ones are unavailable.

Advertise Default Route

Enable: The router advertises a default route to other routers in the OSPF area. This enables forwarding of traffic with unknown destination addresses along a designated path, eliminating the need to maintain detailed routing entries for every external network.

Disable: The router does not advertise a default route to other routers within the OSPF area.

Always Advertise: Regardless of changes in external network connectivity, the OSPF router continually advertises a default route to other routers in its area. This ensures that routers always have a default path available for forwarding traffic destined outside the local area.

SPF Initial Delay

The delay period between a network topology change and the initiation of the SPF algorithm to compute new routes. The value ranges from 1 to 600,000 milliseconds, with a default value of 500 ms.

Min. SPF Delay

The minimum time interval that must elapse between the completion of one SPF calculation and the start of the next. The value ranges from 1 to 600,000 milliseconds, with a default value of 500 ms.

Max. SPF Delay

The maximum allowable delay for the router to perform an SPF calculation following a network change. The value ranges from 1 to 600,000 milliseconds, with a default value of 10,000 ms.

BFD

Enable BFD (Bidirectional Forwarding Detection) to accelerate fault detection and improve network convergence speed.

3) Optional: You can repeat the above operations to configure multiple OSPF processes.

3. Click **Save**.

4. View the created OSPF process in the OSPF process information list or perform other operations.

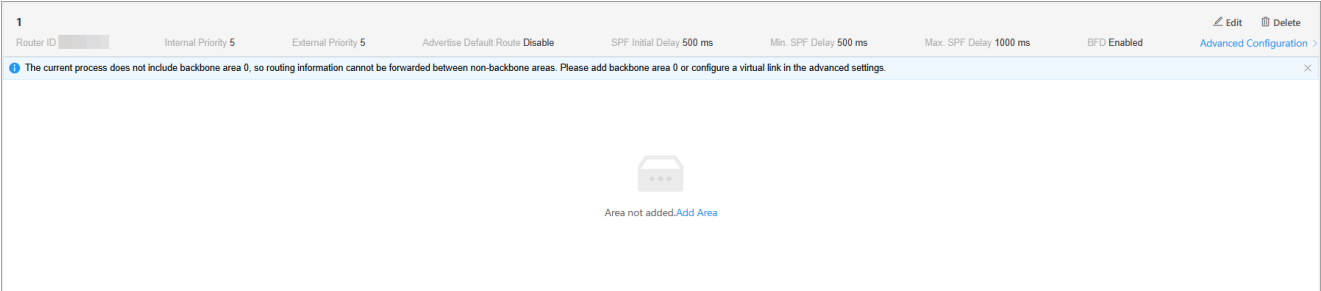


Figure 5-55 View OSPF Process Information

- Click **Edit** to edit the configuration of the created OSPF process.
- Click **Delete** to delete the created OSPF process.

4. Link an area to the OSPF process.

 Note

If an OSPF process does not include the backbone area (Area 0), routing information cannot be forwarded between non-backbone areas. Please add Area 0 as the backbone area or configure a virtual link in **Advanced Configuration**. For details, refer to Configure Advanced OSPF Parameters.

1) Click **Add Area**.

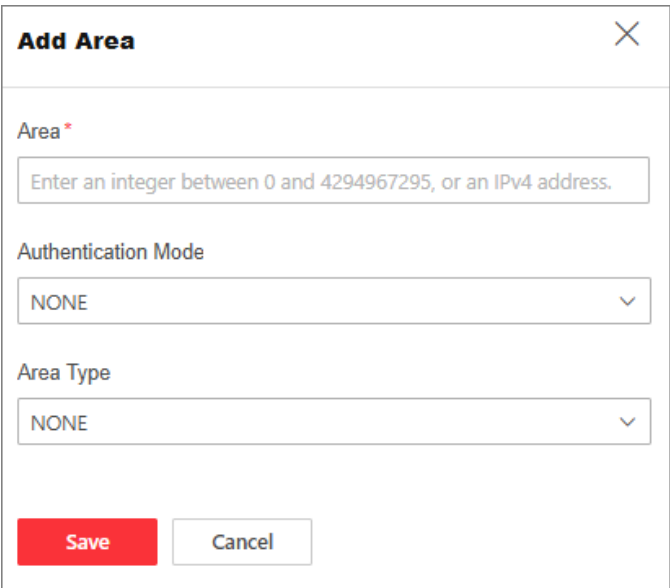
The 'Add Area' dialog box has a title bar with a close button. It contains three input fields: 'Area' with a red asterisk and a placeholder 'Enter an integer between 0 and 4294967295, or an IPv4 address.', 'Authentication Mode' with a dropdown menu showing 'NONE', and 'Area Type' with a dropdown menu showing 'NONE'. At the bottom are 'Save' and 'Cancel' buttons.

Figure 5-57 Add Area

2) Set the area ID. Enter an integer between 0 and 4,294,967,295, or an IPv4 address.

3) Select the authentication mode.

NONE

No authentication is performed. The router accepts OSPF packets directly from neighboring routers without any authentication when establishing OSPF adjacencies.

Simple

Plain text password authentication. A simple authentication password must be configured, with a maximum length of 8 characters. In simple authentication mode, the router includes a pre-configured password in each OSPF packet it sends. The receiving router checks whether the password in the received packet matches its own configured password. If they match, the packet is accepted and an adjacency is established; otherwise, the packet is rejected.

MD5

Message Digest 5 authentication. Both an MD5 key ID (ranging from 1 to 255) and an MD5 password (up to 16 characters) must be configured. In MD5 authentication mode, the router uses the MD5 algorithm to compute a message digest based on the packet content and the pre-configured key/password, and includes this digest in the transmitted packet. Upon receiving the packet, the receiving router uses the same key/password and MD5 algorithm to compute a local message digest. It then compares the locally generated digest with the one received in the packet. If they match, the packet is accepted and an adjacency is established; otherwise, the packet is rejected.

4) Select the area type.

NONE

A standard OSPF area that can receive and propagate Type-3, Type-4, and Type-5 LSAs (Link State Advertisements) from other areas. Routers in a standard area run the full OSPF algorithm and maintain detailed network topology information.

Stub

In a Stub area, the ABR propagates inter-area routes into the area but does not introduce external autonomous system (AS) routes. This significantly reduces the size of the routing table and the number of LSAs within the area.

If you check **Totally Stub** in **Stub Configuration** to configure the area as a Totally Stub area, the ABR does not propagate inter-area or external AS routes into the area. To ensure reachability to other areas within the AS and external destinations, the ABR generates and advertises a default route (Type-3 LSA) to non-ABR switches within the area.

NSSA

An NSSA (Not-So-Stubby Area) allows the introduction of external AS routes. These routes are advertised within the area as Type-7 LSAs by an ASBR (Autonomous System Boundary Router). When a Type-7 LSA reaches the NSSA ABR, it is converted into a Type-5 LSA for propagation to other areas.

Additional parameters can be configured as needed, such as:

- **Advertise Default Route to NSSA**

Enables routers within the NSSA to use the advertised default route to reach external networks when no specific route is available.

- **Do Not Import External Routes**

Prevents the NSSA from receiving external routes from other areas or external routing protocols.

- **Totally NSSA**

A totally NSSA area does not receive Type-4 or Type-5 LSAs from other areas and also prohibits routers within the area from importing external routes.

- **Stability Interval**

The duration during which the NSSA remains in a relatively stable state (i.e., without frequent route changes or topology adjustments). The value ranges from 1 to 120 seconds, with a default value of 40 seconds.

- **Translator Role**

Defines how the ABR handles Type-7 to Type-5 LSA conversion.

- **Always:** The ABR always performs Type-7 to Type-5 LSA conversion and propagation to other OSPF areas upon receiving Type-7 LSAs from the NSSA.
- **Candidate** (Default): The ABR acts as a translator conditionally, based on factors such as network topology, routing policies, or resource availability.
- **Never:** The ABR does not convert Type-7 LSAs to Type-5 LSAs, preventing external routes from the NSSA from being advertised to other OSPF areas.

- **Cost**

A metric used to evaluate link quality and path preference. The value ranges from 0 to 16,777,214, with a default value of 1). In OSPF, each link is assigned a cost value, typically based on factors like bandwidth, delay, and reliability. Within an NSSA, cost is used to determine optimal data forwarding paths.

5) Click **Save**.

6) Optional: Click **Edit** to edit the area information, or click **Delete** to delete the linked area.

Configure OSPF Advanced Parameters

Configure Virtual Link

After the areas are divided, OSPF routing updates between non-backbone areas are exchanged via backbone areas. Therefore, OSPF requires that all non-backbone areas should be connected to the backbone area, and the backbone area itself must also remain connected. However, in practical applications, various conditions may prevent this requirement from being met. In this case, the issue can be resolved by configuring OSPF virtual links on the ABR.

1. Click **Configuration -> Advanced Configuration -> OSPF -> Basic Configuration**.
2. Select the OSPF process for which you want to configure advanced parameters, and click **Advanced Configuration -> Virtual Link**.
3. Click **Add**.

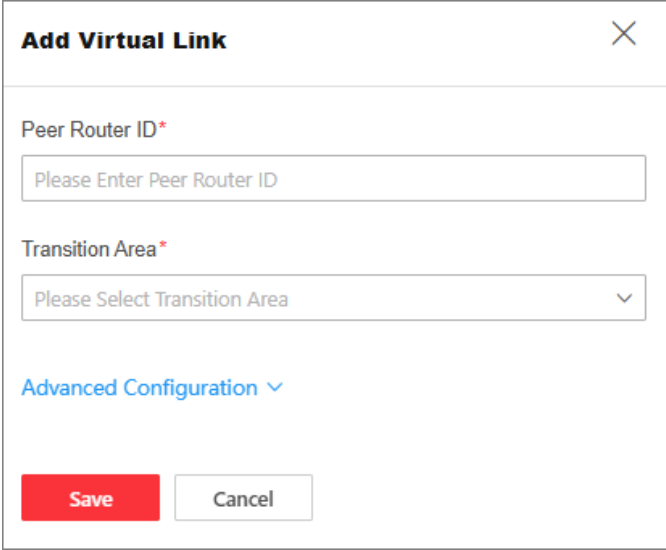


Figure 5-58 Add Virtual Link

- Set the peer router ID and transition area.

Peer Router ID

The unique identifier of the other router corresponding to the local router when establishing a virtual connection. The value range is 0.0.0.1 to 255.255.255.255.

Transition Area

An area between two non-adjacent areas in which virtual connections are established. It is usually a general area, but it functions as a bridge to connect two originally unconnected areas.

- Click **Advanced Configuration** to set other advanced parameters.

Transmission Delay

The time required for data to be transmitted from one router to another over a virtual link. The value ranges from 1 to 1,800 seconds, with a default value of 1 second.

Dead Interval

The time interval after which a router declares a neighbor relationship as down if no Hello messages are received from that neighbor. The value ranges from 2 to 262,140 seconds, with a default value of 40 seconds.

Hello Interval

The time interval between successive Hello messages sent by a router. The value ranges from 1 to 65,535 seconds, with a default of 10 seconds.

Retransmit Interval

The time interval after which an OSPF packet is retransmitted if no acknowledgment is received. The value ranges from 1 to 3,600 seconds, with a default value of 5 seconds.

Authentication Mode

- **NONE**: No authentication is performed.

- **Simple**: Plain text password authentication. A simple authentication password must be configured, with a maximum length of 8 characters.

- **MD5**: Message Digest 5 authentication. Both an MD5 key ID (ranging from 1 to 255) and an MD5 password (up to 16 characters) must be configured.

6. Click **Save**.

7. Check the added virtual link information in the list or perform other operations.



Figure 5-59 View Virtual Link Information

- Click  to modify the configuration of the added virtual link.
- Click  to delete the added virtual link.

Configure Route Introduction

If other routing protocols are also running on the switch besides OSPF, you can configure OSPF to import routes generated by other routing protocols and then advertise these route information to other routers via Type 5 LSA or Type 7 LSA.

1. Click **Configuration** -> **Advanced Configuration** -> **OSPF** -> **Basic Configuration**.
2. Select the OSPF process for which you want to configure advanced parameters, and click **Advanced Configuration** -> **Route Import**.
3. Click **Add**.
4. Set the parameters.

Figure 5-60 Configure Route Import

- a. Select the route type.

Direct

Routes automatically discovered by the link-layer protocol and obtained by the device without manual configuration.

Static

Routes manually configured by a network administrator, requiring explicit setup and maintenance.

RIP

Routes discovered through the Routing Information Protocol (RIP), a distance-vector routing protocol that uses hop count as its metric and is suitable for small-scale networks.

OSPF

Routes discovered through the Open Shortest Path First (OSPF) protocol, a link-state routing protocol that uses cost as its metric and is designed for efficient routing in larger, more complex networks.

IS-IS

Routes discovered through the Intermediate System to Intermediate System (IS-IS) protocol, a link-state routing protocol commonly used in large-scale service provider networks.

BGP

Routes discovered through BGP, the standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems on the internet.

- b. Configure other parameters as needed.

Redistributed Process ID

When the route type is RIP, OSPF, or IS-IS, you need to set the redistributed process ID, which is the RIP process ID, OSPF process ID, or IS-IS process ID.

Enter a number between 1 and 65535. If left blank, all RIP, OSPF, or IS-IS processes will be imported.

Cost

An index for measuring the quality of a path. The value ranges from 0 to 16,777,214, and the default value is 1. It represents the "cost" that a data packet pays when passing through a specific path. In OSPF, the cost is usually calculated based on factors such as link bandwidth.

Type

External routes are categorized into two types: External Type 1 (E1) and External Type 2 (E2).

- E1

When calculating the routing cost, E1 routes combine the external route cost with the internal cost required to reach the ASBR (Autonomous System Boundary Router).

- E2

When calculating the routing cost, E2 routes only consider the external route cost advertised by the ASBR, excluding the internal cost to reach the ASBR.

- 5. Click **Save**.
- 6. View the imported external route information in the list or perform other operations.

Route Type						
All						
+ Add  Delete  Refresh						
☐	No.	Route Type	Redistributed Process ID	Cost	Type	Operation
☐	1	Static	--	1	E2	 
☐	2	BGP	--	1	E1	 

Figure 5-61 View Imported Route Information

- Click  to edit the imported external route.
- Click  to delete the imported external route.
- Select route type and click **Search** to search for the specified type of imported external routes.

Configure Route Summarization

When the OSPF network is large, configuring route summarization can reduce the number of entries in the routing table, decrease resource occupation, and not affect system performance. In addition, if one link in the IP address range to be summarized is frequently up and down, this change will not be notified to devices outside the IP address range to be summarized, which can avoid routing oscillation in the network and improve network stability to some extent.

- 1. Click **Configuration -> Advanced Configuration -> OSPF -> Basic Configuration**.
- 2. Select the OSPF process for which you want to configure advanced parameters, and click **Advanced Configuration -> Route Summarization**.
- 3. Click **Add**.
- 4. Set the parameters.

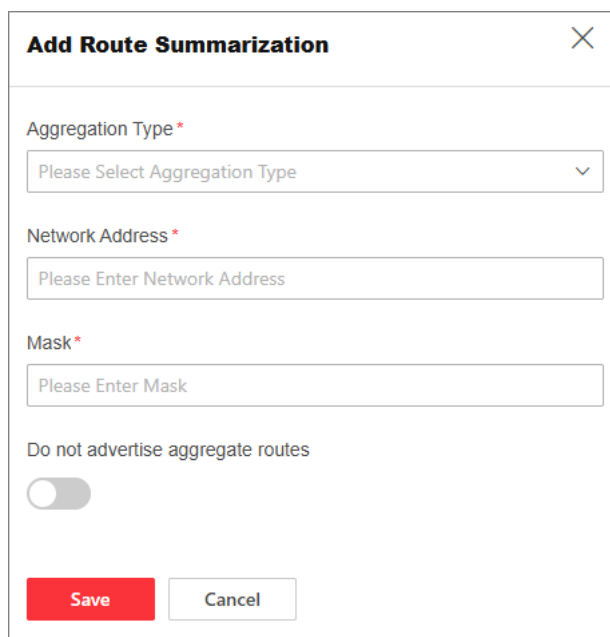
A web-based configuration dialog box titled "Add Route Summarization" with a close button (X) in the top right corner. The dialog contains four input fields: "Aggregation Type" (a dropdown menu with the placeholder text "Please Select Aggregation Type"), "Network Address" (a text input field with the placeholder text "Please Enter Network Address"), "Mask" (a text input field with the placeholder text "Please Enter Mask"), and a toggle switch labeled "Do not advertise aggregate routes" which is currently turned off. At the bottom of the dialog are two buttons: a red "Save" button and a white "Cancel" button with a grey border.

Figure 5-62 Configure Route Summarization

Aggregation Type

- **Inter-Area Route Summarization:** This refers to the process where an ABR summarizes routes with the same prefix from within an OSPF area and advertises only a single summarized route to other areas. After an AS is divided into multiple OSPF areas, each area is connected via an ABR. Summarizing routes between areas helps reduce routing information, shrink the routing table size, and improve switch performance. When configuring inter-area route summarization, a specific area must be selected—and it must be an area already associated with the OSPF process. After calculating intra-area routes, the ABR uses the summarization settings to combine multiple OSPF routes into a single route before advertising it outside the area.
- **Redistributed Route Summarization:** When external routes are imported into OSPF by an ASBR, each route is typically advertised in a separate Type-5 LSA. By configuring redistributed route summarization, the ASBR combines multiple external routes into a single Type-5 LSA, thereby reducing the number of LSAs in the Link State Database (LSDB). If summarization is configured on the ASBR, it will aggregate Type-5 LSAs that fall within the summarized address range. If the ASBR is located within a Not-So-Stubby Area (NSSA), it will instead summarize Type-7 LSAs within the specified address range.

Network Address

The destination IPv4 address of the aggregated route.

Mask

The network mask of the aggregated route in dotted decimal form.

Do not advertise aggregate routes

Do not advertise this summarized route. By default, this feature is disabled, meaning the summarized route is advertised.

- 5. Click **Save**.
- 6. View the summarized route information in the list or perform other operations.

Aggregation Type
All

Search Reset

+ Add - Delete Refresh

Aggregation Type	Area	Network Address	Mask	Operation
☐ Inter-Area Route Summarization			255.255.255.0	
☐ Redistributed Route Summarization	--		255.255.255.255	

5-63 View Summarized Route Information

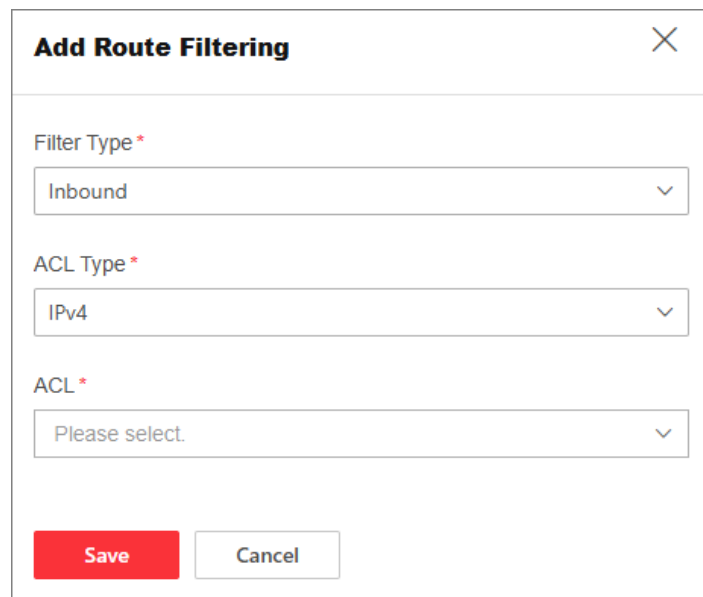
- Click to edit the configured summarized route.
- Click to delete the configured summarized route.
- Select aggregation type and click **Search** to search for the specified type of summarized routes.

Configure Route Filtering

Route filtering is a technology used to control the propagation of routing information in an OSPF network. The object of route filtering is OSPF routing information, including routing entries carried in Link State Advertisements (LSAs). The main purpose of route filtering is to allow or block certain routes from propagating in the OSPF network according to specific rules. Currently, the device supports matching routing information with rules defined by access control lists (ACLs), including conditions such as IP address, subnet mask, and protocol type, to filter routes.

For example: Set an ACL to only allow routes from a specified IP address range to be passed.

- 1. Click **Configuration -> Advanced Configuration -> OSPF -> Basic Configuration**.
- 2. Select the OSPF process for which you want to configure advanced parameters, and click **Advanced Configuration -> Route Filtering**.
- 3. Click **Add**.
- 4. Set the parameters.

A screenshot of a web-based configuration dialog titled "Add Route Filtering". The dialog has a close button (X) in the top right corner. It contains three dropdown menus: "Filter Type *" with "Inbound" selected, "ACL Type *" with "IPv4" selected, and "ACL *" with "Please select." selected. At the bottom, there are two buttons: a red "Save" button and a grey "Cancel" button.

Add Route Filtering

Filter Type *

Inbound

ACL Type *

IPv4

ACL *

Please select.

Save Cancel

Figure 5-64 Configure Route Filtering

Filter Type

- **Inbound:** Filters received routes. When OSPF route update packets are received from other devices, the configured inbound filtering rules are applied to screen these routes. Only routes that meet the criteria are accepted and added to the local routing table.
- **Outbound:** Filters routes during transmission. When sending OSPF route update packets to other devices, the configured outbound filtering rules are used to filter routes from the local routing table. Only routes that satisfy the conditions are included in the update.

Route Type

When configuring outbound route filtering, you must also specify the route type.

- **Direct Route:** Routes automatically discovered by the link-layer protocol and obtained by the device without manual configuration.
- **Static Route:** Routes manually configured by a network administrator, requiring explicit setup and maintenance.
- **OSPF:** Routes discovered through OSPF, a link-state routing protocol that uses cost as its metric and is designed for efficient routing in larger, more complex networks.
- **RIP:** Routes discovered through RIP, a distance-vector routing protocol that uses hop count as its metric and is suitable for small-scale networks.
- **BGP:** Routes discovered through BGP, the standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems on the internet.
- **IS-IS:** Routes discovered through IS-IS, a link-state routing protocol commonly used in large-scale service provider networks.

Redistributed Process ID

When the route type is RIP, OSPF, or IS-IS, you need to set the redistributed process ID, which is the RIP process ID, OSPF process ID, or IS-IS process ID.

Enter a number between 1 and 65535. If left blank, all RIP, OSPF, or IS-IS processes will be imported.

ACL Type

Access Control List (ACL) type. The current device only supports IPv4 ACL.

ACL

Select the ACL to be applied to the OSPF process for route filtering. If no ACL has been configured yet, please go to **Configuration** → **Security Configuration** → **ACL** to configure it. For configuration steps, please refer to ACL Configuration.

5. Click **Save**.

6. View the configured route filtering information in the list or perform other operations.

Filter Type	Route Type	Redistributed Process ID	ACL	Operation
☐ Inbound	--	--	2001	

Figure 5-65 View Route Filtering Information

- Click to edit the configured route filtering entry.
- Click to delete the configured route filtering entry.
- Select route type and click **Search** to search for the specified type of configured route filtering entries.

Enable OSPF

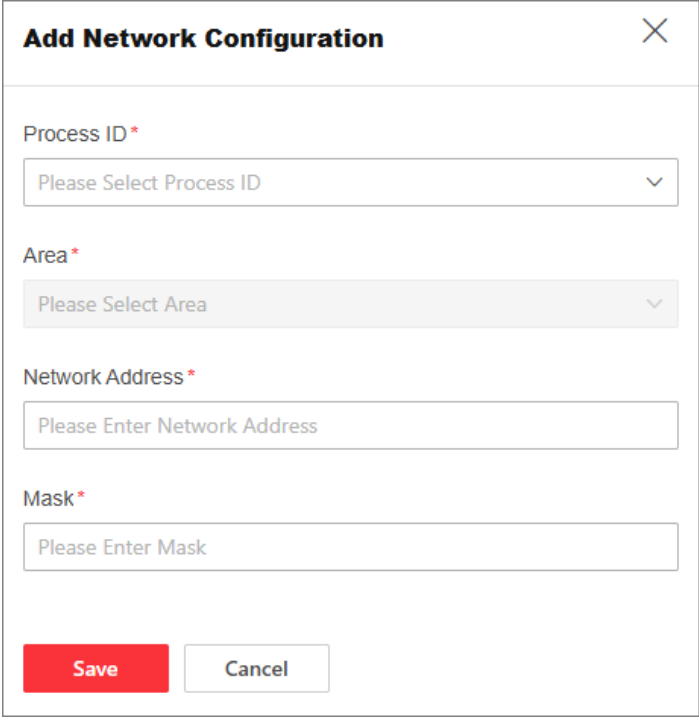
You can enable OSPF on specified network segments or specified interfaces. Enabling OSPF on specified interfaces has a higher priority than enabling it on specified network segments.

Enable OSPF on Specified Network Segment

Configure the network segments included in the area and enable OSPF on the specified segments. This configuration defines which network segments' routing information will be propagated and calculated within the area. By specifying the segments belonging to an area, the network can be divided into different OSPF areas, each with distinct characteristics. For example, the backbone area (Area 0) interconnects other areas, while stub areas restrict the propagation of external routes.

Steps

1. Click **Configuration** -> **Advanced Configuration** -> **OSPF** -> **Network Configuration**.
2. Click **Add**.
3. Set the parameters.

A web-based configuration dialog box titled "Add Network Configuration" with a close button (X) in the top right corner. The dialog contains four input fields: "Process ID *" with a dropdown menu showing "Please Select Process ID"; "Area *" with a dropdown menu showing "Please Select Area"; "Network Address *" with a text input field showing "Please Enter Network Address"; and "Mask *" with a text input field showing "Please Enter Mask". At the bottom, there are two buttons: a red "Save" button and a white "Cancel" button with a grey border.

Add Network Configuration

Process ID *

Please Select Process ID

Area *

Please Select Area

Network Address *

Please Enter Network Address

Mask *

Please Enter Mask

Save Cancel

Figure 5-66 Enable OSPF on Specified Network Segment

Process ID

Select the ID of the created OSPF process.

Area

Select the area linked to this OSPF process.

Network Address

Set the network segment address (IPv4 address) for the interface.

Mask

Specify the IPv4 address mask, which together with the IPv4 address determines the network segment included in the area.

4. Click **Save**.
5. Optional: View or delete OSPF network segment configuration information as needed.

Enable OSPF on Specified Interface

Enable OSPF on the specified interface to activate the OSPF protocol operation on that interface. This allows the interface to participate in sending and receiving OSPF Link State Advertisements (LSAs) and the routing calculation process. As a result, the network segment connected to the interface can be advertised into the OSPF network and receive routing information from other OSPF routers.

Steps

1. Click **Configuration** -> **Advanced Configuration** -> **OSPF** -> **Interface Configuration**.
2. Click **Add**.

OSPF Interface

Select a Layer 3 interface that has been configured with an IP address.



Note

The OSPF function on an interface takes effect only when the interface has been assigned an IP address. If no IP address is configured, go to **Configuration > Basic Configuration > IPv4 Address** to configure one. For details, refer to [Configure IPv4 Address](#).

Process ID

Select the OSPF process that has been created.

Area

Select the area associated with the OSPF process.

Priority

The OSPF interface priority of the switch, ranging from 0 to 255 (default: 1). It is used in the election of the Designated Router (DR) and Backup Designated Router (BDR). Only switches with a priority greater than 0 are eligible for election. A higher priority increases the likelihood of the switch being elected as DR or BDR.

Cost

The OSPF interface cost value, ranging from 1 to 65535 (default: 1). It represents the "cost" for traffic to traverse the interface toward a destination network. In an OSPF network, routing devices select the path with the lowest total cost for forwarding traffic.

Network Type

- **Broadcast:** A typical LAN topology (e.g., Ethernet), where multiple devices connect to a shared medium and can receive broadcast messages. In this type, Hello, LSU, and LSAck packets are sent via multicast (reserved multicast addresses: 224.0.0.5 for OSPF switches, 224.0.0.6 for DR/BDR), while DD and LSR packets are sent via unicast.
- **Non-Broadcast Multi-Access (NBMA):** Multiple access points connected via non-broadcast media (e.g., Frame Relay). Unlike broadcast networks, NBMA does not support broadcast or multicast, so OSPF packets (e.g., Hello, LSA) cannot be automatically propagated. All protocol packets are sent via unicast.
- **Point-to-Multipoint (P2MP):** A topology combining multiple point-to-point links, where a central node communicates with multiple remote nodes through a single interface. By default, protocol packets are sent via multicast (224.0.0.5), but unicast transmission can be configured as needed.
- **Point-to-Point (P2P):** The simplest topology with only two directly connected nodes. Protocol packets are sent via multicast (224.0.0.5).

Hello Interval

The time interval for sending Hello messages, ranging from 1 to 65,535 seconds. Optional; if not configured, the system applies a default value based on the network type.

Dead Interval

The time interval after which a router declares a neighbor relationship down if no Hello message is received, ranging from 2 to 262,140 seconds. Optional; if not configured, the system applies a default value based on the network type.

4. Click **Advanced Configuration** to configure advanced parameters.

Transmission Delay

The time required for data to be transmitted from one router to another over a virtual link, ranging from 1 to 1,800 seconds (default: 1 second).

Retransmit Interval

The interval at which an OSPF packet is retransmitted if no acknowledgment is received after the initial transmission. The value ranges from 1 to 3,600 seconds (default: 5 seconds).

Authentication Mode

- **NONE:** No authentication is performed.
- **Simple:** Simple password authentication. A plaintext password (up to 8 characters) must be configured.
- **MD5:** Message Digest 5 authentication. Requires both an MD5 key ID (1 to 255) and an MD5 password (up to 16 characters).

Silent

Configure an interface as a silent interface as needed. When an interface is set to silent, it stops sending OSPF protocol packets (e.g., Hello messages, LSAs) but continues to receive them. This is typically used in special network scenarios, such as interfaces connected to end-user devices or interfaces that do not need to actively participate in OSPF routing exchanges.

5. Click **Save**.
6. View, edit, or delete the OSPF port configuration information as needed.

View OSPF Neighbor Information

Viewing OSPF neighbor information is a critical aspect of network management and troubleshooting. By examining neighbor details, you can verify whether OSPF routers have successfully established adjacencies, check neighbor statuses, interface addresses, and other relevant information. This helps assess network connectivity, identify potential issues, and optimize network configurations.

To view neighbor information for a created OSPF process, go to **Configuration > Advanced Configuration > OSPF > Neighbor Info**. The displayed information includes the connected neighbor's interface address, router ID, dead interval, neighbor state, etc.

