Smart Managed Switch Web

User Manual

Navigation Page

<table>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td rowspan="3"></td><td></td></tr>
<tr><td></td></tr>
<tr><td></td></tr>
</table>

	• ***Configure PoE Mode*** • ***Configure Power Saving Plan***	
	EEE Configuration	
	QoS Configuration	
	DSCP Configuration	
	SNMP Configuration • ***Configure Basic SNMP Parameters*** • ***Configure SNMP Community*** • ***Configure SNMP Trap Target Host***	
	LLDP Configuration	
	Security Configuration	***DHCP Snooping Configuration***
		ACL Configuration • ***Configure Advanced ACL*** • ***Configure Layer 2 ACL*** • ***Configure Port ACL Application***
		ARP Gateway Protection Configuration
		IPSG Configuration • ***Configure Binding Entry*** • ***Configure Source Address Check***
	Loop Prevention Configuration • ***STP Configuration*** • ***ERPS Configuration***	
System Management	• ***Time Synchronization*** • ***System Maintenance*** • ***Network Configuration*** • ***Network Diagnosis*** • ***Log Management*** • ***Password Modification***	

Note

The hardware information, software versions, etc. of devices may vary, resulting in differences in functions they support. Please refer to the actual web page of your device, as this manual is provided for reference purposes only.

- Only PoE switches support PoE configuration.
- The DS-3EXXXX-SI series switches support ACL, IPSG, gateway ARP protection, and DHCP snooping configurations when running software version V3.1.0 or later. Models with versions below V3.1.0 do not support these features.
- The DS-3EXXXX-EI series switches do not support ACL, IPSG, and gateway ARP protection configurations. However, DHCP snooping is supported on models running software version V3.3.0 or later, while those with versions below V3.3.0 do not support this feature.

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.

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.

Preface

Applicable Models

This manual is applicable to smart managed switches.

About Defaults

- Default administrator account: **admin**
- Super IP address: 10.180.190.200

Note

- The default user name **admin** needs to be activated for first-time login.
- The default IP address of the switch is dynamically assigned. If a DHCP-assigned IP address fails to be obtained, the default IP address of the switch is 192.168.1.64.
- The default Super IP address is 10.180.190.200, which can be customized to align with your network configuration requirements. If the switch is directly connected to a PC, you can use this IP address to access the switch for device management.
- The default IP address serves as the regular management address for a switch, supports DHCP assignment, and is used for routine network management. Its accessibility depends on network configuration—improper VLAN setup may block cross-VLAN access. The super IP address is a fixed address specifically configured for a switch, primarily intended for direct login management when a computer is connected directly to the switch. It operates independently of VLAN or other network settings. If the default IP address becomes unreachable due to configuration errors, the super IP address enables direct web access for configuration purposes.

Symbol Conventions

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

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

Contents

Chapter 1 Product Introduction

Smart managed switches support management via web, supporting functions such as activation and login, device overview, network configuration, device configuration, and system maintenance.

Note

The functions supported vary with device models. If there are differences between the figures shown in this manual and the actual interfaces of your device, the latter prevails.

Chapter 2 Activation and Login

If you use the switch for the first time, you need to activate it and configure the password.

Before You Start

Ensure that your computer and switch are on the same network segment.

Steps

Note

All figures in this manual are for illustration purpose only.

1. Enter the switch's super IP address (10.180.190.200 by default) or default IP address (DHCP-assigned) in the address bar of a web browser, and press **Enter**.

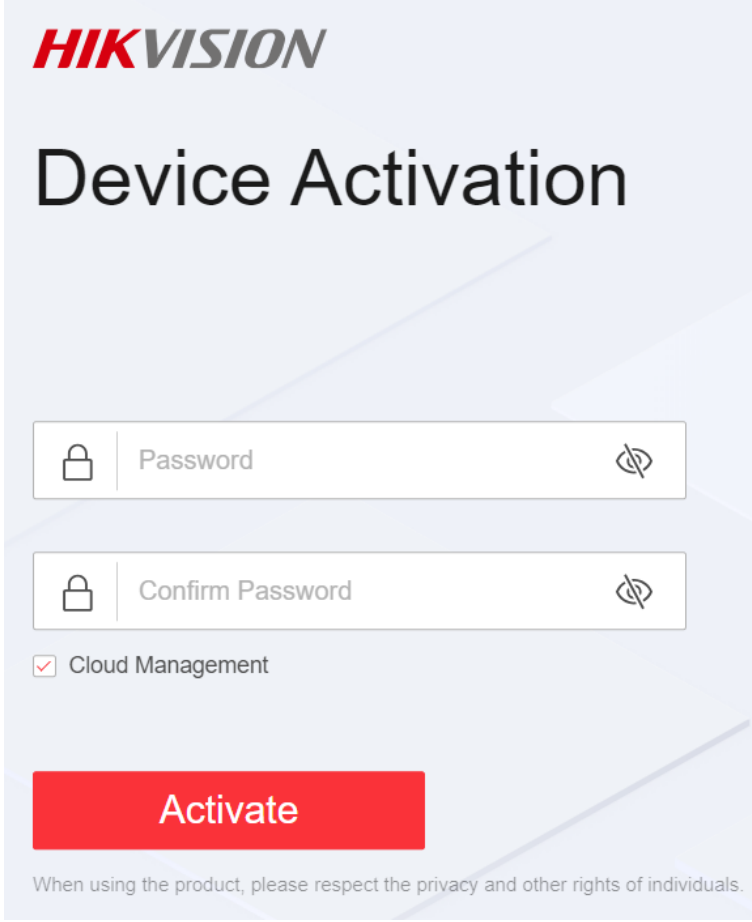


Figure 2-1 Activate Device

Note

- The switch's default IP address is dynamically assigned via DHCP. You can obtain it using the SADP tool.
- You are recommended to use the following web browsers: Microsoft Edge 89 or later, Google Chrome 89 or later, and Firefox 78 or later.

2. Set a password and confirm the password.

Note

- The password should contain 8 to 16 characters, including at least two types of the following categories: uppercase letters, lowercase letters, digits, and special characters.
- The password cannot contain user name, '123', or 'admin' (case-insensitive), 4 or more consecutively increasing or decreasing digits (such as '1234' and '4321'), or 4 or more identical characters (such as '1111' and 'aaaa').
- The password cannot contain only 'hik', 'hkws', or 'hikvision' (case insensitive).
- The password cannot be a common risky password.
- Remember to store your password securely. If you forget it, you can reset the password using the SADP tool or restore the device to factory settings via the reset button. Please note that resetting will erase all device configurations, so proceed with caution.

3. **Optional:** Check **Cloud Management**.

   The Hik-Connect service is enabled.

4. Click **Activate**.

   The network configuration page is displayed.

5. **Optional:** Modify the network configurations.

   1) Go to **System Management → Network Configuration → Network Configuration** .

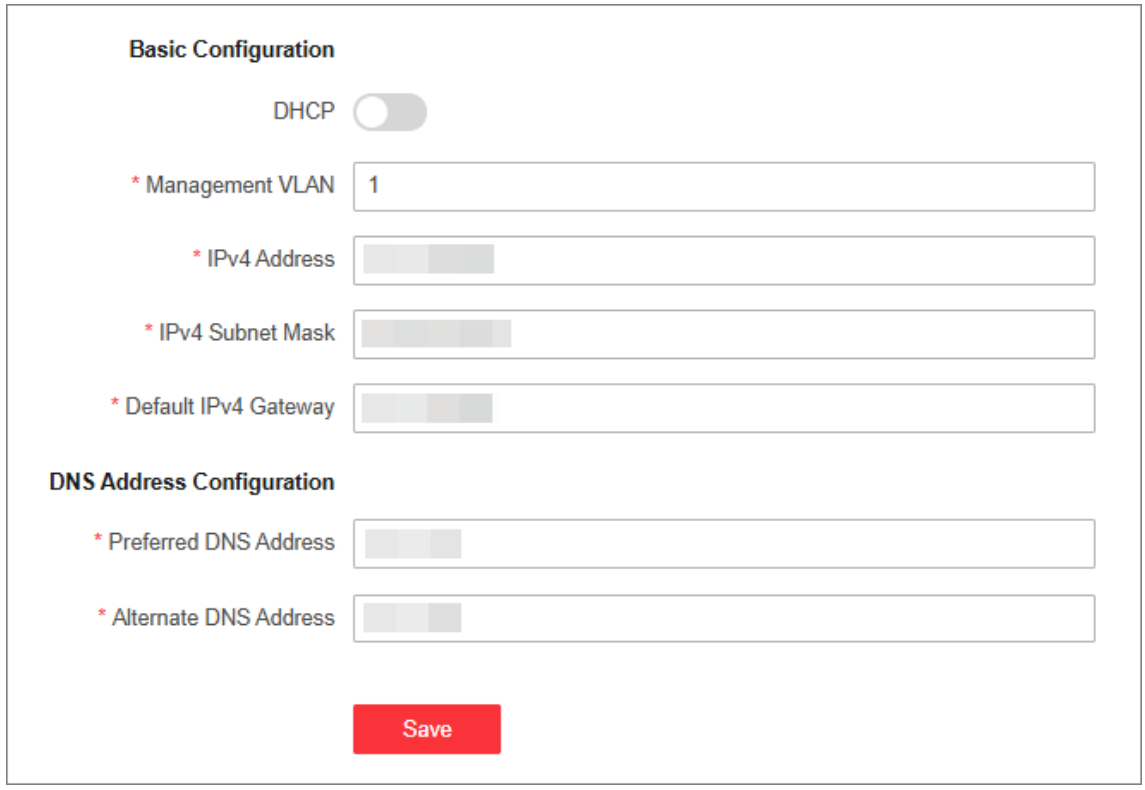


Figure 2-2 Modify Network Parameters

2) Modify the management VLAN, IPv4 address, IPv4 subnet mask, default IPv4 gateway, preferred DNS address, and alternate DNS address as required, or enable **DHCP** for automatic IP address assignment.

Note

You are recommended to modify the network configurations to better manage your switch.

3) Log in to the switch web again with the new IP address after modification.

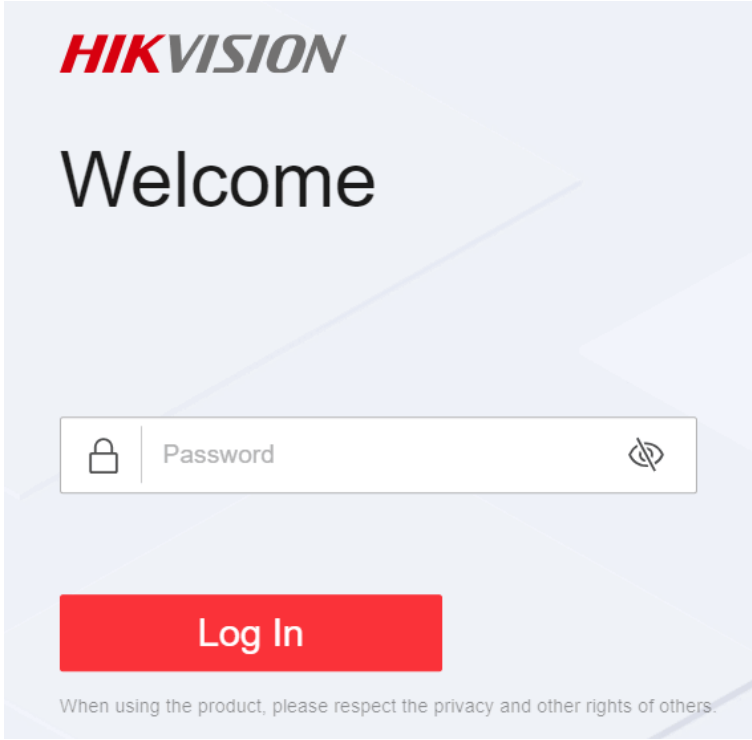


Figure 2-3 Log In

Chapter 3 Device Information

After logging in to the switch web, you can obtain detailed information about the switch, including the device overview information, port status information, and network status information.

3.1 Device Overview

You can view or edit the device overview information on the **Overview** page.

Basic Device Information

You can view the device model, software version, serial number, IP and MAC addresses, as well as CPU usage and memory usage of the switch in the lower right corner of the **Overview** page. For a PoE switch, you can also view the device's hardware information.

Figure 3-1 View Basic Device Information (Example of a PoE Switch)

Device Name

You can view the current device name or click next to it to customize the device name on the **Overview** page. The default device name is the device model.

Figure 3-2 Edit Device Name

System Uptime

You can also view the device's system uptime in the upper right corner of the **Overview** page.

Figure 3-3 View System Uptime

VLANs Added

You can quickly view the number of VLANs that have been added, or click to go to the **VLAN Management** page for VLAN configuration.

Figure 3-4 View Number of VLANs Added

Note

You can also view the maximum number of VLANs allowed by the device, for example, 4094 in the figure above. The maximum number of VLANs allowed by a device varies with device models.

Cloud Platform Connection Status

The **Cloud Platform** module shows whether the device is connected to Hik-Connect.

- If the cloud platform is connected, scan the QR code to add the device to Hik-Partner Pro app for remote management.

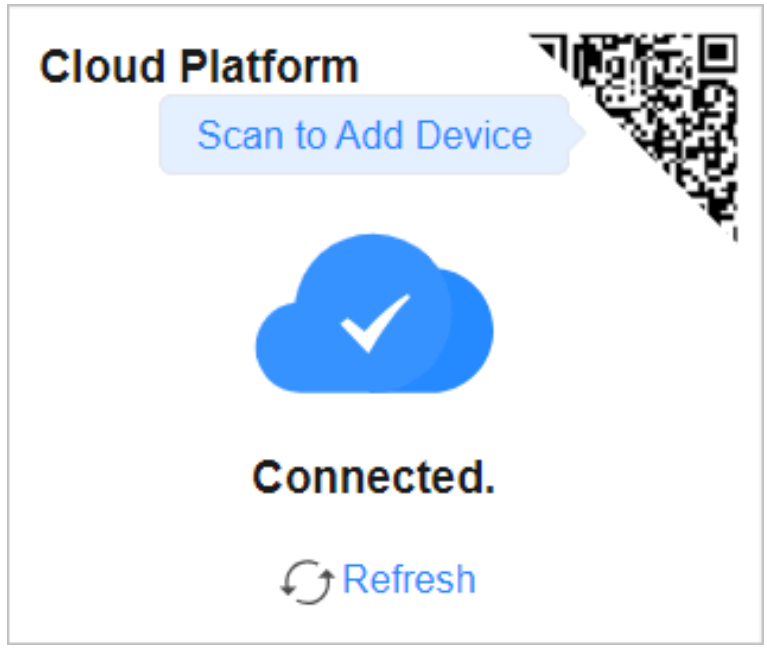


Figure 3-5 View Cloud Platform Connection Status (Connected)

- If the cloud platform is disconnected, click **Refresh** to reconnect, or click **Diagnose** to find out the cause of the connection failure and go to the cloud platform configuration page as prompted for cloud platform configuration.

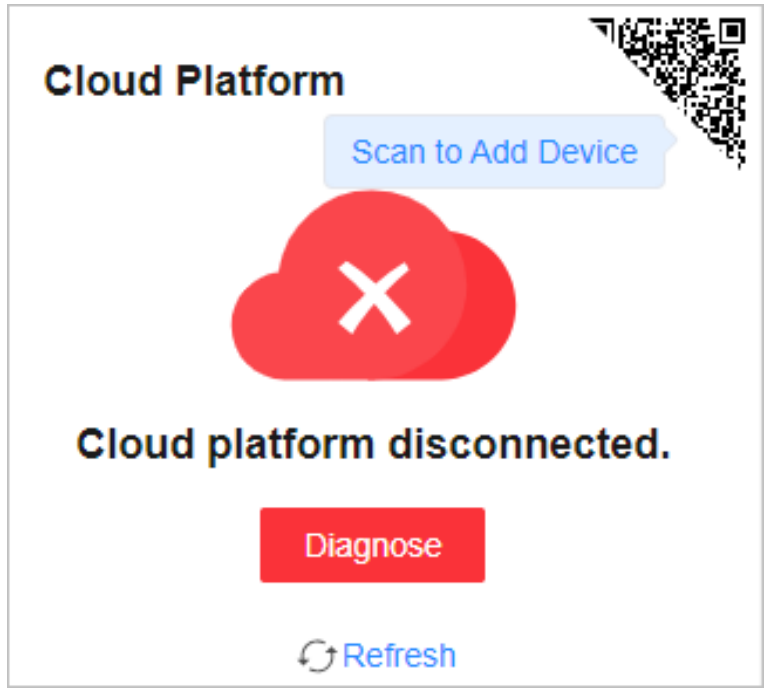


Figure 3-6 View Cloud Platform Connection Status (Disconnected)

3.2 Port Status

The **Overview** page provides a visual representation of the physical ports and shows the connection or power supply status of each port, making it easier for users to manage switch ports.

Port Panel

The **Port Panel** module displays the connection and power supply status of each port. When you hover the mouse over a port, the port name, connection status, rate/duplex, flow control status, and packet receiving/sending rate are displayed. If the port is a PoE port, you can view the PoE power of the port.

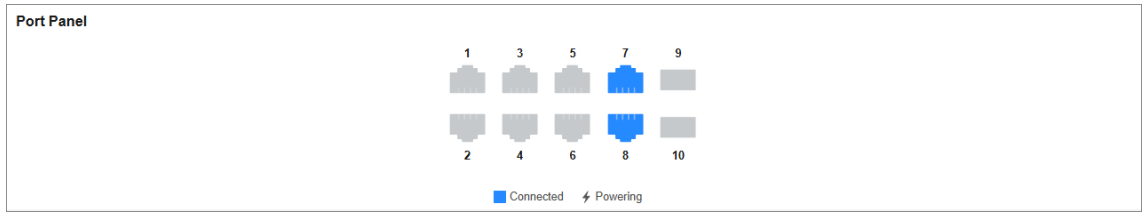


Figure 3-7 View Port Panel

Port Details

The **Port Details** module lists the status parameters of each port. You can also configure the port status, rate/duplex, and flow control of each port, and view the port name, connection status, and actual rate/duplex of each port.