Process ID	Neighbor Interface Address	Neighbor Router ID	Dead Interval	Neighbor State	Designated Router	Designated Secondary Router
1			00h:00m:39s	Full		
1	0.0.0.0		Inactive	Disable	--	--

Figure 5-68 View OSPF Neighbor Information

5.2.6 Time Range Configuration

A time range defines a specific period of time. Users can create a time range and reference it in actual configurations, so that the configuration takes effect only within the defined time range. Some services or functions need to be started at a scheduled time or only activated within a certain cycle; a time range can be configured to impose such restrictions.

You can define a time range in two ways:

- Absolute time range: A specific time period defined by a start time and an end time. For example, from 9:00 on January 1, 2010, to 18:00 on January 2, 2010.
- Periodic time range: A recurring time range based on a weekly cycle, specifying valid days from Sunday to Saturday. For example, every Friday from 9:00 to 18:00.

Absolute time ranges can be used to restrict when periodic time ranges take effect.

Absolute and periodic time ranges can be combined, following these activation principles:

- Multiple periodic time ranges are combined using OR logic.
- The combination of periodic and absolute time ranges uses AND logic.

For example: A time range named "test" is configured with three active periods:

- Absolute time range: From 00:00 on January 1, 2010, to 23:59 on December 31, 2010.
- Periodic time range 1: Monday to Friday, 8:00–18:00.
- Periodic time range 2: Saturday and Sunday, 14:00–18:00.

As a result, "test" will be active during:

- Weekdays (Mon–Fri) 8:00–18:00, and
- Weekends (Sat–Sun) 14:00–18:00,

but only within the absolute period from January 1, 2010, to December 31, 2010.

Steps

1. Click **Configuration -> Advanced Configuration -> Time Range**.
2. Click **Add**.
3. Set the name of the time range.
4. Configure absolute time range(s) and/or periodic time range(s) as needed.

< Add Time Range

When both absolute and periodic time ranges are configured, the actual effective time is the repeating periods within the absolute time range.

*Time Range Name

Please Enter Time Range Name

Absolute Time Range

Absolute Time Range

Start Time

-

End Time

+

Periodic Time Range

Periodic Time Range

Start Time

-

End Time

+

Period

Mon

Tue

Wed

Thu

Fri

Sat

Sun

Save

Cancel

Figure 5-69 Configure Time Range

- Absolute time range: Enable **Absolute Time Range**, and then click any position the **Absolute Time Range** drop-down list or  to set start date & time and end date & time, and click **OK**. Click  to add multiple absolute time ranges, or click  to delete the configured absolute time range(s).
- Periodic time range: Enable **Periodic Time Range**, and then click any position on the **Periodic Time Range** drop-down list or  to set start time and end time, and click **OK**. Select any day from Monday to Sunday. Click  to add multiple periodic time ranges, or click  to delete the configured periodic time range(s).

5. Click **Save**.

6. View the configured time ranges in the list, or perform other operations.

Time Range ID	Time Range Name	Status	Operation
> 1	test	 Ineffective	 

Figure 5-70 View Time Range Configuration Information

- Click  to edit the time range. The time range name cannot be modified.
- Click  to delete the time range.
- Click  next to the time range ID to view detailed information.

 **Note**

A configured time range must be referenced before it can take effect.

5.2.7 ERPS Configuration

98

In Ethernet networks, redundant links are commonly deployed for link backup and enhanced reliability. However, such redundancy can introduce loops, potentially leading to issues such as broadcast storms and MAC address table instability, which may degrade communication quality or even cause service interruptions. To address this, a standardized ring network protocol with carrier-grade convergence performance is required.

ERPS (Ethernet Ring Protection Switching) meets this need by selectively blocking redundant links within the ring to eliminate loops while preserving backup connectivity. This mechanism ensures rapid convergence and effectively maintains high-quality user communication.

Configure ERPS Ring

An ERPS ring refers to a group of interconnected switches configured with the same control VLAN, serving as the basic unit of the ERPS protocol. In a multi-ring topology, the structure consists of one main ring and at least one sub-ring. Creating an ERPS ring is a prerequisite for configuring subsequent functions.

Steps

1. Click **Configuration** -> **Advanced Configuration** -> **ERPS**.

ERPS Configuration

 A ring member port should be configured as a trunk or hybrid port with STP disabled.

Ring ID *

Please Enter Ring ID

Port 0

Click on the left port panel to select port(s).

Port 1

Click the input box, and then select from the left port panel.

Description

Please Enter Description

Ring Type

☒ Major Ring

☐ Sub Ring

ERPS Instance

Instance Configuration

+ Add

 Delete

Save

Figure 5-71 Configure ERPS Ring

- Set the ERPS ring ID, ranging from 1 to 128.
- Click the input box for **Port 0** or **Port 1**, and then select the desired port on the port panel to configure Port 0 and Port 1 respectively as the member ports of this ERPS ring.

Note

A single device can have at most two ports join the same ERPS ring. Additionally, these member ports must be configured as Trunk or Hybrid type, and STP must be disabled on them. To configure a port as Trunk or Hybrid mode, please go to VLAN Configuration. To disable the STP function on a port, please go to STP Port Configuration.

- Enter a description for the ERPS ring. The description string must not exceed 127 characters.

5. Set the ERPS ring type as **Major Ring** or **Sub Ring**.



An ERPS ring consists of a major ring and a sub ring. By default, all ERPS rings are major rings. The major ring is a closed ring, and the sub ring is an open ring.

6. Click **Save**.

The successfully added ERPS ring will be displayed in the **ERPS Info** List.

7. Optional: Edit or delete the configured ERPS ring as needed.

- Click to select the **configured** ERPS ring above the port panel, and modify and save the configuration parameters in the right ERPS configuration area.
- Click to select the **configured** ERPS ring above the port panel, and then click **Delete Ring** in the right ERPS configuration area to delete the ERPS ring.

Configure ERPS Instance

Before You Start

An ERPS ring has been created.

Steps

1. Click **Configuration** -> **Advanced Configuration** -> **ERPS**.
2. Click the created ERPS ring above the port panel.
3. In the right ERPS configuration area, click **Add** to add an ERPS instance.

Add Instance ✕

Instance ID *

Please Enter Instance ID

Port 0

Ge 1/0/5

Role

Set up the control VLAN first, then configure port roles. ▾

Port 1

Ge 1/0/6

Role

Set up the control VLAN first, then configure port roles. ▾

Control VLAN

Please Enter Control VLAN

Protection Instance

Please Enter Protection Instance

[Advanced Configuration ▾](#)

Save

Cancel

Figure 5-72 Configure ERPS Instance

4. Set the ERPS instance ID, ranging from 1 to 128.
5. Set the control VLAN for passing ERPS protocol messages. The value ranges from 2 to 4094.

Note

- You must use an uncreated VLAN for configuration.
- There is exactly one control VLAN in an ERPS instance. All devices in the same ERPS instance must be configured with the same control VLAN, and different ERPS instances cannot use control VLANs with the same ID.

6. Configure the roles for Port 0 and Port 1.



Note

Before configuring port roles, you must first configure the control VLAN. Additionally, an ERPS port cannot be assigned both the Owner and Neighbor roles simultaneously.

- **Owner:** Each ERPS ring allows only one Owner port. When the ring is operating normally, this port is blocked to prevent loops. If a link failure occurs in the ring, the Owner port is unblocked to ensure normal forwarding of user traffic.
- **Neighbor:** Each ERPS ring allows only one Neighbor port, which must be configured on the peer port connected to the Owner port for the ERPS ring to function correctly. Typically, the Neighbor port is blocked or unblocked together with the Owner port to eliminate loops and enhance network reliability.
- **Normal:** All ports in an ERPS ring, except the Owner and Neighbor ports, are Normal ports. These ports are responsible for receiving and forwarding both protocol packets and data packets within the link.

7. Set the protection instance, ranging from 0 to 63.



Note

The protection VLAN for forwarding user traffic should be mapped to the protection instance so that ERPS can block and forward the user traffic in the protection instance, or broadcast storm may occur.

8. Optional: Click **Advanced Configuration** to configure other advanced parameters as needed.

Description

Enter descriptive information for the ERPS instance. The string length must not exceed 127 characters.

Version

Select the appropriate instance version based on the actual network requirements. Version v1 focuses primarily on basic Ethernet ring protection switching functionality. Version v2 offers faster convergence compared to v1 and typically completes protection switching in a shorter time.

Packet Level

The MEL field in the ERPS protocol packet identifies the Maintenance Entity Level, with a valid range of 1 to 7. The packet level is used to distinguish between different maintenance instances, which may correspond to different VLANs or service flows, enabling differentiated protection and management of various types of service data within the ring network.

Guard Timer

The value range from 10 to 2,000 milliseconds, with a default value of 500 milliseconds. After a link failure, failure recovery, or a clear operation is performed, the device starts the Guard Timer. Before this timer expires, the device does not process R-APS messages to prevent handling outdated SF R-APS messages. If NR R-APS messages are still received from other ports after the timer expires, the local port transitions to the Forwarding state.

Hold-off Timer

The value ranges from 0 to 10,000 milliseconds (must be a multiple of 100), with a default value of 0 milliseconds. In multi-layer service applications—for example, after a server failure—users may wish to allow time for server recovery without the client perceiving the failure, meaning protection switching should not occur immediately. The Hold-off Timer serves this purpose: when a failure occurs, it is not immediately reported to ERPS. Only if the failure persists after the Hold-off Timer expires will it be reported.

WTR Timer

The value ranges from 1 to 12 minutes, with a default value of 5 minutes. When the RPL (Ring Protection Link) owner port is unblocked due to a failure on another device or link, and the failure is later resolved, some ports may not yet have transitioned from Down to Up state. To prevent immediate blocking of the RPL owner port and avoid oscillation of the blocking point, the WTR Timer is started upon receiving an NR R-APS message from a port. If an SF R-APS message is received from another port before the timer expires, the WTR Timer is canceled, and the RPL owner port remains unblocked. If no SF R-APS messages are received from other ports before the WTR Timer expires, the RPL owner port is blocked upon timeout, and an NRRB R-APS message is sent. Other ports set their forwarding state to Forwarding after receiving this message.

Last Byte of R-APS Packet

The last byte of the destination MAC address in the R-APS (Ring Auto Protection Switching Protocol Data Unit) packet. The value ranges from 1 to 239, with a default value of 1. The last byte of the destination MAC address, combined with the control VLAN, is used to differentiate between instances.

Port 0's Switchover Mode

Switching mode configuration is only supported in ERPS v2.

- **Manual Switchover:** In the event of an ERPS ring failure, network administrators must manually intervene to trigger a switchover from the faulty link to the backup link.
- **Forced Switchover:** The network device automatically switches data transmission from the working link to the backup link based on predefined policies and rules when specific failure conditions are detected or certain criteria are met. No manual operation is required to initiate the switchover process.

Port 1's Switchover Mode

Switching mode configuration is only supported in ERPS v2.

- **Manual Switchover:** In the event of an ERPS ring failure, network administrators must manually intervene to trigger a switchover from the faulty link to the backup link.
- **Forced Switchover:** The network device automatically switches data transmission from the working link to the backup link based on predefined policies and rules when specific failure conditions are detected or certain criteria are met. No manual operation is required to initiate the switchover process.

Revertive Mode

In ERPS v2, it is necessary to configure whether **Revertive Mode** is enabled. After an ERPS link returns to normal, this setting determines whether the RPL owner port should be blocked again.

- In Revertive Mode: If the failed link recovers, the RPL owner port is re-blocked after the WTR Timer expires, and the blocked link switches back to the RPL. This ensures that traffic follows the preset path after failure recovery, restoring the network to its normal topology and maintaining stability and reliability.
- In Non-Revertive Mode: When a failed link recovers, the WTR Timer is not started, and the blocked link remains on the original failure path without switching back to the RPL. This mode is suitable for specific network scenarios—for example, when temporary failures are repaired and immediate path changes are undesirable to avoid impacting ongoing services.

9. Click **Save**.

10. Optional: View the instance configuration information in the ERPS instance list, or perform other operations.

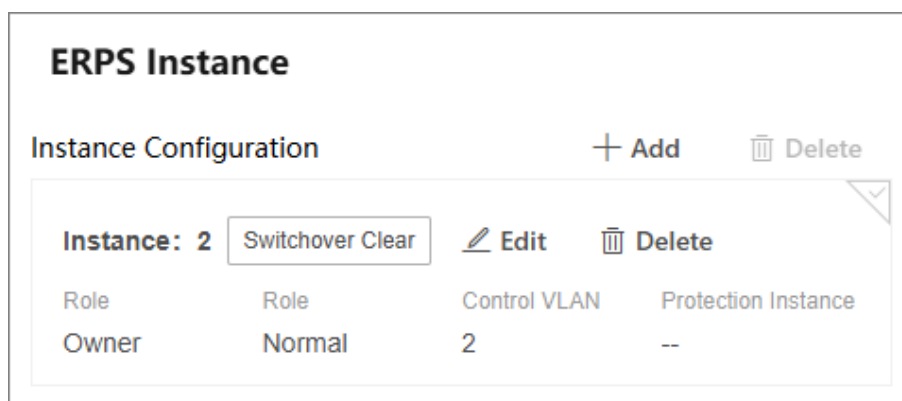


Figure 5-73 View ERPS Instance Configuration Information

- Select the ERPS instance you want to edit and click **Edit** to edit its configuration information.
- Select the ERPS instance you want to delete and click **Delete**.
- Select the ERPS instances to be deleted, click ✓ in the upper-right corner to batch select them, and then click **Delete** to delete the selected instances in batch.

5.2.8 SNMP Configuration

SNMP (Simple Network Management Protocol) enables remote management and operation of network devices, allowing administrators to manage devices on the network through a Network Management System (NMS).

Configure Basic SNMP Parameters

Enable the SNMP service and configure the SNMP version. Only when the NMS and devices use the same SNMP version can they connect to each other.

1. Click **System Configuration -> Network Configuration -> SNMP -> Basic Settings**.

SNMP Service ☒

Parameter Configuration

Enabled SNMP Version ☐ v1 ☒ v2c ☐ v3

Basic Info Configuration

Device Physical Location

Administrator's Contact Info

Engine ID

Save

Figure 5-74 Configure SNMP Basic Parameters

2. Enable the SNMP service.

3. Select the SNMP version to enable on the device. Options include SNMPv1, SNMPv2c, and SNMPv3.

 Note

No version is selected by default. The supported SNMP versions may vary by device. Please refer to the actual interface for available options.

4. Set the physical location of the device and the contact information of the administrator.

 Note

Both the device location and administrator contact information support up to 128 characters.

5. Optional: Configure the engine ID.

 Note

The device is assigned a globally unique SNMP Engine ID at the factory. SNMPv3 elements such as the username and encrypted password are associated with this Engine ID. If the Engine ID is modified, the previously configured username and password under the original Engine ID will become invalid. Therefore, it is recommended not to change the SNMP Engine ID unless necessary.

6. Click **Save**.

Configure SNMP View

An SNMP view is a subset of the MIB. By binding a community name to an SNMP view, you can restrict the MIB objects accessible to the NMS.

1. Click **System Configuration** -> **Network Configuration** -> **SNMP** -> **SNMP View**.
2. Click **Add** to add an SNMP view.

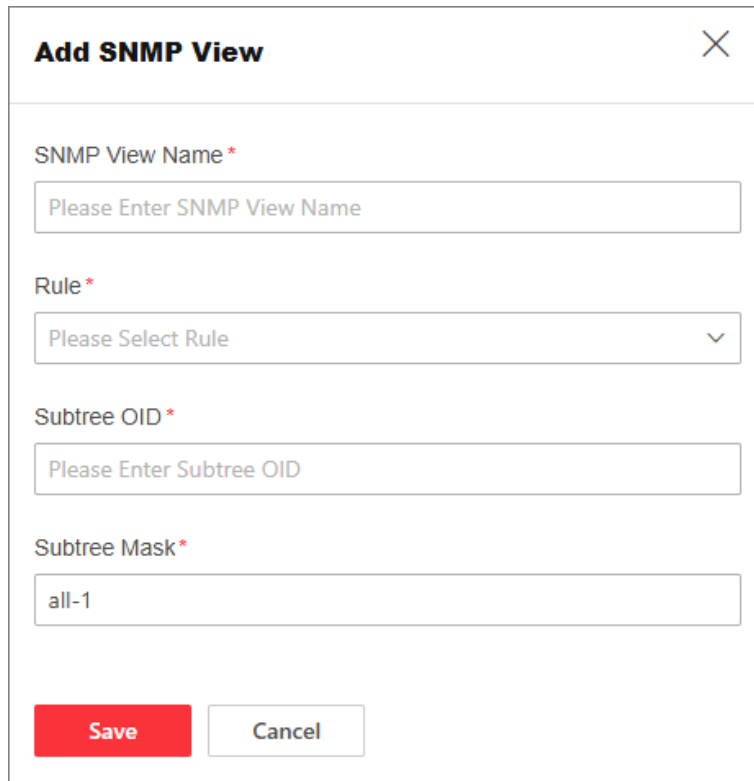
A screenshot of the 'Add SNMP View' dialog box. The dialog has a title bar with 'Add SNMP View' and a close button (X). It contains four input fields: 'SNMP View Name *' with a placeholder 'Please Enter SNMP View Name', 'Rule *' with a dropdown menu showing 'Please Select Rule', 'Subtree OID *' with a placeholder 'Please Enter Subtree OID', and 'Subtree Mask *' with the value 'all-1'. At the bottom, there are two buttons: a red 'Save' button and a white 'Cancel' button.

Figure 5-75 Configure SNMP View

Note

No more than 32 SNMP views can be added to the current device.

3. Configure the required parameters if any.

SNMP View Name

Specify the name of the SNMP view. The name must be 1 to 32 characters long.

Rule

Define rules to include or exclude objects determined by the MIB subtree OID and subtree mask within the scope of the view. A single view can contain multiple rules.

Subtree OID

Set the OID of the root node of the MIB subtree (e.g., 1.3.6.1.6.3.15). The OID must be 1 to 63 characters long (equivalent to 1 to 32 OID digits, excluding decimal points).

The MIB subtree OID indicates the node’s position in the MIB tree and uniquely identifies a subtree within the MIB library.

Subtree Mask

Specify the subtree mask. The mask must be a 2 to 32 digit hexadecimal string starting with 0x, or **all-1**. If no mask is specified, the default mask (**all-1**, i.e., all bits set to 1) is used.

- 4. Click **Save**.
- 5. In the SNMP view list, view the SNMP view name, rule, subtree OID, and subtree mask, or perform other operations.

View Name	Rule	Subtree OID	Subtree Mask	Operation
internet	Include	1.3.6	all-1	 
internet	Exclude	1.3.6.1.6.3.15	all-1	 
internet	Exclude	1.3.6.1.6.3.16	all-1	 

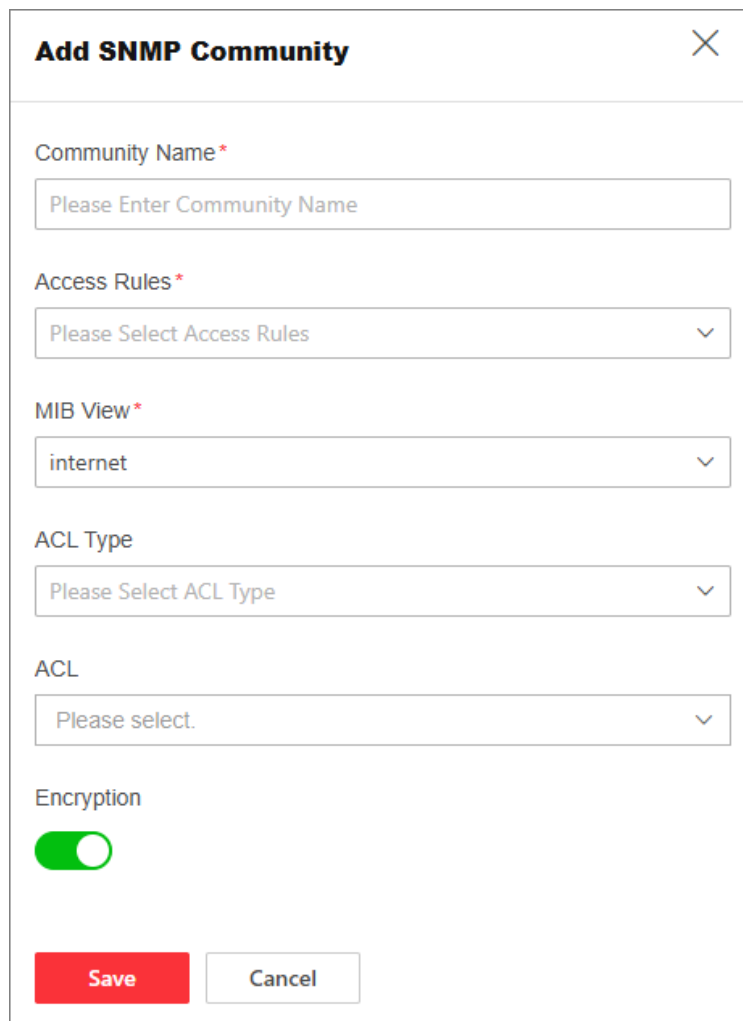
Figure 5-76 View SNMP View Information

Configure SNMP Community

Creating an SNMP community provides basic access control for SNMPv1/v2c devices. The community name (e.g., "public") functions as a plaintext password—devices authenticate requests by matching the community name to grant either read-only or read-write access permissions.

Steps

- 1. Click **System Configuration -> Network Configuration -> SNMP -> SNMP Community**.
- 2. Click **Add** to add a SNMP community.



The image shows a web-based configuration dialog titled "Add SNMP Community". It contains several input fields and a toggle switch. The fields are: "Community Name*" (text input), "Access Rules*" (dropdown menu), "MIB View*" (dropdown menu), "ACL Type" (dropdown menu), and "ACL" (dropdown menu). The "Encryption" section has a green toggle switch that is currently turned on. At the bottom, there are two buttons: "Save" (red) and "Cancel" (white).

Add SNMP Community

Community Name*

Please Enter Community Name

Access Rules*

Please Select Access Rules

MIB View*

internet

ACL Type

Please Select ACL Type

ACL

Please select.

Encryption

☒

Save Cancel

Figure 5-77 Configure SNMP Community

 Note

No more than 32 SNMP communities can be added to the current device.

3. Configure the parameters as needed.

Community Name

Specify the name of the SNMP community, which must be 1 to 32 characters long. The community name serves as an authentication mechanism, similar to a password, to restrict data transmission between the NMS and the Agent.

Access Rules

Define the access permissions for the NMS when using this community to interact with the Agent.

- **Read-only:** Allows read-only access to MIB objects. When the NMS uses this community name to access the Agent, only read operations are permitted.

- **Read/Write:** Grants read and write access to MIB objects. The NMS can perform both read and write operations using this community name.

MIB View

Associate the community with a specific MIB view to limit the MIB objects that the NMS can access on the Agent. Only existing MIB views can be selected.

ACL Type

Set the basic ACL type to IPv4 or IPv6.

ACL

Bind the community to a basic ACL to allow or deny access to the Agent from NMS devices with specific source IP addresses. Only existing ACLs can be selected.

Encryption

Enable or disable encryption for the community name.

4. Click **Save.****5. Optional: View the SNMP community name, whether it is encrypted, access rules, MIB view, and ACL type and number in the SNMP community list, or perform other operations.**

- Click  to edit the access rules, MIB view, ACL type, ACL No., etc.
- Click  to delete the SNMP community.

Configure SNMP User

The purpose of creating an SNMP user group is to streamline user permission management and simplify configuration. By associating multiple SNMPv3 users with the same group, administrators can uniformly define access permissions (such as read-only or read/write) and specify the scope of accessible data (e.g., OID subtrees).

**Note**

SNMP user group configuration is only supported on devices running SNMPv3.

Steps

- 1. Click **System Configuration** -> **Network Configuration** -> **SNMP** -> **SNMP User**.**
- 2. Click **Add** to add a SNMP user group.**

Add SNMP User Group ✕

SNMP User Group Name*

Read-Only View

Read/Write View

Notification View

ACL Type

ACL

Figure 5-78 Configure SNMP User Group

 Note

No more than 32 SNMP user groups can be added to the current device.

3. Configure the parameters as needed.

SNMP User Group Name

Specify the name of the SNMP user group, which must be 1 to 32 characters long.

Read-Only View

Assign a read-only view to the SNMP user group. Only existing read-only views can be selected, with the default being the "internet" view.

Read/Write View

Assign a read/write view to the SNMP user group. Only existing read/write views are available for selection. If no read/write view is specified, the NMS will not be able to perform write operations on any MIB objects of the device.

Notification View

Assign a notification view to the SNMP user group, which defines the scope of Trap messages that can be sent. Only existing notification views can be selected. If no notification view is configured, the Agent will not send any Trap messages to the NMS.

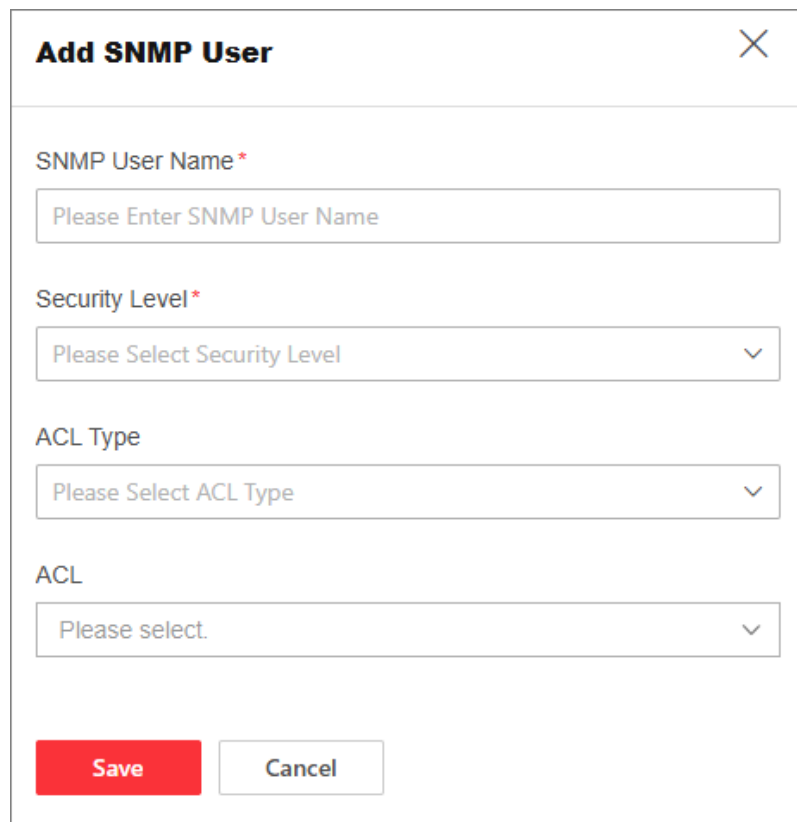
ACL Type

Set the basic ACL type to IPv4 or IPv6.

ACL

Bind the user group to a basic ACL to restrict SNMP packet source IP addresses. This allows or denies SNMP packets from specific source IP addresses, thereby further controlling communication between the NMS and Agent. Only existing ACLs can be selected.

4. Click **Save**.
5. Optional: View information such as SNMP user group name, read-only view, read/write view, and notification view in the SNMP user group list, or perform other operations.
 - Click  to edit the SNMP user group to modify the read-only view, read/write view, notification view, ACL type, and ACL number.
 - Click  to delete the SNMP user group.
6. Add users to an existing user group.
 - 1) Click **Add SNMP User** on the created user group.

A web-based dialog box titled "Add SNMP User" with a close button (X) in the top right corner. It contains four input fields: "SNMP User Name *" (text input with placeholder "Please Enter SNMP User Name"), "Security Level *" (dropdown menu with placeholder "Please Select Security Level"), "ACL Type" (dropdown menu with placeholder "Please Select ACL Type"), and "ACL" (dropdown menu with placeholder "Please select."). At the bottom, there are two buttons: a red "Save" button and a white "Cancel" button with a grey border.

Add SNMP User

SNMP User Name *

Please Enter SNMP User Name

Security Level *

Please Select Security Level

ACL Type

Please Select ACL Type

ACL

Please select.

Save Cancel

Figure 5-79 Configure SNMP User

 Note

No more than 32 SNMP users can be added to the current device.

SNMP User Name

Specify the SNMP user name, which must be 1 to 32 characters long.

Security Level

Set the security level for the SNMP user. Options include:

- **No Authentication, No Encryption**
- **Authentication Only, No Encryption**
- **Authentication and Encryption**

Authentication Mode

Required when the security level is set to **Authentication Only, No Encryption** or **Authentication and Encryption**. Choose between MD5 and SHA1.

**Note**

MD5 and SHA1 are both cryptographic hash functions, but SHA1 provides stronger security with a longer hash length and better resistance to collisions compared to MD5.

Authentication Password

Required when the security level is set to **Authentication Only, No Encryption** or **Authentication and Encryption**. The password must be 2 to 32 characters long and include at least two types of the following: digits, lowercase letters, uppercase letters, or special characters.

Encryption Mode

Required when the security level is set to **Authentication and Encryption**. Choose between DES56 and AES128.

**Note**

For enhanced security, AES128 encryption is recommended.

Encryption Password

Required when the security level is set to **Authentication and Encryption**. The password must be 2 to 32 characters long and include at least two types of the following: digits, lowercase letters, uppercase letters, or special characters.

ACL Type

Set the basic ACL type to IPv4 or IPv6.

ACL

Bind the user to a basic ACL to restrict SNMP packet source IP addresses. This allows or denies SNMP packets from specific source IP addresses, thereby permitting or blocking designated NMSs from accessing the Agent using this user name. Only existing ACLs can be selected.

3) Click **Save**.

4) (Optional) Click  of a created user group and repeat the above steps to add multiple SNMP users to the same group.

7. Optional: View the SNMP user name, authentication mode, encryption mode, and ACL No., etc., in the SNMP user list, or perform other operations.

- Click  to edit SNMP user to modify parameters such as security level, ACL type, and ACL No.
- Click  to delete the SNMP user.

Configure SNMP Trap Target Host

By configuring the SNMP trap target host, alarms generated by the device are synchronized to the target server.

Steps

1. Click **System Configuration -> Network Configuration -> SNMP -> SNMP Trap Target Host**.
2. Enable **SNMP Trap**.
3. Click **Add** to add an SNMP trap target host.

Add SNMP Trap Target Host

Destination IP Address Type *

IPv4

Destination IP Address *

Alarm Type *

Trap

Security Word *

Please Enter Security Word

UDP Port No. *

162

Security Mode *

☐ v1

☐ v2c

☐ v3

Save

Cancel

5-81 Configure SNMP Trap Target Host

 Note

Up to 32 SNMP trap target hosts can be added to the current device.

4. Set the type of the target server's IP **address** for sending SNMP trap messages.

Destination IP Address Type

Select the type of destination IP address.

Destination IP Address

Specify the IP address of the destination host (i.e., the NMS). The IP address must not be a broadcast or multicast address.

Alarm Type

Set the type of SNMP trap (alarm). Options include: Trap and Inform. Trap is an unacknowledged SNMP notification sent by an agent, while Inform is a confirmed version requiring acknowledgment from the NMS.

Security Word

Specify the security word, which refers to the community name for SNMPv1/SNMPv2c (or the user name for SNMPv3). The value must be 1 to 32 characters long.

UDP Port No.

Set the UDP port number. Valid values range from 1 to 65535, with a default value of 162.

 Note

Port 162 is the default port defined by the SNMP protocol for receiving Trap messages. It is recommended to use this default port unless otherwise required. If modified, the port number must match the configuration on the NMS.

Security Mode

Select the SNMP version. Options include: SNMPv1, SNMPv2c, or SNMPv3 (if supported by the device).

- If SNMPv1 or SNMPv2c is selected, the security level defaults to **No Authentication, No Encryption** and cannot be modified.
- If SNMPv3 is selected, you must configure the security level, which determines the authentication and encryption method for SNMP Trap messages.

 Note

- When the trap type is set to **Inform**, the security mode can be SNMPv2c or SNMPv3. When the trap type is set to **Trap**, SNMPv1, SNMPv2c, or SNMPv3 can be selected.
- The security mode must match the SNMP version running on the NMS; otherwise, Traps will not be received. A successful connection between the NMS and Agent requires both to use the same SNMP version.

Security Level

Required when **Security Mode** is SNMPv3. Set the security level for the SNMP trap target host.

Options include:

- **No Authentication, No Encryption**
- **Authentication Only, No Encryption**
- **Authentication and Encryption**

5. Click **Save**.

6. Optional: In the **SNMP Trap Target Host** list, view the destination IP address, alarm type, security word, UDP port No., security mode, security level, and effective status, or perform other operations.

5.3 Security Configuration

5.3.1 ACL Configuration

An Access Control List (ACL) is a collection of conditions and rules. A rule is a sentence that describes the conditions for packet matching, such as source address, destination address, and port number. An ACL is essentially an access control technology based on packet filtering. It can filter packets on the interface according to the set conditions and allow them to pass or discard them. By using an ACL, you can effectively control user access to the network and ensure network security to the maximum extent.

Based on the ACL number range division, ACL types include:

- **Basic ACL:** The rule number is between 2000 and 2999. Basic ACL rules only contain source IP address, which consume less device CPU resources and can be used in simple deployment scenarios.
- **Advanced ACL:** The rule number is between 3000 and 3999. Advanced ACL rules contain protocol information (IP, ICMP, TCP, or UDP), which can match network data more precisely.
- **Layer 2 ACL:** The rule number is between 4000 and 4999. Use Layer 2 ACLs to control the traffic based on Layer 2 information such as source MAC address, destination MAC address, 802.1p priority, and Layer 2 protocol type.



Basic ACL supports filtering packets based on source IP address; Advanced ACL supports filtering packets based on both source and destination IP addresses; Layer 2 ACL supports filtering packets based on source/destination MAC address.

ACL rules are applied to filter packets on interfaces, VLANs, or globally for both inbound and outbound traffic. Packets that match ACL rules are allowed or denied based on the defined matching actions, while packets that do not match any ACL rules are handled according to the specified default action.

Configure ACL

Configure Basic ACL

Steps

1. Click **Configuration** -> **Security Configuration** -> **ACL** -> **Basic ACL**.
2. Click **Add**.
3. Configure the relevant parameters.

ACL Type

IPv4

*ACL

Please enter an ACL number between 2000 and 2999, or an ACL name th...

*Matching Order

Config

*Step

5

Description

No more than 64 characters are allowed.

ACL Rule

Rule Configuration

+ AddDeleteRefresh

	Rule ID	Action	Effective Ti...	Hit Count	Operation
No data.					

Total 0

<1>

Go to

1

Save

Cancel

Figure 5-82 Add Basic ACL

ACL Type

Set the ACL type to IPv4 ACL or IPv6 ACL. Some devices support only IPv4 ACL.

- IPv4 ACL: Also referred to as ACL4, and commonly called ACL, it filters only IPv4 packets.
- IPv6 ACL: Also referred to as ACL6, it filters only IPv6 packets.

ACL

Specify an ACL number or ACL name.

- The ACL number must fall within the range of 2000 to 2999.
- The ACL name must be 1 to 32 characters long and start with a letter (a–z or A–Z).

Matching Order

Set the ACL rule matching order to **Config**.

When the matching order is **Config**, the system arranges rules in ascending order of their numbers and matches packets accordingly. Rules with smaller numbers are matched first.

Step

Set the step value for ACL rule numbering, which must be between 1 and 20.

Since rule numbers affect the matching sequence, when the system automatically assigns rule numbers, it reserves space between adjacent rules to allow for future insertions. This reserved interval is called the rule numbering step—the difference between two consecutive rule numbers.

Description

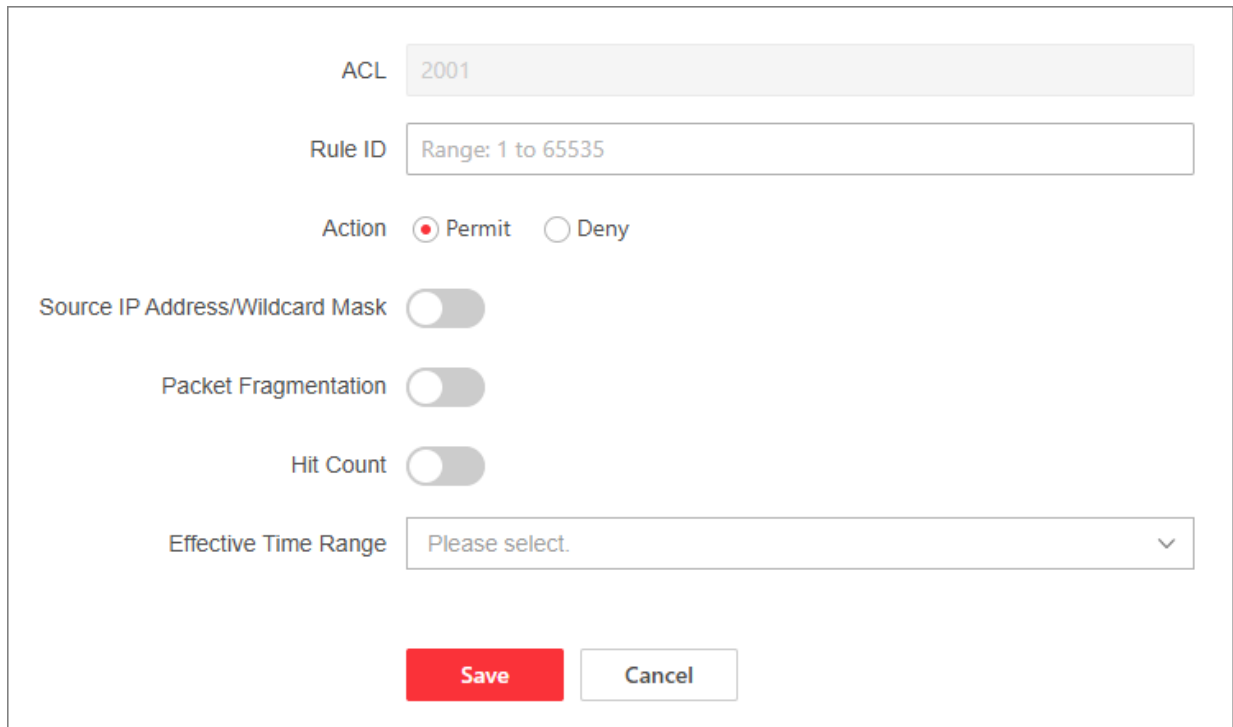
Enter a description for the ACL, which can contain up to 64 characters.

4. Click **Save.****5. Optional: View basic ACL information or perform related operations in the basic ACL list.**

- Click  to edit the basic ACL.
- Click  to delete the basic ACL.
- Enter the ACL number or name, or select ACL type, and click **Search** to search for the specified type of basic ACLs.

6. Optional: Configure basic ACL rules.

- 1) Click  in the **Operation** column of the specified ACL.
- 2) In the **ACL Rule** area, click **Add**.
- 3) Set the parameters as needed.



ACL 2001

Rule ID Range: 1 to 65535

Action ☒ Permit ☐ Deny

Source IP Address/Wildcard Mask ☐

Packet Fragmentation ☐

Hit Count ☐

Effective Time Range Please select. ▼

Save Cancel

Figure 5-83 Add Basic ACL Rule

Configuration Item	Note
Rule ID	Set the ACL rule number within the range of 1 to 65535.
Action	Set the ACL rule action to Permit or Deny. ● Permit: Allows packets matching the rule to pass. ● Deny: Blocks packets matching the rule from passing.
Source IP Address/Wildcard Mask	Source IPv4 address information of the ACL rule. This parameter is required when adding basic IPv4 ACL rules. If you enable this function, you need to set the source IPv4 address.
Source IP Address	Set the source IPv4 address for the IPv4 ACL rule.
Wildcard Mask	Set the wildcard mask for the source IPv4 address. ● A wildcard mask of 0.0.0.0 indicates a host address. ● A wildcard mask of 255.255.255.255 indicates any IPv4 address, equivalent to the any parameter.
Source IPv6 Address/Prefix Length	Source IPv6 address information of the ACL rule. This parameter is required when adding basic IPv6 ACL rules. If you enable this function, you need to set the source IPv6 address.
Source IPv6 Address	Set the source IPv6 address for the IPv6 ACL rule.
Prefix Length	Set the prefix length for the source IPv6 address, in the range of 1 to 128.
Packet Fragmentation	Enable or disable ACL filtering for fragmented packets. When enabled, the device matches not only non-fragmented packets and the first fragment (which is processed in the same way as non-fragmented packets) but also subsequent fragments for rule-based filtering.

Hit Count	Enable or disable ACL packet statistics. When enabled, the number of packets matching a specific ACL rule is counted.
Effective Time Range	Set the time range during which the ACL rule is active. You may select a pre-configured time range or click Add to create a new one.  Note It is recommended to create time ranges in Configuration > Advanced Configuration > Time Range before configuring this parameter.

 Note

The configurable ACL rule parameters vary depending on the basic ACL type. Refer to the actual device interface for specific details.

4) Click **Save**.

5) Optional: View ACL rule information or perform related operations in the ACL rule list.

- Click  to edit the ACL rule.
- Click  in the **Operation** column to delete a single ACL rule, or select multiple rules and click **Delete** to delete ACL rules in batch.

Configure Advanced ACL

Steps

1. Click **Configuration** -> **Security Configuration** -> **ACL** -> **Advanced ACL**.
2. Click **Add**.
3. Configure the relevant parameters.

Type

IPv4

* ACL

Please enter an ACL number between 3000 and 3999, or an ACL name th...

* Matching Order

Config

* Step

5

Description

No more than 64 characters are allowed.

ACL Rule

Rule Configuration

+ AddDeleteRefresh

	Rule ID	Action	Effective Ti...	Hit Count	Operation
No data.					

Total 0

<1>

Go to

1

Save

Cancel

Figure 5-84 Add Advanced ACL

ACL Type

Set the ACL type to IPv4 ACL or IPv6 ACL. Some devices support only IPv4 ACL.

- IPv4 ACL: Also referred to as ACL4, and commonly called ACL, it filters only IPv4 packets.
- IPv6 ACL: Also referred to as ACL6, it filters only IPv6 packets.

ACL

Specify an ACL number or ACL name.

- The ACL number must fall within the range of 3000 to 3999.
- The ACL name must be 1 to 32 characters long and start with a letter (a–z or A–Z).

Matching Order

Set the ACL rule matching order to **Config**.

When the matching order is **Config**, the system arranges rules in ascending order of their numbers and matches packets accordingly. Rules with smaller numbers are matched first.

Step

Set the step value for ACL rule numbering, which must be between 1 and 20.

Since rule numbers affect the matching sequence, when the system automatically assigns rule numbers, it reserves space between adjacent rules to allow for future insertions. This reserved interval is called the rule numbering step—the difference between two consecutive rule numbers.

Description

Enter a description for the ACL, which can contain up to 64 characters.

4. Click **Save**.

5. Optional: View advanced ACL information or perform related operations in the advanced ACL list.

- Click  to edit the advanced ACL.
- Click  to delete the advanced ACL.
- Enter the ACL number or name, or select ACL type, and click **Search** to search for the specified type of advanced ACLs.

6. Optional: Configure advanced ACL rules.

- 1) Click  in the **Operation** column of the specified ACL.
- 2) In the **ACL Rule** area, click **Add**.
- 3) Set the parameters as needed.

ACL 3001

Rule ID Range: 1 to 65535

Action ☒ Permit ☐ Deny

* Protocol Type ip

Source IP Address/Wildcard Mask ☐

Destination IP Address/Wildcard Mask ☐

DSCP Priority ☐

IP Priority ☐

ToS Priority ☐

Packet Fragmentation ☐

Hit Count ☐

Effective Time Range Please select.

Save Cancel

Figure 5-85 Add Advanced ACL Rule

Configuration Item	Note
Rule ID	Set the ACL rule number within the range of 1 to 65535.
Action	Set the ACL rule action to Permit or Deny . ● Permit: Allows packets matching the rule to pass. ● Deny: Blocks packets matching the rule from passing.
Protocol Type	Set the protocol type for ACL rules. Protocol numbers 1 to 255 correspond to different protocol types. Specific enumerations: TCP (6), UDP (17), ICMP (1), IGMP (2), OSPF (89), IP-in-IP (4), GRE (47).

	 Note Different protocol types require different rule parameters. Please refer to the actual interface configuration for details.
Source IP Address/Wildcard Mask	Source IPv4 address information of the ACL rule. This parameter is required when adding advanced IPv4 ACL rules. If you enable this function, you need to set the source IPv4 address.
Source IP Address	Set the source IPv4 address for the IPv4 ACL rule.
Wildcard Mask	Set the wildcard mask for the source IPv4 address. • A wildcard mask of 0.0.0.0 indicates a host address. • A wildcard mask of 255.255.255.255 indicates any IPv4 address, equivalent to the any parameter.
Source IPv6 Address/Prefix Length	Source IPv6 address information of the ACL rule. This parameter is required when adding advanced IPv6 ACL rules. If you enable this function, you need to set the source IPv6 address.
Source IPv6 Address	Set the source IPv6 address for the IPv6 ACL rule.
Prefix Length	Set the prefix length for the source IPv6 address, in the range of 1 to 128.
Destination IP Address/Wildcard Mask	Destination IPv4 address information of the ACL rule. This parameter is required when adding advanced IPv4 ACL rules. If you enable this function, you need to set the destination IPv4 address.
Destination IP Address	Set the destination IPv4 address for the IPv4 ACL rule.
Wildcard Mask	Set the wildcard mask for the destination IPv4 address. • A wildcard mask of 0.0.0.0 indicates a host address. • A wildcard mask of 255.255.255.255 indicates any IPv4 address, equivalent to the any parameter.
Destination IPv6 Address/Prefix Length	Destination IPv6 address information of the ACL rule. This parameter is required when adding advanced IPv6 ACL rules. If you enable this function, you need to set the destination IPv6 address.

Destination IPv6 Address	Set the destination IPv6 address for the IPv6 ACL rule.
Prefix Length	Set the prefix length for the destination IPv6 address, in the range of 1 to 128.
ICMP Message Type and Code	When the protocol type is set to ICMP, this parameter must be configured. Once ICMP Message Type and Code is enabled, you need to specify the ICMP message type and code. Both values range from 0 to 255. The actual type of an ICMP message is determined by the combination of its type and code fields.
ICMPv6 Message Type and Code	When the protocol type is set to ICMPv6, this parameter must be configured. Once ICMPv6 Message Type and Code is enabled, you need to specify the ICMPv6 message type and code. Both values range from 0 to 255. The actual type of an ICMPv6 message is determined by the combination of its type and code fields.
Source Port No. of TCP Packet	This parameter is required when the protocol type is set to TCP. Once Source Port No. of TCP Packet is enabled, you need to set the TCP source port number or define a port range by specifying both the start and end port numbers. The port number ranges from 0 to 65535.
Destination Port No. of TCP Packet	This parameter is required when the protocol type is set to TCP. Once Destination Port No. of TCP Packet is enabled, you need to set the TCP destination port number or define a port range by specifying both the start and end port numbers. The port number ranges from 0 to 65535.
TCP Packet Flag	This parameter is required when the protocol type is set to TCP. Once TCP Packet Flag is enabled, you can set TCP flags by enabling or disabling ACK, FIN, PSH, RST, SYN, and URG, and assigning a value of 0 or 1 to each flag field.
Source Port No. of UDP Packet	This parameter is required when the protocol type is set to UDP. Once Source Port No. of UDP Packet is enabled, you need to set the UDP source port number or define a port range by specifying both the start and end port numbers. The port number ranges from 0 to 65535.

Destination Port No. of UDP Packet	This parameter is required when the protocol type is set to UDP. Once Destination Port No. of UDP Packet is enabled, you need to set the UDP destination port number or define a port range by specifying both the start and end port numbers. The port number ranges from 0 to 65535.
DSCP Priority	Once DSCP Priority is enabled, you need to set the DSCP priority with a value between 0 and 63. A higher value indicates a higher priority.
Packet Fragmentation	Enable or disable ACL filtering for fragmented packets. When enabled, the device matches not only non-fragmented packets and the first fragment (which is processed in the same way as non-fragmented packets) but also subsequent fragments for rule-based filtering.
Hit Count	Enable or disable ACL packet statistics. When enabled, the number of packets matching a specific ACL rule is counted.
Effective Time Range	Set the time range during which the ACL rule is active. You may select a pre-configured time range or click Add to create a new one.  Note It is recommended to create time ranges in Configuration > Advanced Configuration > Time Range before configuring this parameter.

Note

The configurable ACL rule parameters vary depending on the advanced ACL type. Refer to the actual device interface for specific details.

4) Click **Save**.

5) Optional: View ACL rule information or perform related operations in the ACL rule list.

- Click  to edit the ACL rule.

- Click  in the **Operation** column to delete a single ACL rule, or select multiple rules and click **Delete** to delete ACL rules in batch.

Configure Layer 2 ACL

Steps

1. Click **Configuration** -> **Security Configuration** -> **ACL** -> **Layer 2 ACL**.
2. Click **Add**.
3. Configure the relevant parameters.

* ACL

Please enter an ACL number between 4000 and 4999, or an ACL name th...

* Matching Order

Config

* Step

5

Description

No more than 64 characters are allowed.

ACL Rule

Rule Configuration

+ Add

 Delete

 Refresh

☐	Rule ID	Action	Effective Ti...	Outbound/I...	Operation
 No data.					

Total 0

<

1

>

Go to

1

Save

Cancel

Figure 5-86 Add Layer 2 ACL

ACL

Specify an ACL number or ACL name.

- The ACL number must fall within the range of 4000 to 4999.

- The ACL name must be 1 to 32 characters long and start with a letter (a–z or A–Z).

Matching Order

Set the ACL rule matching order to **Config**.

When the matching order is **Config**, the system arranges rules in ascending order of their numbers and matches packets accordingly. Rules with smaller numbers are matched first.

Step

Set the step value for ACL rule numbering, which must be between 1 and 20.

Since rule numbers affect the matching sequence, when the system automatically assigns rule numbers, it reserves space between adjacent rules to allow for future insertions. This reserved interval is called the rule numbering step—the difference between two consecutive rule numbers.

Description

Enter a description for the ACL, which can contain up to 64 characters.

7. Click **Save.****8. Optional: View Layer 2 ACL information or perform related operations in the Layer 2 ACL list.**

- Click  to edit the Layer 2 ACL.
- Click  to delete the Layer 2 ACL.
- Enter the ACL number or name and click **Search** to search for the specified type of Layer 2 ACLs.

9. Optional: Configure Layer 2 ACL rules.

- 1) Click  in the **Operation** column of the specified ACL.
- 2) In the **ACL Rule** area, click **Add**.
- 3) Set the parameters as needed.

ACL

4001

Rule ID

Range: 1 to 65535

Action

☒ Permit ☐ Deny

Source MAC Address/Wildcard Mask

☐

Destination MAC Address/Wildcard Mask

☐

802.1p Priority

☐

Link Layer Protocol Type

☐

Hit Count

☐

Effective Time Range

Please select. ▼

Save

Cancel

Figure 5-85 Add Layer 2 ACL Rule

Configuration Item	Note
Rule ID	Set the ACL rule number within the range of 1 to 65535.
Action	Set the ACL rule action to Permit or Deny . ● Permit: Allows packets matching the rule to pass. ● Deny: Blocks packets matching the rule from passing.
Source MAC Address/Wildcard Mask	Source MAC address information of the ACL rule. This parameter is required when adding Layer 2 ACL rules. If you enable this function, you need to set the source MAC address.
Source MAC Address	Set the source MAC address for the ACL rule.

Wildcard Mask	Specify the wildcard mask for the source MAC address. The MAC address wildcard mask follows the same format as a MAC address, represented in hexadecimal and consisting of six bytes (48 bits). It indicates which bits in the MAC address should be inspected. Similar to an IP address wildcard mask, a bit value of 0 means "check the corresponding bit" while a value of 1 means "ignore the corresponding bit". A mask of 0000-0000-0000 indicates that every bit of the MAC address will be checked.
Destination MAC Address/Wildcard Mask	Destination MAC address information of the ACL rule. This parameter is required when adding Layer 2 ACL rules. If you enable this function, you need to set the destination MAC address.
Destination MAC Address	Set the destination MAC address for the ACL rule.
Wildcard Mask	Specify the wildcard mask for the destination MAC address. The MAC address wildcard mask follows the same format as a MAC address, represented in hexadecimal and consisting of six bytes (48 bits). It indicates which bits in the MAC address should be inspected. Similar to an IP address wildcard mask, a bit value of 0 means "check the corresponding bit" while a value of 1 means "ignore the corresponding bit". A mask of 0000-0000-0000 indicates that every bit of the MAC address will be checked.
802.1p Priority	Once 802.1p Priority is enabled, you need to set the 802.1p priority with a value between 0 and 7. A higher value indicates a higher priority.
Link Layer Protocol Type	Once Link Layer Protocol Type is enabled, you need to set the link-layer protocol type within the valid value range of 600 to FFFF.
Hit Count	Enable or disable ACL packet statistics. When enabled, the number of packets matching a specific ACL rule is counted.

Effective Time Range	Set the time range during which the ACL rule is active. You may select a pre-configured time range or click Add to create a new one.  Note It is recommended to create time ranges in Configuration > Advanced Configuration > Time Range before configuring this parameter.
----------------------	---

4) Click **Save**.

5) Optional: View ACL rule information or perform related operations in the ACL rule list.

- Click  to edit the ACL rule.
- Click  in the **Operation** column to delete a single ACL rule, or select multiple rules and click **Delete** to delete ACL rules in batch.

Configure ACL Application

The most fundamental application of ACL is packet filtering. By applying ACL rules globally, to specific interfaces, or in specific VLANs—in either the inbound or outbound direction—the system can filter incoming or outgoing packets.

Note

When conflicting ACL rules are applied globally, on a port, and to a VLAN, the ACL enforcement priority follows this order: global configuration > port configuration > VLAN configuration.

Configure Global ACL Application

Steps

1. Click **Configuration -> Security Configuration -> ACL -> Global ACL Application**.
2. Select the global ACL application direction, and click  to add an inbound or outbound ACL application.
3. Configure the parameters in the specified direction, for example, inbound.

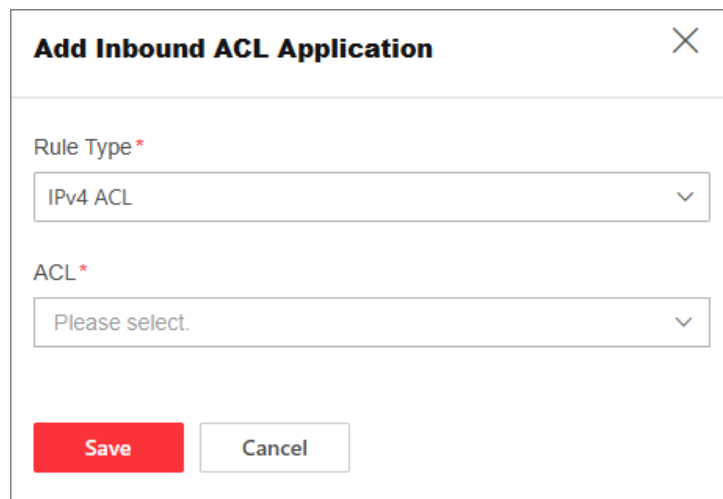
A dialog box titled "Add Inbound ACL Application" with a close button (X) in the top right corner. It contains two dropdown menus: "Rule Type *" with "IPv4 ACL" selected, and "ACL *" with "Please select." selected. At the bottom are two buttons: "Save" (red) and "Cancel" (white with grey border).

Figure 5-88 Configure Global ACL Application

Rule Type

Specifies the ACL type: IPv4 ACL, IPv6 ACL, or Layer 2 ACL.

ACL

Select an existing IPv4 ACL, IPv6 ACL, or Layer 2 ACL by its number or name.

4. Click **Save**.

Note

- Up to 2 global ACL applications can be configured per direction.
 - Once successfully configured, global ACL applications will be displayed in the card area below the corresponding direction, showing the ACL number/name, ACL type, and description applied in that direction.
5. Optional: Hover the mouse over the specified inbound or outbound ACL application and click **Delete** to delete the global ACL application of this direction.

Configure Port ACL Application

Steps

1. Click **Configuration** -> **Security Configuration** -> **ACL** -> **Port ACL Application**.
2. Select one or more ports on the port panel, or click the aggregation group icon above the port panel to select the entire aggregate interface.
3. Enable **ACL Application**.
4. Configure the relevant parameters.

Port ACL Application Configuration

Selected Port(s) + Add All 🗑 Clear



No port selected. Click on the left port panel to select a port first.

ACL Application ☒

Application Direction *

Inbound

Rule Type *

IPv4 ACL

ACL *

Please select.

Save

Figure 5-89 Configure Port ACL Application

Application Direction

Select the direction for applying ACL rules to filter interface packets. Options include inbound or outbound.

Rule Type

Choose the ACL type: IPv4 ACL, IPv6 ACL, or Layer 2 ACL. Note that some devices only support IPv4 ACL or Layer 2 ACL.

ACL

Select a specific IPv4, IPv6, or Layer 2 ACL by its number or name. Note that some devices only support IPv4 ACL or Layer 2 ACL.

5. Click **Save**.

6. Optional: View port ACL application details in the **Port ACL Details** list.

Port ACL Details

Port	Direction	Rule Type	ACL
Ge 1/0/5	Inbound	IPv4	2001
Ge 1/0/6	Inbound	IPv4	2001

Figure 5-90 View Port ACL Application Information

Configure VLAN ACL Application

Steps

- 1. Click **Configuration** -> **Security Configuration** -> **ACL** -> **VLAN ACL Application**.
- 2. Click **Add**.
- 3. Configure the relevant parameters.

Add VLAN ACL Application

VLAN ID *

Please Select VLAN ID

Application Direction *

Please Select Application Direction

Rule Type *

IPv4 ACL

ACL *

Please select.

Save

Cancel

Figure 5-91 Configure VLAN ACL Application

VLAN ID

Select the VLAN interface to which the ACL rules will be applied. You can choose from the configured VLAN ID(s).

Application Direction

Specify the direction in which ACL rules filter packets on the VLAN interface. Options include inbound or outbound.

Rule Type

Choose the type of ACL rule: IPv4 ACL, IPv6 ACL, or Layer 2 ACL. Note that some devices only support IPv4 ACL or Layer 2 ACL.

ACL

Select a specific IPv4, IPv6, or Layer 2 ACL by its number or name. Note that some devices only support IPv4 ACL or Layer 2 ACL.

- 4. Click **Save**.
- 5. View information about VLAN ACL applications or perform relevant operations in the VLAN ACL application details list.

+ Add Delete Refresh				
☐	VLAN	Direction	Rule Type	ACL
☐	VLAN 1	Inbound	IPv4	2001

Figure 5-92 View VLAN ACL Application Information

- Click  to delete the specified ACL application on the VLAN interface.
- Select one or more VLAN interface ACL applications and click **Delete** to batch delete them.
- Click **Refresh** to refresh the VLAN interface ACL application information.

5.3.2 QoS Configuration

For network services, key factors affecting Quality of Service (QoS) include bandwidth, delay, packet loss rate, and jitter. To enhance QoS performance, it is essential to ensure sufficient transmission bandwidth, minimize transmission delay, reduce packet loss, and control jitter.

A QoS strategy consists of three core components: traffic classifier, traffic behavior, and traffic policy. Users can flexibly apply QoS configurations by binding specific traffic classifiers with corresponding behaviors.

The complete workflow for configuring a QoS strategy is as follows:

1. Configure traffic classifier
2. Configure traffic behavior
3. Configure QoS policy
4. Apply QoS policy



Note

Click  in the upper-right corner of the page to view QoS configuration help.

Configure Traffic Classifier

A traffic classifier defines a set of traffic matching rules to identify and categorize packets based on specified characteristics, with its key elements including the class name, classification rules, and the logical relationship among multiple rules when more than one is configured.

Steps

1. Click **Configuration** -> **Security Configuration** -> **QoS** -> **Traffic Classifier**.
2. Add a traffic classifier.
 - 1) Click **Add**.

Figure 5-93 Add Traffic Classifier

- 2) Enter the traffic classifier name.
- 3) Select the logical relationship between the rules included in this classifier.

Logical AND

- When the traffic classifier contains ACL rules, a packet must satisfy both of the following conditions to be classified into this category:

- Match at least one ACL rule.
- Match all non-ACL rules.
- If the traffic classifier contains no ACL rules, a packet must match all non-ACL rules to qualify.

Logical OR

A packet is considered to belong to this category as long as it matches any one rule in the traffic classifier.

- 4) Check the rule type(s) to be added to the traffic classifier, click to add, and then configure the specific operation values for each type.

All Packets

Applies to all packets without distinction.

All IPv4 Packets

Applies to all IPv4 packets.

All IPv6 Packets

Applies to all IPv6 packets.

Match the Layer 2 ACL

A pre-configured Layer 2 ACL must be selected (match by ACL number).

Match the IPv4 ACL

A pre-configured IPv4 ACL must be selected (match by ACL number).

Match the IPv6 ACL

A pre-configured IPv6 ACL must be selected (match by ACL number).

Match the IP precedence

Permitted values: 0 to 7.

Match the DSCP priority

Permitted values: 0 to 63.

Match the source MAC address

Format: AA:BB:CC:DD:EE:FF.