Port Name	Alias	Connection Status	Port Up	Actual Rate/Duplex	Configured Rate/Duplex	Flow Control
Ge1	--	Disconnected		--	Auto/Auto	
Ge2	--	Connected		1000 Mbps/Full-Duplex	Auto/Auto	
Ge3	--	Disconnected		--	Auto/Auto	
Ge4	--	Disconnected		--	Auto/Auto	
Ge5	--	Disconnected		--	Auto/Auto	
Ge6	--	Disconnected		--	Auto/Auto	

Figure 3-8 View Port Details

Alias

Click to configure a port alias. A port alias refers to a user-defined descriptive name assigned to a network port for easier identification (e.g., labeling port "Ge1" as "Conference_Room_Camera").

Connection Status

The connection status of a port: **Connected** or **Disconnected**.

Port Up

Enable a port (port up) or disable a port (port down). By default, a port is in the up state.

Actual Rate/Duplex

The actual rate and duplex mode of a port.

Configured Rate/Duplex

Configure the rate and duplex mode of a port. The default value is **Auto/Auto**. You can select different combinations of rates and duplex modes as required.

Flow Control

Enable or disable flow control of a port. By default, flow control is enabled. Enabling flow control can effectively reduce the impact of large amounts of data on the network and maintain the stability of the network.

PoE Power

You can view the whole device PoE power and peak PoE power in last seven days of the switch. Click in the upper right corner of the module to go to the **PoE Management** page for PoE function configuration.

Figure 3-9 View PoE Power

Note

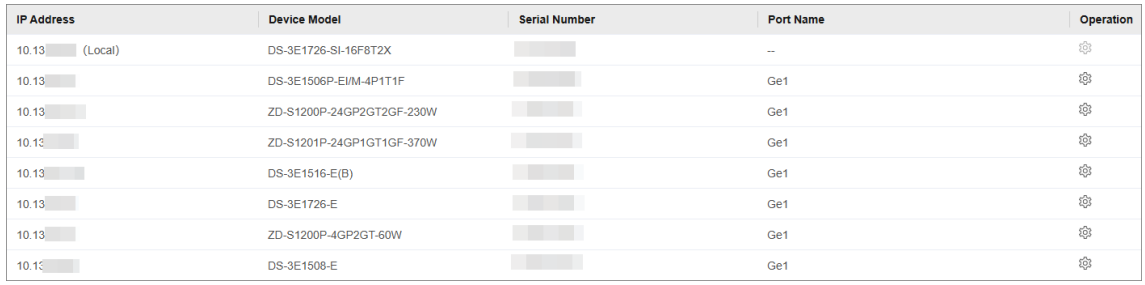
PoE power display is only available for switches supporting PoE.

3.3 Network Status

Network Monitoring allows you to view the same-LAN network device information, MAC addresses learned by ports, port statistics, and cable status.

Find Network Devices

Device Discovery automatically detects and identifies network devices and terminal devices within the same LAN as the switch. Go to **Network Monitoring → Device Discovery → Device Discovery** , and you can view the IP address, device model, serial number, and connected switch port of the detected device(s). You can also click in the **Operation** column of your desired device to access the device's web configuration page.



IP Address	Device Model	Serial Number	Port Name	Operation
10.13 (Local)	DS-3E1726-SI-16F8T2X		--	
10.13	DS-3E1506P-EI/M-4P1T1F		Ge1	
10.13	ZD-S1200P-24GP2GT2GF-230W		Ge1	
10.13	ZD-S1201P-24GP1GT1GF-370W		Ge1	
10.13	DS-3E1516-E(B)		Ge1	
10.13	DS-3E1726-E		Ge1	
10.13	ZD-S1200P-4GP2GT-60W		Ge1	
10.13	DS-3E1508-E		Ge1	

Figure 3-10 Network Devices Found

Additionally, you can go to **Network Monitoring → Device Discovery → Device Discovery Settings** to enable or disable **SADP Agent** or **Third-Party Terminal Recognition** according to the actual needs.

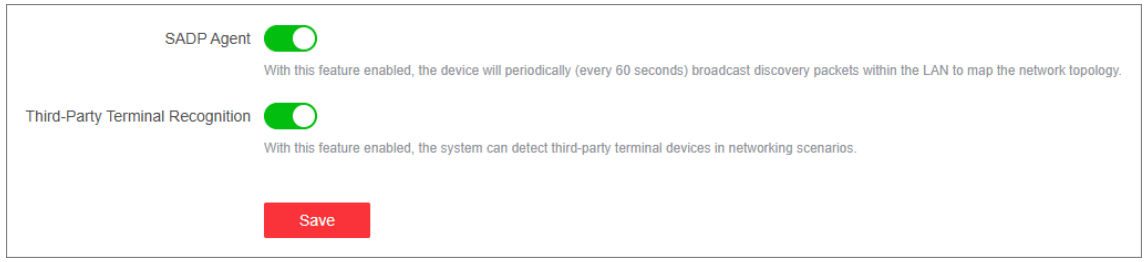


Figure 3-11 Device Discovery Settings

- When **SADP Agent** is enabled, the device broadcasts discovery packets within the LAN every 60 seconds to map the network topology.
- When **Third-Party Terminal Recognition** is enabled, the system identifies and displays third-party terminal devices for cross-brand topology management. When disabled, only Hikvision terminals are shown.

Query Port MAC Address

You can query the MAC address(es) learned by each port. Go to **Network Monitoring → MAC Address** , select the desired port from the **Port** drop-down list, and click **Search**. The MAC address(es) learned by the port and type(s) of the MAC address(es) are displayed in the list below.

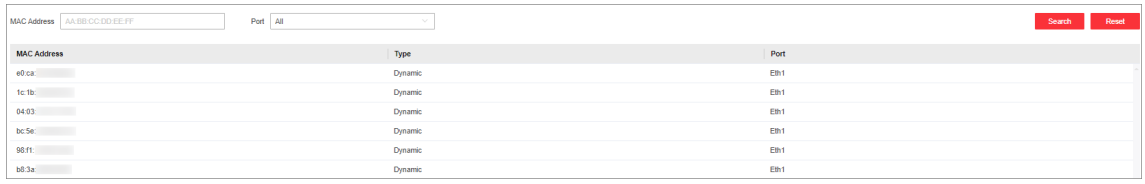


Figure 3-12 Query Port MAC Addresses

View Port Statistics

You can monitor and collect statistics on the transmitted data of device ports. Go to **Network Monitoring → Port Statistics** , and you can view the current connection status of each port and the data transmitted by each port in the statistics list.

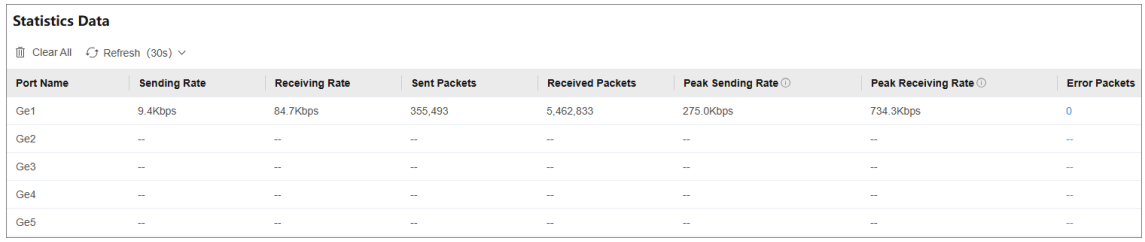


Figure 3-13 View Port Statistics

You can also perform the following operations:

- Clear port statistics: You can click **Clear All** to clear all the port statistics.
- Manually refresh port statistics: You can click to manually refresh the port statistics.
- Auto refresh port statistics: You can set the interval for automatically refreshing port statistics: 30 seconds or 60 seconds.
- View error packets details: You can click the number in the **Error Packets** column to view detailed information about error packets, including the number of CRC error packets and the number of flow control frames.

Detect Cable Status

Cable Detection is a function that detects the statuses of Ethernet port cables, for example, to check whether there is a short circuit or an open circuit in the receiving or sending direction of a cable, and if any, to locate the faulty cable. Go to **Network Monitoring → Cable Detection** , select the desired port on the left port panel, and click **Detect** to view the detection result.

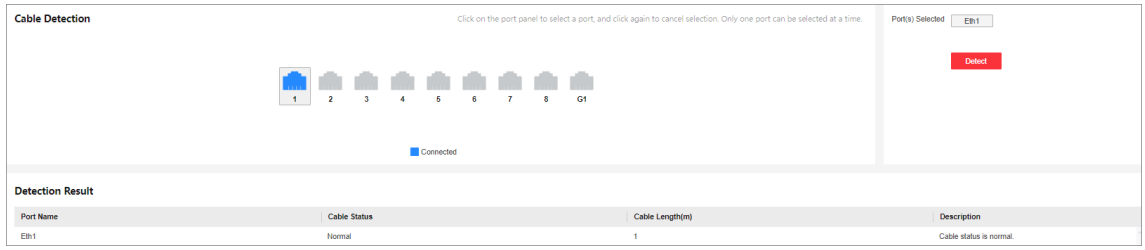


Figure 3-14 Detect Cable Status

Note

Only RJ45 ports support cable detection, while SFP/SFP+ fiber optical ports do not.

Diagnose Optical Module

Digital Diagnostic Monitoring (DDM) is a function used to monitor real-time parameters of an optical module, such as operating temperature, operating voltage, operating current, and Rx and Tx optical power. In addition, the DDM diagnosis result shows an optical module's converter type, interface type, central Tx wavelength, maximum transmission distance, and brand.

1. Go to **Network Monitoring → DDM** .

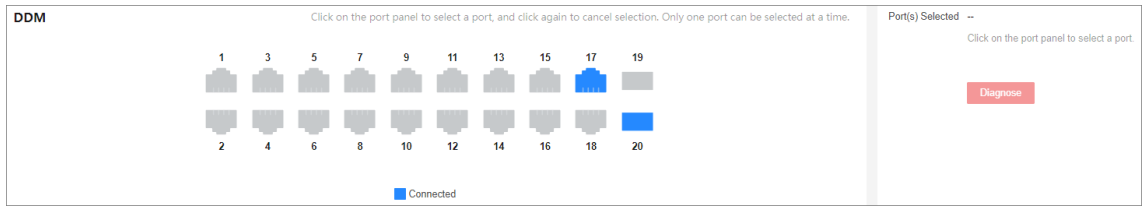


Figure 3-15 Configure Optical Module Diagnosis

2. Select an optical port with an optical module plugged into on the port panel.
3. Click **Diagnose**.

Note

After diagnosis is complete, you can view the DDM diagnosis result in the **Diagnosis Information** area.

Figure 3-16 View DDM Diagnosis Result

4. Click ⓘ next to **Temperature**, **Voltage**, **Current**, **Rx Power**, or **Tx Power** to check whether the values of these parameters are within the normal range.

Chapter 4 Device Configuration

4.1 Port Configuration

4.1.1 Configure Port Attributes

The basic attributes can influence the working status of a port.

Steps

1. Go to **L2 Configuration → Port Attributes** .

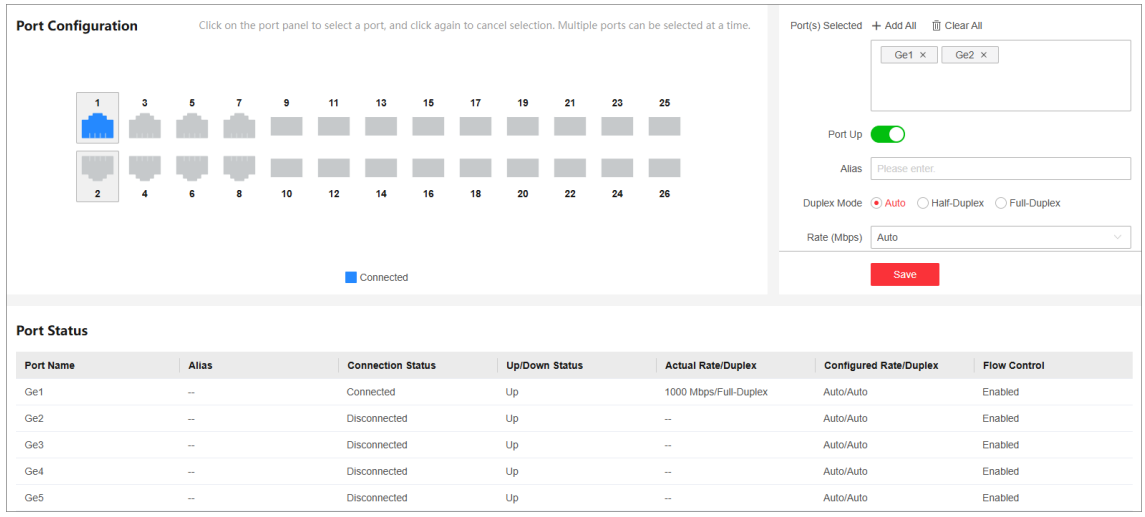


Figure 4-1 Configure Port Attributes

2. Select the desired port(s) and set the parameters as required.

Note

You can also click + Add All or Clear All on the right to batch select or deselect all ports.

Port Up

Enable or disable the selected port(s). If a port is enabled, it is in the up state; if a port is disabled, it is in the down state. No data will be transmitted on a "down" port.

Alias

User-defined descriptive name assigned to a network port for easier identification. You can set a port alias as required, for example, labeling port "Ge1" as "Conference_Room_Camera".

Duplex Mode

The duplex mode of a port. The configurable duplex modes of ports include **Half-Duplex**, **Full-Duplex**, and **Auto**, which may vary with device models.

Rate (Mbps)

The data transmission speed of a port of a port. The configurable rates of ports include **10M**, **100M**, **1000M**, and **Auto**, which may vary with device models.

Flow Control

Enable or disable flow control of a port. Enabling flow control can prevent data loss in data transmission.

3. Click **Save**.
4. **Optional:** View the port attributes in the **Port Status** list.

4.1.2 Configure Link Aggregation

Link aggregation is used to combine multiple physical links together to make a logical high-bandwidth data path, which provides a stronger and faster network connection.

Steps

1. Go to **L2 Configuration → Link Aggregation** .

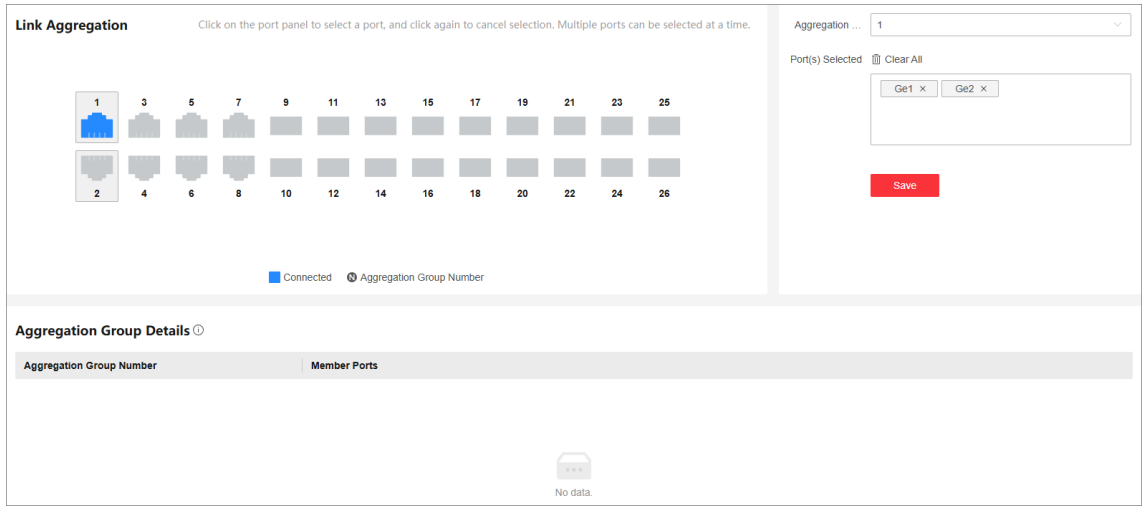


Figure 4-2 Configure Link Aggregation (No Aggregation Group Configured)

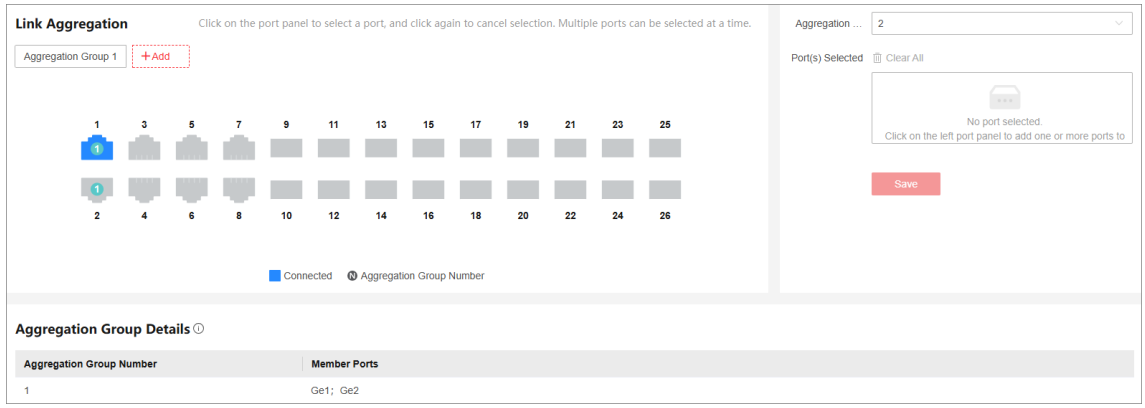


Figure 4-3 Configure Link Aggregation (At Least 1 Aggregation Group Exists)

2. **Optional:** Click +Add .