Match the destination MAC address

Format: AA:BB:CC:DD:EE:FF.

Match the VLAN based on the outer VLAN tag

Permitted VLAN IDs: 1 to 4094.

Match the VLAN ID of the inner VLAN tag

Permitted VLAN IDs: 1 to 4094.

Match the 802.1p priority based on the outer VLAN tag

Permitted values: 0 to 7.

Match the 802.1p priority of the inner VLAN tag

Permitted values: 0 to 7.

**Note**

- Available rule types may differ by device model. Please refer to the device interface for specific options.
- To remove a selected traffic classifier, check its box and click ☐ to deselect.
- Multiple rule types can be configured simultaneously. However, due to logical constraints and mutual exclusivity among certain rule definitions, valid combinations within a single traffic classifier are subject to the restrictions displayed on the interface.
- When **All Packets** is selected, no additional rule definitions can be configured.
- 802.1p priority matching supports multiple values and value ranges (e.g., 3,5,10-100).
- Matching by ACL number or name is supported.
 - Under Logical AND, only one ACL type is allowed, and only one ACL can be configured.
 - Under Logical OR, up to two ACL types are supported, with a maximum of one ACL per type.
- Under Logical AND, MAC address matching cannot be used together with Layer 2 ACL matching. Both source and destination MAC address matching can be enabled simultaneously, but only one MAC address entry is allowed per field.
- IP precedence matching supports multiple values and value ranges (e.g., 3,5,10-100). Under Logical AND, it cannot be used with DSCP priority matching.
- VLAN ID matching supports multiple values and value ranges (e.g., 3,5,10-100).
- DSCP priority matching supports multiple values and value ranges, but a maximum of 8 priority values are allowed (e.g., 3,5,10-15). Under Logical AND, it cannot be used with IP precedence matching.

5) Click **Save**.

3. Optional: Select an existing traffic classifier and click **Delete** to delete it.

4. Optional: Select an existing traffic classifier and click **Edit** to edit its parameters.

Configure Traffic Behavior

A traffic behavior defines the actions applied to a specific category of packets, consisting of two key elements: the behavior name and the set of actions defined within it. Supported actions include packet filtering, priority remarking, VLAN remarking, redirection, traffic policing, traffic statistics, and traffic mirroring.

Steps

1. Click **Configuration** -> **Security Configuration** -> **QoS** -> **Traffic Behavior**.

2. Add a traffic behavior.

1) Click **Add**.

*Name

Behavior

Not Selected (0/14)

Type
☐ Remark the DSCP priority of packets
☐ Remark the IP precedence of packets
☐ Remark the 802.1p priority of packets
☐ Remark the inner 802.1p priority of p...
☐ Remark the queue priority of packets
☐ Remark the outer VLAN ID of packets
☐ Remark the inner VLAN ID of packets
☐ Redirect Traffic to
☐ Mirror Traffic to
☐ Rate Limit
☐ Collect Statistics by Byte
☐ Collect Statistics by Packet

>

<

Selected (0/0)

Type	Operation
------	-----------

Figure 5-94 Add Traffic Behavior

2) Enter the traffic behavior name.

3) Check the behavior type(s) to be added to the traffic behavior, click to add, and then configure the specific operation values for each type.

Remark the DSCP priority of packets

Permitted values: 0 to 63.

Remark the IP precedence of packets

Permitted values: 0 to 7.

Remark the 802.1p priority of packets

Permitted values: 0 to 7.

Remark the inner 802.1p priority of packets

Permitted values: 0 to 7.

Remark the queue 802.1p priority of packets

Permitted values: 0 to 7.

Remark the outer VLAN ID of packets

Permitted VLAN IDs: 1 to 4094.

Remark the inner VLAN ID of packets

Permitted VLAN IDs: 1 to 4094.

Redirect Traffic to

Redirects traffic to a specified port or the CPU.

Mirror Traffic to

Mirrors traffic to a pre-configured mirroring group.

Rate Limit

Configurable parameters include:

- CIR (Committed Information Rate): Minimum guaranteed throughput. Value range: 16 to 16,000,000 kbps, in multiples of 16.
- PIR (Peak Information Rate): Maximum allowed throughput. Value range: 16 to 16,000,000 kbps, in multiples of 16.
- CBS (Committed Burst Size): Burst tolerance under CIR. Value range: 256 to 4,096,000 bytes, in multiples of 128.
- EBS (Excess Burst Size): Additional burst allowance beyond CBS. Value range: 0 to 4,096,000 bytes, in multiples of 128.
- greenAction: Applied to green packets (rate $\leq$ CIR). Options: **pass**.
- yellowAction: Applied to yellow packets (CIR < rate $\leq$ PIR). Options: **discard** or **pass**.
- redAction: Applied to red packets (rate > PIR). Options: **discard** or **pass**.



Note

- Generally, packets are marked green when the rate is less than or equal to the CIR, yellow when the rate is between the CIR and PIR (inclusive), and red when the rate exceeds the PIR.
- In actual configuration, it is necessary to ensure that PIR $\geq$ CIR and EBS $\geq$ CBS.
- Some device models only support CIR configuration. Please refer to the actual device interface for supported features.

Collect Statistics by Byte

Collects and counts traffic volume in bytes.

Collect Statistics by Packet

Collects and counts the number of packets.

Discard Packets

Discards matched packets.

Forward Packets

Allows matched packets to pass.

Note

- Supported behavior types vary by device. Refer to the device interface for available options.
- To remove a selected traffic behavior, check its box and click  to deselect.
- Multiple behavior types can be configured simultaneously. However, due to logical constraints and mutual exclusivity among certain behavior definitions, valid combinations within a single traffic behavior are subject to the restrictions displayed on the interface.
- DSCP and IP priority remarking are mutually exclusive; only one can be configured per traffic behavior.
- If a mirroring group has a source port configured, traffic mirroring to that group cannot be enabled, and vice versa.

4) Click **Save**.

3. Optional: Select an existing traffic behavior and click **Delete** to delete it.

4. Optional: Select an existing traffic behavior and click **Edit** to edit its parameters.

Configure QoS Policy

A QoS policy binds specified traffic classifiers to corresponding traffic behaviors, enforcing the actions defined in the behavior on packets that match the classifier conditions. Key elements include the policy name, along with the names of the bound classifiers and behaviors. Multiple classifier-behavior bindings can be defined within a single policy.

Steps

1. Click **Configuration** -> **Security Configuration** -> **QoS** -> **QoS Policy**.

2. Add a QoS policy.

1) Click **Add**.

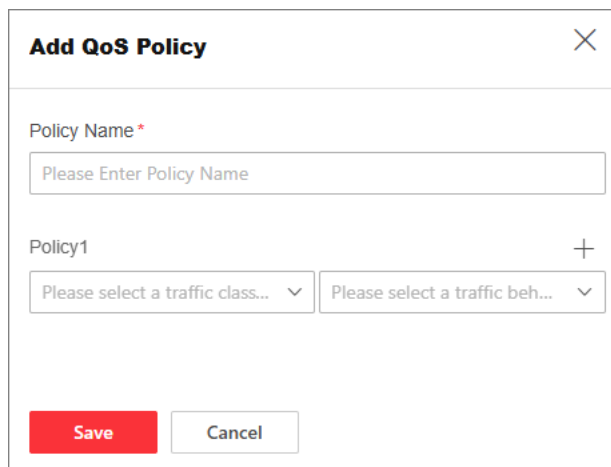


Figure 5-95 Add QoS Policy

- 2) Enter the QoS policy name.
- 3) Bind the created traffic classifier to the corresponding traffic behavior.
- 4) (Optional): Click  to add more bindings.

Note

Up to 16 policies can be configured at the same time.

- 5) Click **Save**.
3. Optional: Select an existing QoS policy and click **Delete** to delete it.
4. Optional: Select an existing QoS policy and click **Edit** to edit its parameters.

Configure QoS Policy Application

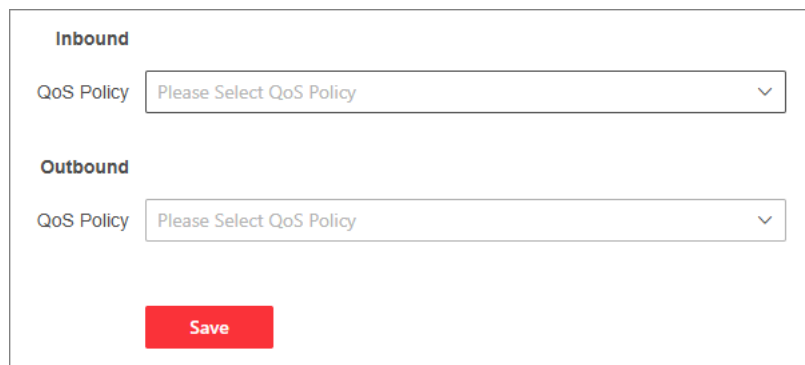
Note

When mutually exclusive QoS policies are applied globally, on a port, and to a VLAN, the QoS policy enforcement priority follows this order: global configuration > port configuration > VLAN configuration.

Configure Global QoS Policy Application

Steps

1. Click **Configuration** -> **Security Configuration** -> **QoS** -> **Global QoS Policy Application**.
2. Configure global QoS policy for inbound and (or) outbound traffic.



The screenshot displays a web interface for configuring global QoS policy application. It is divided into two main sections: 'Inbound' and 'Outbound'. Each section contains a 'QoS Policy' label followed by a dropdown menu. The dropdown menus currently show the text 'Please Select QoS Policy' and a downward arrow. At the bottom of the interface, there is a prominent red button labeled 'Save'.

Figure 5-96 Configure Global QoS Policy Application

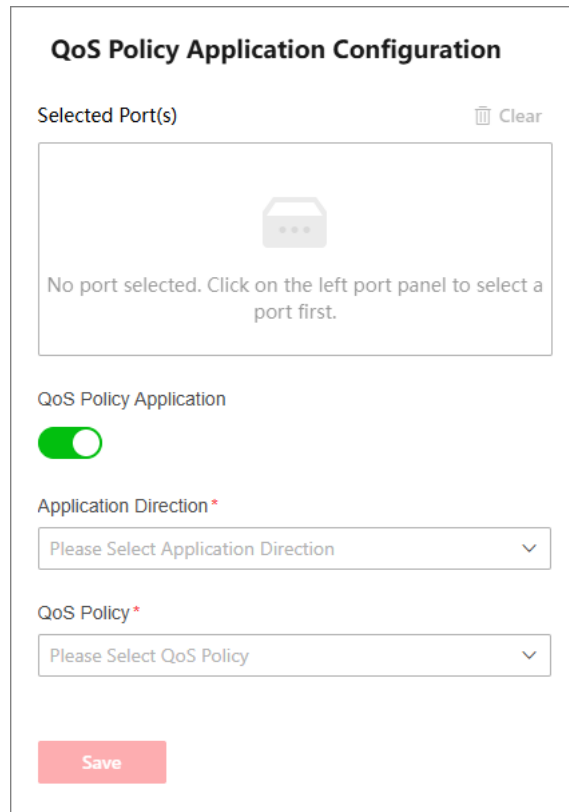
3. Click **Save**.

Configure Port QoS Policy Application

You can apply the configured QoS policy to the port(s) as needed.

Steps

1. Click **Configuration** -> **Security Configuration** -> **QoS** -> **Port QoS Policy Application**.



The screenshot shows the 'QoS Policy Application Configuration' page. At the top, it says 'Selected Port(s)' with a 'Clear' button. Below this is a large box with a port icon and the text 'No port selected. Click on the left port panel to select a port first.' Underneath is a 'QoS Policy Application' toggle switch, which is currently turned on (green). Below the toggle is an 'Application Direction*' dropdown menu with the placeholder text 'Please Select Application Direction'. Below that is a 'QoS Policy*' dropdown menu with the placeholder text 'Please Select QoS Policy'. At the bottom of the form is a red 'Save' button.

Figure 5-97 Configure Port QoS Policy Application

2. Click to select one or more ports on the port panel, or click the aggregation group icon to select the corresponding aggregate interface above the port panel.

 Note

- Up to 30 ports can be selected.
 - The member ports of an aggregation group are not supported.
3. Enable **QoS Policy Application**.
 4. Select the application direction as inbound or outbound.
 5. Select a pre-configured QoS policy.
 6. Click **Save**.

The QoS policy application details of the selected port(s) will be displayed in the **Port QoS Details** list.

7. Optional: To edit the QoS policy applied on the port(s), repeat the above steps.

Configure VLAN QoS Policy Application

Steps

1. Click **Configuration** -> **Security Configuration** -> **QoS** -> **VLAN QoS Policy Application**.
2. Click **Add**.
3. Configure the parameters as needed.

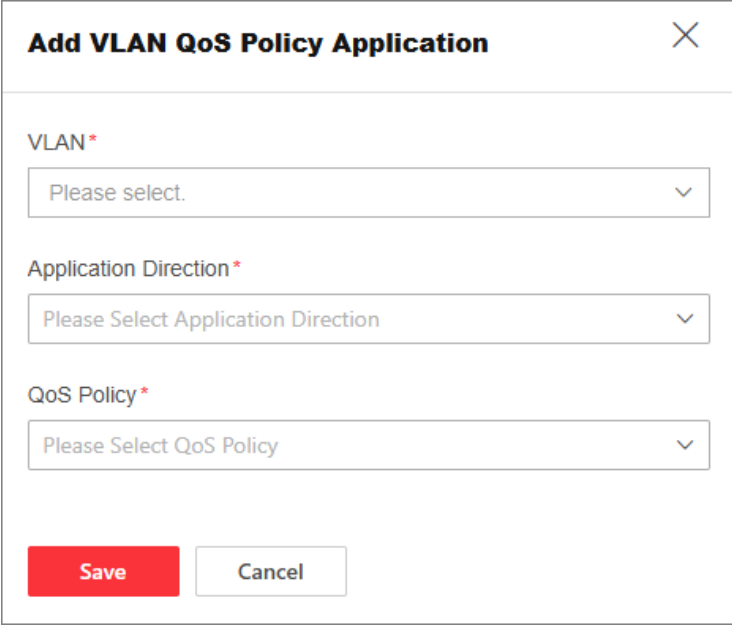


Figure 5-98 Configure VLAN QoS Policy Application

VLAN

Select the VLAN interface to which the QoS policy will be applied. Choose from the configured VLAN IDs.

Application Direction

Specify the direction in which the QoS policy will filter packets on the VLAN interface. Options include inbound or outbound.

QoS Policy

Select a pre-configured QoS policy.

4. Click **Save**.
5. Optional: View the details of QoS policies applied to the VLAN(s) in the VLAN QoS policy details list, or perform other operations.
 - Select a QoS policy application for a VLAN interface and click  to remove the policy from the specified interface.
 - Select multiple QoS policy applications for VLAN interfaces, and click **Delete** to batch remove the policies from the selected interfaces.
 - Click **Refresh** to update the QoS policy application information for VLAN interfaces.

Configure Port Priority and Trust Mode

The device can assign priority parameters to packets based on the mapping table by configuring the port priority and trust mode.

Steps

1. Click **Configuration** -> **Security Configuration** -> **QoS** -> **Port QoS Configuration** -> **Priority**.

Port	Priority	Trusted Mode
Ge 1/0/1	0	Port
Ge 1/0/2	0	Port
Ge 1/0/3	0	Port
Ge 1/0/4	0	Port
Ge 1/0/5	0	Port
Ge 1/0/6	0	Port
Ge 1/0/7	0	Port
Ge 1/0/8	0	Port
Ge 1/0/9	0	Port
Ge 1/0/10	0	Port

Figure 5-99 Configure Port Priority and Trust Mode

2. Configure the priority of the desired port(s).



Note

The port priority ranges from 0 to 7, with a default value of 0.

3. Optional: Configure the trust mode of the port(s).

Port: Trust the port.

External 802.1p: Trust the outer 802.1p priority carried in the packet and use it for priority mapping.

Internal 802.1p: Trust the inner 802.1p priority carried in the packet and use it for priority mapping.

DSCP: Trust the DSCP value carried in the IP packet and use it for priority mapping.

4. Click **Save**.

5. Optional: Select port, priority, or trust mode, and click **Search** to filter out the specified port QoS configuration information.

Configure Priority Mapping

Upon receiving a packet, the device assigns or modifies its priority value based on the mapping rules. This priority mapping function translates the priority field in the packet into a corresponding

priority value, which determines the packet's scheduling capability. The resulting priority value serves as the basis for queue scheduling and congestion control, enabling effective management of the packet's forwarding scheduling level.

1. Click **Configuration -> Security Configuration -> QoS -> Port QoS Configuration -> Mapping**.

802.1p Priority	Local Preference
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Figure 5-100 Configure Priority Mapping

Note

The supported priority mapping configurations vary by device. Please refer to the actual interface for details.

2. Optional: Configure the mapping from 802.1p priority to local priority.

- 1) Click **802.1p-to-Local Priority Mapping**.
- 2) Configure the corresponding local priority based on the 802.1p priority.

Note

The local priority value ranges from 0 to 7.

- 3) (Optional) Click **Restore Default Settings** to reset the mapping parameters in the table to their default values.
- 4) Click **Refresh** to view the latest priority mapping table configuration.
- 5) Click **Save**.
3. Optional: Configure the mapping from 802.1p priority to 802.1p priority.
 - 1) Click **802.1p-to-802.1p Priority Mapping**.
 - 2) Configure the corresponding 802.1p priority based on the 802.1p priority.

Note

The 802.1p priority value ranges from 0 to 7.

- 3) (Optional) Click **Restore Default Settings** to reset the mapping parameters in the table to their default values.

- 4) Click **Refresh** to view the latest priority mapping table configuration.
- 5) Click **Save**.
4. Optional: Configure the mapping from DSCP priority to 802.1p priority.
 - 1) Click **DSCP-to-802.1p Priority Mapping**.
 - 2) Configure the corresponding 802.1p priority based on the DSCP priority.

 Note

The 802.1p priority value ranges from 0 to 7.

- 3) (Optional) Click **Restore Default Settings** to reset the mapping parameters in the table to their default values.
- 4) Click **Refresh** to view the latest priority mapping table configuration.
- 5) Click **Save**.
5. Optional: Configure the mapping from DSCP priority to local priority.
 - 1) Click **DSCP-to-Local Priority Mapping**.
 - 2) Configure the corresponding local priority based on the DSCP priority.

 Note

The local priority value ranges from 0 to 7.

- 3) (Optional) Click **Restore Default Settings** to reset the mapping parameters in the table to their default values.
- 4) Click **Refresh** to view the latest priority mapping table configuration.
- 5) Click **Save**.
6. Optional: Configure the mapping from 802.1p priority to drop priority.
 - 1) Click **802.1p-to-Drop Priority Mapping**.
 - 2) Configure the corresponding drop priority based on the 802.1p priority.

 Note

The drop priority value ranges from 0 to 2.

- 3) (Optional) Click **Restore Default Settings** to reset the mapping parameters in the table to their default values.
- 4) Click **Refresh** to view the latest priority mapping table configuration.
- 5) Click **Save**.
7. Optional: Configure the mapping from DSCP priority to drop priority.
 - 1) Click **DSCP-to-Drop Priority Mapping**.
 - 2) Configure the corresponding drop priority based on the DSCP priority.

 Note

The drop priority value ranges from 0 to 2.

- 3) (Optional) Click **Restore Default Settings** to reset the mapping parameters in the table to their default values.
 - 4) Click **Refresh** to view the latest priority mapping table configuration.
-

5) Click **Save**.

8. Optional: Configure the mapping from DSCP priority to DSCP priority.

1) Click **DSCP-to-DSCP Priority Mapping**.

2) Configure the corresponding DSCP priority based on the DSCP priority.

**Note**

The DSCP priority value ranges from 0 to 63.

3) (Optional) Click **Restore Default Settings** to reset the mapping parameters in the table to their default values.

4) Click **Refresh** to view the latest priority mapping table configuration.

5) Click **Save**.

9. Optional: Configure the mapping from 802.1p priority to DSCP priority.

1) Click **802.1p-to-DSCP Priority Mapping**.

2) Configure the corresponding DSCP priority based on the 802.1p priority.

**Note**

The DSCP priority value ranges from 0 to 63.

3) (Optional) Click **Restore Default Settings** to reset the mapping parameters in the table to their default values.

4) Click **Refresh** to view the latest priority mapping table configuration.

5) Click **Save**.

Configure Queue Scheduling

In complex environments with group switching and multiple user services coexisting, congestion management is usually achieved via queues (SP queue and WRR queue).

Steps

1. Click **Configuration -> Security Configuration -> QoS -> Port QoS Configuration -> Port Scheduling Algorithm**.

2. Configure the port scheduling algorithm.

1) Click  in the **Operation** column of the desired port.

2) Select the queue scheduling algorithm and complete the queue-related configuration.

Edit Port Scheduling Algorithm

Port Name

Ge 1/0/2

Queue Scheduling Algorithm

SP

Queue ID

Que...	Queue Algorithm G...	Minimum Bandwid...
0	sp	
1	sp	
2	sp	
3	sp	
4	sp	
5	sp	
6	sp	
7	sp	

Save

Cancel

Figure 5-101 Configure Port Queue Scheduling

WRR (Weighted Round Robin)

A weighted polling queue method that configures the output queue scheduling policy as frame-number-weighted round-robin. It cycles through queues in rotation to ensure each queue receives a certain amount of service time. When WRR is selected, you need to configure the queue algorithm group, weight (range: 1 to 127), and minimum bandwidth guarantee (recommended to be an integer that is a multiple of 16).

SP (Strict Priority)

Configures the output queue scheduling policy to strict priority mode. Packets in higher-priority queues are sent first according to the priority order from high to low. When SP is selected, configure the queue algorithm group and minimum bandwidth guarantee (recommended as an integer that is a multiple of 16).

WFQ (Weighted Fair Queueing)

Configures the output queue scheduling policy as weighted fair queueing. Similar to WRR, it schedules queues in rotation to ensure each receives a certain service time. When WFQ is selected, configure the queue algorithm group, weight (range: 1 to 127), and minimum bandwidth guarantee (recommended as an integer that is a multiple of 16).



Note

The supported queue scheduling algorithms and their specific configuration options vary by device. Please refer to the actual interface for details.

4) Click **Save**.

4. Optional: In the port scheduling algorithm details list, click  next to the queue ID to see detailed scheduling algorithm configurations for each queue on the port.

5.3.3 AAA Configuration

AAA (Authentication, Authorization, and Accounting) is a security management mechanism for access control in network security, offering three security services: authentication, authorization, and accounting.

- **Authentication:** Verifies the identity of network users to determine whether the visitor is legitimate.
- **Authorization:** Grants different access rights to users, limiting the services they can use.
- **Accounting:** Records all operations performed by users when they access network services, including service types, start time, and data traffic.

AAA can be implemented through multiple protocols, which define how user information is transmitted between the access server and the AAA server.



Note

Currently, some devices support only the RADIUS (Remote Authentication Dial-In User Service) protocol, while others support both RADIUS and TACACS+ (Terminal Access Controller Access Control System). Please refer to the actual device specifications for supported protocols.

Configure RADIUS Scheme

RADIUS (Remote Authentication Dial-In User Service) is a distributed, client/server-based protocol designed to secure networks against unauthorized access. It is commonly deployed in environments that require both high security and support for remote user access.

Steps

1. Click **Configuration** -> **Security Configuration** -> **AAA** -> **RADIUS**.
2. Add a RADIUS scheme.
 - 1) Click **Add**.

* Scheme Name

Please Enter Scheme Name

Authentication Server

Authentication Server + Add

No server added.

Shared Key

Please Enter Shared Key

Accounting Server

Accounting Server + Add

No server added.

Shared Key

Please Enter Shared Key

Advanced Configuration

Source IPv4 Address for Outgoing RADI...

Source IPv6 Address for Outgoing RADI...

Source IPv6 Address for Outgoing RADI...

Server Response Timeout

Server Response Timeout sec

RADIUS Packet Retransmission Times

Please Enter RADIUS Packet Retransmission Times

Server Quiet Period

Server Quiet Period min

Real-Time Accounting Interval

Please Enter Real-Time Accounting Interval min

Accounting-Update Request Retransmis...

Please Enter Accounting-Update Request Retransmission Times

Stop-Accounting Request Retransmissi...

Please Enter Stop-Accounting Request Retransmission Times

User Name Format

Please Select User Name Format

Save

Cancel

Figure 5-102 Add RADIUS Scheme

2) Enter the scheme name.

3) In the **Authentication Server/Accounting Server** configuration area, click **Add** and configure the server parameters.

IP Address Type

The type of IP address used by the server. Some devices only support IPv4. Refer to the actual interface for details.

IP Address

The specific IP address of the server.

Port

Specify the service port. Valid range: 1 to 65535.

Key

The private key of the currently configured server.

**Note**

If a server private key is used, ensure that the key configured on the device matches exactly the one set on the RADIUS server. Before configuration, ensure that the authentication/accounting RADIUS server exists, or specify the private key for the server during the configuration of the authentication/accounting RADIUS server.

Status

Server status:

- Active: Indicates the server is available.
- Block: Indicates the server is unavailable.

Priority

Specify whether the server is the primary or secondary server.

**Note**

Only one primary authentication/accounting server can be configured. Multiple secondary authentication/accounting servers are allowed.

Shared Key

A shared key configured for all current authentication/accounting servers.

**Note**

If a shared key is used, ensure that the key configured on the device matches exactly the one set on the RADIUS server.

4) Optional: Configure advanced parameters for the RADIUS scheme.

Source IPv4 Address for Outgoing RADIUS Packets

Configure the source IPv4 address used for sending RADIUS packets.

Source IPv6 Address for Outgoing RADIUS Packets

Configure the source IPv6 address used for sending RADIUS packets.

Server Response Timeout

The waiting time for retransmitting a RADIUS request packet if no response is received from the RADIUS server. Valid range: 1 to 10 seconds.

RADIUS Packet Retransmission Times

The maximum number of retransmission attempts after a server response timeout. Valid range: 1 to 20.

Server Quiet Period

If a server becomes unreachable, the device marks it as blocked and starts a timer. After the specified recovery time, the server status is restored to active. Valid range: 0 to 255 minutes.

Real-Time Accounting Interval

To enable real-time accounting, the device periodically sends user accounting information to the server at the configured interval. Valid range: 1 to 60 minutes.

Accounting-Update Request Retransmission Times

The maximum number of real-time accounting request attempts allowed. If no response is received from the RADIUS server after the specified number of attempts, the user connection is terminated. Valid range: 1 to 255.

Stop-Accounting Request Retransmission Times

The maximum number of stop-accounting request attempts allowed. Valid range: 10 to 65535.

User Name Format

Options include: **keep-original** (same as user input), **with-domain** (with domain name), or **without-domain** (without domain name).

5) Click **Save**.

3. Optional: Select a scheme and click  to delete it.
4. Optional: Select a scheme and click  to modify the scheme information.
5. Optional: Click  next to the number of secondary authentication/accounting servers in the list to view detailed configuration information for secondary servers in the scheme.

Configure TACACS Scheme

TACACS+ (Terminal Access Controller Access Control System) also uses a client/server model to enable communication between the NAS and the TACACS+ server.



TACACS scheme configuration is only supported on certain devices. Please refer to the actual device interface for details.

Steps

1. Click **Configuration** -> **Security Configuration** -> **AAA** -> **TACACS**.
2. Add a TACACS scheme.
 - 1) Click **Add**.

* Scheme Name

Please Enter Scheme Name

Authentication Server

+ Add

No server added.

Shared Key

Please Enter Shared Key

Authorization Server

+ Add

No server added.

Authorization Shared Key

Please Enter Authorization Shared Key

Accounting Server

+ Add

No server added.

Shared Key

Please Enter Shared Key

Advanced Configuration

Source IPv4 Address for Outgoing TAC...

Source IPv6 Address for Outgoing TAC...

Server Response Timeout

Server Quiet Period

Stop-Accounting Request Retransmissi...

User Name Format

Please Enter Source IPv6 Address for Outgoing TACACS Packets

Please Enter Server Response Timeout

Please Enter Server Quiet Period

Please Enter Stop-Accounting Request Retransmission Times

Please Select User Name Format

Save

Cancel

Figure 5-103 Add TACACS Scheme

- 2) Enter the scheme name.
- 3) In the **Authentication Server/Authorization Sever/Accounting Server** configuration area, click **Add** and configure the server parameters.

IP Address Type

The type of IP address used by the server. Some devices only support IPv4. Refer to the actual interface for details.

IP Address

The specific IP address of the server.

Port

Specify the service port. Valid range: 1 to 65535.

Key

The private key of the currently configured server.

**Note**

If a server private key is used, ensure that the key configured on the device matches exactly the one set on the TACACS+ server. Before configuration, ensure that the authentication/authorization/accounting TACACS+ server exists, or specify the private key for the server during the configuration of the authentication/authorization/accounting TACACS+ server.

Status

Server status:

- Active: Indicates the server is available.
- Block: Indicates the server is unavailable.

Priority

Specify whether the server is the primary or secondary server.

**Note**

Only one primary authentication/authorization/accounting server can be configured. Multiple secondary authentication/authorization/accounting servers are allowed.

Shared Key

A shared key configured for all current authentication/authorization/accounting servers.

**Note**

If a shared key is used, ensure that the key configured on the device matches exactly the one set on the TACACS+ server.

- 4) Optional: Configure advanced parameters for the TACACS scheme.

Source IPv4 Address for Outgoing TACACS Packets

Configure the source IPv4 address used for sending TACACS packets.

Source IPv6 Address for Outgoing TACACS Packets

Configure the source IPv6 address used for sending TACACS packets.

Server Response Timeout

The waiting time for retransmitting a TACACS request packet if no response is received from the TACACS server. Valid range: 1 to 10 seconds.

Server Quiet Period

If a server becomes unreachable, the device marks it as blocked and starts a timer. After the specified recovery time, the server status is restored to active. Valid range: 0 to 255 minutes.

Stop-Accounting Request Retransmission Times

The maximum number of stop-accounting request attempts allowed. Valid range: 10 to 65535.

User Name Format

Options include: **keep-original** (same as user input), **with-domain** (with domain name), or **without-domain** (without domain name).

5) Click **Save**.

6. Optional: Select a scheme and click  to delete it.

7. Optional: Select a scheme and click  to modify the scheme information.

Optional: Click  next to the number of secondary authentication/authorization/accounting servers in the list to view detailed configuration information for secondary servers in the scheme.

Configure AAA Domain

An AAA domain is a logical area within the AAA system used to categorize and manage users. Network devices utilize AAA domains to differentiate and administer users based on type or department. Each domain can be associated with distinct authentication, authorization, and accounting schemes, enabling differentiated network access rights and quality of service for various user groups. This allows network administrators to configure authentication methods, authorization policies, and accounting settings separately for each domain according to specific user needs and security requirements, thereby improving the flexibility and precision of network access control.