Note

Only perform this step when one or more aggregation groups exist.

3. Set **Aggregation Group Number**.

Note

The number of aggregation groups allowed varies with device models.

4. Select at least two desired ports.

Note

- Only the selectable ports can be added to an aggregation group.
- 2 to 4 ports are allowed for each link aggregation group.
- Some ports can only be added to a specific aggregation group. Please refer to the actual situation.
- The rate, duplex mode, flow control, long-range mode, and VLAN configurations of ports in one aggregation group should be the same.
- Ports in an aggregation group do not support port-specific configurations, including port attributes, port isolation, port rate limiting, port storm control, long-range function, VLAN, DHCP snooping, etc.

5. Click **Save**.
6. **Optional:** Edit the aggregation group.
   1) Click an existing aggregation group, for example, "Aggregation Group 1".
   2) Select the desired port(s) on the left port panel to add to the group, or deselect the desired port(s) on the right to delete from the group.
   3) Click **Edit** to save the modification.
7. **Optional:** Delete the aggregation group.
   1) Click an existing aggregation group, for example, "Aggregation Group 1".
   2) Click **Delete** on the right.

8. **Optional:** View the member ports of each aggregation group in the **Aggregation Group Details** list.

4.1.3 Configure Port Isolation

Port isolation is a feature to add multiple ports to an isolation group so that ports in the same isolation group cannot communicate with each other. For example, by using port isolation function, you can achieve the goal of preventing PCs under different ports communicating with each other without configuring VLANs.

Steps

1. Go to **Security → Port Isolation** .

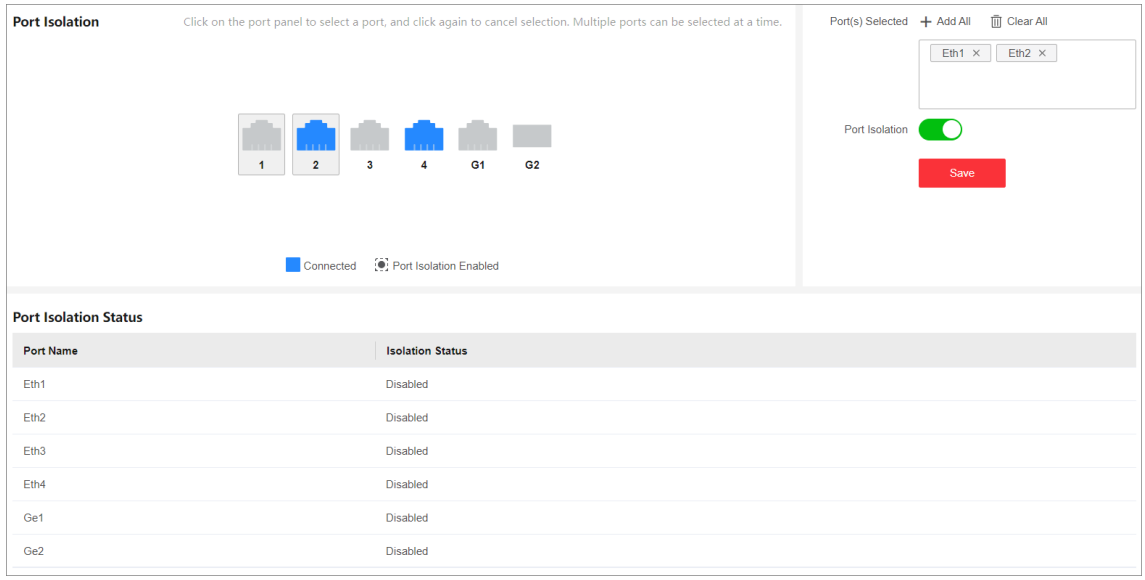


Figure 4-4 Configure Port Isolation

2. Select the desired port(s) on the port panel.

Note

You can also click + Add All or Clear All on the right to batch select or deselect all ports.

3. Enable or disable **Port Isolation** as required.
4. Click **Save**.
5. **Optional:** View the port isolation status of each port in the **Port Isolation Status** list.

4.1.4 Configure Port Mirroring

Port mirroring is a feature in network switches that allows administrators to monitor traffic on one port (mirrored port) and replicate this data to another port (mirroring port) for analysis. This

replication occurs in real-time, allowing an administrator to view a "mirror" or exact duplicate of the traffic moving on the mirrored port.

Steps

1. Go to **L2 Configuration → Port Mirroring** .

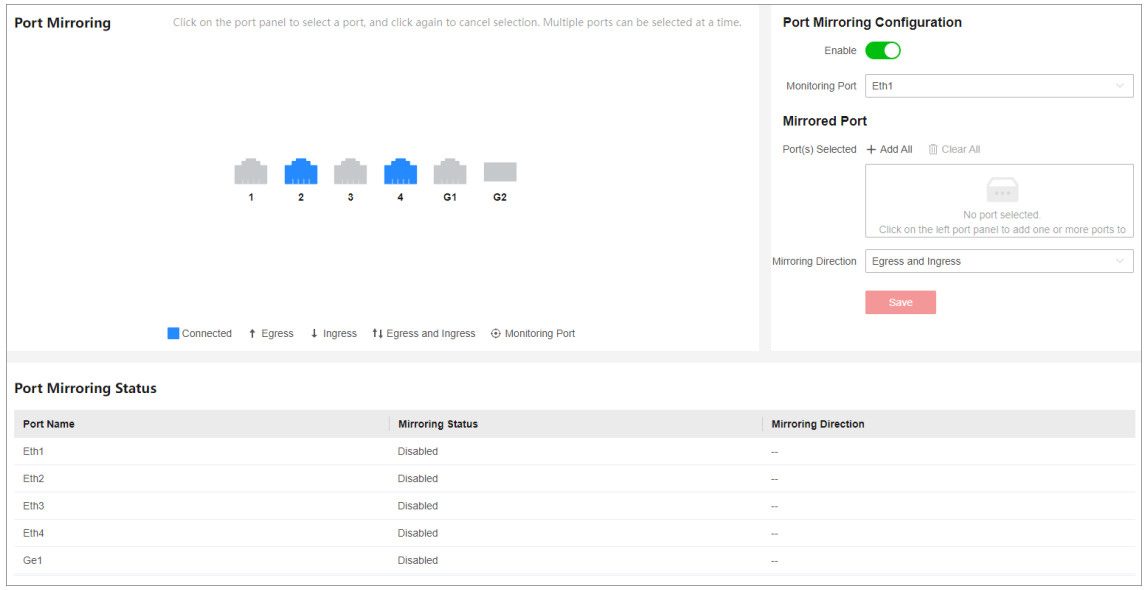


Figure 4-5 Configure Port Mirroring

2. Select the desired port(s) on the port panel as the mirrored port(s), and set the parameters as required.

Note

You can also click + Add All or Clear All on the right to batch select or deselect all ports.

Enable

Enable or disable port mirroring of the selected port(s).

Monitoring Port

Only one port can be set as the monitoring port (mirroring port).

Mirroring Direction

Ingress

The data received by the source port will be under monitoring.

Egress

The data sent by the source port will be under monitoring.

Egress and Ingress

Both the data received by and the data sent from the source port will be under monitoring.

3. Click **Save**.

Note

The latest configuration will overwrite the previous configuration.

4. **Optional:** View the mirroring status of each port in the **Port Mirroring Status** list.

4.1.5 Configure Port Rate Limiting

Port rate limiting refers to limitation of a port's sending and receiving rates. This feature may not be available on all devices. Please consult your device specifications for compatibility details.

Steps

1. Go to **Service Quality → Port Rate Limiting** .

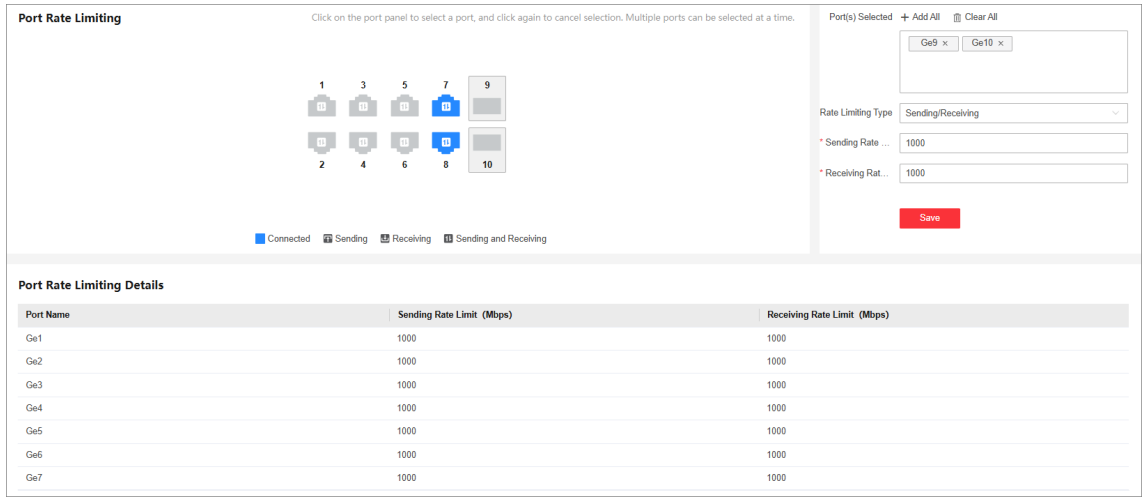


Figure 4-6 Configure Port Rate Limiting

2. Select the desired port(s) on the port panel, and set the parameters as required.

Note

You can also click + Add All or Clear All on the right to batch select or deselect all ports.

Rate Limiting Type

- **Sending**: Only the sending rate of the selected port(s) is limited.
- **Receiving**: Only the receiving rate of the selected port(s) is limited.
- **Sending/Receiving**: Both the sending and receiving rates of the selected port(s) are limited.
- **No Limit**: Neither the sending rate nor the receiving rate of the selected port(s) is limited.

Sending Rate Limit(Mbps)

Set the upper limit of sending rate when **Rate Limiting Type** is **Sending** or **Sending/Receiving**. This parameter dynamically adjusts its valid input range based on the port's physical bandwidth:

- For a 100 Mbps Ethernet port, the configurable range is 1 to 100 Mbps.
- For a 1000 Mbps Ethernet port, the configurable range is 1 to 1000 Mbps.
- For a 10 Gbps Ethernet port, the configurable range is 1 to 10,000 Mbps.

Receiving Rate Limit(Mbps)

Set the upper limit of receiving rate when **Rate Limiting Type** is **Receiving** or **Sending/ Receiving**. This parameter dynamically adjusts its valid input range based on the port's physical bandwidth:

- For a 100 Mbps Ethernet port, the configurable range is 1 to 100 Mbps.
- For a 1000 Mbps Ethernet port, the configurable range is 1 to 1000 Mbps.
- For a 10 Gbps Ethernet port, the configurable range is 1 to 10,000 Mbps.

3. Click **Save**.
4. **Optional:** View the rate limiting details of each port in the **Port Rate Limiting Details** list.

4.1.6 Configure Port Storm Control

Storm control allows you to limit the amount of broadcast, multicast, or unknown unicast traffic that can be received on a port. When such traffic exceeds a specified threshold, the excess broadcast, multicast, or unknown unicast packets will be discarded to prevent network storms. This feature may not be available on all devices. Please consult your device specifications for compatibility details.

Steps

1. Go to **Service Quality → Port Storm Control** .

Note

Some devices support both global and port-based storm control configuration, while others support only global storm control configuration. The actual device conditions prevail.

2. Set storm control parameters as required.
   - Global Storm Control:

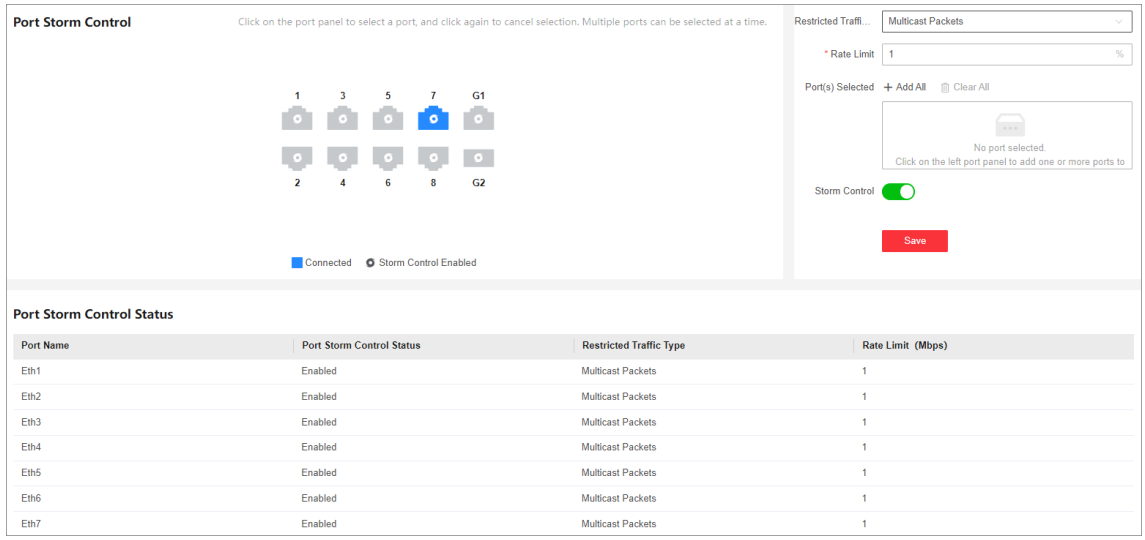


Figure 4-7 Configure Global Storm Control

a. Set **Restricted Traffic Type** and **Rate Limit**.

Restricted Traffic Type

Broadcast Packets

The data packets are sent to all the devices on the same network.

Multicast Packets

The data packets are sent to the specified devices.

Unknown Unicast Packets

The data packets are sent to the specified device.

Rate Limit

Set the rate limit percentage of the selected port(s). The valid range of this parameter varies depending on the device model and port type/speed. Please refer to the actual interface display for accurate information.

b. Select the desired port(s) on the port panel.

Note

You can also click + Add All or Clear All on the right to batch select or deselect all ports.

c. Enable storm control of the selected port(s).

- Port-Based Storm Control:

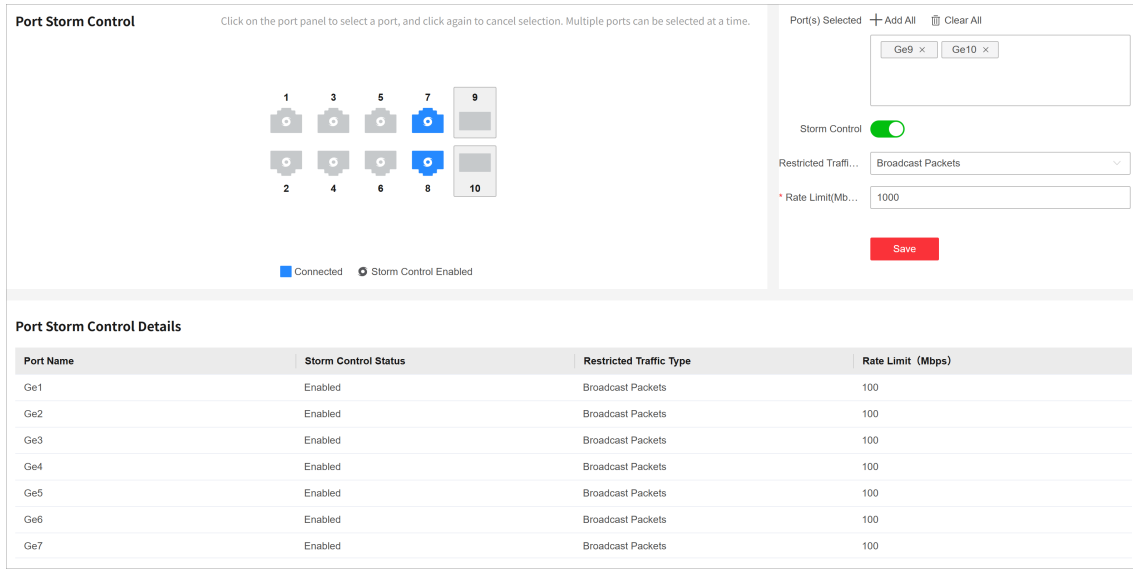


Figure 4-8 Configure Port-Based Storm Control

a. Select the desired port(s) on the port panel.

Note

You can also click + Add All or Clear All on the right to batch select or deselect all ports.

b. Enable storm control of the selected port(s).

c. Set **Restricted Traffic Type** and **Rate Limit(Mbps)**.

Restricted Traffic Type

Broadcast Packets

The data packets are sent to all the devices on the same network.

Multicast Packets

The data packets are sent to the specified devices.

Unknown Unicast Packets

The data packets are sent to the specified device.

Rate Limit(Mbps)

Set the rate limit of the selected port(s). The valid range of this parameter varies depending on the device model and port type/speed. Please refer to the actual interface display for accurate information.

3. Click **Save**.
4. **Optional:** View the storm control status of each port in the **Port Storm Control Status** list.

4.1.7 Configure Long-Range Function

Enabling the long-range function allows the long-range port(s) to achieve a transmission distance of up to 300 meters at a rate of 10 Mbps. Actual performance may vary depending on the device model and environmental conditions.

Steps

1. Go to **L2 Configuration → Long-Range Configuration** .

Note

Some devices support both auto and manual long-range modes, while others support only manual long-range mode. Please refer to the actual interface display for accurate information.

2. **Optional:** Set **Long-Range Mode** to **Auto** or **Manual**.

Note

This step is only required when the device supports both auto and manual long-range modes. If the device supports only manual long-range mode, skip this step.

- **Auto**: The device will automatically enable or disable the long-range function based on the terminal device connected to the long-range port. No manual configuration is required.

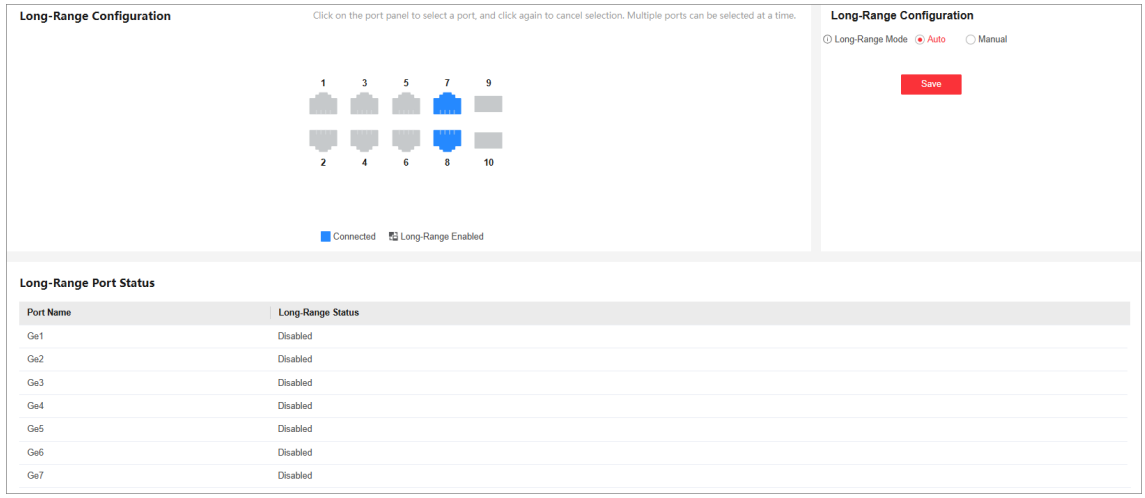


Figure 4-9 Configure Auto Long-Range Mode

Note

For devices supporting both auto and manual long-range modes, auto mode is enabled by default.

- **Manual**: Manual configuration is required. Please refer to Steps 3 and 4 for detailed instructions.

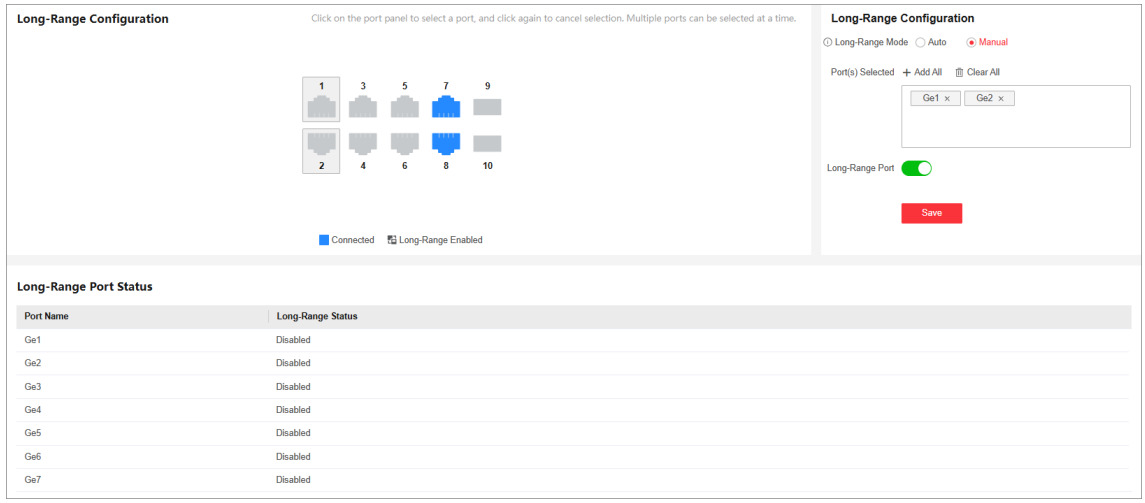


Figure 4-10 Configure Manual Long-Range Mode

3. **Optional:** Select the desired port(s) on the port panel.

Note

- You can also click + Add All or Clear All on the right to batch select or deselect all ports.
- If you choose **Auto** long-range mode, skip this step.

4. **Optional:** Enable or disable **Long-Range Port** as required.

Note

If you choose **Auto** long-range mode, skip this step.

5. Click **Save**.
6. **Optional:** View the long-range status of each port in the **Long-Range Port Status** list.

Note

- In auto long-range mode, the **Long-Range Status** column displays the actual enabling status of the long-range function. For example, if a device port is connected with a long network cable for long-range transmission, the status will show as **Enabled**.
- In manual long-range mode, the **Long-Range Status** column shows the configured status of the long-range function. For example, when the long-range function is manually enabled on a port, the status will display as **Enabled**.

4.1.8 Configure High-Priority Port

High-priority ports are identified by a red area on the device front panel. In the case of uplink congestion, the data of ports in this area is preferentially transmitted.

Steps

1. Go to **Service Quality → High-Priority** .

Note

High-priority port configuration is only supported when the switch has high-priority ports.

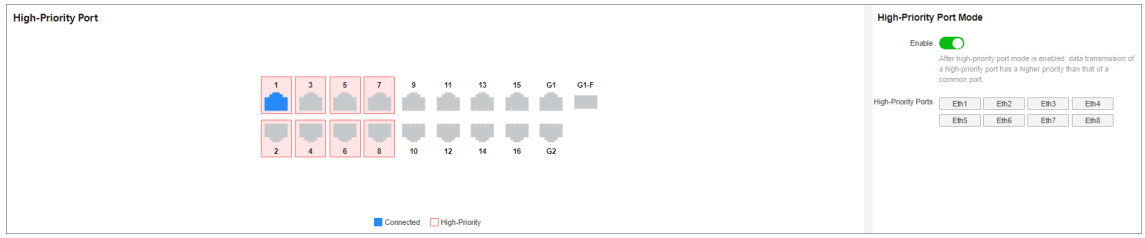


Figure 4-11 Configure High-Priority Port

2. In **High-Priority Port Mode**, toggle on **Enable** to batch enable high-priority ports.

Note

The number of high-priority ports varies with different device models. Please refer to the actual situation.

All high-priority ports of the switch are enabled, with a higher data transmission priority than common ports.

4.2 VLAN Configuration

Virtual Local Area Networks (VLANs) separate an existing physical network into multiple logical networks. Thus, each VLAN creates its own broadcast domain. With VLANs configured on a switch, users in the same VLAN can communicate with each other, while users in different VLANs are isolated. In this way, different broadcast domains are isolated, enhancing network security.

4.2.1 Add VLAN

Steps

1. Click **VLAN Management** in the left navigation pane.
2. In **Global VLAN Configuration**, click **Edit → Add** .
3. Select an adding mode.
   - **Single**: Only one VLAN is added at a time.

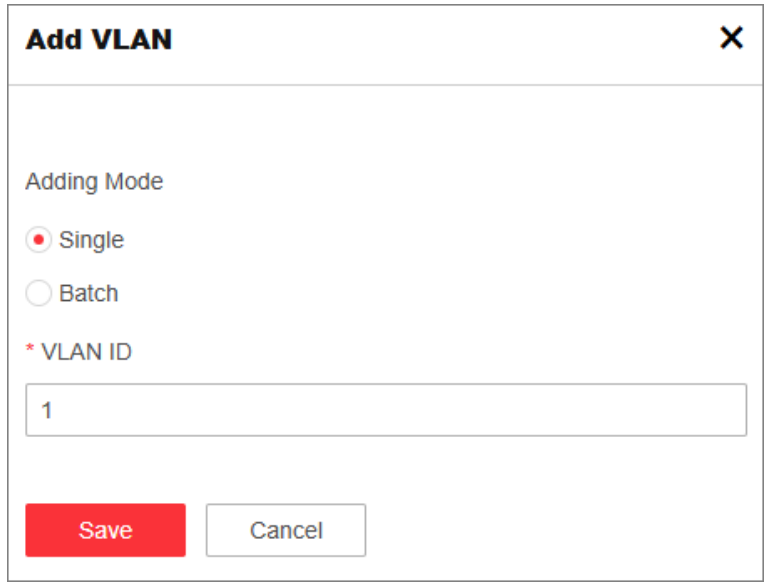


Figure 4-12 Add a Single VLAN

- **Batch**: Multiple VLANs are added in a batch.

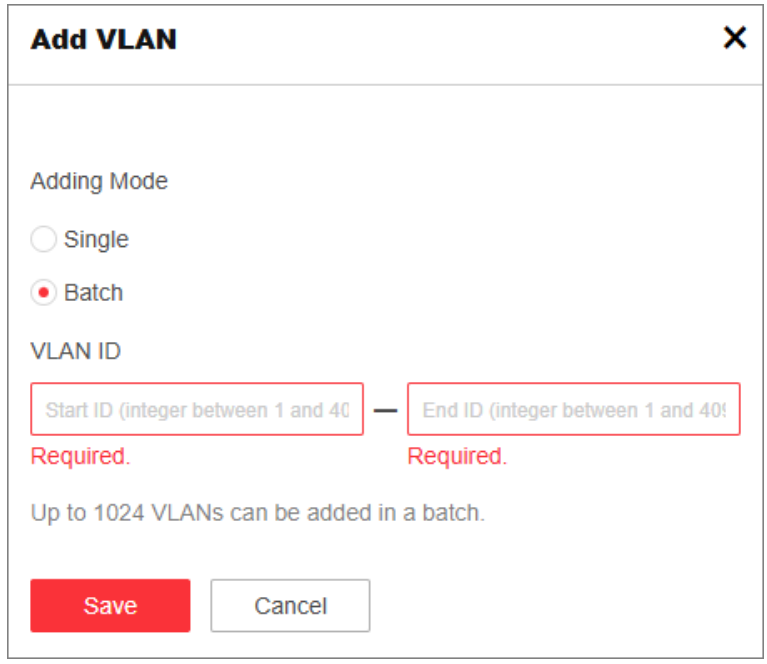


Figure 4-13 Batch Add VLANs

Note

The maximum number of VLANs that can be added in a batch varies with device models. Please refer to the actual situation.

4. Set **VLAN ID**.

- **Single**: Enter a VLAN ID.
- **Batch**: Enter the start VLAN ID and end VLAN ID.

Note

- The VLAN ID should be an integer between 1 and the maximum number of VLANs allowed by the device. For example, if the maximum number of VLANs allowed is 4094, the VLAN ID should be integer between 1 and 4094.
- The end VLAN ID should be greater than the start VLAN ID.
- The number of VLANs to be batch added should be no more than the maximum number of VLANs that can be added in a batch. For example, in the case that the maximum number of VLANs that can be added in a batch is 128, if you set the start VLAN ID to 1, the end ID cannot be greater than 128.

5. Click **Save**.
6. **Optional:** Select the desired VLAN(s) and click **Delete** to delete one or more VLANs.

Note

The default VLAN 1 cannot be deleted.

4.2.2 Configure Port VLAN

Steps

1. Select the desired port(s) on the port panel.

Note

- You can also click + Add All or Clear All on the right to batch select or deselect all ports.
- VLAN configuration is not allowed for ports in an aggregation group.

2. Configure the port VLAN type.

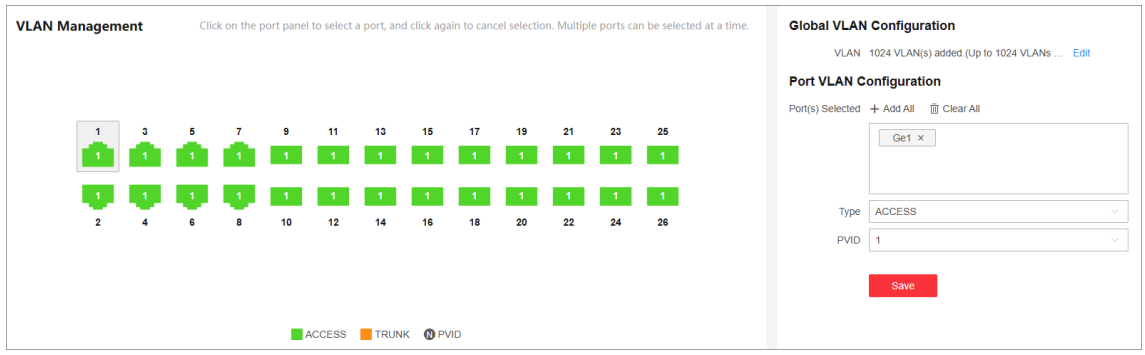
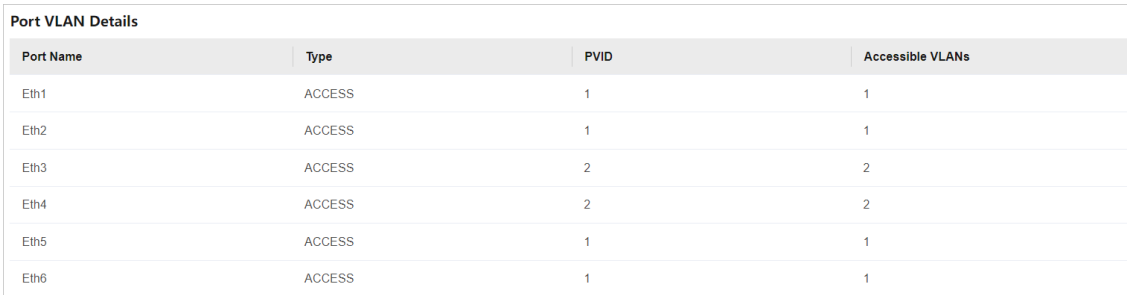


Figure 4-14 Configure Port VLAN

- **ACCESS**: An ACCESS port can have only one VLAN configured on the interface, and it can carry traffic for only one VLAN, usually the default VLAN (VLAN 1). Select **Type** as **ACCESS**, and set **PVID**.

- **TRUNK**: A TRUNK port can have two or more VLANs configured on the interface, and it can carry traffic for several VLANs simultaneously. Select **Type** as **TRUNK**, set **PVID**, and enter **Accessible VLANs**.

3. Click **Save**.
4. **Optional:** View the VLAN configuration information of each port in the **Port VLAN Details** list.



Port VLAN Details

Port Name	Type	PVID	Accessible VLANs
Eth1	ACCESS	1	1
Eth2	ACCESS	1	1
Eth3	ACCESS	2	2
Eth4	ACCESS	2	2
Eth5	ACCESS	1	1
Eth6	ACCESS	1	1

Figure 4-15 Port VLAN Details

4.3 PoE Configuration

PoE configuration, exclusively available on PoE-supported switches, comprises four modules: port-level PoE settings, PoE watchdog configuration, PoE mode setup, and power saving plan configuration.

4.3.1 Configure Port PoE

Enable PoE for the selected port(s) to deliver IEEE 802.3af/at/bt compliant power to connected powered devices (PDs).

Steps

1. Click **PoE Management → PoE Management → Port PoE Configuration** .

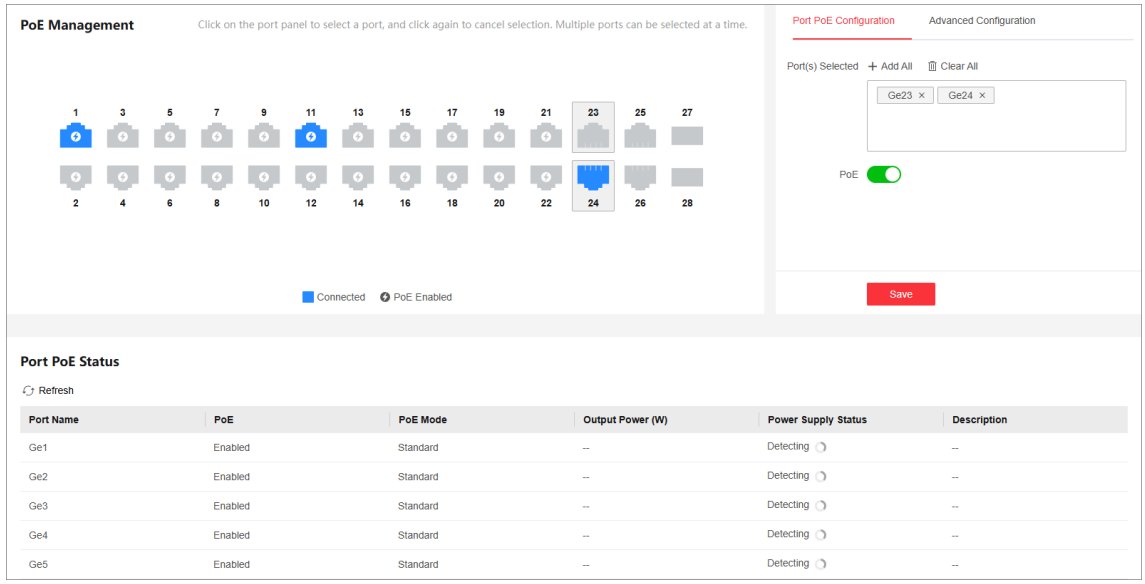


Figure 4-16 Configure Port-Level PoE

2. Select the desired port(s) on the port panel.

Note

You can click + Add All or Clear All to batch select or deselect all ports.

3. Enable **PoE** to supply power to the PD(s) connected to the port(s).

4. Click **Save**.

4.3.2 Configure PoE Watchdog

Click **PoE Management → PoE Management → Advanced Configuration** , and enable PoE watchdog to auto-detect and restart IP cameras that do not respond.