Steps

1. Click **Configuration** -> **Security Configuration** -> **AAA** -> **AAA Domain**.
2. Add an AAA domain.

1) Click **Add**.

* Domain Name

Please Enter Domain Name

* Domain Status

Please Select Domain Status

Max. Access Users

Please Enter Max. Access Users

Login Access

Login Access

LAN Access

LAN Access

Portal Access

Portal Access

CLI Access

CLI Access

Default Access

Authentication Scheme

Authentication Scheme

☐ RADIUS Server Group Authentication

☐ TACACS Server Group Authentication

☐ Local Authentication

☐ Not Authenticate

Authorization Scheme

Authentication Scheme

☐ RADIUS Server Group Authorization

☐ TACACS Server Group Authorization

☐ Local Authorization

☐ Not Authorize

Accounting Scheme

Accounting Scheme

☐ RADIUS Server Group Accounting

☐ TACACS Server Group Accounting

☐ Local Accounting

☐ Not Account

Save

Cancel

Figure 5-104 Add AAA Domain

- 2) Enter the domain name, which should be less than 32 characters in length.
- 3) Configure the domain status.

Block

The users in the domain cannot request network service.

Active

The users in the domain can request network service.

- 4) Optional: Set **Max. Access Users**. Valid range: 1 to 2,500.
- 5) Optional: Enable the desired access methods as needed, and configure the corresponding authentication, authorization, and accounting schemes for each method.

Login Access

Configure authentication, authorization, and accounting schemes for login users (users logging into the device).

LAN Access

Configure authentication, authorization, and accounting schemes for LAN access users. TACACS scheme is not supported for this method.

Portal Access

Configure authentication, authorization, and accounting schemes for Portal access users. TACACS scheme is not supported for this method.

CLI Access

Configure authorization and accounting schemes for command line access users. RADIUS scheme is not supported for this method.

Default Access

This method is used when no other access method is configured. Configure authentication, authorization, and accounting schemes to be applied by default.

**Note**

- Some devices only support **Login Access**, **LAN Access**, and **Default Access**. Please refer to the actual device for supported methods.
 - The available authentication, authorization, and accounting configuration options vary depending on the access method. Refer to the device interface for specific settings.
 - If you select a RADIUS or TACACS server group for authentication, authorization, or accounting, you must first configure the corresponding RADIUS or TACACS scheme. For configuration steps, refer to **Configure RADIUS Scheme** or **Configure TACACS Scheme**.
 - If both RADIUS and TACACS server groups are selected for authentication, authorization, or accounting, configure **Server Priority** to specify which server group takes precedence.
- 6) Click **Save**.

3. Optional: Select an existing domain and check **Set as Default Domain** to set it as the default domain.
4. Optional: Select an existing domain and click **Delete** to delete it.
5. Optional: Select an existing domain and click **Edit** to edit the domain information.

5.3.4 802.1X Configuration

802.1X is a port-based network access control protocol operating at Layer 2. It authenticates users and devices attempting to access the network through the ports of LAN access devices, thereby regulating their access to network resources.

Configure Global 802.1X Authentication

Enable the 802.1X authentication function on the switch.

Steps

1. Click **Configuration** -> **Security Configuration** -> **802.1X** -> **Global Configuration**.

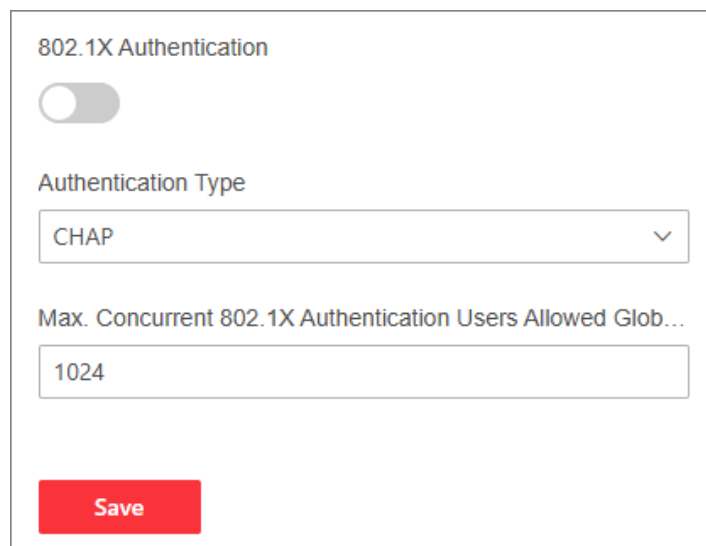


Figure 5-105 Configure Global 802.1x Authentication

2. Enable **802.1X Authentication**.
3. Select the authentication type.

CHAP (Challenge Handshake Authentication Protocol)

CHAP is a three-way handshake authentication protocol. It transmits only the username—not the password—within RADIUS packets. Compared to other methods, CHAP offers stronger security and better confidentiality, making it more reliable.

PAP (Password Authentication Protocol)

PAP is a two-way handshake authentication protocol that transmits passwords in plaintext as part of RADIUS packets. Due to its low security, this method is generally not recommended.

EAP (Extensible Authentication Protocol)

With EAP authentication enabled, the device does not process received EAP packets containing user authentication information. Instead, it encapsulates them directly into RADIUS packets and forwards them to the RADIUS server for authentication.



Note

PAP and CHAP are termination-based authentication methods, whereas EAP operates as a relay authentication method.

4. Set **Max. Concurrent 802.1X Authentication Users Allowed Globally.**

The value should be an integer ranging from 1 to 1024, and the default value is 1024.

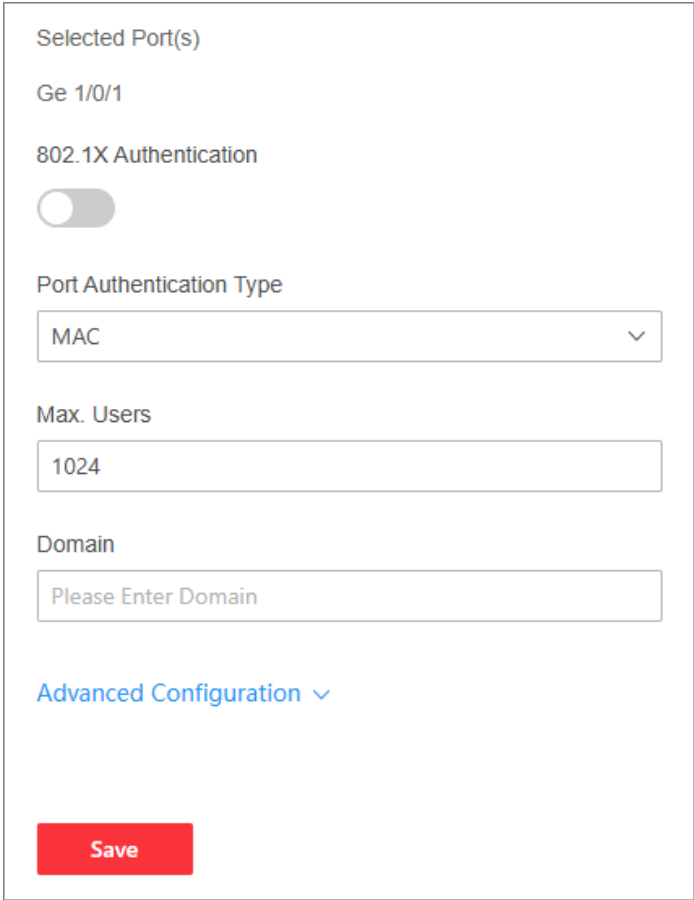
5. Click **Save.**

Configure Port 802.1X Authentication

Enable 802.1X authentication on the required ports and configure the authentication mode and other parameters of the ports if needed.

Steps

- 1. Click **Configuration** -> **Security Configuration** -> **802.1X** -> **Port 802.1X Configuration**.**
- 2. Select a port on the port panel, or click the aggregation group icon above the port panel to select the whole aggregate interface.**



Selected Port(s)

Ge 1/0/1

802.1X Authentication

☐

Port Authentication Type

MAC

Max. Users

1024

Domain

Please Enter Domain

[Advanced Configuration](#) ▾

Save

Figure 5-106 Configure Port 802.1X Authentication

4. Enable **802.1X Authentication** if required.

5. Configure 802.1X authentication parameters.

Port Authentication Type

- **MAC:** In MAC address-based access control mode, all users connected to this port need separate authentication. If one user logs off, other users can still access the network.
- **Port:** In port-based access control mode, if the first user connected to a port successfully authenticates, other users accessing through the same port can join the network without further authentication. However, once the authenticated user goes offline, all other users on that port will be denied access to network resources.

Max. Users

Set the maximum number of users allowed on the current port. Valid range: 1 to 1024. Default value: 1024.

Domain

Specify the name of the authentication domain. The string length should not exceed 32 characters.

6. Optional: Click **Advanced Configuration** to configure the advanced parameters of port 802.1X authentication.

Authorized Status

- **Authorized-force:** The port is in a force-authorized state. Users connected to the port can access network resources without authentication.
- **Forcible Unauthorization:** The port is in a force-unauthorized state. Users on the port cannot be authorized and are denied access to network resources.
- **Auto Recognize:** The port initially operates in an unauthorized state, allowing only authentication packets to be transmitted. By default, users cannot access network resources. If a user passes 802.1X authentication, access is granted.

Periodic Reauthentication

When **Periodic Reauthentication** is enabled, the system periodically initiates reauthentication for all online 802.1X users on the port.

Reauthentication Interval

The time interval between periodic reauthentication cycles for all online 802.1X users on the port. Valid range: 120 to 65,535 seconds. Default: 3600 seconds.

Online User Handshake

When **Online User Handshake** is enabled, the access device sends periodic handshake requests to detect whether users are still online.

Online Handshake Interval

The interval at which handshake request packets are sent.
Valid range: 5 to 1,024 seconds. Default: 15 seconds.

Online User Response

When **Online User Response** is enabled, users can periodically send reply packets to indicate they are still online.

EAP-Request/Identity Message Retransmission Interval

The time interval before resending an EAP-Request/Identity packet if no response is received from the client.

Valid range: 10 to 120 seconds. Default: 30 seconds.

EAP-Request/Identity Message Retransmissions

The number of retransmission attempts for EAP-Request/Identity packets.
Valid range: 1 to 6. Default: 3.

EAP-Request/MD5 Challenge Packet Retransmission Interval

The time interval before resending an EAP-Request/MD5 Challenge packet if no response is received from the client.

Valid range: 10 to 120 seconds. Default: 30 seconds.

EAP-Request/MD5 Challenge Message Retransmissions

The number of retransmission attempts for EAP-Request/MD5 Challenge packets.
Valid range: 1 to 6. Default: 3.

Unicast Trigger

When the device receives a packet from an unknown source MAC address, it proactively sends a unicast EAP-Request/Identity message to that MAC address to trigger a client response and initiate the authentication process.

Multicast Trigger

The device periodically sends multicast EAP-Request/Identity packets to trigger client responses and begin the authentication process.

Failed VLAN

Valid range: 1 to 4,094.

When the failed VLAN is configured, 802.1X users who fail authentication (e.g., due to incorrect credentials) can access resources within the failed VLAN (such as virus database updates).

Guest VLAN

Valid range: 1 to 4,094.

When the guest VLAN is configured, 802.1X users who have not yet been authenticated (e.g., without client software installed) can access resources in the guest VLAN (such as downloading client software or accessing virus databases).

Critical VLAN

Valid range: 1 to 4,094.

When the critical VLAN is configured, 802.1X users can access critical VLAN resources (e.g., virus databases or limited resources) when the authentication server times out (e.g., due to network disconnection or server failure).

Server Timeout

The timeout period for receiving a response from the authentication server.

Valid range: 60 to 200 seconds. Default: 100 seconds.

Quiet Period

After an 802.1X user fails authentication, the device silences the user for a specified duration.

During this period, the device ignores authentication requests from that user.

Valid range: 10 to 120 seconds. Default: 60 seconds.

7. Click **Save.**

The successfully configured 802.1X authentication port information will be displayed in the **Port 802.1X Authentication Info** list.

8. Optional: To edit the 802.1X authentication information of the port(s), repeat the above steps.

5.3.5 IP-MAC Binding Configuration

IP-MAC binding is a security mechanism that filters packets by maintaining a binding table on the device that maps IP addresses to corresponding MAC addresses. When a packet is received, the device looks up the binding table using the source IP address to retrieve the authorized MAC address, then compares it with the actual source MAC address in the packet's frame header. If the two addresses do not match, the packet is deemed invalid and discarded.

This feature is primarily used to prevent:

- IP address spoofing: An attacker uses their own MAC address while forging another device's IP address for unauthorized communication or data theft.
- ARP spoofing: An attacker sends forged ARP messages using another device's or the gateway's MAC address to conduct man-in-the-middle attacks or traffic hijacking.

Note

- The IP-MAC binding feature is only applicable in environments using static IP addresses. If DHCP is used to assign IP addresses, this function may not work correctly and could disrupt communication for legitimate users.
- The IP-MAC binding table is distinct from the ARP table and the MAC forwarding table. The binding table validates the authenticity of incoming packets, whereas the ARP and MAC forwarding tables are used to determine destination MAC addresses and egress interfaces during packet transmission.
- When configuring IP-MAC binding, ensure that the IP and MAC addresses are correctly paired. If the binding relationship changes, update the configuration promptly to maintain normal service operation.
- Some devices only support binding IPv4 addresses to MAC addresses. For specific capabilities, refer to the actual device documentation.

Enable IP-MAC Binding

If you enable the IP-MAC binding function, devices will compare the IP address and MAC address binding relationship of received packets. Packets that do not match the binding table will be discarded.

Steps

1. Click **Configuration -> Security Configuration -> IP-MAC Binding -> Global Configuration**.
2. Enable **IPv4 Traffic Filtering** and/or **IPv6 Traffic Filtering** to globally enable IP-MAC binding.

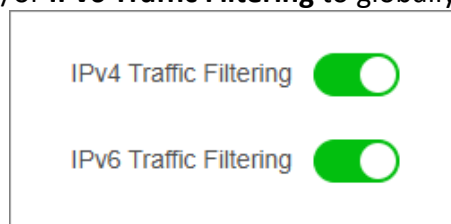


Figure 5-107 Enable IP-MAC Binding

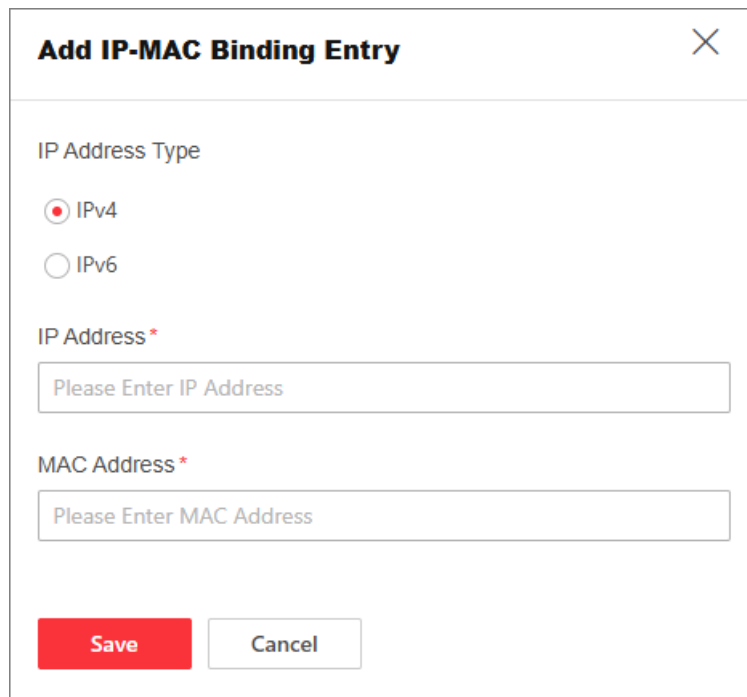
 Note

Some devices only support IPv4 traffic filtering. Please refer to the actual device interface for details.

Configure IP-MAC Binding Entry

After the IP-MAC binding table is configured, when a device receives a packet, it extracts the source IP and MAC addresses from the packet header and compares them against the entries in the binding table. If the addresses do not match any valid entry, the packet is considered invalid and discarded.

1. Click **Configuration** -> **Security Configuration** -> **IP-MAC Binding** -> **IP-MAC Binding Entry**.
2. Click **Add**.



The dialog box titled "Add IP-MAC Binding Entry" contains the following fields and controls:

- IP Address Type:** Two radio buttons, "IPv4" (selected) and "IPv6".
- IP Address *:** A text input field with the placeholder text "Please Enter IP Address".
- MAC Address *:** A text input field with the placeholder text "Please Enter MAC Address".
- Buttons:** A red "Save" button and a grey "Cancel" button.

Figure 5-108 Configure IP-MAC Binding Entry

3. Configure the parameters of the IP-MAC binding entry.

IP Address Type

The type of IP address used in an IP-MAC binding entry. Options include IPv4 or IPv6. Note that some devices only support binding IPv4 addresses to MAC addresses. Please refer to the device interface for actual support details.

IP Address

The IP address used in an IP-MAC binding entry. Some devices only support IPv4 addresses.

MAC Address

The MAC address used in an IP-MAC binding entry.



Note

IP-MAC binding follows the principle of "one IP address to one MAC address, one MAC address to multiple IP addresses":

- Each IP address can only be bound to a single MAC address.
- A MAC address can be bound to multiple IP addresses.

When modifying binding relationships:

- To change the MAC address associated with an IP address, you must first delete the original binding entry before creating a new one.
- To bind additional IP addresses to an existing MAC address, simply add a new entry. Existing binding entries for that MAC address can be retained or removed as needed.

4. Click **Save.**

5. Optional: View the configured IP address and MAC address binding relations in the list, or perform other operations.

- Click **Refresh** to update the list of IP-MAC binding entries.
- Select an IP-MAC binding entry and click  in the **Operation** column to edit the entry.
- Select an IP-MAC binding entry and click  in the **Operation** column to delete the entry.
- Select multiple IP-MAC binding entries and click **Delete** to batch delete the entries.
- Click **Clear IPv4 Entries** to batch delete all IPv4 binding entries.
- Click **Clear IPv6 Entries** to batch delete all IPv6 binding entries.
- Select IP address type or enter the IP address and MAC address, and click **Search** to filter the specified binding entries.

Configure Filter-Exempt Port

By enabling the filter-exempt port feature, you can designate specific ports on network devices to bypass IP-MAC binding filtering rules. This allows these ports to receive and forward packets normally without being restricted by IP-MAC binding policies.

Steps

- 1. Click **Configuration** -> **Security Configuration** -> **IP-MAC Binding** -> **Filter-Exempt Port**.**
- 2. Configure the port(s) to be exempted from filtering.**

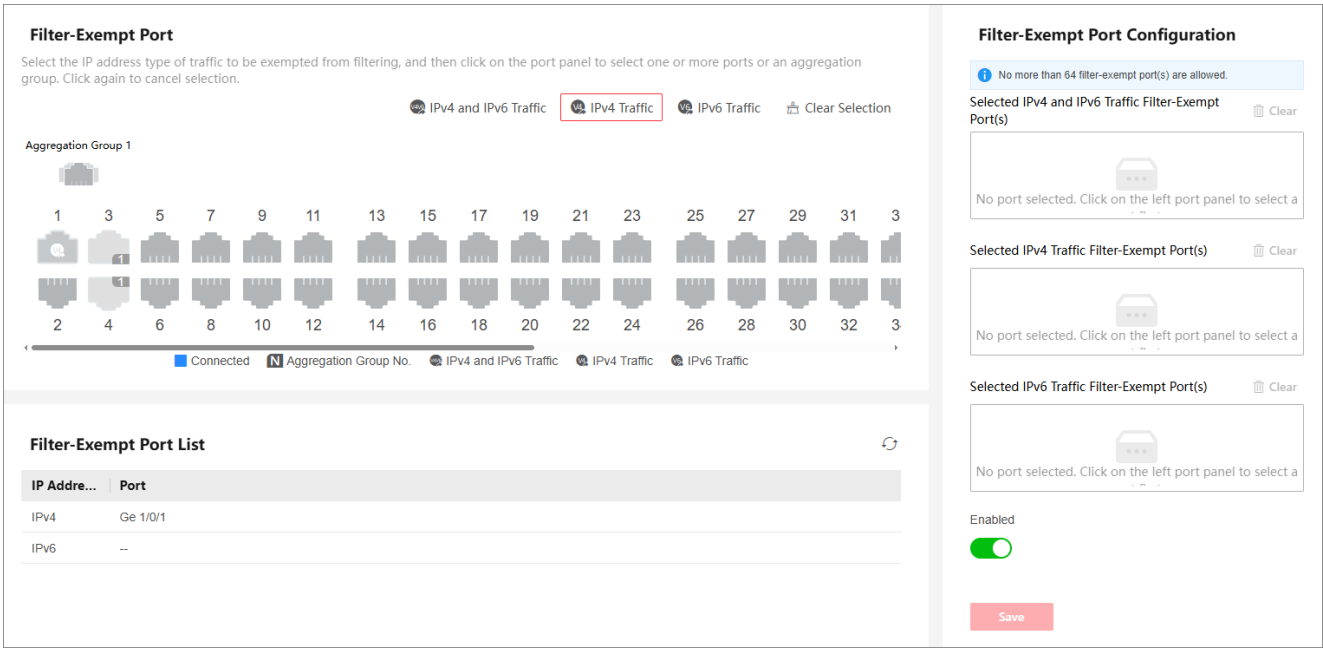


Figure 5-110 Configure Filter-Exempt Port

- Click **IPv4 and IPv6 Traffic**, **IPv4 Traffic**, or **IPv6 Traffic** to select the IP address type of traffic to be exempted from filtering.
- Select one or more ports on the port panel or click the aggregation group icon above the port panel to batch select the entire aggregate interface to add the port(s) to the list of selected IPv4 and IPv6 traffic filter-exempt port(s), Selected IPv4 traffic filter-exempt port(s), or selected IPv6 traffic filter-exempt port(s).

Note

Select the IP address type of traffic to be exempted from filtering first, and then select ports. You can directly select one or more ports on the port panel or click the aggregation group icon above the port panel to batch select the entire aggregate port. If you need to configure other IP address types of traffic to be exempted from filtering, change to the other IP address type first, and then select ports.

3. Enable IP-MAC binding filter exemption for the selected ports. P+MAC binding from filtering.

Note

No more than 64 filter-exempt ports are allowed.

4. Click **Save**.

The successfully configured ports will be displayed in the **Filter-Exempt Port** list.

5.3.6 DHCP Snooping Configuration

DHCP Snooping is a security feature of DHCP that can block illegal DHCP servers on the network.

Configure Global DHCP Snooping

Enable global DHCP Snooping first. Then you can proceed with DHCP Snooping configuration for specific ports.

Steps

1. Go to **Configuration -> Security Configuration -> DHCP Snooping -> Global Configuration**.

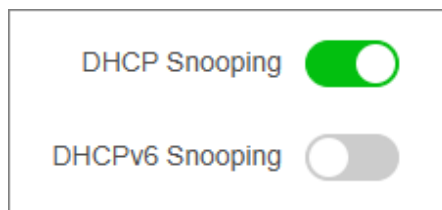


Figure 5-111 Configure Global DHCP Snooping

2. Enable **DHCP Snooping** and/or **DHCPv6 Snooping** globally as needed.

Configure Port DHCP Snooping

Port DHCP Snooping allows you to configure the DHCP Snooping feature individually on each device port as needed.

Before You Start

Enable global DHCP snooping first.

Steps

1. Go to **Configuration -> Security Configuration -> DHCP Snooping -> Port Configuration**.

Selected Port(s)

+ Add All

Clear

No port selected. Click on the left port panel to select a port first.

Type

☒ IPv4

☐ IPv6

DHCP Snooping

☒

Set as Trusted Port

☐

MAC Address Check

☐

Anti-Request Packet Attack Check

☐

DHCP Message Blocking

☐

Max. Learned Entries

Please Enter Max. Learned Entries

Save

Figure 5-112 Configure Port DHCP Snooping

2. Select one or more ports on the port panel or click the aggregation group icon above the port panel to batch select the entire aggregate interface.

 Note

- You can click **Add All** to batch select all Ethernet ports and aggregation groups, or click **Clear** to deselect the selected port(s).
- The member ports of an aggregation group are not supported.

3. Configure the DHCP snooping parameters.

Type

Select IPv4 or IPv6 to specify whether the port processes DHCPv4 or DHCPv6 packets. Some devices only support IPv4—please refer to the device interface for supported options.

DHCP Snooping

Enable or disable the DHCP Snooping function for the selected port(s).

Set as Trusted Port

When this feature is enabled, the port is configured as trusted and will forward received DHCP messages normally.

MAC Address Check

When this feature is enabled, the DHCP server checks whether the chaddr field in the received DHCP request matches the source MAC address in the Ethernet frame. If they match, the packet is considered valid and processed further; otherwise, it is discarded.

Anti-Request Packet Attack Check

When this feature is enabled, the system blocks Request, Decline, or Release packets that have the same IP address as an existing entry but differ in MAC address, VLAN, or ingress port.

DHCP Message Blocking

When this feature is enabled, all DHCP request-direction packets received on the port are discarded.

Max. Learned Entries

Set the maximum number of DHCP Snooping binding entries that the port can learn. Valid range: 1 to 1024.

4. Click **Save**.

The information of ports on which DHCP Snooping has been successfully configured will be displayed in the **Port Configuration Info** list.

5. Optional: To edit the configuration information, repeat the above steps.

Configure VLAN DHCP Snooping

Before You Start

Enable global DHCP snooping first.

Steps

1. Go to **Configuration -> Security Configuration -> DHCP Snooping -> Global VLAN Configuration**.
2. Configure VLAN DHCP Snooping.
 - 1) Click **Add**.

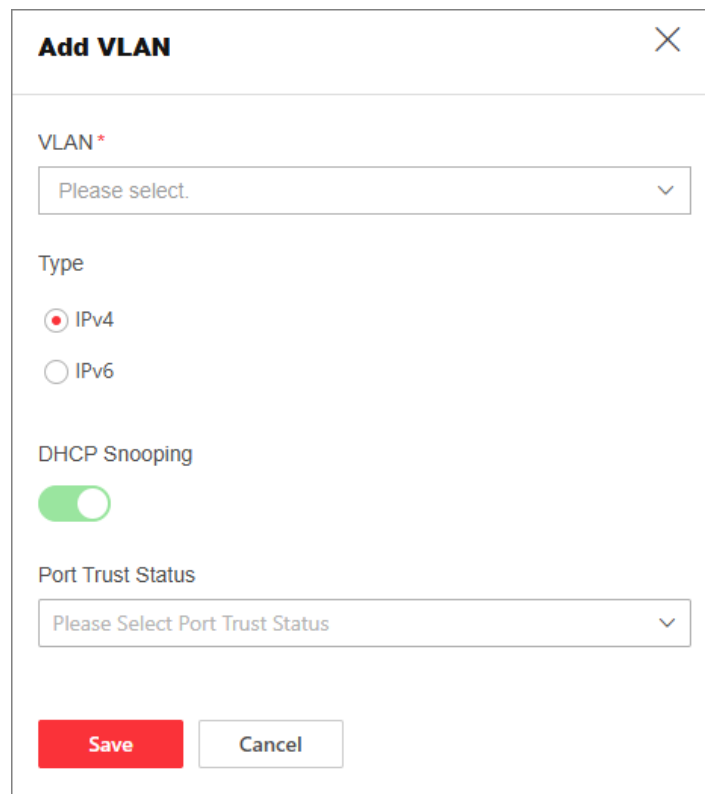
The image shows a web-based configuration dialog box titled "Add VLAN" with a close button (X) in the top right corner. The dialog contains several fields: a "VLAN *" dropdown menu with the text "Please select." and a downward arrow; a "Type" section with two radio buttons, "IPv4" (which is selected) and "IPv6"; a "DHCP Snooping" section with a green toggle switch that is turned on; and a "Port Trust Status" dropdown menu with the text "Please Select Port Trust Status" and a downward arrow. At the bottom of the dialog are two buttons: a red "Save" button and a white "Cancel" button with a grey border.

Figure 5-113 Configure VLAN DHCP Snooping

- 2) Select a pre-configured VLAN.
- 3) Select IPv4 or IPv6 to specify whether the VLAN processes DHCPv4 or DHCPv6 packets.
- 4) Enable or disable **DHCP Snooping** for the selected VLAN.
- 5) Set port(s) or aggregation group(s) from the **Port Trust Status** drop-down list to set them as trusted port(s).
- 6) Click **Save**.

The information of VLANs to which DHCP Snooping has been successfully configured will be displayed in the VLAN configuration info list.

3. Optional: Select a VLAN and click  to edit the VLAN DHCP Snooping configuration.

- 4. Optional: Select a VLAN and click  to delete VLAN DHCP Snooping configuration.
- 5. Optional: Enter the VLAN ID and click **Search** to filter specified VLANs with DHCP Snooping configured.

View DHCP Snooping Binding Entries

- Steps
- 1. Go to **Configuration -> Security Configuration -> DHCP Snooping -> Binding Table**.

Type

IP Address

MAC Address

Port Name

All

Please Enter IP Address

Please Enter MAC Address

All

Search

Reset

Refresh

IP Address	Type	MAC Address	VLAN ID	Port	Remaining Lease Time
------------	------	-------------	---------	------	----------------------

Figure 5-114 View DHCP Snooping Binding Entries

- 2. View the existing DHCP snooping binding entries.
- 3. Optional: Select IP address type and port, or enter the IP address and MAC address, and click **Search** to filter specified DHCP snooping binding entries.

5.3.7 Security Protection Configuration

You can enable the security protection function globally, designate specific ports as security ports, and authorize connected terminal devices to ensure that only approved terminals can transmit data through these protected ports.

Global Configuration

- 1. Click **Configuration -> Security Configuration -> Security Protection -> Global Configuration**.
- 2. Enable **Security Protection** globally.