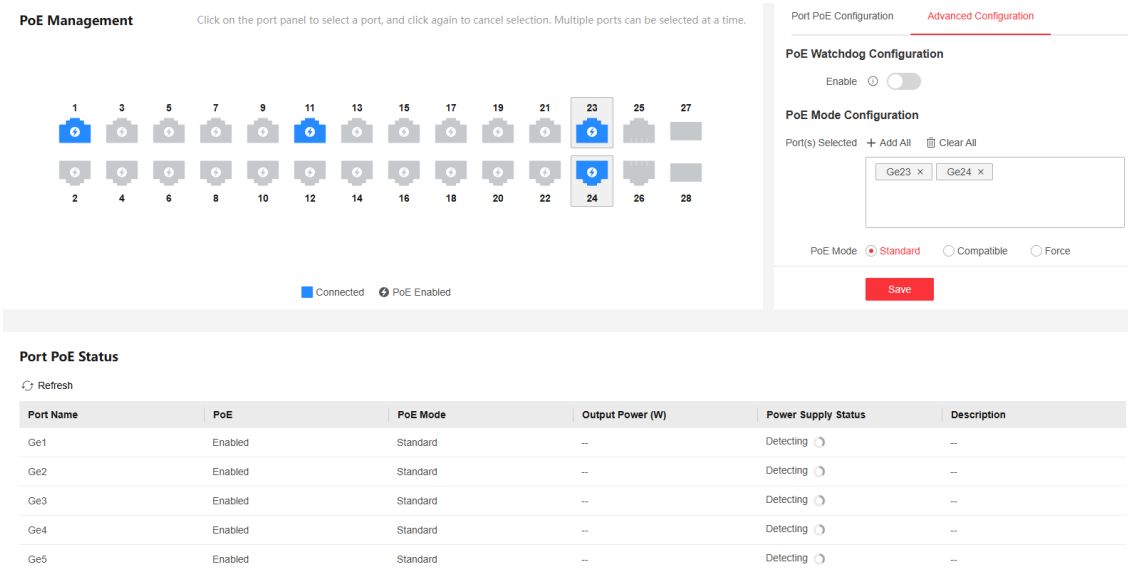


Figure 4-17 Configure PoE Watchdog

4.3.3 Configure PoE Mode

PoE mode configuration determines how power is delivered through the port.

The available modes include:

- Standard – Follows IEEE PoE standards for interoperability.
- Compatible – Supports non-standard powered devices.
- Force – Provides continuous power, bypassing device negotiation.

Steps

1. Click **PoE Management → PoE Management → Advanced Configuration** .

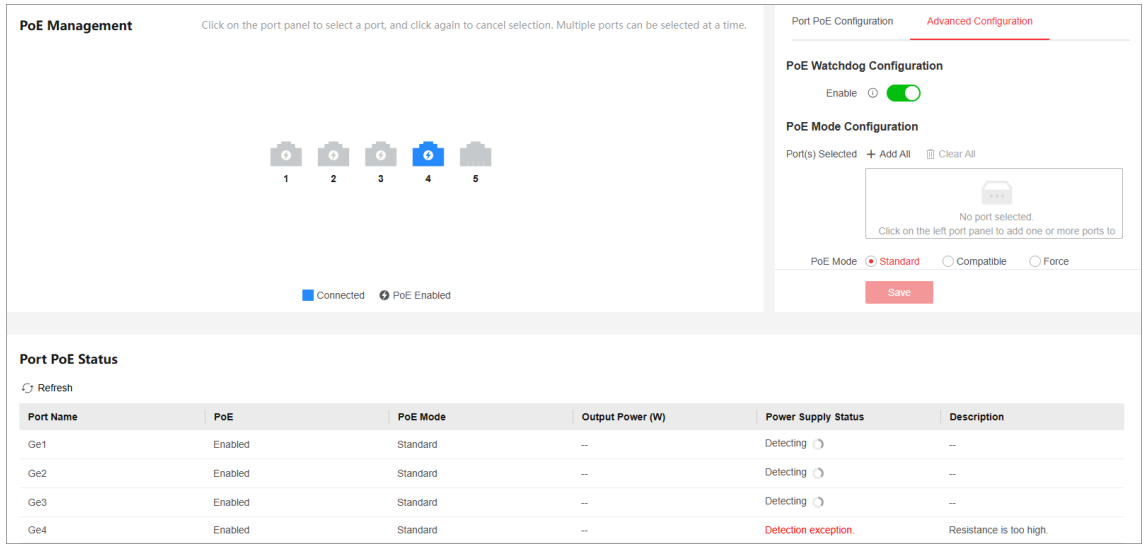


Figure 4-18 Configure PoE Mode

2. Select the desired port(s) on the port panel.

Note

You can click + Add All or Clear All to batch select or deselect all ports.

3. Set **PoE Mode** to **Standard**, **Compatible**, or **Force**.

Standard

Enabling standard mode allows the selected port(s) on the switch (acting as a PSE) to supply power to IEEE 802.3af/at/bt-compliant PDs. This mode is recommended as the first choice.

Compatible

Enabling compatible mode enhances compatibility for certain powered devices (PDs), preventing potential power supply failures. Although this mode improves compatibility for non-standard IPCs and APs, it may reduce the PD detection sensitivity of PoE ports. It is recommended to enable this mode when certain PDs cannot receive power from the switch, allowing PoE ports to detect and supply power to devices that do not comply with standard PoE protocols.

Force

Enabling force mode bypasses PoE negotiation to forcibly deliver power to the connected device. It is recommended that you enable this mode only after verifying the connected device's PoE compatibility, as an incorrect configuration may result in permanent damage to the device.

4. Click **Save**.
5. **Optional:** View the PoE enabling status, PoE mode, output power, and power supply status, etc. of PoE ports in the **Port PoE Status** list.

Note

The **Description** column displays PD classification when power is supplied normally, or shows exception information when an abnormal power supply occurs, helping to identify PoE power-on issues.

4.3.4 Configure Power Saving Plan

The power saving plan allows you to set basic rules for powering off PoE ports during specified time periods on designated days of the week, contributing to power conservation.

Before You Start

Set system date and time in **System Management → Time Configuration** first for the power saving rule(s) to take effect.

Steps

1. Click **PoE Management → Power Saving Plan** .

Note

By default, no power saving plan is configured.

2. In **Rule Configuration**, click **Add**.

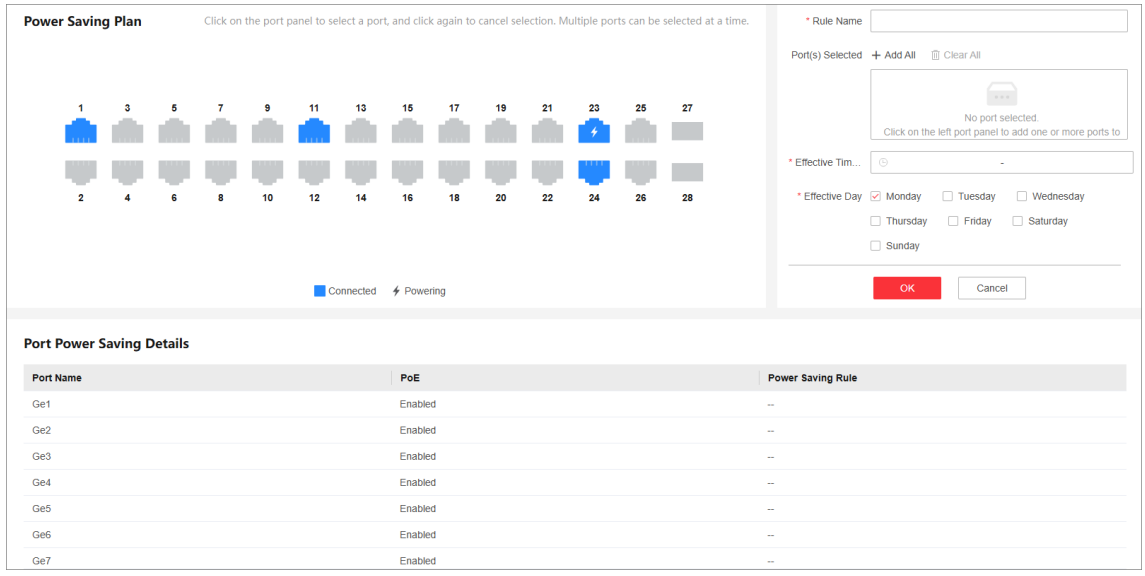


Figure 4-19 Configure Power Saving Plan

3. Set **Rule Name**, for example, ***Daytime***.
4. **Optional:** Select the desired PoE port(s) on the port panel.

Note

- You can also click + Add All or Clear All to batch select or deselect all PoE ports.
- You can also choose not to select any PoE ports. After the configuration is saved, the rule will not take effect.

5. Manually set **Start Time** and **End Time** to define the effective time period of the newly added rule within a 24-hour cycle.

Note

The start time should be earlier than the end time.

6. Set **Effective Day** to specify on which day(s) of the week the newly added rule will take effect.
7. Click **OK**.
8. **Optional:** Repeat the above steps to add multiple basic power-saving rules.

Note

Up to 7 basic power-saving rules can be configured, and the rule configurations will still persist after the device is powered off and restarted.

9. **Optional:** Select a power saving rule, and click **Edit** or **Delete** to edit or delete the rule.

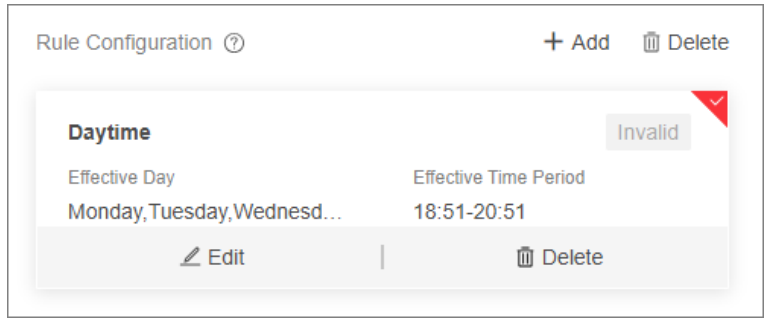


Figure 4-20 Edit/Delete Rule

Note

If you no longer want this rule to be effective for the selected PoE port(s), you can edit the rule and deselect the selected ports. After the modification is saved, the rule will still exist and will not be deleted, but it will no longer take effect. When you want this rule to be effective for the specified port(s) again, you can edit the rule and select the desired port(s).

4.4 EEE Configuration

Energy Efficient Ethernet (EEE), standardized as IEEE 802.3az, enhances traditional Ethernet by reducing power consumption during low-activity periods while maintaining full compatibility with existing networks. Unlike conventional Ethernet where devices remain constantly active, EEE

enables physical layer devices to enter a Low Power Idle (LPI) state during network inactivity, significantly cutting energy use without impacting performance.

1. Go to **L2 Configuration → EEE Mode** .
2. Toggle on **Enable** to enable EEE mode.

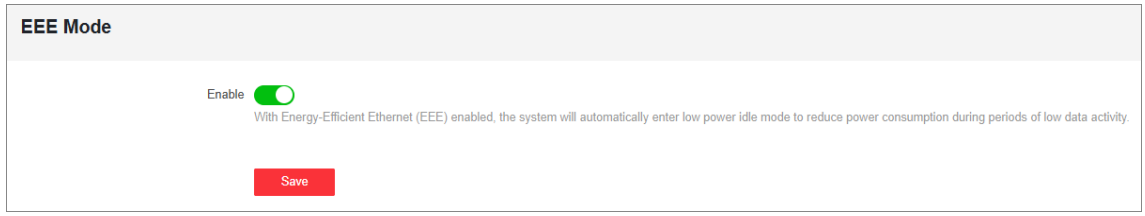


Figure 4-21 Configure EEE

Note

With this feature enabled, the system will automatically enter low power idle mode during periods of low data activity.

4.5 QoS Configuration

Quality of Service (QoS) is a technology used to solve issues such as network congestion, delay, jitter, and packet loss. In the case of limited bandwidth resources, QoS allocates appropriate bandwidth for various services and preferentially forwards applications such as voice, video, and important data to ensure the operation of end-to-end services.

Steps

1. Go to **Service Quality → QoS** .
2. In **QoS Configuration**, toggle on **Enable** to globally enable QoS.
3. Set **Scheduling Mode** to **WRR** or **SP**.

WRR

Weighted Round Robin mode: Send messages based on respective weights for low-priority and high-priority ports. In WRR mode, you need to set **Weight for Low-Priority Ports** and **Weight for High-Priority Ports**. Ensure that the weight for high-priority ports is larger than that for low-priority ports.

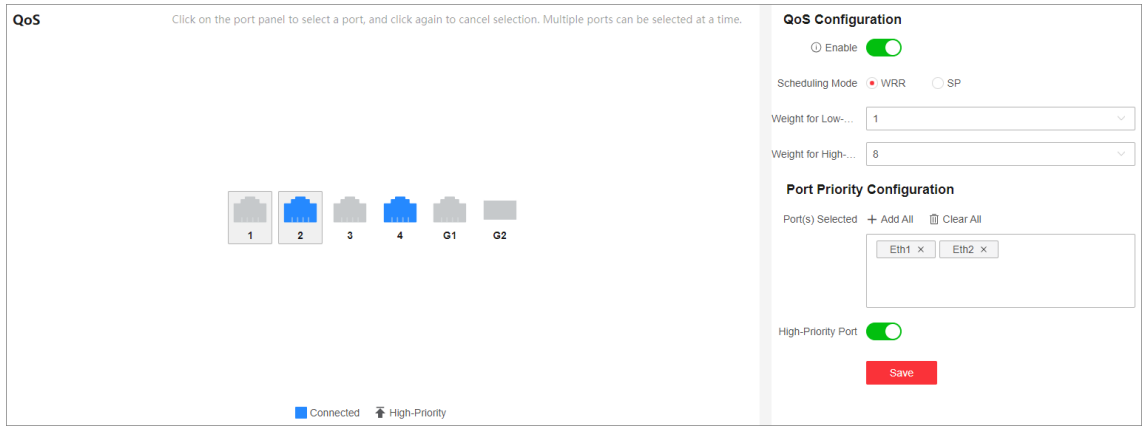


Figure 4-22 Select WRR Mode

SP

Strict Priority mode: Send messages based on actual port priority configuration.

Figure 4-23 Select SP Mode

4. Select the desired port(s) on the port panel.

Note

You can also click + Add All or Clear All on the right to batch select or deselect all ports.

5. Enable **High-Priority Port** to set the selected port(s) as high-priority port(s).
6. Click **Save**.

Note

When QoS mode is enabled, the high-priority port mode is automatically disabled. In this configuration, only the high-priority ports configured through QoS will support high-priority data transmission, while the physical high-priority ports (i.e., VIP ports marked by a red area on the device panel) will become unavailable.

4.6 DSCP Configuration

DSCP (Differentiated Services Code Point) enables intelligent traffic prioritization and Quality of Service (QoS) enforcement by marking IP packets with priority values (0-63). This allows critical applications like VoIP and video conferencing to receive low-latency forwarding and guaranteed bandwidth, while less time-sensitive traffic is deprioritized. By mapping DSCP values to specific queues and applying flow policies, switches can dynamically manage congestion, minimize packet loss for high-priority flows, and maintain end-to-end service level agreements (SLAs).

Steps

1. Go to **Service Quality → DSCP** .
2. In **DSCP-Based Priority Forwarding**, toggle on **Enable** and click **Save** to enable the DSCP function first.

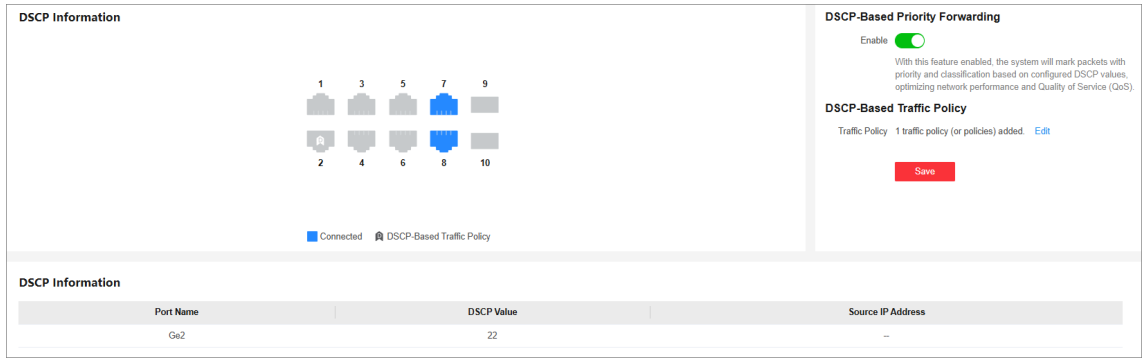


Figure 4-24 Enable DSCP-Based Priority Forwarding

3. In **DSCP-Based Traffic Policy**, click **Edit → Add** .
4. Set parameters as required and click **Add** to add a traffic policy.

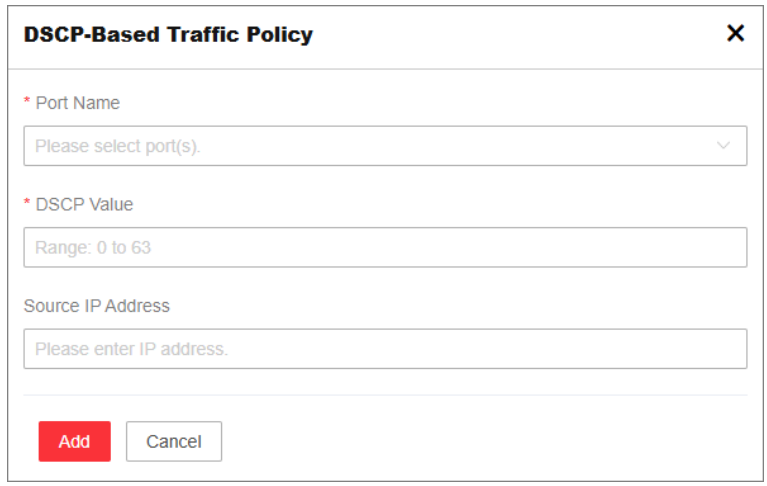


Figure 4-25 Add DSCP-Based Traffic Policy

Port Name

Port Name determines **where** the policy is applied. Select a port where the new traffic policy will be enforced.