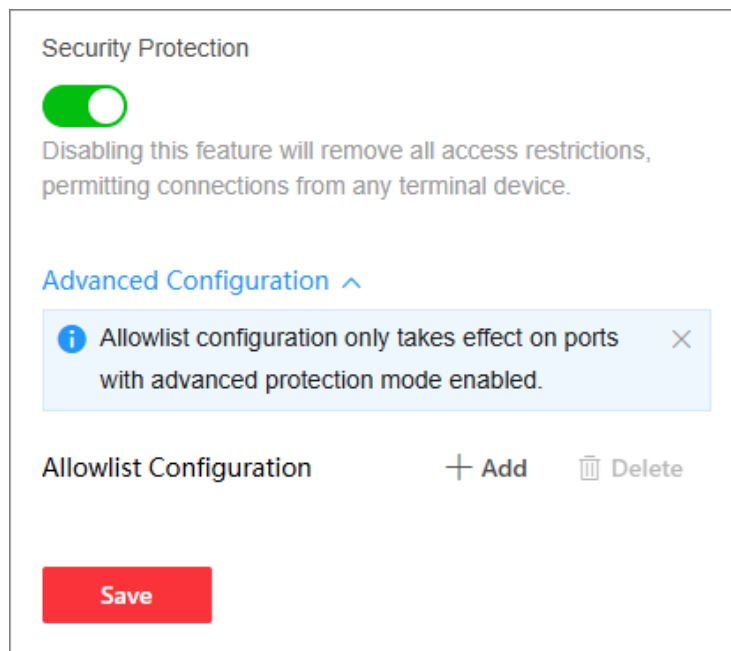


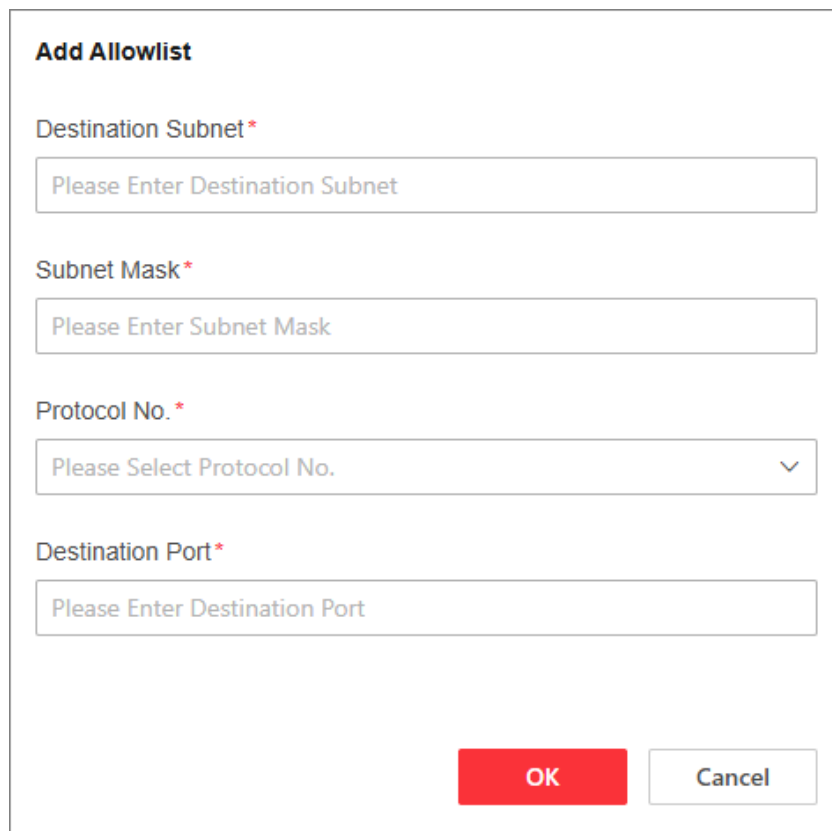
Figure 5-115 Enable Security Protection Globally

 Note

Security protection is enabled by default. Disabling this feature will remove all port protection settings and permit unrestricted terminal access to the system. Please proceed with caution.

3. Configure the allowlist.

- a. Click **Advanced Configuration** -> **Add**.

**Figure 5-116** Configure Allowlist

- b. Set the parameters.

Destination Subnet

Specify the IPv4 address in the allowlist. Access control based on IPv4 addresses enables precise management of network permissions, allowing or restricting access for specific devices.

Subnet Mask

Set the subnet mask for the IPv4 address in the allowlist. Used in conjunction with the IP address, it helps define a range of IP addresses that share the same network prefix.

Protocol No.

Specify the protocol number in the allowlist to indicate the type of network protocol allowed or restricted. Options include: UDP, TCP, and ICMP.

Destination Port

Define the destination port in the allowlist to specify the application or service for which access is permitted or denied. The destination port refers to the port used by the receiving application at the transport layer (e.g., TCP or UDP). Configuration of the destination port is only supported when the protocol is set to UDP or TCP. Valid values range from 0 to 65535.

- c. Click **OK**.

- d. Click **Save** to save the allowlist configuration.

4. Optional: Repeat the above steps to add more allowlist(s).

- Optional: Select one or more allowlist(s) and click **Delete** to delete the allowlist(s).

Port Configuration

- Click **Configuration -> Security Configuration -> Security Protection -> Port Configuration**.



Figure 5-117 Port Configuration Security Protection

- Select one or more ports on the port panel.

Note

- You can click **Add All** to batch select all Ethernet ports, or click **Clear** to deselect the selected port(s).
 - The member ports of an aggregation group are not supported.
- Set the security protection type for the selected port(s) to **No protection**, **General**, or **Advanced**.

Note

To configure and activate an allowlist, it is recommended to select advanced protection.

- Click **Save**.
- Optional: Select one or more ports to which terminal device(s) are connected in the **Terminal Authorization** list and click **Authorize** to batch enable terminal authorization. Alternatively, toggle on **Terminal Authorization** for the ports to manually enable terminal authorization.

Note

This ensures that only authorized terminals can forward data through these ports. After authorization, the ports will be bound to the connected terminal device(s). To cancel authorization, click **Cancel Authorization** or toggle off **Terminal Authorization** to disable terminal authorization.

5.3.8 IPSG Configuration

IP Source Guard (IPSG) is a Layer 2 interface-based IP address filtering technology. It filters and controls packets received by an interface, typically deployed on access-layer interfaces to prevent unauthorized users from transmitting packets, thereby restricting illegitimate use of network resources (e.g., malicious hosts spoofing legitimate user IP addresses to gain network access).

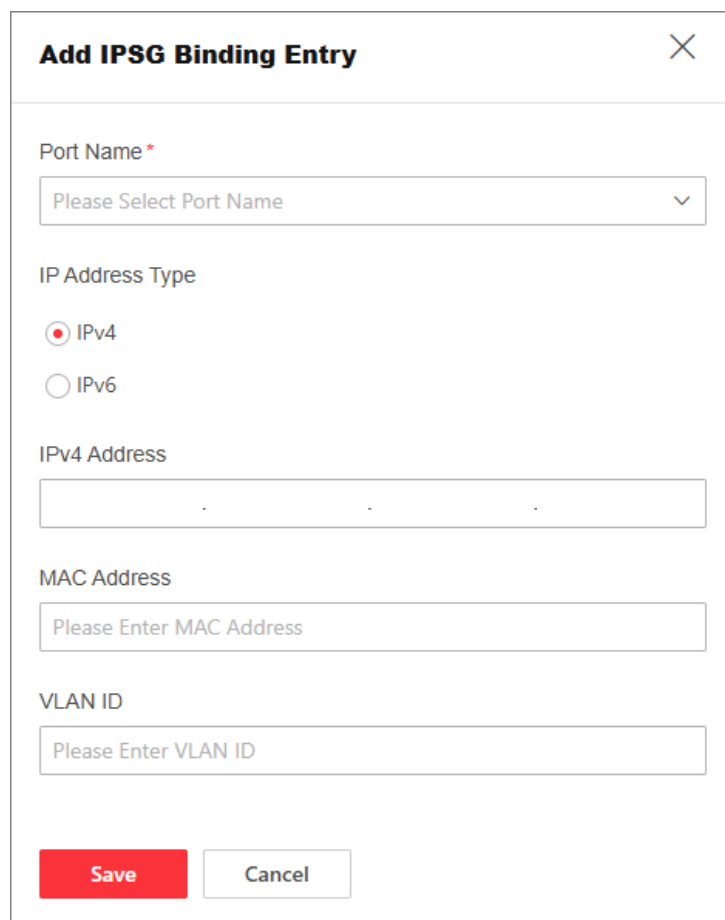
Create Static Binding Entry

The IPSG binding table includes both dynamic and static entries. The IPSG module filters IPv4 packets received by an interface based on these binding entries. Packets that match an entry are forwarded normally, while those that do not match are discarded.

- Dynamic bindings are automatically generated through the DHCP Snooping feature. When DHCP Snooping is enabled on a switch, it monitors DHCP interactions, records the IP and MAC addresses obtained by clients, and adds this information to the dynamic binding table.
- Static bindings are manually configured entries that bind an IP address, MAC address, or a combination of these parameters to a specific port. These entries are only effective on the port where they are configured. A packet is forwarded normally only if its IP address, MAC address, and incoming VLAN ID exactly match all parameters specified in the static binding entry on that port.

Steps

1. Click **Configuration** -> **Security Configuration** -> **IPSG** -> **Binding Entry**.
2. Click **Add**.
3. Configure the parameters as needed.



The image shows a web-based dialog box titled "Add IPSG Binding Entry" with a close button (X) in the top right corner. The dialog contains several input fields and radio buttons. The "Port Name" field is a dropdown menu with the placeholder text "Please Select Port Name". Below it, the "IP Address Type" section has two radio buttons: "IPv4" (which is selected) and "IPv6". The "IPv4 Address" field is a text input with a placeholder "Please Enter IPv4 Address". The "MAC Address" field is a text input with a placeholder "Please Enter MAC Address". The "VLAN ID" field is a text input with a placeholder "Please Enter VLAN ID". At the bottom, there are two buttons: a red "Save" button and a white "Cancel" button.

Figure 5-119 Configure Static Binding Entry

Port Name

Select the port, aggregation group, or **Any** to which the static binding entry will be applied.

IP Address Type

Choose between IPv4 or IPv6. Note that some devices only support IPv4 static binding entries; please refer to the actual interface for available options.

IPv4 Address

Specify the IPv4 address for the static binding entry. It must be a valid IPv4 address belonging to Class A, B, or C. Addresses such as 127.x.x.x and 0.0.0.0 are not allowed.

IPv6 Address

Specify the IPv6 address for the static binding entry. It must be a valid global unicast or unique local address (e.g., 2001:db8::1 or fd00::1). Addresses such as ::1, ::, multicast addresses, and unspecified addresses are prohibited.

MAC Address

Specify the MAC address for the static binding entry. It must be a valid MAC address and cannot be all zeros, all F's, or a multicast MAC address.

VLAN ID

Specify the VLAN ID of the incoming interface for the static binding entry. The VLAN ID ranges from 1 to 4094.



Note

- The current device supports up to 256 IPSG binding entries in total (including both IPv4 and IPv6 static binding entries).
- IP address, MAC address, and VLAN ID can be configured in any combination. However, at least one of the IPv4/IPv6 address or MAC address must be specified; they cannot both be left empty. If a parameter is not specified, it is treated as "Any".

4. Click **Save**.

The successfully configured static binding entries of IPSG will be displayed in the list.

5. Optional: Select port name, IP address type, or entry type, or enter the IP address, MAC address, or VLAN ID, and click **Search** to filter the specified IPv4 or IPv6 binding entries.

Configure Source Address Check

For dynamic binding entries, IPSG check items must be configured. If only static binding entries are used to filter packets on an interface, the interface will filter packets based on the configured static binding parameters, and this function does not need to be enabled.

Steps

1. Click **Configuration** -> **Security Configuration** -> **IPSG** -> **Source Address Check**.
2. Click **Add**.
3. Set the parameters as needed.

Figure 5-120 Configure Source Address Check

Port

Select the port to be configured with IPSG check items. You may choose any physical port, aggregation group, or VLAN interface.

IP Address Type

Choose between IPv4 or IPv6. Note that some devices only support IPv4 Source Guard check items; please refer to the actual interface for supported options.

IP Address Check

Enable IP address check for packets received on the interface. A packet is forwarded normally only if its source IP address matches the IP address parameter in a dynamic binding entry automatically generated by DHCP Snooping. Otherwise, the packet is discarded.

MAC Address Check

Enable MAC address check for packets received on the interface. A packet is forwarded normally only if its source MAC address matches the MAC address parameter in a dynamic binding entry automatically generated by DHCP Snooping. Otherwise, the packet is discarded.

VLAN Check

Enable ingress VLAN check for packets received on the interface. A packet is forwarded normally only if its ingress VLAN matches the VLAN parameter in a dynamic binding entry automatically generated by DHCP Snooping. Otherwise, the packet is discarded. This parameter is not applicable to VLAN interfaces.

Note

- By default, IP address, MAC address, and VLAN checks are all enabled.
- At least one of the IP address check or MAC address check must be enabled.

4. Click **Save**.

Ports with successfully configured IPSG check items will be displayed in the list.

5. Optional: Click to delete the configured IPSG check items of the port.

6. Optional: Click to edit the configured IPSG check items of the port.

Configure Filter-Exempt VLAN

By default, IPv4 packets not matching any configured binding entry are discarded after IPSG is enabled on an interface. To prevent legitimate user traffic from being dropped due to unmatched entries, the IPSG VLAN filtering exemption feature can be configured. When this feature is enabled, IPv4 packets meeting the exemption condition bypass IPSG inspection and are allowed to pass through the interface directly.

Steps

1. Click **Configuration** -> **Security Configuration** -> **IPSG** -> **Filter-Exempt VLAN**.
2. Click **Add**.

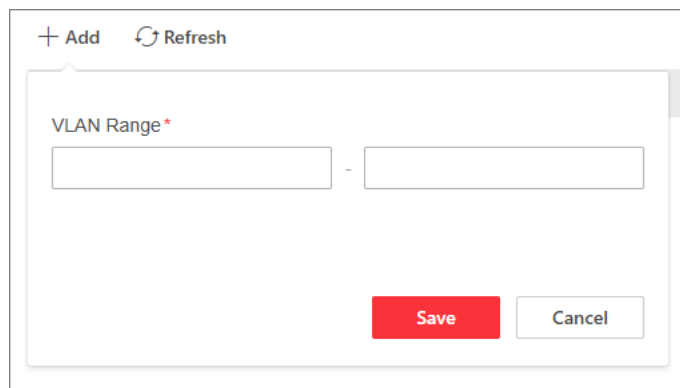


Figure 5-121 Configure Filter-Exempt VLAN

3. Enter the start VLAN ID and end VLAN ID to set the filter-exempt VLAN range.
4. Click **Save**.

5.3.9 Port Security Configuration

Port security is a MAC address-based access control mechanism that extends 802.1X and MAC address authentication. It restricts unauthorized devices from accessing the network by validating the source MAC address of incoming frames and inspecting the destination MAC address of outgoing frames. The core functionality allows administrators to define multiple security policies, enabling devices to recognize authorized MAC addresses for effective network management. When illegal packets are detected, port security triggers predefined actions to mitigate security threats according to configured rules.

Configure Port Security

Steps

1. Click **Configuration** -> **Security Configuration** -> **Port Security** -> **Port Security** -> **Port Security Configuration**.

Selected Port(s)

+ Add All

Clear

No port selected. Click on the left port panel to select a port first.

Port Security

☒

MAC Address Limit

1

Sticky MAC

☐

Protection Action

Protect

Save

Figure 5-122 Configure Port Security

2. Select one or more ports on the port panel.



Note

- You can click **Add All** to batch select all Ethernet ports, or click **Clear** to deselect the selected port(s).
- The member ports of an aggregation group are not supported.
- Up to 52 ports can be selected.

3. Enable **Port Security**.

4. Set the parameters as needed.

MAC Address Limit

Specifies the maximum number of secure MAC addresses allowed by port security on an interface. For example, if the MAC address limit is set to 5 on a port, that port can only establish connections with up to 5 devices using different MAC addresses. If a device with a 6th unique MAC address attempts to connect, the port security mechanism will take action based on the preconfigured protection mode.

The value ranges from 1 to 1024, and the default value is 1.

Sticky MAC

When this feature is enabled, the port automatically learns the MAC addresses of connected devices and converts them into secure MAC addresses. These addresses are stored in the device's running configuration. Unlike dynamically learned MAC addresses, Sticky MAC entries remain effective after a device reboot—provided the configuration is not cleared.

Protection Action

When port security detects illegal packets or violations of the security policy, it triggers a predefined protection action. Available options include: **Protect** and **Error-Down**.

- **Protect**: In this mode, the device discards packets from illegal MAC addresses without generating log entries. The port continues normal operation, and communication from authorized MAC addresses is unaffected.
- **Error-Down**: In this mode, upon detecting packets from an unauthorized MAC address, the device immediately shuts down the port and sets its status to error-disabled. The port stops forwarding all traffic, and all connected devices lose communication.

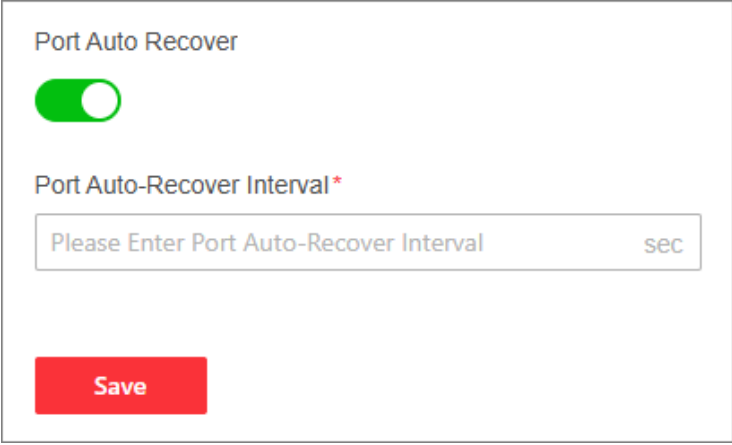
5. Click **Save**.

The successfully configured ports will be displayed in the **Port Security Info** list.

6. Optional: Select the port that need to be restored manually and click to restore it from exception status to normal working status.

7. Optional: Configure the port auto-recovery function.

1) Click **Global Configuration**.



Port Auto Recover

☒

Port Auto-Recover Interval *

Please Enter Port Auto-Recover Interval sec

Save

Figure 5-123 Configure Port Auto Recover

2) Enable **Port Auto Recover**.

 Note

After you enable this function, when a port is in an exception status due to security policy violations (such as devices with illegal MAC addresses connected to the port, and actions such as port closure triggered), the port can automatically return to normal operation without manual intervention.

3) Set the port auto-recovery interval.

 Note

The port auto-recovery interval refers to the time duration between when a port enters an abnormal state (e.g., err-disabled) due to a security policy violation and when it automatically restarts and resumes normal operation under the port security mechanism. The value ranges from 30 to 86,400 seconds.

4) Click **Save**.

Configure Secure MAC Address

In network environments, MAC addresses uniquely identify devices. Configuring secure MAC addresses is a key port security mechanism that enhances network protection by defining which MAC addresses are authorized to communicate on a specific port. Once a secure MAC address is configured on a port, only devices whose source MAC addresses matches the permitted entries can transmit data through that port. Traffic from unauthorized MAC addresses will be restricted by port security—such as being discarded or triggering protective actions.

Secure MAC addresses are categorized into three types:

- Dynamic secure MAC address: Automatically learned by the port.
- Static secure MAC address: Manually configured by network administrators.
- Sticky MAC address: Converted from dynamically learned addresses after the Sticky MAC feature is enabled, and retained across device reboots.

Before You Start

- Port security is enabled.
- The maximum number of allowed MAC addresses for port security has been set.
- The port must be configured to allow the specified VLAN or be a member of that VLAN, and the VLAN must already exist.

Steps

1. Click **Configuration** -> **Security Configuration** -> **Port Security** -> **Secure MAC Address**.
2. Click **Add**.
3. Set the parameters as needed.

Figure 5-124 Configure Secure MAC Address

Port Name

Select a physical port to configure a secure MAC address.

VLAN ID

Specifies the VLAN ID to which the secure MAC address belongs. The value ranges from 1 to 4094. In secure MAC address configuration, the VLAN ID determines the virtual network scope of the secure MAC address.



Note

The VLAN ID must already exist.

MAC Address Type

Specifies the secure MAC address type as **Static** or **Sticky**.

- **Static:** Manually configured by a network administrator. These addresses explicitly identify authorized devices permitted to communicate on a specific port and VLAN. In environments requiring strict access control—such as data centers in financial institutions—server MAC addresses are typically configured statically. This ensures only pre-approved servers can access the network, preventing unauthorized connections and protecting sensitive data.
- **Sticky:** When Sticky MAC is enabled, the port automatically learns the MAC addresses of connected devices, converts them into secure MAC addresses, and stores them in the device's running configuration. This method suits environments with frequent device changes or additions, as it adapts automatically and reduces administrative overhead. For example, in a small office network, when a new employee's computer connects to a switch port for the first time, the port automatically learns the MAC address and adds it as a secure MAC address.

MAC Address

Enter the MAC address to be configured as a secure MAC address.

Format: XX:XX:XX:XX:XX:XX

4. Click **Save**.

The successfully configured secure MAC address(es) will be displayed in the list.

5. Optional: Delete the configured secure MAC address(es).

- Select a secure MAC address and click  in the **Operation** column to delete it.
- Select multiple MAC addresses and click **Delete** to batch delete them.
- Click **Clear Static Secure MAC Addresses**, **Clear Dynamic Secure MAC Addresses**, or **Clear Sticky MAC Addresses** to batch delete all static secure MAC addresses, dynamic secure MAC addresses, or sticky MAC addresses.

6. Optional: Enter the VLAN ID or select port and MAC address type, and then click **Search** to filter the specified secure MAC address(es).

Chapter 6 Device Diagnosis

6.1 Network Diagnosis

The device supports network connectivity assessment to determine if the network is functioning properly and quickly locate issues. It provides two network diagnostic tools: Ping and Trace.

- Ping is used to verify host reachability.
- Trace (Traceroute) can be used to further test IP network connectivity and diagnose network faults when communication is interrupted.

6.1.1 Configure Ping

1. Click **Diagnosis -> Diagnostic Tool -> Ping**.
2. Select **Domain Name**, **IPv4**, or **IPv6** as the Ping target, and configure the relevant parameters as prompted.
 - Ping Domain Name

Ping

☒ Domain Name

☐ IPv4

☐ IPv6

*Destination Domain Name

Please Enter Destination Domain Name

Ping with Custom Parameters

☒

Number of Packets

5

Load Length

64

B

Timeout

5000

ms

Outbound Interface

Please Select Outbound Interface

▼

Takes effect when the domain name is bound to an IPv6 address.

Start

Figure 6-1 Ping Domain Name

Destination Domain Name

Set the domain name of the target host to test connectivity using the Ping command. The domain name must be 1 to 64 characters long. Before pinging a domain name, ensure that the device is configured with the correct DNS server.

Ping with Custom Parameters

Enable or disable the “Ping with Parameters” function as needed. A standard Ping command simply sends an ICMP (Internet Control Message Protocol) request to the target host and waits for a response. In contrast, Ping with Parameters allows users to perform more granular network testing by customizing settings such as the number of requests, packet size, etc.

Number of Packets

Set the number of ICMP request packets sent by the Ping command. The value ranges from 1 to 64, and the default value is 5.

Load Length

Set the length of the data portion in the ICMP request packet sent by the Ping command. An ICMP packet consists of a header and a data section—the load length indicates the size (in bytes) of the data section in the ICMP packet. The value ranges from 20 to 10,000 bytes, and the default value is 64 bytes.

Timeout

Set the maximum time the Ping command waits for a response from the target host. If no response is received within this period, the packet is considered lost. The value ranges from 1 to 10,000 ms, and the default value is 5,000 ms.

Outbound Interface

Specify the network interface used to send Ping requests. On devices with multiple interfaces, this setting determines which interface the packets are sent from. Supported options include the management port, physical ports, aggregate interfaces, VLAN interfaces, and Loopback interfaces.



Note

The outbound interface setting only takes effect when the domain name is bound to an IPv6 address.

- Ping IPv4 Address

Ping ☐ Domain Name ☒ IPv4 ☐ IPv6

*Destination IP Address

Ping with Custom Parameters ☒

Number of Packets

Load Length B

Source Address

TTL

Timeout ms

Start

Figure 6-2 Ping IPv4 Address

Destination IP Address

Set the IPv4 address of the target host whose connectivity you want to test using the Ping command.

Ping with Custom Parameters

Enable or disable the “Ping with Parameters” function as needed. A standard Ping command simply sends an ICMP request to the target host and waits for a response. In contrast, Ping with Parameters allows users to perform more granular network testing by customizing settings such as the number of requests, packet size, etc.

Number of Packets

Set the number of ICMP request packets sent by the Ping command. The value ranges from 1 to 64, and the default value is 5.

Load Length

Set the length of the data portion in the ICMP request packet sent by the Ping command. An ICMP packet consists of a header and a data section—the load length indicates the size (in bytes) of the data section in the ICMP packet. The value ranges from 20 to 10,000 bytes, and the default value is 64 bytes.

Source Address

Specify the IPv4 address of the device sending the Ping request. On devices with multiple IPv4 addresses, this setting determines which address is used as the source of the Ping request.

TTL

Set the Time to Live (TTL) value, which defines the maximum number of hops (routers) that the ICMP packet can traverse through the network. The value ranges from 1 to 255, and the default value is 255.

For example, when a device sends a Ping packet, it sets an initial TTL value. Each router that forwards the packet decrements the TTL by 1. If the TTL reaches 0, the router discards the packet and sends an ICMP Time-Exceeded message back to the source device.

Timeout

Set the maximum time the Ping command waits for a response from the target host. If no response is received within this period, the packet is considered lost. The value ranges from 1 to 10,000 ms, and the default value is 5,000 ms.

- Ping IPv6 Address

Ping ☐ Domain Name ☐ IPv4 ☒ IPv6

*Destination IP Address

Ping with Custom Parameters ☒

Number of Packets

Load Length B

Source Address

Timeout ms

Outbound Interface

Start

Figure 6-3 Ping IPv6 Address

Destination IP Address

Set the IPv6 address of the target host whose connectivity you want to test using the Ping command.

Ping with Custom Parameters

Enable or disable the “Ping with Parameters” function as needed. A standard Ping command simply sends an ICMP request to the target host and waits for a response. In contrast, Ping with Parameters allows users to perform more granular network testing by customizing settings such as the number of requests, packet size, etc.

Number of Packets

Set the number of ICMP request packets sent by the Ping command. The value ranges from 1 to 64, and the default value is 5.

Load Length

Set the length of the data portion in the ICMP request packet sent by the Ping command. An ICMP packet consists of a header and a data section—the load length indicates the size (in bytes) of the data section in the ICMP packet. The value ranges from 20 to 10,000 bytes, and the default value is 64 bytes.

Source Address

Specify the IPv6 address of the device sending the Ping request. On devices with multiple IPv6 addresses, this setting determines which address is used as the source of the Ping request.

Timeout

Set the maximum time the Ping command waits for a response from the target host. If no response is received within this period, the packet is considered lost. The value ranges from 1 to 10,000 ms, and the default value is 5,000 ms.

Outbound Interface

Specify the network interface used to send Ping requests. On devices with multiple interfaces, this setting determines which interface the packets are sent from. Supported options include the management port, physical ports, VLAN interfaces, and Loopback interfaces.

3. Click **Start**.

Ping Result

```
PING [redacted] : 64 data bytes
Reply from [redacted] : bytes=64 time=3ms TTL=199 icmp_seq=1
Reply from [redacted] : bytes=64 time=4ms TTL=199 icmp_seq=2
Reply from [redacted] : bytes=64 time=2ms TTL=199 icmp_seq=3
Reply from [redacted] : bytes=64 time=3ms TTL=199 icmp_seq=4
Reply from [redacted] : bytes=64 time=3ms TTL=199 icmp_seq=5
PING Statistics for [redacted]
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 2/3/4
```

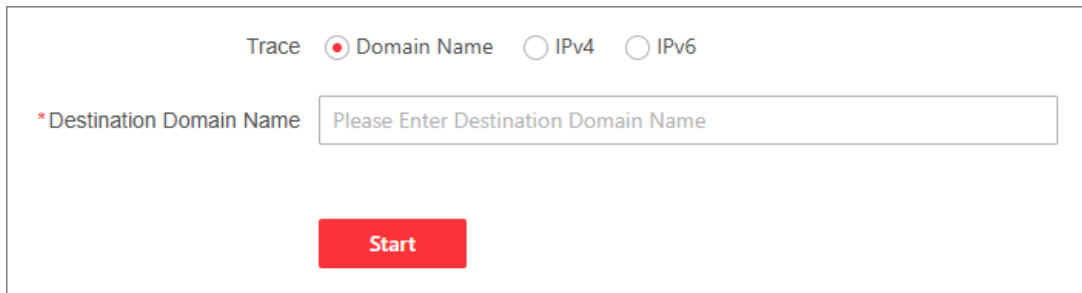
Figure 6-3 View Ping Results **Note**

You can click **Stop** at any time to stop the Ping process manually.

6.1.2 Configure Trace

1. Click **Diagnosis -> Diagnostic Tool -> Trace**.
2. Select **Domain Name**, **IPv4**, or **IPv6** as the Trace target, and configure the relevant parameters as prompted.

- Trace Domain Name



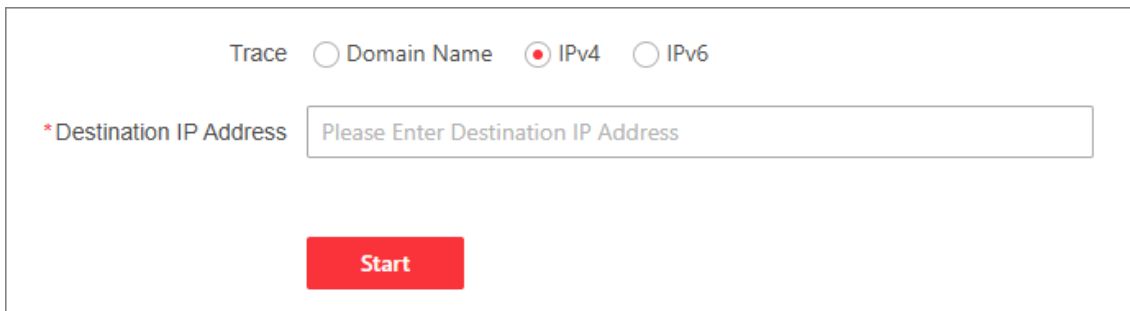
The screenshot shows a web interface for tracing a domain name. At the top, there is a 'Trace' label followed by three radio buttons: 'Domain Name' (which is selected), 'IPv4', and 'IPv6'. Below this, there is a label '*Destination Domain Name' followed by a text input field containing the placeholder text 'Please Enter Destination Domain Name'. At the bottom of the form is a red button labeled 'Start'.

Figure 6-4 Trace Domain Name

Destination Domain Name

Set the domain name of the target host whose packet transmission path you want to trace using the Trace tool. The domain name must be 1 to 64 characters long.

- Trace IPv4 Address



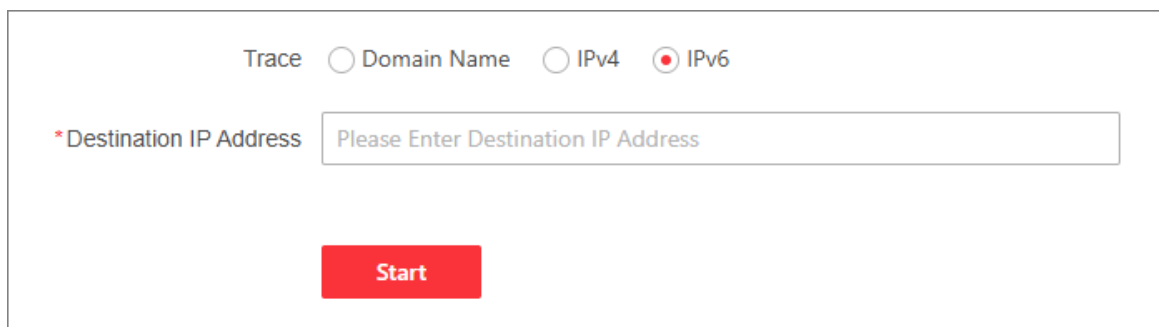
The screenshot shows a web interface for tracing an IPv4 address. At the top, there is a 'Trace' label followed by three radio buttons: 'Domain Name', 'IPv4' (which is selected), and 'IPv6'. Below this, there is a label '*Destination IP Address' followed by a text input field containing the placeholder text 'Please Enter Destination IP Address'. At the bottom of the form is a red button labeled 'Start'.

Figure 6-5 Trace IPv4 Address

Destination IP Address

Set the IPv4 address of the target host whose packet transmission path you want to trace using the Trace tool.

- Trace IPv6 Address



The screenshot shows a web interface for tracing an IPv6 address. At the top, there is a 'Trace' label followed by three radio buttons: 'Domain Name', 'IPv4', and 'IPv6' (which is selected). Below this, there is a label '*Destination IP Address' followed by a text input field containing the placeholder text 'Please Enter Destination IP Address'. At the bottom of the form is a red button labeled 'Start'.

Figure 6-6 Trace IPv6 Address

Destination IP Address

Set the IPv6 address of the target host whose packet transmission path you want to trace using the Trace tool.

3. Click **Start**.

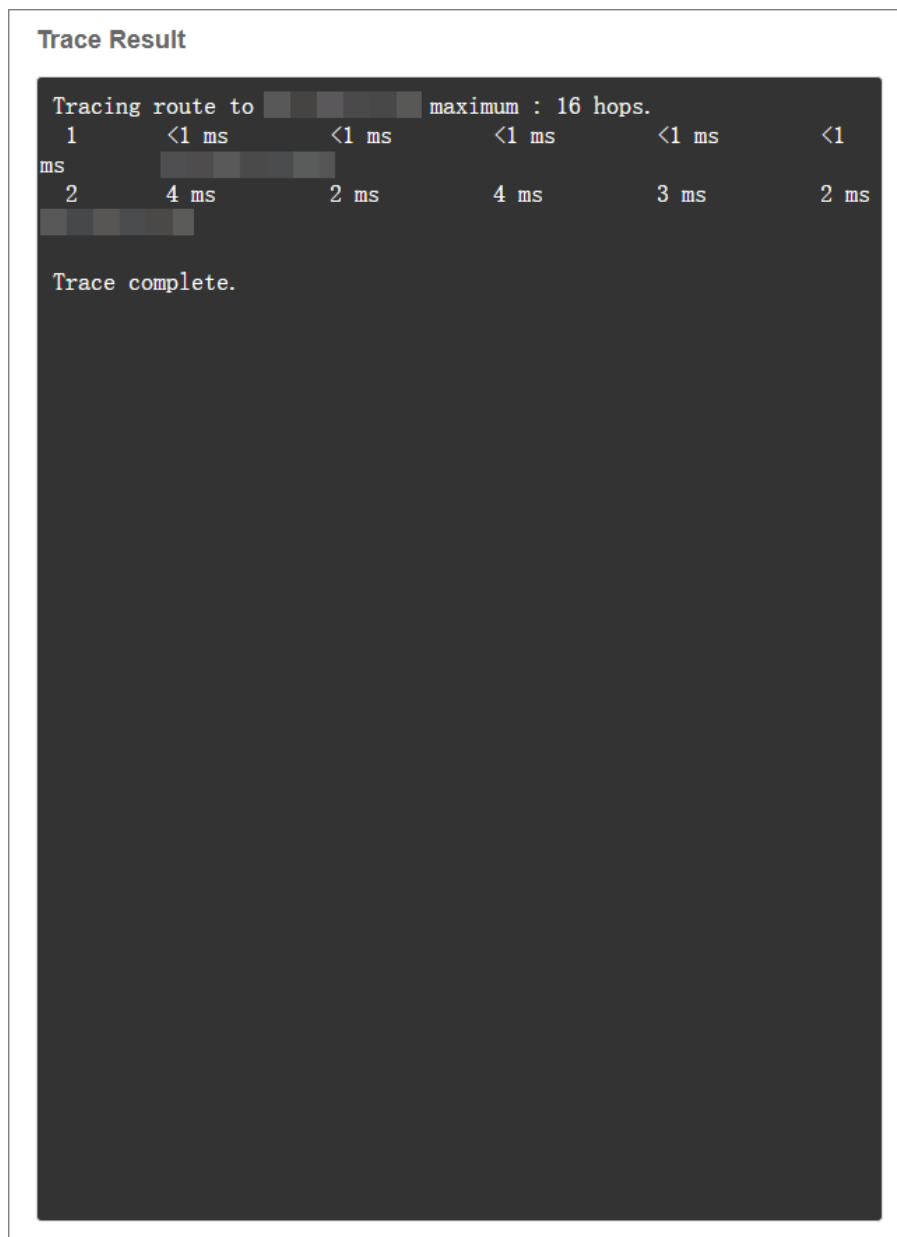


Figure 6-7 View Trace Results

 Note

You can click **Stop** at any time to stop the Trace process manually.

6.2 Cable Detection

You can monitor and check the cable connection status for each port.

Go to **Diagnosis > Cable Detection**, select the desired port on the port panel, and click **Detect**. The cable detection results will be displayed in the **Detection Result** area.

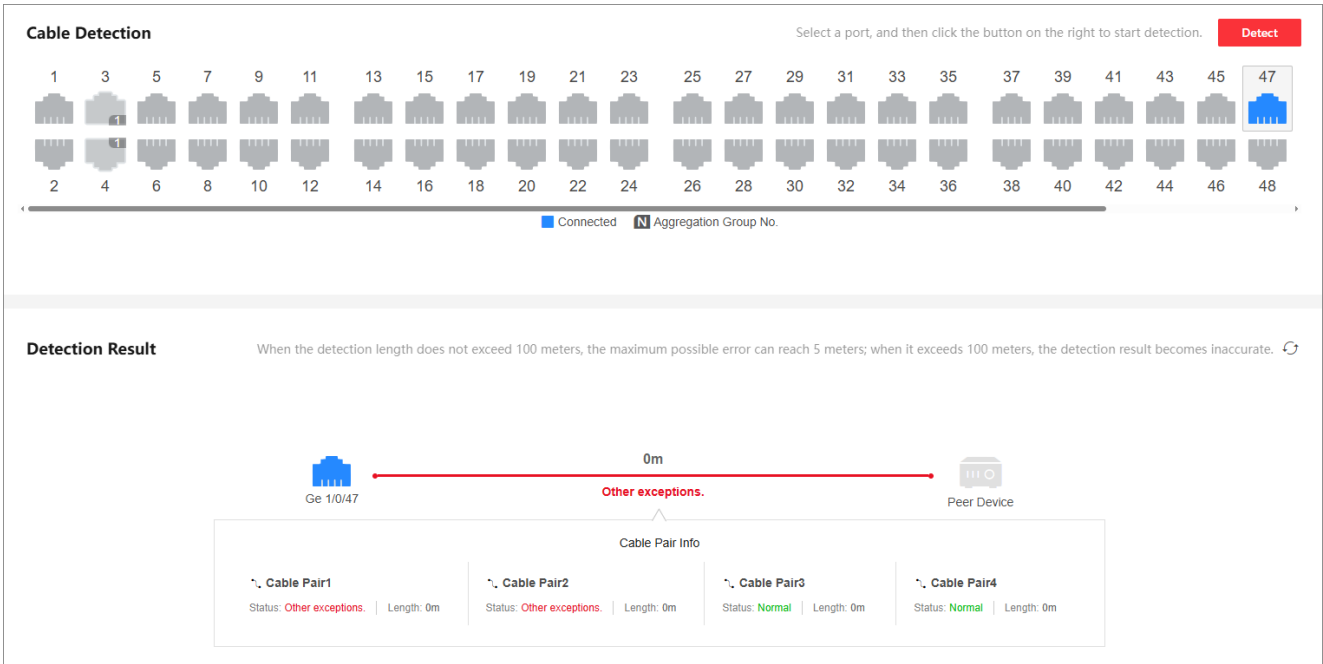


Figure 6-6 Configure Cable Detection

Note

- Cable detection is not available on some models. Refer to the actual device interface for support details.
- Fiber optical ports do not support cable detection.
- For cable lengths up to 100 meters, the maximum detection error is 5 meters. Results are not accurate for lengths over 100 meters.

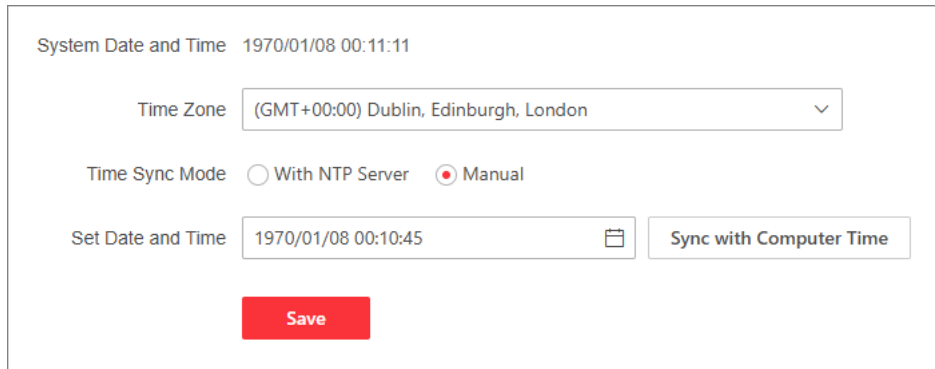
Chapter 7 System Configuration

7.1 Time Configuration

7.1.1 Configure Time Synchronization

Steps

1. Click **System Configuration** -> **Time Configuration** -> **Time Configuration**.
2. Select the time zone.
3. Set the time synchronization mode.
 - **Manual:** Click  to set the device time manually, or click **Sync with Computer Time** to automatically synchronize the device time with the computer time. The configurable time range is from 2001-01-01 00:00:00 to 2036-12-31 23:59:59.



The screenshot displays the 'System Date and Time' configuration page. At the top, it shows the current system date and time as '1970/01/08 00:11:11'. Below this, there is a 'Time Zone' dropdown menu currently set to '(GMT+00:00) Dublin, Edinburgh, London'. Under 'Time Sync Mode', the 'Manual' option is selected with a red radio button, while 'With NTP Server' is unselected. The 'Set Date and Time' field shows '1970/01/08 00:10:45' with a calendar icon to its right. A 'Sync with Computer Time' button is located to the right of the date field. At the bottom center, there is a prominent red 'Save' button.

Figure 7-1 Configure Manual Time Synchronization

- **With NTP Server**

System Date and Time1970/01/08 00:12:16

Time Zone

(GMT+00:00) Dublin, Edinburgh, London

Time Sync Mode

☒ With NTP Server

☐ Manual

NTP

NTP Server

Add

Delete

Refresh

NTP Mode

Server IP Address

Interface

Multicast IP Addr...

Authentication K...

Version

Operation

No data.

Advanced Configuration

Save

Figure 7-2 Configure Time Synchronization with NTP Server

- a. Enable **NTP**.
- b. Click **Add** to add a NTP server and configure it as needed.

Add NTP Server

NTP Mode *

Unicast

IP Address Type *

IPv4

Server IP Address *

Please Enter Server IP Address

NTP Authentication Key ID

Please select.

Version

Please Select Version

Polling Interval

For example, if you enter 10, the value of polling interval will be 1024 (2^{10}).

Max. Polling Interval

Please Enter Max. Polling Interval

Min. Polling Interval

Please Enter Min. Polling Interval

Save

Cancel

Figure 7-3 Configure NTP Server

NTP Mode

Choose from **Unicast**, **Peer**, **Multicast**, or **Broadcast** mode. The default mode is **Unicast**.

Note

Some devices only support **Unicast** mode. Refer to the actual interface for details.

- **Unicast:** The client actively sends time requests to a preset NTP server (UDP port 123), and the server responds with timestamp data.
- **Peer:** Two NTP devices exchange time information bidirectionally as peers, calibrating based on combined clock offsets.

- **Multicast:** The NTP server periodically sends time packets to a multicast group address (e.g., 224.0.1.1). Clients listening to this group automatically synchronize.
- **Broadcast:** The server periodically sends time packets via a broadcast address (e.g., 255.255.255.255), and clients passively receive them.

IP Address Type

Select **IPv4** or **IPv6** for the NTP server IP address type.



Note

Some devices only support IPv4. Refer to the actual interface.

Server IP Address

Enter the IPv4 or IPv6 address of the NTP server.

NTP Authentication Key ID

Select a pre-configured NTP authentication key ID, or click **Add** to configure a new one. When adding a new key ID, configure the following parameters:

- Authentication Key ID (range: 1 to 4,294,967,295)
- Authentication Mode (currently only MD5 is supported)
- Authentication Key Encryption Method (currently only plaintext is supported)
- Authentication Key (string, up to 32 characters)



Note

If no key ID is configured, go to **System Configuration -> Time Configuration -> Authentication Key ID Configuration** to configure a key ID first. Refer to **7.1.2 Configure Authentication Key** for details.

Version

Set the NTP server version (NTPv1 to NTPv4). Higher versions offer better time synchronization accuracy.



Note

This setting is only required for IPv4 addresses.

Max. Polling Interval

Set the maximum interval for the NTP client to send synchronization requests.

Enter a value from 4 to 17, corresponding to an actual interval of 16 (2^4) to 131,072 (2^{17}) seconds.



Note

The maximum polling interval be greater than or equal to the minimum polling interval.

Min. Polling Interval

Set the minimum interval for the NTP client to send synchronization requests.

Enter a value from 4 to 17, corresponding to an actual interval of 16 (2^4) to 131,072 (2^{17}) seconds.

Note

The minimum polling interval must be less than or equal to the maximum polling interval.

c. Click **Save**.

Note

- The successfully configured NTP servers will be displayed in the list. You can edit or delete existing NTP servers.
- Up to 8 NTP servers are supported.

4. Click **Advanced Configuration** to configure additional NTP time synchronization settings.

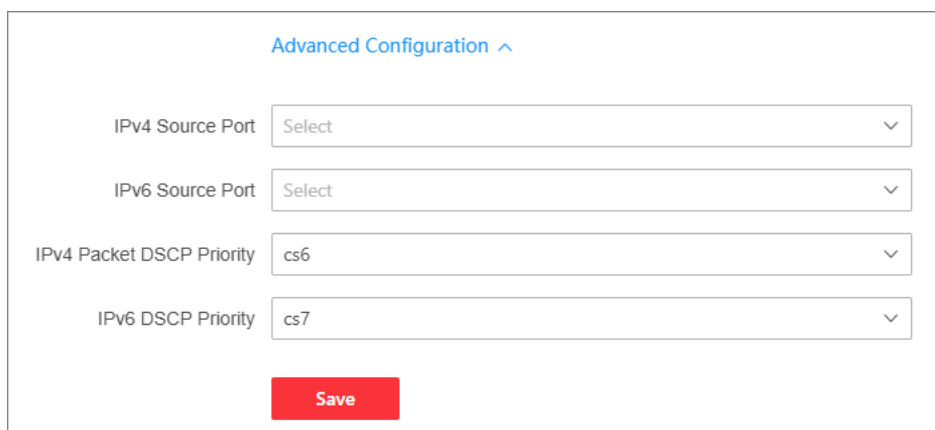


Figure 7-4 Configure Advanced Parameters for NTP Time Synchronization

IPv4 Source Port

Select the source port used by the NTP client for sending requests. Only created VLAN interfaces are supported.

IPv6 Source Port

Select the source port used by the NTP client for sending requests. Only created VLAN interfaces are supported.

IPv4 Packet DSCP Priority

Network devices prioritize packet handling based on DSCP values. Setting this ensures proper NTP packet treatment. Higher values indicate higher priority.

IPv6 DSCP Priority

Network devices prioritize packet handling based on DSCP values. Setting this ensures proper NTP packet treatment. Higher values indicate higher priority.

 Note

Some devices only support configuring IPv4 source ports and IPv4 DSCP priority. Refer to the actual interface.

5. Click **Save**.

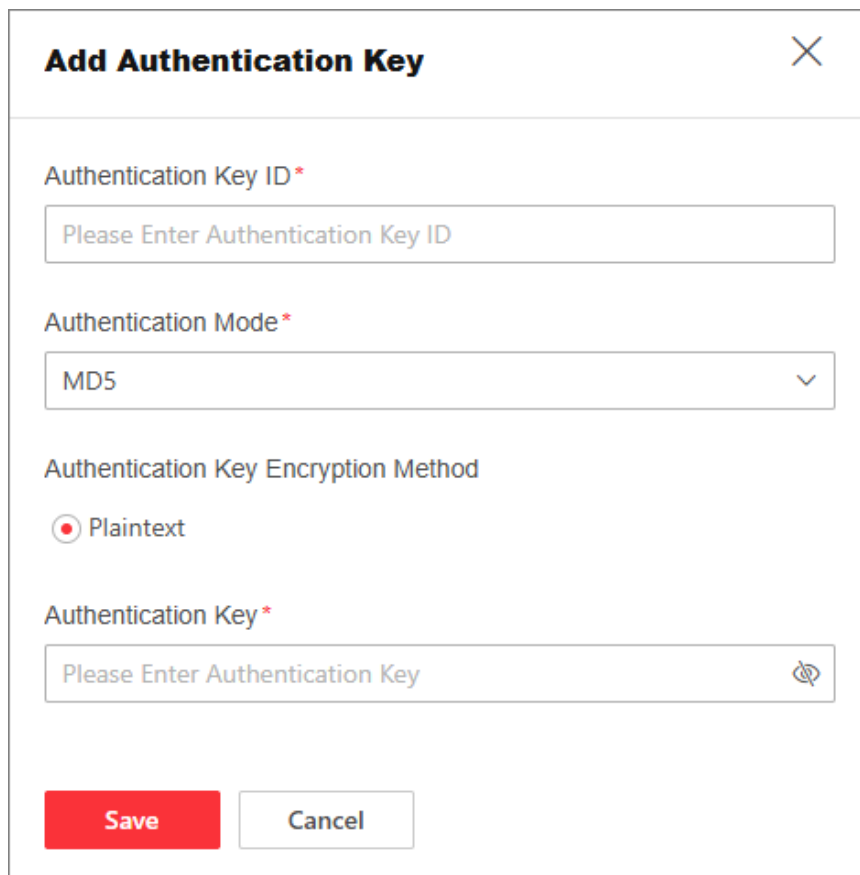
7.1.2 Configure Authentication Key

When the time synchronization mode is set to **With NTP Server**, you need to configure the authentication key.

 Note

When the time synchronization mode is set to **Manual**, the authentication key ID configuration tab page is grayed out by default and does not require configuration.

1. Click **System Configuration** -> **Time Configuration** -> **Authentication Key ID Configuration**.
2. Click **Add**.
3. Configure the new authentication key as needed, and click **Save**.



The dialog box titled "Add Authentication Key" contains the following fields and controls:

- Authentication Key ID ***: A text input field with the placeholder text "Please Enter Authentication Key ID".
- Authentication Mode ***: A dropdown menu currently showing "MD5".
- Authentication Key Encryption Method**: A radio button labeled "Plaintext" is selected.
- Authentication Key ***: A text input field with the placeholder text "Please Enter Authentication Key" and a toggle icon on the right.
- Buttons**: A red "Save" button and a white "Cancel" button at the bottom.

Figure 7-5 Configure Authentication Key ID

Authentication Key ID

Set the authentication key ID. Valid values range from 1 to 4,294,967,295.

Authentication Mode

Currently, only MD5 is supported. When MD5 authentication is used between the NTP client and server, both sides share a common key, which is used to generate and verify message digests.

Authentication Key Encryption Method

Currently, only plaintext is supported. During NTP authentication, the key exists in an unencrypted and directly readable form.

Authentication Key

Manually set the authentication key as a string with a maximum length of 32 characters.



Note

- The successfully configured authentication keys will be displayed in the list. You can delete the configured authentication key(s).
- Up to 20 authentication keys can be configured.

3. Select a **trusted** authentication key ID from the dropdown list.
4. Enable **Authentication Mode** to make the trusted authentication key ID effective.
5. Click **Save**.

7.2 System Maintenance

Click **Maintenance and Security** -> **System Maintenance** to remotely restart the device, upgrade the device firmware, back up device configuration, reset the device, or export the diagnosis information of the device.

7.2.1 Restart Device

Click **Restart** to remotely restart the switch.

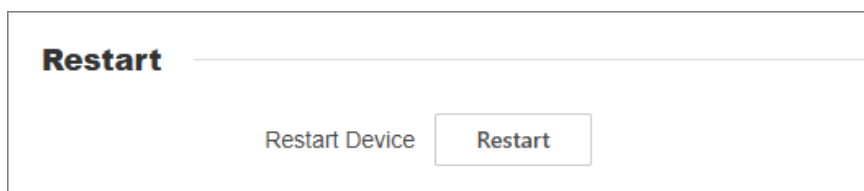
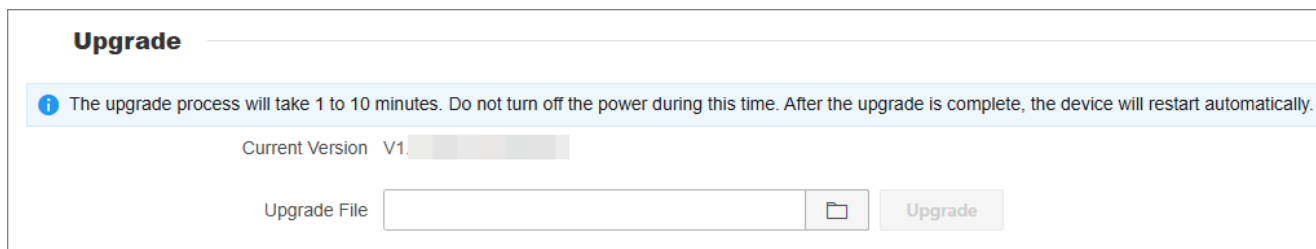


Figure 7-6 Restart Device

7.2.2 Upgrade Device

If the current version of the device is not the latest version, you can upgrade the switch. Click , upload the upgrade file, and then click **Upgrade** to upgrade the device.



7-7 Upgrade Device

Note

- The firmware upgrade process may take approximately 1 to 10 minutes. Do not power off the device during this period. Once the upgrade is completed, the device will automatically restart and redirect to the login page. It is recommended to save the current configuration before restarting to avoid configuration loss.
- If the upgrade fails or the device does not function properly afterward, please contact technical support.

7.2.3 Back Up Device

The system supports exporting configuration files containing device parameters for local backup.

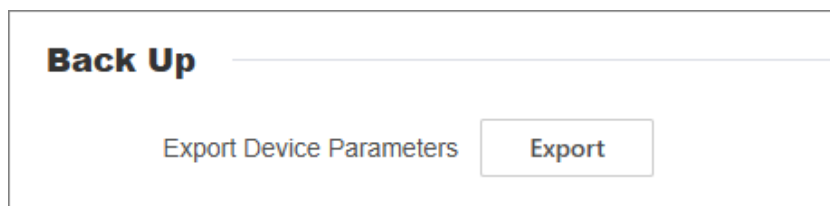


Figure 7-8 Back Up Device

Steps

1. Click **Export**.
2. Set a password and confirm it to encrypt the file.
3. Click **OK**.

7.2.4 Reset Device

The system enables resetting the switch device by either restoring the default parameters or re-importing device parameters.

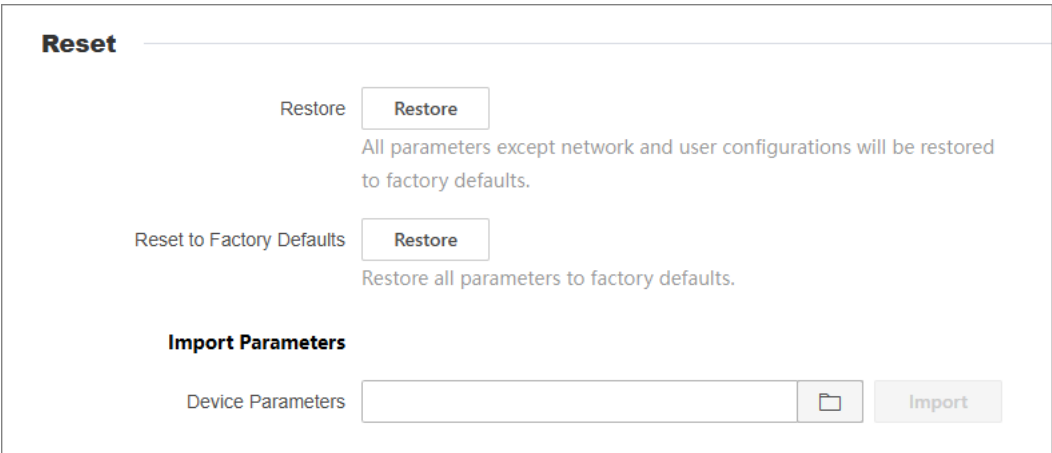


Figure 7-9 Reset Device

- Simple Restore to Defaults: Click **Restore** and enter the login password for secondary authentication to restore all parameters—except network and user configurations—to factory settings.
- Reset to Factory Defaults: Click **Restore** and enter the login password for secondary authentication to restore all parameters to factory settings.
- Import Device Parameters: Click  to select a configuration file containing device parameters, click **Import**, enter the password to decrypt the file, and then click **OK** to import the configuration file for fast device configuration.

 Note

- The “Reset to Factory Defaults” operation will clear all device parameter configurations, which cannot be recovered. The IP address will revert to the initial address, and the web will become inaccessible. Proceed with caution.
- It is recommended to export and locally back up the configuration file before performing a reset operation.

7.2.5 Export Diagnostic Info

You can export diagnostic information for troubleshooting, system optimization, security auditing, and remote technical support.

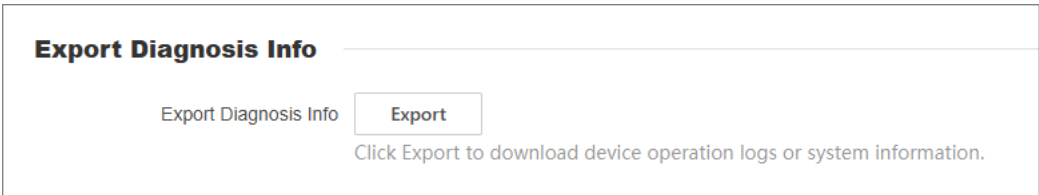


Figure 7-9 Export Diagnostic Info

Click **Export** to download the device's operational logs and system information.

**Note**

Diagnostic information is exported to a TXT file, with a prompt shown upon successful completion.

7.3 Network Configuration

7.3.1 Configure Management Address

In large-scale enterprise networks, numerous hosts and devices require network parameters such as IP addresses. Manually configuring these parameters is not only time-consuming and difficult to manage, but may also result in issues such as IP address conflicts if users make unauthorized modifications.

By using DHCP (Dynamic Host Configuration Protocol) to assign IP addresses and other network parameters, administrators can significantly reduce their workload and avoid address conflicts that arise from manual configuration.

The device allows configuration of network parameters—including IP address, subnet mask, and gateway address—to accommodate the needs of different clients during device deployment.

Steps

1. Click **System Configuration** -> **Network Configuration** -> **Management Address**.
2. Set network parameters of the device.

DHCP ☐

* Management VLAN

* IPv4 Address

* IPv4 Subnet Mask

Default IPv4 Gateway

Save

7-10 Configure Management Address

- Auto configuration: Enable **DHCP**. The device will then automatically retrieve an IP address from a DHCP server, eliminating the need for manual configuration.
- Manual configuration: Disable **DHCP**, and manually configure the management VLAN, IPv4 address, IPv4 subnet mask, and default IPv4 gateway.

3. Click **Save**.

 Note

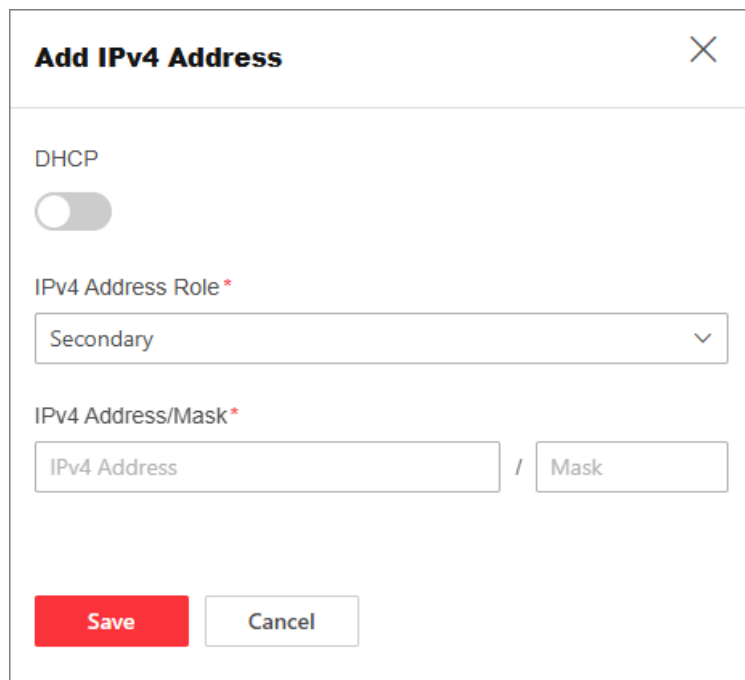
- After the IP address is modified, the browser will be automatically redirected to the web login page of the new IP address.
- If the IP address is modified, the device's IP address may fall outside the client computer's subnet, making device management and configuration impossible. We recommend using the SADP tool to properly configure the IP address during initial device activation.