DSCP Value

DSCP Value specifies **how** the traffic is prioritized. The DSCP value (ranging from 0 to 63) determines the priority treatment of packets by a network switch. For instance:

- **Low latency** (e.g., EF/DSCP 46 for VoIP traffic)
- **High bandwidth** (e.g., AF41/DSCP 34 for video streaming)

Assign a specific DSCP value to a designated traffic type to enforce the new traffic policy.

Source IP Address

Source IP Address defines **which** traffic is matched. This field identifies the origin of traffic for classification purposes. It enables differentiation between:

- User groups (e.g., department VLANs)
- Device types (e.g., IP phones vs. servers)
- Application sources (e.g., 192.168.2.X/24 for voice traffic marked EF/46)

IP-based classification ensures appropriate QoS handling per traffic source. Specify the source IP address of traffic as required.

Note

Source IP address is optional but critical for subnet/device-specific traffic policies.

5. **Optional:** Repeat steps 3 and 4 to add more traffic policies.
6. **Optional:** Click in the **Operation** column of the desired traffic policy to modify its DSCP value or source IP address.
7. **Optional:** Select one or more traffic policies and click **Delete** to delete the desired traffic policy (or policies).

Note

Once the DSCP function is disabled, all existing traffic policies will be automatically deleted.

8. **Optional:** View the existing or newly added traffic policies in the **DSCP Information** list.

4.7 SNMP Configuration

Simple Network Management Protocol (SNMP) is an application-layer communication protocol used to monitor network performance. SNMP network is composed of the Network Management System (NMS) and Agent. NMS is the SNMP manager, and Agent sends Traps to NMS. SNMP configuration includes basic configuration, community configuration, and trap target host configuration.

4.7.1 Configure Basic SNMP Parameters

Go to **L2 Configuration → SNMP → Basic Settings** . Enable SNMP as required, set **Supported SNMP Version**, and click **Save** to complete basic configuration.

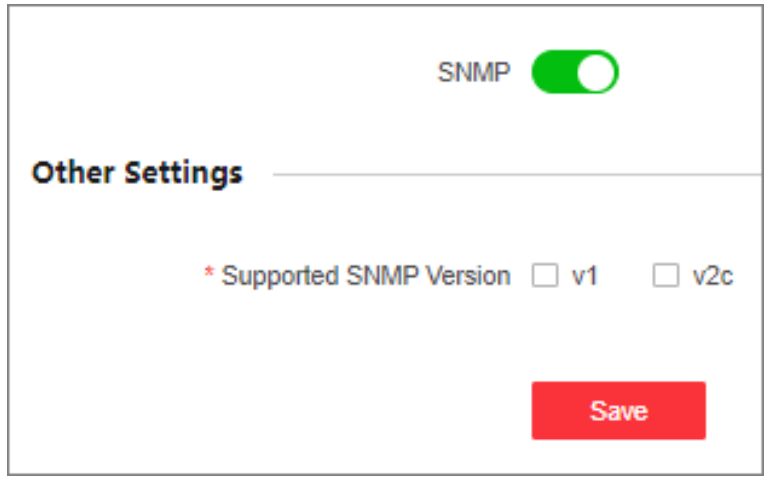


Figure 4-26 Configure Basic SNMP Parameters

4.7.2 Configure SNMP Community

Steps

1. Go to **L2 Configuration → SNMP → Community Settings** .

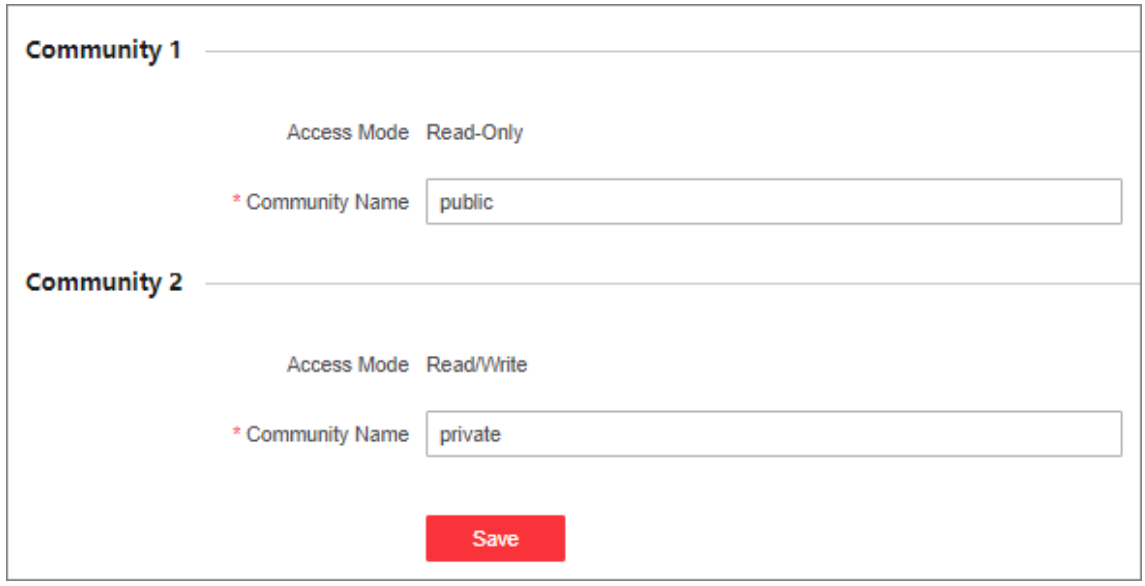


Figure 4-27 Configure SNMP Community

2. Set **Community Name** for community 1 (read-only access) and community 2 (read/write access).

   Community Name

   Used for authentication, similar to password. **Community Name** can be user-defined.

   Access Mode

   Access Mode is unconfigurable.

   - **Ready-Only**: The community has a read-only permission to access the NMS. The default community name is **public**.
   - **Read/Write**: The community has a read/write permission to access the NMS. The default community name is **private**.

3. Click **Save**.

4.7.3 Configure SNMP Trap Target Host

Steps

1. Go to **L2 Configuration → SNMP → Trap Target Host Settings** .

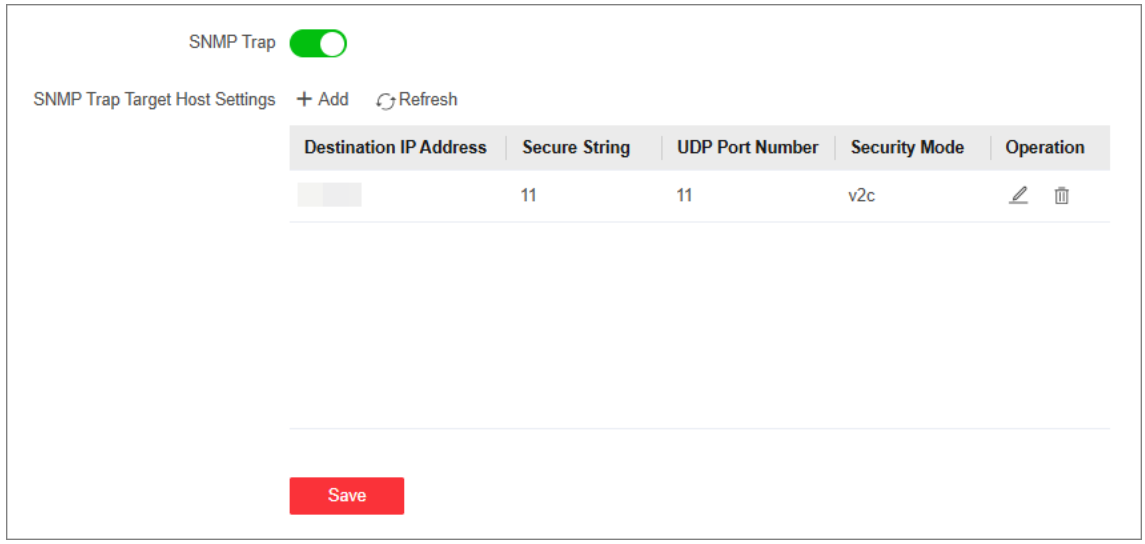


Figure 4-28 Configure SNMP Trap Target Host

2. Enable **SNMP Trap**.
3. Click **Add** to add an SNMP trap target host.

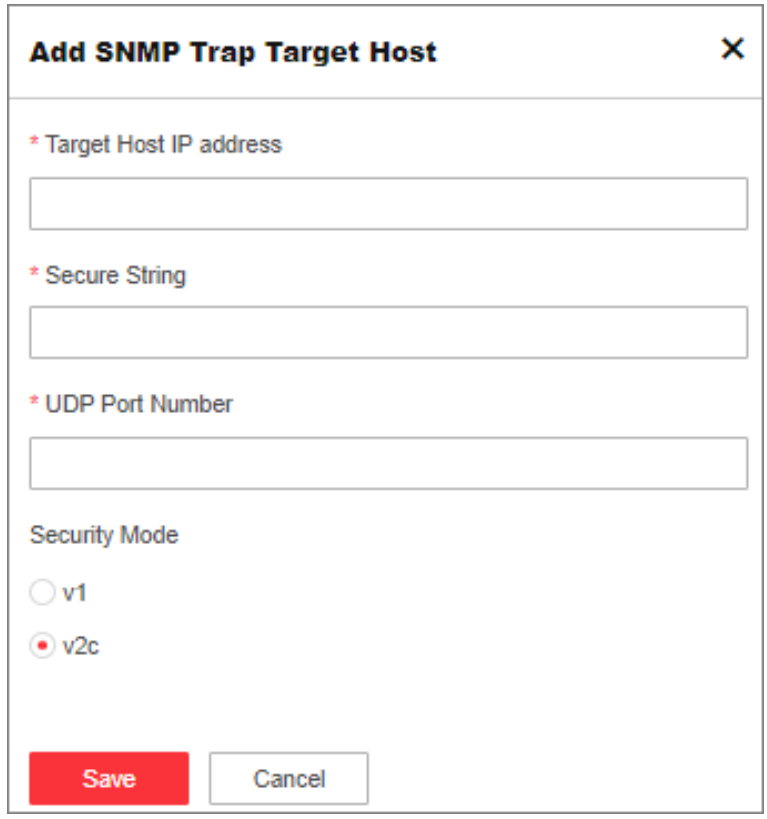


Figure 4-29 Add SNMP Trap Target Host

1) Set the parameters as required.

Target Host IP address

Specifies the IP address of the destination host (usually an NMS that can parse Trap and Inform messages) for receiving SNMP alarms. The IP address cannot be a broadcast or multicast IP address.

Secure String

Specifies the security word used for authentication or authorization. No more than 32 characters are allowed.

- Authentication: The security string is used to verify the identity of the device that sends Trap messages. The NMS can determine whether a Trap message comes from a known and trusted device by checking the security string.
- Authorization: The security string is used to determine which device has the permission to send Trap messages. Only devices with a valid security string can send Trap messages to the NMS.

Caution

In SNMPv1 or SNMPv2c mode, you are advised to set the security string to any community name. Otherwise, SNMP Trap messages may fail to be sent.

UDP Port Number

Specifies the destination port of SNMP Trap messages.

Security Mode

Specifies **Security Mode** to SNMPv1 (**v1**) or SNMPv2c (**v2c**).

2) Click **Save**.

4. Click **Save**.
5. **Optional:** View the details about of existing SNMP trap target hosts. Alternatively, edit or delete the desired target host in the SNMP trap target host list.

4.8 LLDP Configuration

Link Layer Discovery Protocol (LLDP) is a Layer 2 neighbor discovery protocol that enables devices to share information with their directly connected neighbors. When LLDP is enabled, network devices transmit LLDP Data Units (LLDPDUs) to notify adjacent devices of their current status. This protocol assists in mapping network topology and identifying misconfigurations within the network.

Steps

1. Go to **L2 Configuration → LLDP** .
2. Enable or disable LLDP.

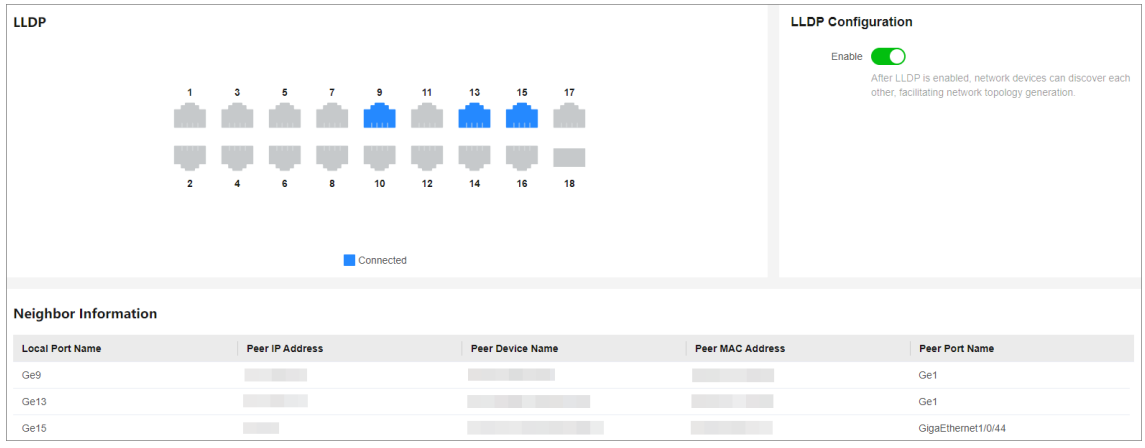


Figure 4-30 Configure LLDP

Note

After LLDP is enabled, network devices can automatically discover each other, which facilitates network topology mapping.

3. **Optional:** View the local port(s), along with the device name(s), IP address(es), MAC address(es), and peer port(s) of the peer device(s) directly connected to the switch in the **Neighbor Information** list.

4.9 Security Configuration

4.9.1 DHCP Snooping Configuration

DHCP Snooping is a security technology used on Layer 2 switches to prevent unauthorized DHCP servers from accessing the network. Preventing untrusted hosts from becoming DHCP servers, DHCP Snooping works as a protection from man-in-the-middle attacks. After DHCP Snooping is enabled, you can set the port connected to an authorized DHCP server as a trusted port so that DHCP response packets received on the trusted port are forwarded while DHCP response packets received on the untrusted port are discarded.

Steps

1. Go to **Security → DHCP Snooping** .

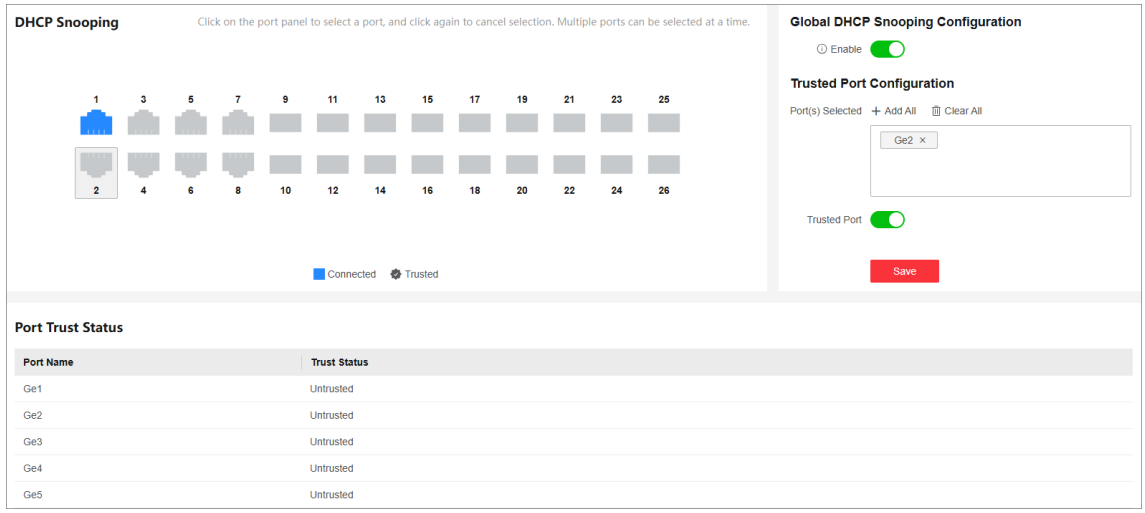


Figure 4-31 Configure DHCP Snooping

2. In **Global DHCP Snooping Configuration**, toggle on **Enable** to globally enable DHCP Snooping.
3. Select the desired port(s) on the port panel.

Note

You can also click + Add All or Clear All on the right to batch select or deselect all ports.

4. Enable **Trusted Port** to configure the selected port(s) as trusted port(s).
5. Click **Save**.
6. **Optional:** View the trust status of each port in the **Port Trust Status** list.

Note

For some devices with software versions below V3.3.0, you can view the trust status, IP address, MAC address, VLAN ID, and remaining lease time of ports in the **DHCP Snooping Details** list. Please refer to the actual situation.

4.9.2 ACL Configuration

An Access Control List (ACL) is a set of rules used to control user access to a network device or resource. An ACL matches packets against the rules it contains to filter packets. One or more rules describe the packet matching conditions, such as the source address, destination address, and port number of a packet. For packets that match the ACL rules configured on a device, the device forwards or discards these packets according to the specified conditions.

ACLs are classified into numbered ACLs and named ACLs. Numbered ACLs are classified into basic ACLs, advanced ACLs, and Layer 2 ACLs. These ACLs have different number ranges.

- For a basic ACL, the ACL number ranges from 2000 to 2999.
- For an advanced ACL, the ACL number ranges from 3000 to 3999.
- For a layer 2 ACL, the ACL number ranges from 4000 to 4999.

Note

- A basic ACL filters packets based on the source IP address, an advanced ACL filters packets based on source and destination IP addresses, while a layer 2 ACL filters packets based on source and destination MAC addresses.
- Currently, only advanced or layer 2 ACLs can be configured. A total of 64 advanced and layer 2 ACLs are allowed.

Configure Advanced ACL

Steps

1. Go to **Security → ACL → IPv4 ACL** .
2. Click **Add**.

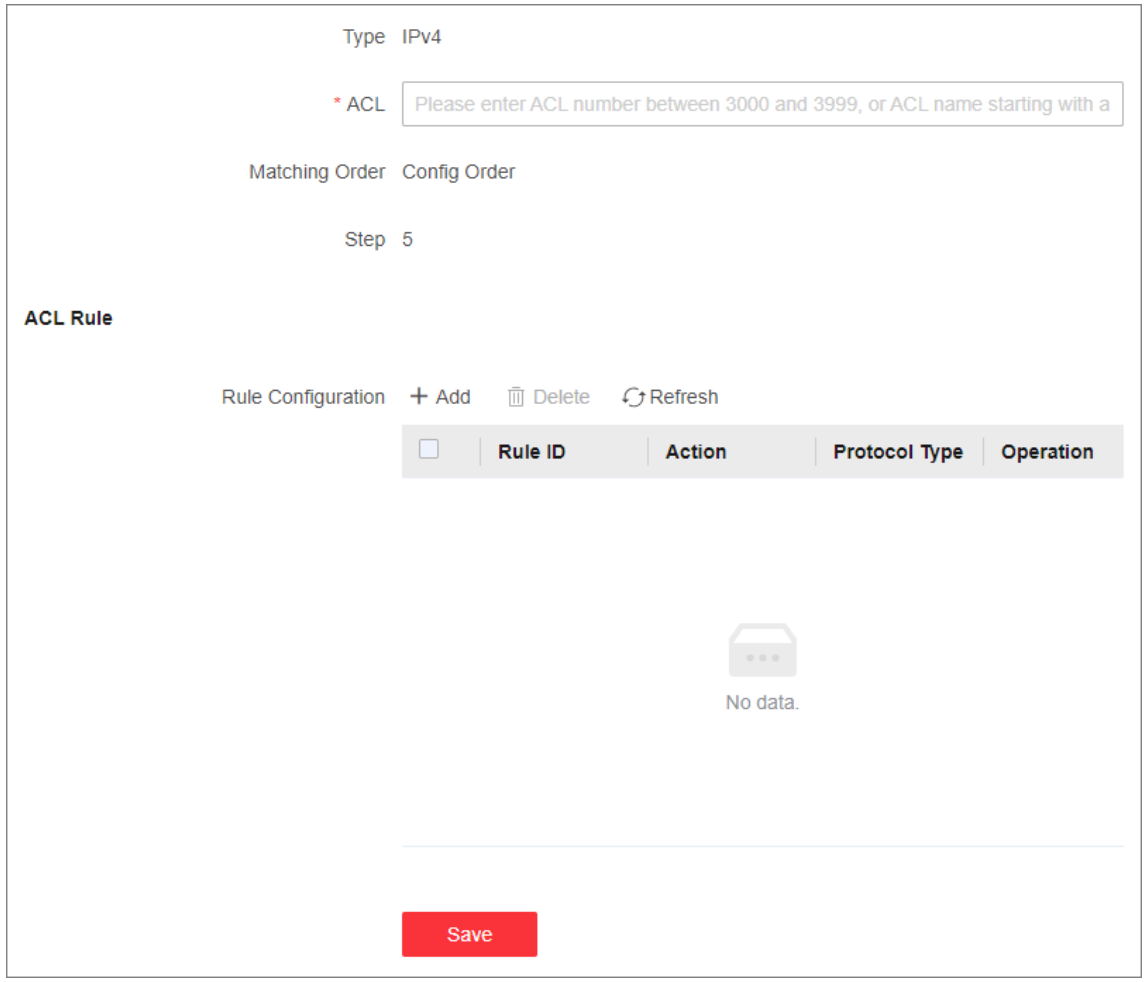


Figure 4-32 Configure Advanced ACL

3. Set the parameters as required to add an advanced ACL.

ACL

Specifies the ACL number or ACL name. The ACL number ranges from 3000 to 3999. The ACL name should contain 1 to 32 characters and start with a-z or A-Z. Entering 'all' (case insensitive) is not allowed.

Matching Order

The matching order of ACL rules is **Config Order** by default, which is unconfigurable. The system matches packets against ACL rules in ascending order of rule IDs. The rule with the smallest ID is processed first.

Step

A step is an increment between neighboring rule IDs automatically allocated by the system. The rule ID must be an integer. For example, if an ACL contains rule 5 and rule 13, and the default step is 5, the system automatically allocates 15 as the ID of a new rule (because 15 is

greater than 13 and is the minimum multiple of 5) when the new rule is added to this ACL. The step of ACL rules is **5** by default, which is unconfigurable.

4. Click **Save**.
5. **Optional:** Configure rule(s) for the new advanced ACL.
   a. In **ACL Rule**, click **Add**.

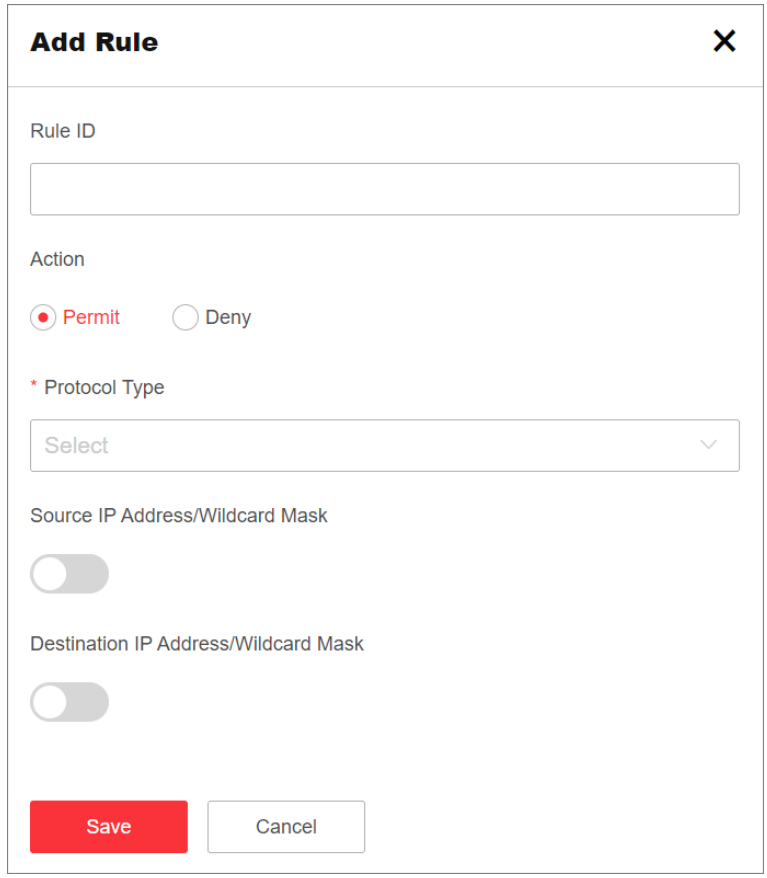


Figure 4-33 Add ACL Rule(s)

   b. Set the parameters as required.

Table 4-1 ACL Rule Parameters

Parameter	Description
Rule ID	Specifies the ID of an ACL rule. The value ranges from 1 to 65535.
Action	Specifies the action of an ACL rule to **Permit** or **Deny**. - **Permit**: The system forwards matched packets. - **Deny**: The system discards matched packets.

Parameter	Description
Protocol Type	Specifies the protocol type of an ACL rule. Protocol numbers 1 to 255 correspond to different protocol types. Specific enumerations: tcp(6), udp(17), icmp(1), igmp(2), ospf(89), ipinip(4), gre(47).
Source IP Address/ Wildcard Mask	The source IPv4 address and wildcard mask need to be set if **Source IP Address/Wildcard Mask** is enabled.
Source IP Address	Specifies the source IPv4 address of an ACL rule.
Wildcard Mask	Specifies the wildcard mask of the source IPv4 address of an ACL rule. The wildcard mask is an inverse mask, for example, 192.168.1.1/0.0.0.255 takes effect as 192.168.1.0/0.0.0.255.
Destination IP Address/Wildcard Mask	The destination IPv4 address and wildcard mask need to be set if **Destination IP Address/Wildcard Mask** is enabled.
Destination IP Address	Specifies the destination IPv4 address of an ACL rule.
Wildcard Mask	Specifies the wildcard mask of the destination IPv4 address of an ACL rule. The wildcard mask is an inverse mask, for example, 192.168.1.1/0.0.0.255 takes effect as 192.168.1.0/0.0.0.255.

c. Click **Save**.
d. View, edit, or delete the configured ACL rule(s) in the ACL rule list.

Configure Layer 2 ACL

Steps

1. Go to **Security → ACL → Layer 2 ACL** .
2. Click **Add**.

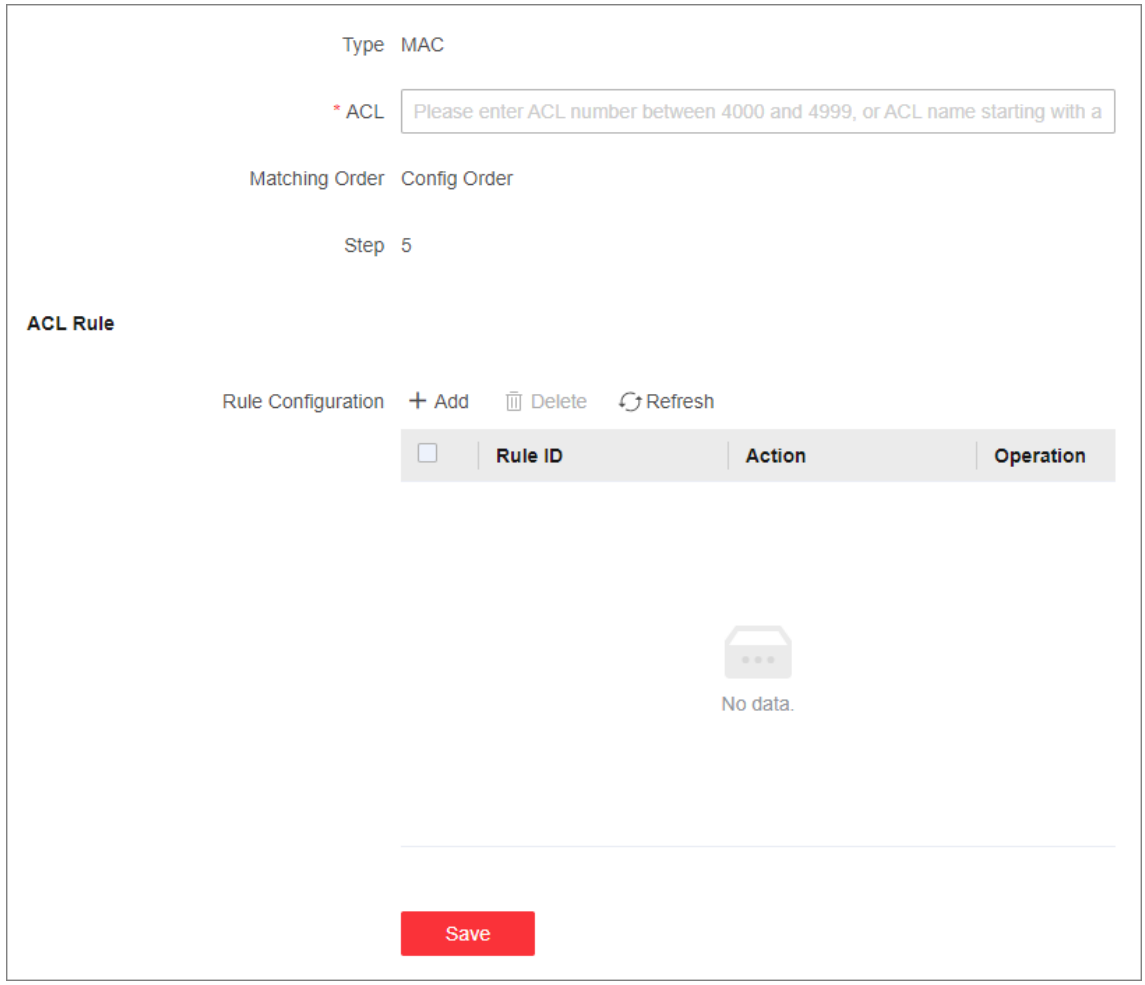


Figure 4-34 Configure Layer 2 ACL

3. Set the parameters as required to add an advanced ACL.

ACL

Specifies the ACL number or ACL name. The ACL number ranges from 4000 to 4999. The ACL name should contain 1 to 32 characters and start with a-z or A-Z. Entering 'all' (case insensitive) is not allowed.

Matching Order

The matching order of ACL rules is **Config Order** by default, which is unconfigurable. The system matches packets against ACL rules in ascending order of rule IDs. The rule with the smallest ID is processed first.

Step

A step is an increment between neighboring rule IDs automatically allocated by the system. The rule ID must be an integer. For example, if an ACL contains rule 5 and rule 13, and the default step is 5, the system automatically allocates 15 as the ID of a new rule (because 15 is

greater than 13 and is the minimum multiple of 5) when the new rule is added to this ACL. The step of ACL rules is **5** by default, which is unconfigurable.

4. Click **Save**.
5. **Optional:** Configure rule(s) for the new layer 2 ACL.
   a. In **ACL Rule**, click **Add**.

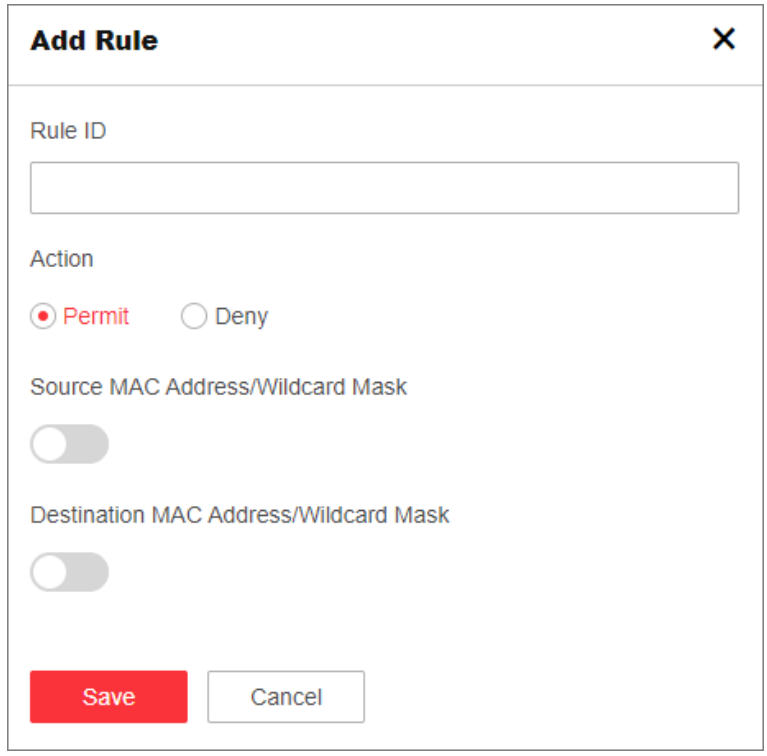


Figure 4-35 Add ACL Rule(s)

   b. Set the parameters as required.

Table 4-2 ACL Rule Parameters

Parameter	Description
Rule ID	Specifies the ID of an ACL rule. The value ranges from 1 to 65535.
Action	Specifies the action of an ACL rule to **Permit** or **Deny**. - **Permit**: The system forwards matched packets. - **Deny**: The system discards matched packets.
Protocol Type	Specifies the protocol type of an ACL rule. Protocol numbers 1 to 255 correspond to different protocol types. Specific enumerations: tcp(6), udp(17), icmp(1), igmp(2), ospf(89), ipinip(4), gre(47).
Source MAC Address/ Wildcard Mask	The source MAC address and wildcard mask need to be set if **Source MAC Address/Wildcard Mask** is enabled.

Parameter	Description
Source MAC Address	Specifies the source MAC address of an ACL rule.
Wildcard Mask	Specifies the wildcard mask of the source IPv4 address of an ACL rule. The wildcard mask is an inverse mask, for example, 98-f1-12-0a-e9-1c/00-00-00-00-00-FF takes effect as 98-f1-12-0a-e9-00/00-00-00-00-00-FF.
Destination MAC Address/Wildcard Mask	The destination MAC address and wildcard mask need to be set if **Destination MAC Address/Wildcard Mask** is enabled.
Destination MAC Address	Specifies the destination MAC address of an ACL rule.
Wildcard Mask	Specifies the wildcard mask of the destination IPv4 address of an ACL rule. The wildcard mask is an inverse mask, for example, 98-f1-12-0a-e9-1c/00-00-00-00-00-FF takes effect as 98-f1-12-0a-e9-00/00-00-00-00-00-FF.

c. Click **Save**.

d. View, edit, or delete the configured ACL rule(s) in the ACL rule list.

Configure Port ACL Application

Port ACL application refers to applying ACL rules to the selected port(s). ACL rules are used to filter packets in a certain direction on a port. Packets that match the ACL rules are permitted or denied according to the action defined in rules, while packets that do not match any ACL rules are processed according to the default action.