7.3.2 Configure Management Port

The management port on a switch is specifically designed for device administration, monitoring, and maintenance. It isolates management traffic from data traffic to improve security, operational stability, and efficiency. Configuring the management port entails setting an IPv4 or IPv6 address, which enables network accessibility and supports remote management, compatibility with existing tools (such as IPv4 in legacy environments), and adaptation to modern network requirements (e.g., IPv6 for expanded addressing and automation). Dual-stack configuration, which involves assigning both an IPv4 and an IPv6 address to the management interface, allows the device to be accessed using either protocol. This setup offers flexibility during network transitions and provides redundancy in the event of protocol-specific issues.

Steps

1. Click **System Configuration -> Network Configuration -> Management Port**.
2. Click **Add** to configure an IPv4 address, an IPv6 address, or both.
3. Set the parameters accordingly.
 - IPv4 Address: Enable **DHCP** for automatic IPv4 address assignment, or manually configure **IPv4 Address Role** and **IPv4 Address/Mask**.



Add IPv4 Address

DHCP

☐

IPv4 Address Role *

Secondary

IPv4 Address/Mask *

IPv4 Address / Mask

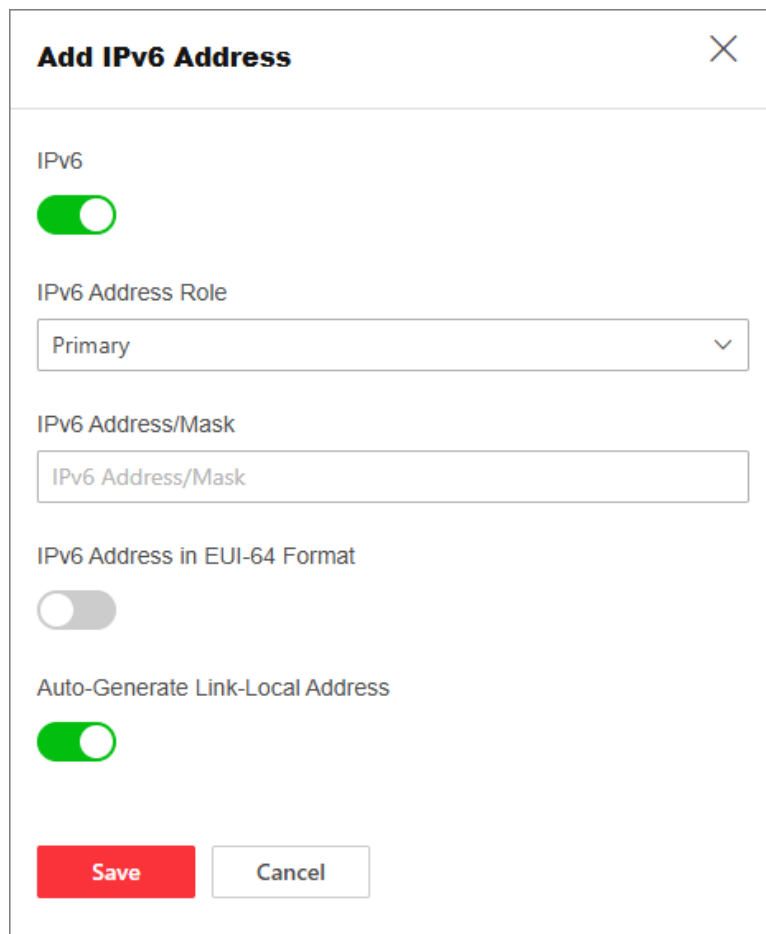
Save Cancel

Figure 7-11 Configure IPv4 Address

 Note

- A primary IP address serves as the main address for an interface, while a secondary address provides additional aliases on the same interface.
- The default IP address of the management port is 192.168.1.64/24. To establish connectivity, configure the switch's management port IP address to be on the same subnet as the computer's IP address. Then you can access the switch using the management port's IP address from the computer.

- IPv6 Address:



The screenshot shows a web-based configuration dialog titled "Add IPv6 Address" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- IPv6:** A green toggle switch is turned on.
- IPv6 Address Role:** A dropdown menu showing "Primary" with a downward arrow.
- IPv6 Address/Mask:** A text input field containing the placeholder text "IPv6 Address/Mask".
- IPv6 Address in EUI-64 Format:** A grey toggle switch is turned off.
- Auto-Generate Link-Local Address:** A green toggle switch is turned on.
- Buttons:** At the bottom, there are two buttons: a red "Save" button and a white "Cancel" button with a grey border.

Figure 7-12 Configure IPv6 Address

- a. Enable **IPv6**.
- b. Manually configure **IPv6 Address Role** and **IPv6 Address/Mask**.
- c. (Optional) Enable **IPv6 Address in EUI-64 Format** to allow nodes to automatically generate IPv6 addresses using the EUI-64 format when no DHCP server is available on the network.
- d. (Optional) Disable **Auto-Generate Link-Local Address** to prevent automatic generation of IPv6 link-local addresses via EUI-64.

4. Click **Save**.

5. Optional: Click  or  to edit or delete the configured IPv4 address or IPv6 address for the management port.

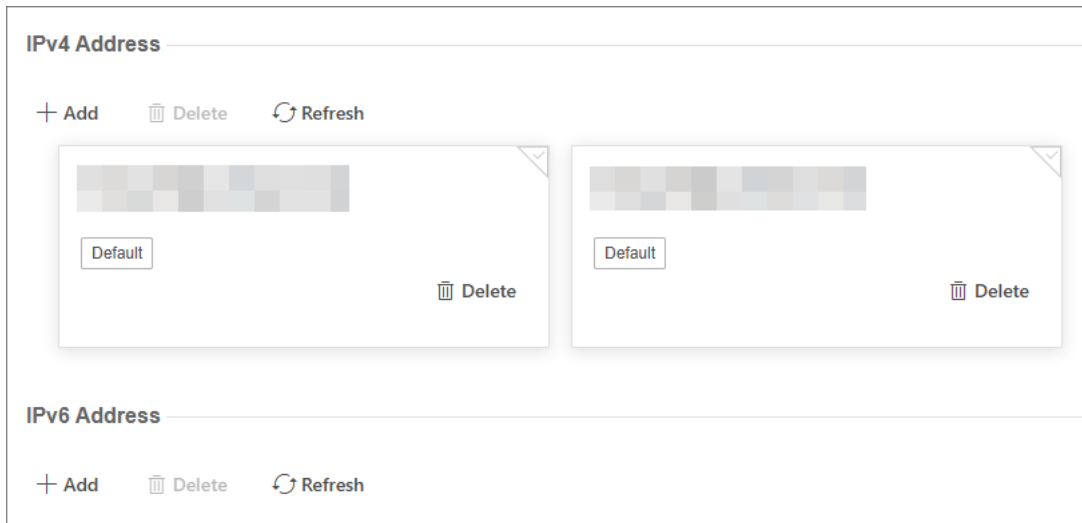
7.3.3 Configure DNS Server

Configuring DNS server addresses on a switch enables bidirectional resolution between domain names and IP addresses. This allows the device to access remote management platforms, cloud services, or third-party resources using domain names, eliminating the need for manual static IP configuration. Such a setup not only simplifies network management—for example, by enabling quick

device location via domain names—but also supports advanced functionalities such as software upgrades and security protection. The use of multiple DNS servers enhances redundancy, while selecting trusted DNS providers helps mitigate hijacking risks, thereby ensuring efficient and stable network operation. If no DNS server is configured, all domain name-dependent functions will be unavailable, which can significantly impact operational efficiency.

Steps

1. Click **System Configuration** -> **Network Configuration** -> **DNS Server**.
2. Add one or more DNS server IP addresses as needed.



The screenshot displays the 'DNS Server' configuration page. It is divided into two main sections: 'IPv4 Address' and 'IPv6 Address'. Each section has a header bar with '+ Add', 'Delete' (trash icon), and 'Refresh' (circular arrow icon) buttons. Below each header is a list of configured addresses. Each address is shown in a card-like format with a blurred IP address, a 'Default' button, and a 'Delete' (trash icon) button. The IPv4 section currently shows two entries, and the IPv6 section shows one entry.

Figure 7-11 Configure DNS Server IP Address

- IPv4: Click **Add**, enter the IPv4 address, and then click the blank area to finish adding static IPv4 address.
- IPv6: Click **Add**, enter the IPv6 address, and then click the blank area to finish adding static IPv6 address.

Note

- The total number of static IPv4 and IPv6 addresses cannot exceed 6.
- When multiple DNS addresses exist, the DNS server will use them in the order of static address, dynamic address, and default address, and give priority to the former address.

3. Optional: Delete the configured DNS server IP address(es) if needed.

- Click **Delete** below the desired DNS server address to delete a single DNS server address.
- Select multiple DNS server addresses and click **Delete** above the DNS server address list to batch delete them.

7.3.4 Configure Cloud Service

The device can be bound to a cloud account via the Hik-Partner Pro app, enabling cloud-based management.

Steps

1. Click **System Configuration** -> **Network Configuration** -> **Cloud Service**.

Enabled ☒

The service you are enabling requires Internet access. Please confirm you have read and agreed to [Terms of Service](#) and [Privacy Policy](#).

*Server Address

☒ Customize

Network Connection Status ✔ Online [Refresh](#)

[Save](#)

Account Binding Settings

Account Binding Status ✖ No cloud account bound.

The device's account status may not be updated. Please refer to the account status shown in the mobile app.

Account Binding Settings

Binding via QR Code

Scan the device's QR code below with the mobile app to bind it to your cloud account.

Device QR Code

[Click to View](#)

Figure 7-12 Configure Cloud Service

2. Enable cloud service.
3. Optional: Select **Customize** to configure the server IP address.
4. Optional: View or refresh the device network connection status.
5. Click **Save**.
6. Click to view the device QR code.



7-13 View Device QR Code

7. Scan the device's QR code with the Hik-Partner Pro app to bind it to a cloud account. Once the device is successfully bound to a cloud account, the account status will show **Cloud account bound**.

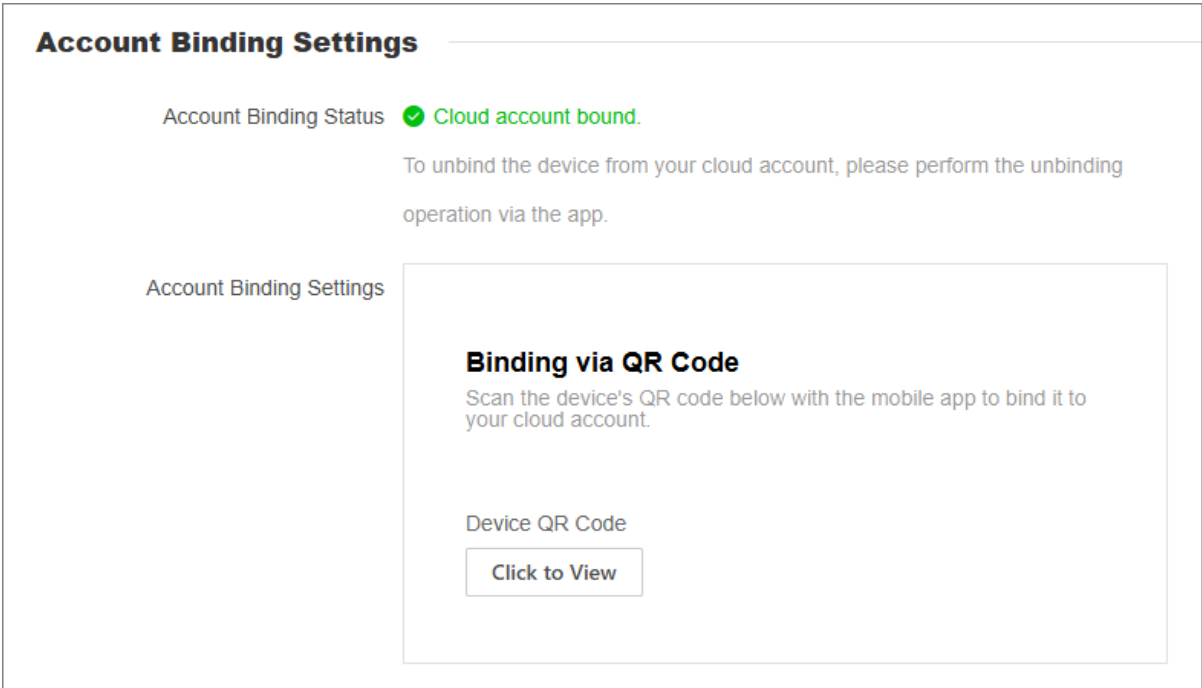


Figure 7-14 Device Bound to Cloud Account

 Note

- You can only bind the device to a cloud account if its network connection status is **Online**. This enables cloud platform management and configuration.
- If you need to unbind the device later, please use the Hik-Partner Pro app to do so.

7.3.5 Configure SADP

The device supports SADP device discovery.

Steps

1. Click **System Configuration** -> **Network Configuration** -> **SADP**.

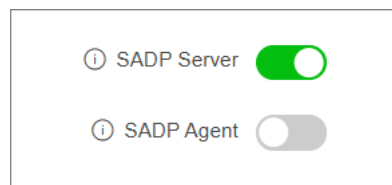


Figure 7-15 Configure SADP

2. Enable **SADP Server** or **SADP Agent** as needed.

SADP Server

Designed for automatic discovery and management of Hikvision devices (e.g., device activation, IP address modification) within a local area network (LAN), and enabled by default. When the SADP server is enabled, it can search for SADP-supported devices and display their information.

SADP Agent

Enables device discovery and configuration across subnets or in complex network environments by leveraging agent relay to bypass network isolation. When the SADP agent is enabled, the device periodically broadcasts discovery packets (every 60 seconds) within the LAN to map the network topology.

 Note

- Enabling the SADP server allows you to search for this switch via the SADP tool on your computer and view its information.
- Enabling the SADP agent allows this switch to discover other devices on the LAN by sending query messages regularly.

7.4 Remote Service

The device supports remote login and management through HTTP, HTTPS, Telnet, FTP, TFTP, and SSH protocols.

Go to **System Configuration -> Network Configuration -> Remote Management**, configure the parameters as needed, and click **Save**.

HTTP

Enabled ☒

Port

The available port numbers may be related to the browser's type and version.
Please refer to the actual support status of the browser.

HTTPS

Enabled ☒

Port

The available port numbers may be related to the browser's type and version.
Please refer to the actual support status of the browser.

Telnet

IPv4 ☐

IPv6 ☐

FTP

IPv4 ☐

IPv6 ☐

TFTP

IPv4 ☐

IPv6 ☐

SSH

Enabled ☐

Save

Figure 7-16 Configure Remote Service

HTTP (HyperText Transfer Protocol)

HTTP transmits web page data in plaintext without encryption.

You can enable or disable HTTP login. If it is enabled, configure the HTTP service port (default: 80, range: 1 to 65535).

HTTPS (HTTP Secure)

HTTPS is an encrypted version of HTTP for secure transmission of sensitive data.

You can enable or disable HTTPS login. If it is enabled, configure the HTTPS service port (default: 443, range: 1 to 65535).

Telnet (Telecommunication Network)

Telnet enables remote device login and management but transmits data in plaintext.

You can enable or disable IPv4/IPv6 Telnet service as needed (disabled by default).

FTP (File Transfer Protocol)

FTP is used for file transfers. By default, data is transmitted in plaintext, but FTP over TLS/SSL (FTPS) can encrypt transmissions.

You can enable or disable IPv4/IPv6 FTP service as needed (disabled by default).

TFTP (Trivial File Transfer Protocol)

TFTP supports simple file transfers without encryption. Unlike FTP, it requires no authentication and is easy to deploy in trusted networks.

You can enable or disable IPv4/IPv6 TFTP service as needed (disabled by default).

SSH (Secure Shell)

SSH provides encrypted remote login and management, replacing Telnet. All data is encrypted to prevent leaks.

You can enable or disable SSH service.

7.5 Security Service

Go to **Maintenance and Security** -> **Security Service** to enable/disable the console port. Enabling it allows users to perform data transmission, debugging, firmware updates, and device access control operations.

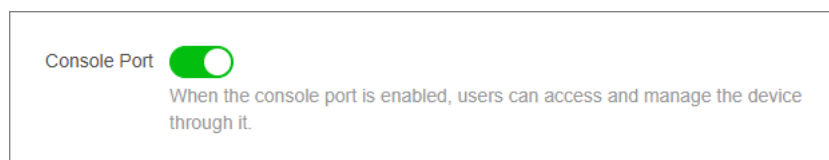


Figure 7-17 Enable Console Port

7.6 Log Management

The device keeps two types of logs for log management purpose.

- **Security Audit Log** saves records of who accessed the system and did what (like remote user login or device power-on), stored securely for future review. Only "admin" users can view security audit logs.
- **Device Operation Log** tracks how each module of the device is working (like port link up), helpful for fixing technical issues. Anyone can view device operation logs.

By reviewing these logs, network administrators can effectively monitor network operations, diagnose faults promptly, and perform real-time analysis of user access for behavior auditing.

7.6.1 Query Security Audit Logs

Steps

1. Click **Maintenance and Security -> Log Management -> Security Audit Log -> Security Audit Log**.

Time
1970/01/01 00: - 2026/04/16 23:

Major Type
All

Sub Type
All

Search

Refresh

Time	Major Type	Sub Type	Description
2026/04/16 09:20:46	Operation	Operation - Remote Login	User Name:admin;IP Address:;Additional Info:User logged in. [UserName=admin; Host=]
2026/04/16 09:20:46	Operation	Operation - Remote Login	User Name:admin;Additional Info:User logged in successfully. [UserName=admin; Type=HTTP]
2026/04/16 09:11:50	Operation	Operation - Remote Logout	User Name:admin;IP Address:;Additional Info:User logged out. [UserName=admin; Host=]
2026/04/16 08:53:15	Operation	Operation - Remote Login	User Name:admin;IP Address:;Additional Info:User logged in. [UserName=admin; Host=]
2026/04/16 08:53:15	Operation	Operation - Remote Login	User Name:admin;Additional Info:User logged in successfully. [UserName=admin; Type=HTTP]
2026/04/16 08:18:15	Operation	Operation - Remote Logout	User Name:admin;IP Address:;Additional Info:User logged out. [UserName=admin; Host=]
2026/04/16 08:06:22	Operation	Operation - Remote Login	User Name:admin;IP Address:;Additional Info:User logged in. [UserName=admin; Host=]
2026/04/16 08:06:22	Operation	Operation - Remote Login	User Name:admin;Additional Info:User logged in successfully. [UserName=admin; Type=HTTP]
2026/04/16 07:57:44	Operation	Operation - Remote Logout	User Name:admin;IP Address:;Additional Info:User logged out. [UserName=admin; Host=]
2026/04/16 07:47:34	Operation	Operation - Remote Login	User Name:admin;IP Address:;Additional Info:User logged in. [UserName=admin; Host=]
2026/04/16 07:47:34	Operation	Operation - Remote Login	User Name:admin;Additional Info:User logged in successfully. [UserName=admin; Type=HTTP]
2026/04/16 07:46:59	Operation	Operation - Remote Logout	User Name:admin;IP Address:;Additional Info:User logged out. [UserName=admin; Host=]
2026/04/16 07:36:56	Operation	Operation - Remote Login	User Name:admin;IP Address:;Additional Info:User logged in. [UserName=admin; Host=]
2026/04/16 07:36:56	Operation	Operation - Remote Login	User Name:admin;Additional Info:User logged in successfully. [UserName=admin; Type=HTTP]
2026/04/16 07:35:29	Operation	Operation - Remote Logout	User Name:admin;IP Address:;Additional Info:User logged out. [UserName=admin; Host=]

Figure 7-18 Query Security Audit Logs

2. Set time period, major type, or sub type, and click **Search**.



Note

The device can cache up to 2,000 security audit logs.

The security audit logs meeting the condition(s) will be displayed in the log information list.

7.6.2 Configure Log Server

Users can specify the output destination of log information according to their requirements. By default, the system will save log records in the local database. Meanwhile, the system supports sending log information to a syslog server.

Steps

1. Go to **Maintenance and Security -> Log Management -> Security Audit Log -> Log Server Settings**.

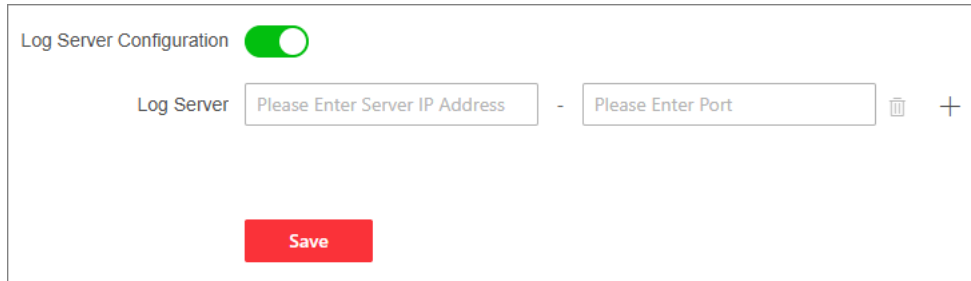


Figure 7-19 Configure Log Server

2. Enable **Log Server Configuration**.

3. Enter the server IP address and port number.

Note

Both IPv4 and IPv6 addresses are supported, with port numbers ranging from 1 to 65535.

4. **Optional:** Click  to add more log servers.

Note

Up to 16 log servers can be configured.

5. Click **Save**.

6. **Optional:** Click  to delete a configured log server.

7.6.3 Query Alarm Logs

Steps

1. Go to **Maintenance and Security -> Log Management -> Alarm Logs**.

Time1970/01/01 00: - 2026/04/16 23:

LevelAll

ModuleAll

Keyword

Please Enter Keyword

Search

Reset

Clear

Export

Refresh

Time	Log Level	Alarm Module	Description
2026/04/16 09:43:48	Notice	CLI Module	Additional Info:OID: , User logged in successfully. [UserName=admin]
2026/04/16 09:33:45	Notice	CLI Module	Additional Info:OID: , User logged in successfully. [UserName=admin]
2026/04/16 09:32:22	Notice	CLI Module	Additional Info:OID: , User logged in successfully. [UserName=admin]
2026/04/16 09:20:46	Notice	CLI Module	Additional Info:OID: , User logged in successfully. [UserName=admin]
2026/04/16 08:53:15	Notice	CLI Module	Additional Info:OID: , User logged in successfully. [UserName=admin]
2026/04/16 08:06:22	Notice	CLI Module	Additional Info:OID: , User logged in successfully. [UserName=admin]
2026/04/16 07:47:34	Notice	CLI Module	Additional Info:OID: , User logged in successfully. [UserName=admin]
2026/04/16 07:36:56	Notice	CLI Module	Additional Info:OID: , User logged in successfully. [UserName=admin]
2026/04/16 05:52:16	Notice	CLI Module	Additional Info:OID: , User logged in successfully. [UserName=admin]
2026/04/16 05:52:12	Notice	CLI Module	Additional Info:OID: , User logged in successfully. [UserName=admin]
2026/04/16 03:50:16	Notice	CLI Module	Additional Info:OID: , User logged in successfully. [UserName=admin]
2026/04/16 03:10:21	Notice	CLI Module	Additional Info:OID: , User logged in successfully. [UserName=admin]
2026/04/16 02:05:26	Notice	CLI Module	Additional Info:OID: , User logged in successfully. [UserName=admin]
2026/04/16 01:45:20	Notice	CLI Module	Additional Info:OID: , User logged in successfully. [UserName=admin]

Figure 7-20 Query Alarm Logs

2. Set time period, level, or module, or enter keyword, and click **Search**.

Note

The device can cache up to 2,000 alarm logs.

The alarm logs meeting the condition(s) will be displayed in the log information list.

3. **Optional:** Perform the following operations as needed:

- Click **Clear** to clear all alarm logs in the cache.
- Click **Export** to export the alarm logs to your local computer.

7.7 User Management

User management enables authentication, permission assignment, and access control for users accessing the device. This ensures that only authorized users can log in and operate the switch, preventing unauthorized access and malicious activities. Additionally, permissions can be customized based on user roles—for example, administrators may have full configuration rights, while general users are restricted to view-only access—thereby maintaining the stability of the device system.

Steps

1. Go to **System Configuration -> User Management**.

Note

Only the administrator account (admin) can perform user management operations.

2. Click **Add** to create a user authorized to log in to the switch via the web interface.

Add User 

User Name *

User Password *
 

Confirm Password *
 

Confirm Password (Currently Logged-in User) *
 

User Type *
 

Access Mode

☐ Telnet

☐ FTP

☐ Console

☐ Access

☐ SSH

☐ HTTP

☐ HTTPS

☐ Portal

Max. Concurrent Online Users

[Advanced Configuration](#) 

Save

Cancel

Figure 7-21 Add User

3. Configure the basic parameters as needed.**User Name**

Enter the name of the user to be created. The name should be no more than 32 characters long and cannot contain special characters such as `/?\\:*?"<->|'()``$&;`.

User Password

Enter the password for the user. The password must be 8 to 16 characters in length and cannot contain:

- The user name (case-insensitive)
- Strings such as 123, admin, hik, hkws, or hikvision (appearing as whole words/phrases, case-insensitive)
- Four or more consecutive increasing or decreasing digits (e.g., 1234, 4321)
- Four or more consecutive identical characters (e.g., 1111, aaaa)
- Any password listed in the common risky passwords list

Confirm Password

Enter the password again to confirm.

Confirm Password (Currently Logged-in User)

Enter the login password for the account (e.g., the administrator account "admin"), used to verify the user's identity and permissions.

User Type

User types (user roles) can be selected as administrator, operator, user, or guest. Different user roles correspond to different permissions.

- Administrator (admin): High permission role capable of performing all configuration operations, such as creating/deleting users, upgrading system firmware, and viewing all logs and system information.
- Operator: An intermediate permission role that can view configuration and status information, perform some non-critical configurations, but is not allowed to edit system-level settings or create/delete users.
- User: A basic permission role that can only view basic information, perform simple status queries, and cannot make any configuration modifications.
- Guest: A low permission role with temporary access only, limited to viewing restricted information on the system.

Access Mode

The methods for users to log in to the switch include Telnet, FTP, Console, Access, SSH, HTTP, HTTPS, and Portal.

For the differences between these access methods, see Table 7-1.

Table 7-1 Common Device Access Methods

Access Method	Description
Telnet	Used for logging into the switch command-line interface (CLI) via plaintext (without encryption). Note that this method transmits data in plaintext and is not secure for sensitive environments.
FTP	Used for transferring configuration or system files to the switch, typically for maintenance purposes.
Console	Used for local configuration of the switch via a console cable, typically for initial setup or troubleshooting.
Access	Out-of-Band Management A method of accessing and managing network devices through a dedicated interface (e.g., MGMT port) that is physically or logically isolated from the service network.
SSH	A cryptographic network protocol operating on port 22, designed for secure remote CLI login, data communication, and other network services over an unsecured network. It replaces insecure protocols like Telnet.
HTTP	HTTP (Port 80) Web Management Access the switch's management interface via a web browser using unencrypted HTTP
HTTPS	HTTPS (Port 443) Web Management Access the switch's management interface via a web browser using encrypted HTTPS.
Portal	Web-Based Authentication (Captive Portal) A method that requires users to log in via a web page to gain access to the switch's management functions or network services. Commonly used for guest networks, BYOD (Bring Your Own Device), or public Wi-Fi scenarios

Max. Concurrent Online Users

The maximum number of concurrent sessions allowed for specified user names. This limit applies to the total sessions initiated by these users via Console, SSH, Telnet, HTTP/HTTPS, etc.

The value must be between 1 and 32.

4. Optional: Click **Advanced Configuration** to configure the advanced parameters as needed.

Lockout Duration After Consecutive Login Failures

When continuous authentication failures are detected across multiple sessions, the system will automatically lock the user account or IP address for a specified duration, during which login is prohibited. The duration can be set between 0 and 65,535 minutes.

Max. Failed Login Attempts Before Account Lockout

If the number of consecutive authentication failures exceeds the configured threshold, the system will lock the user account or IP address. The threshold can be set from 1 to 10 attempts.

5. Click **Save**.

6. **Optional:** In the user information list, you can view the user name, user type, and access method of the created user, or perform other operations.

- Click  to delete the specified user.
- Click  to edit the specified user.
- Enter the user name or select the user type, and then click **Search** to search for the specified user(s).

7.8 Login Management

The device provides web-based login management capabilities, enabling configuration of connection timeout, illegal login lockout policies, and password strength requirements. Administrators can also view the list of locked users and unlock them when necessary.

1. Go to **Maintenance and Security** -> **Login Management**.

HTTP/HTTPS Connection Timeout 10 min

Illegal Login Lockout

Lockout Type ☐ IP Address ☒ User

* Global Failed Login Attempts Before Lockout 5 Frequency

* Global User Account Lockout Duration 5 min

Password Strength

* Min. Password Length 8

* Password Strength Medium

Save

Figure 7-21 Configure Login Settings

2. Configure the parameters as needed.

HTTP/HTTPS Connection Timeout

The maximum allowable duration for maintaining a connection between the client and server or waiting for a response. The value is configurable between 5 and 999 minutes, with a default setting of 10 minutes.

Lockout Type

Lockout methods:

- **IP Address:** Triggered by failed login attempts from a specific IP address.
- **User:** Activated after repeated authentication failures for a user account.

Failed Attempts Allowed Before IP Address Lockout

Specifies the maximum number of consecutive incorrect password attempts allowed before the IP address is locked.

- Default value: 5
- Value range: 1 to 10

IP Address Lockout Duration After Consecutive Login Failures

Defines the period during which an IP address remains locked after exceeding the maximum allowed consecutive login failures.

- Default value: 5 minutes
- Value range: 1 to 65535 minutes

Global Failed Login Attempts Before Locking User Account

Specifies the maximum number of consecutive incorrect password attempts allowed before the user account is locked.

- Default value: 5
- Value range: 1 to 10

Global User Account Lockout Duration After Consecutive Login Failures

Defines the period during which a user account remains locked after exceeding the maximum allowed consecutive login failures.

- Default value: 5 minutes
- Value range: 0 to 65535 minutes

If this parameter is set to 0, the user account will be locked out unless the administrator unlocks it.

Min. Password Length

Specifies the minimum length requirement for login passwords. The valid range is 8 to 16 characters, with a default value of 8 characters.

Password Strength

Defines the complexity requirements for login passwords, with two levels:

- Medium (default): The password should contain two or more of the following categories: digits, lower case letters, upper case letters, and special characters.
- High: The password should contain at least three of the following categories: digits, lower case letters, upper case letters, and special characters.

**Note**

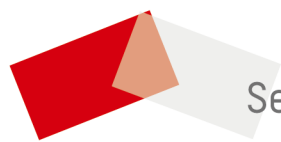
Configure minimum password length and strength requirements to prevent the use of weak passwords. If a newly entered password fails to meet the specified criteria, the settings cannot be applied.

3. Click **Save**.

4. Optional: Click **Locked User List** to view currently locked user accounts or IP addresses.

**Note**

Administrators can unlock locked user accounts or IP addresses.



See Far, Go Further