Steps

1. Go to **Security → ACL → Port ACL Application** .

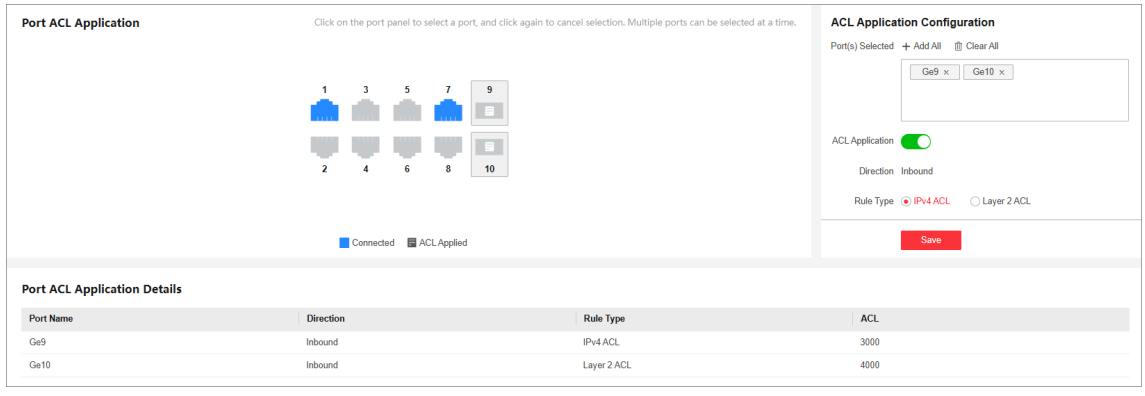


Figure 4-36 Configure Port ACL Application

2. Select one or more ports to which ACL rules are to be applied on the port panel.

Note

You can also click + Add All or Clear All on the right to batch select or deselect all ports.

3. Enable **ACL Application**.
4. Set the parameters as required.

   Direction

   Specifies the direction in which the ACL rules are applied to filter packets on a port. The default value is **Inbound**, which is unconfigurable.

   Rule Type

   Specifies the rule type to **IPv4 ACL** or **Layer 2 ACL**.

   ACL

   Specifies an existing numbered or named IPv4 ACL or Layer 2 ACL.
5. Click **Save**.

   The ports to which ACL rules have been applied are displayed on the port panel.
6. **Optional:** View details about the ports to which ACL rules have been applied in the **Port ACL Application Details** list.

4.9.3 ARP Gateway Protection Configuration

You can configure ARP gateway protection on ports not connected to a gateway to prevent gateway spoofing attacks. Upon receiving an ARP packet, the port checks whether the source IP address of the ARP packet is the same as that of any protected gateway. If yes, the packet is considered invalid and discarded. If not, the packet is considered valid and processed correctly.

Steps

1. Go to **Security → ARP Gateway Protection** .

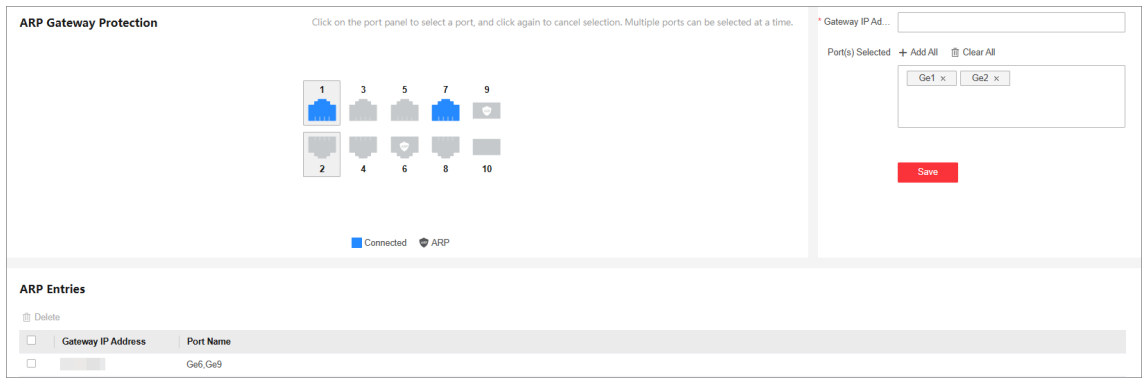


Figure 4-37 Configure ARP Gateway Protection

2. Set **Gateway IP Address**.
3. Select one or more desired ports on the port panel.

Note

You can also click + Add All or Clear All on the right to batch select or deselect all ports.

4. Click **Save**.

Note

- You can repeat the preceding operations to configure multiple ARP entries.
- Multiple ARP entries can be configured for one port.

5. **Optional:** View or delete configured ARP entries in the **ARP Entries** list.

4.9.4 IPSG Configuration

IP Source Guard (IPSG) checks IP packets received on Layer 2 interfaces against a binding table that contains the bindings of source IP addresses, source MAC addresses, VLANs, and inbound interfaces. Only the packets matching the binding table are forwarded, and other packets are considered as attack packets and discarded.

Configure Binding Entry

IPSG binding entries include dynamic entries and static entries. Dynamic entries can be dynamically learned by DHCP snooping: Existing DHCP Snooping entries will be automatically bound to IPSG after source address check is enabled on a port. Static entries need to be manually configured.

Steps

1. Go to **Security → IP Source Guard → Binding Entry** .
2. Click **Add**.

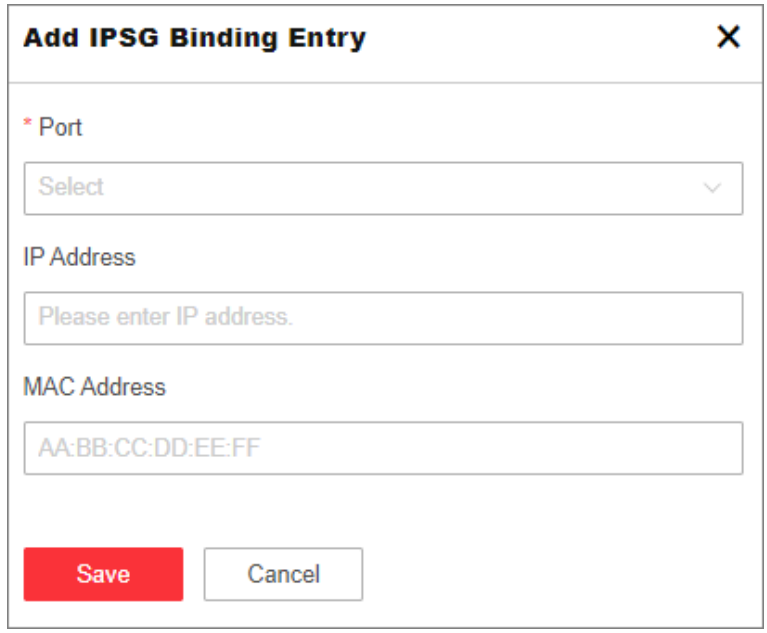


Figure 4-38 Add Static Binding Entry

3. Set **Port**, **IP Address**, and/or **MAC Address** as required.
4. Click **Save**.
5. **Optional:** Set the search criteria such as **Port**, **IP Address/MAC Address**, or **Entry Type** to search the desired binding entry (or entries), or delete a binding entry in the list below.

Figure 4-39 Search/Delete Binding Entry

Configure Source Address Check

IPSG filters packets received on Layer 2 interfaces against IP addresses and/or MAC addresses in dynamic or static binding entries. These entries take effect only when source address check is enabled. Otherwise, all packets will be forwarded.

Steps

1. Go to **Security → IP Source Guard → Source Address Check** .
2. Click **Add**.

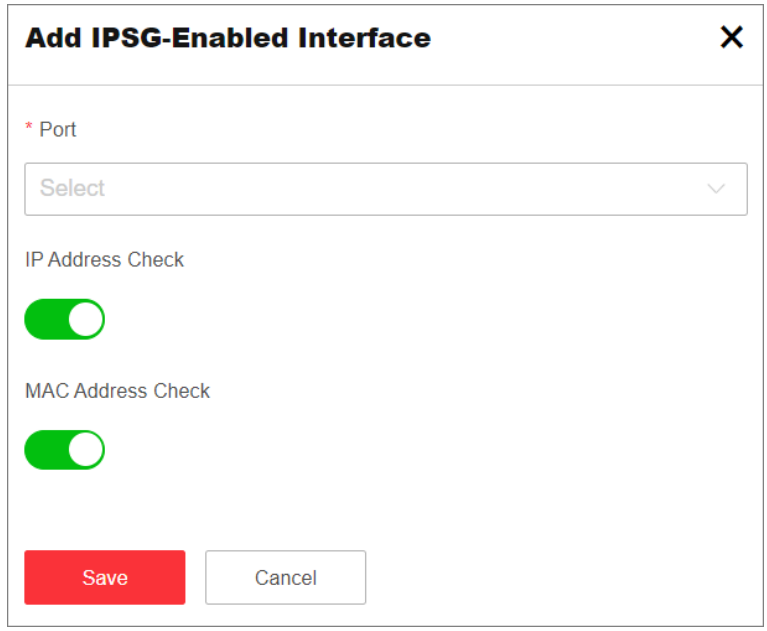


Figure 4-40 Configure IPSG Source Address Check

3. Select a desired port.
4. Enable **IP Address Check** and/or **MAC Address Check** as required.
   - If only **IP Address Check** is enabled, packets are filtered against source IP addresses. Only packets whose source IP address matches any binding entry are forwarded.
   - If only **MAC Address Check** is enabled, packets are filtered against source MAC addresses. Only packets whose source MAC address matches any binding entry are forwarded.
   - If both **IP Address Check** and **MAC Address Check** are enabled, packets are filtered against both source IP address and source MAC address. Only packets whose source IP and MAC addresses simultaneously match any binding entry are forwarded.
5. Click **Save**.
6. **Optional:** View, edit, or delete the ports configured with source address check in the list below.

4.10 Loop Prevention Configuration

4.10.1 STP Configuration

Spanning Tree Protocol (STP) is a layer-2 link management protocol that provides path redundancy and prevents loops in a network topology. STP uses a spanning-tree algorithm to select one switch as the root of a spanning tree, and determines the network topology by transmitting Bridge Protocol Data Unit (BPDU) packets between devices, helping to create a stable network.

Steps

1. Go to **L2 Configuration → STP** .

Figure 4-41 Configure STP

2. In **Global STP Configuration**, enable **STP**.
3. Set the parameters as required.

Table 4-3 STP Parameters

Parameter	Description
Bridge Priority	• The value ranges from 0 to 61440, in an increment of 4096. The default value is 32768. Valid values are 0, 4096, 8192, 12288, 16384, ..., and 61440. • The smaller the value, the higher the bridge priority of a switch. A switch with higher bridge priority is more likely to become the root bridge.
Hello Time	The interval between each BPDU that is sent on a port, which is used for port link diagnosis. The value ranges from 1 to 10 seconds. The default value is 2 seconds.
Max. Aging Time	The maximum length of time interval that a STP-enabled switch port saves its configuration BPDU information. The value ranges from 6 to 40 seconds. The default value is 20 seconds. **Note** The Max. aging time must meet the following conditions: 2 × (Hello Time + 1) ≤ Max. Aging Time ≤ 2 × (Forwarding Delay – 1)
Forwarding Delay	The time interval that is spent in the listening and learning state when the topology changes. The value ranges from 4 to 30 seconds. The default value is 15 seconds.

4. Click **Save**.
5. **Optional:** Click **Port Status** or **STP Status** to view the STP status of each port or global STP configuration.

Note

- The **Port Status** information includes the port name, path cost, port role, and port status.
- The **STP Status** information includes the bridge ID, root bridge ID, as well as hello time, Max. aging time, and forwarding delay of the root bridge.

4.10.2 ERPS Configuration

By selectively blocking redundant links, Ethernet Ring Protection Switching (ERPS) is a protocol used to prevent broadcast storms and implement fast switchover on a network where loops occur, which effectively ensures uninterrupted communication and network reliability.

Steps

1. Go to **L2 Configuration → ERPS** .

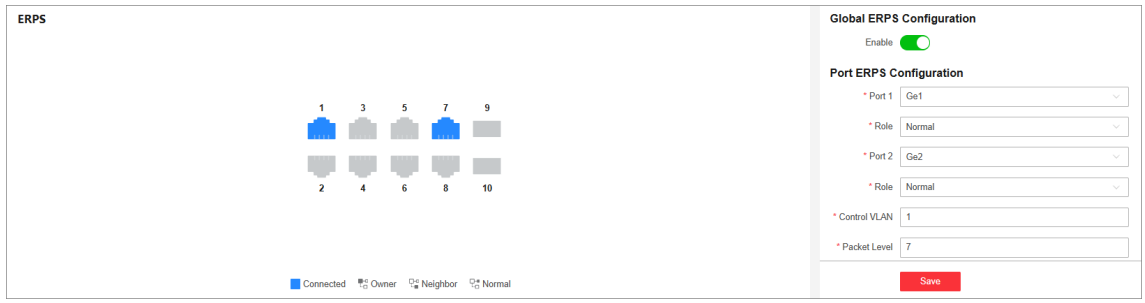


Figure 4-42 Configure ERPS

2. In **Global ERPS Configuration**, enable ERPS.

Note

ERPS and STP cannot be configured simultaneously.

3. In **Port ERPS Configuration**, set **Port 1**, **Port 2**, and their roles respectively.

Owner

The primary node in an ERPS ring. An owner port is responsible for blocking and unblocking traffic over the Ring Protection Link (RPL) to prevent loops. An ERPS ring has only one owner port.

Neighbor

The neighbor node in an ERPS ring. A neighbor port is directly connected to an owner port. Both the owner port and neighbor port(s) are blocked in normal situations to prevent loops.

Common

Common ports refer to ring ports other than the owner and neighbor ports. A common port monitors the status of a directly-connected ERPS link and sends RAPS PDUs to notify the other ports of its link status changes.

Note

- Port 1 and port 2 should be different ports.
- ERPS configuration is not supported by member ports in an aggregation group.
- The roles of port 1 and port 2 cannot all be owner or neighbor, or cannot be owner and neighbor simultaneously.

4. Set other parameters as required.

Table 4-4 ERPS Parameters

Parameter	Description
Control VLAN	A control VLAN is configured in an ERPS ring to transmit RAPS PDUs. After a port is added to an ERPS ring configured with a control VLAN, the port is automatically added to this control VLAN. Different ERPS rings must use different control VLANs. The value ranges from 2 to 4094.
Packet Level	Level of RAPS PDUs. The value ranges from 0 to 7. **Note** A node does not process RAPS PDUs with a higher level than its own.
Guard Timer	This timer is started after the port detects that a faulty link is recovered to prevent unnecessary network flapping caused by message residue due to network forwarding delay. The value ranges from 10 to 2000 milliseconds.
Hold-off Timer	This timer is started after the port detects a faulty link. If a fault persists after the Hold-off timer expires, this fault will be reported. The Hold-off timer affects fault reporting speed and link switchover performance when a fault occurs. The value ranges from 0 to 10000 milliseconds.
WTR Timer	If the RPL owner port is blocked due to a link fault, the port may not be Up immediately after the link is recovered. Blocking the RPL owner port may cause network flapping. To prevent this problem, the node where the RPL owner port is located starts the Wait to Restore (WTR) timer after receiving RAPS PDUs to avoid frequent network flapping caused by intermittent faulty links on the ring network. The value ranges from 1 to 12 minutes.

5. Click **Save**.
6. **Optional:** View the ERPS node status and port status in the **ERPS Status** list.

Chapter 5 System Management

5.1 Time Synchronization

Steps

1. Go to **System Management → Time Configuration** .
2. Set **Time Zone**.
3. Set **Time Sync Mode**.
   - **Manually**: Manually set the date and time, or check **Sync with Computer Time** to synchronize the system date and time.

Figure 5-1 Configure Time Manually

   - **With NTP Server**: Enter the NTP server address, port number, and time sync interval for automatic time synchronization.

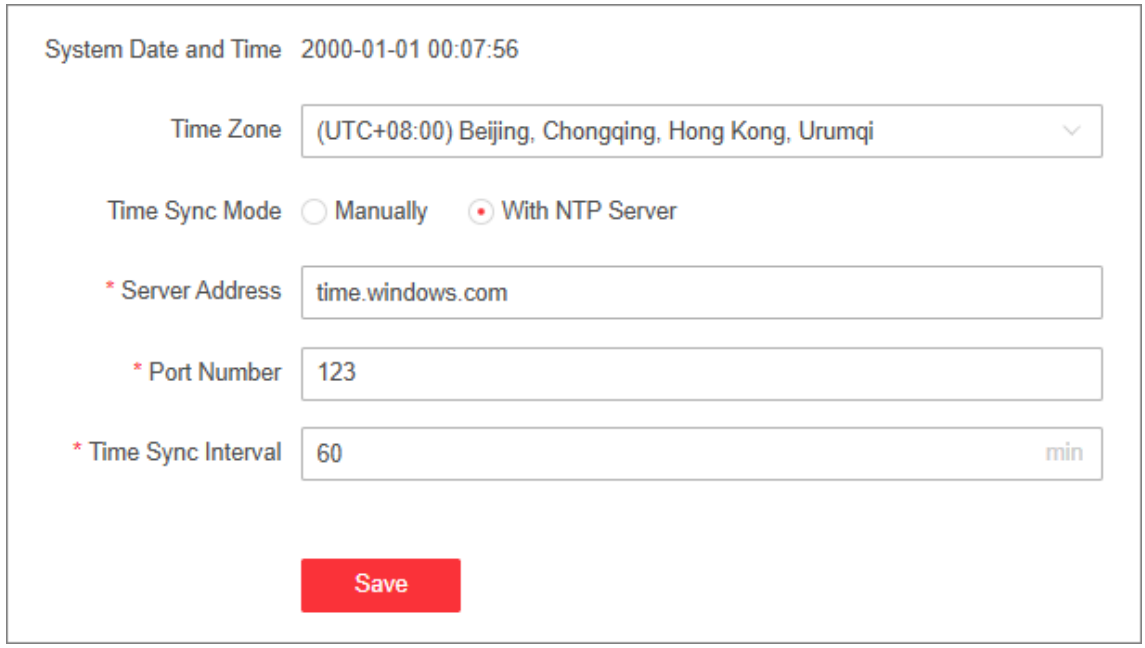


Figure 5-2 Configure Time with NTP Server

4. Click **Save**.

5.2 System Maintenance

Go to **System Management → System Maintenance → System Maintenance** to restart the device, upgrade the device, back up the device, reset the device, or export diagnostic information about the device.

Restart Device

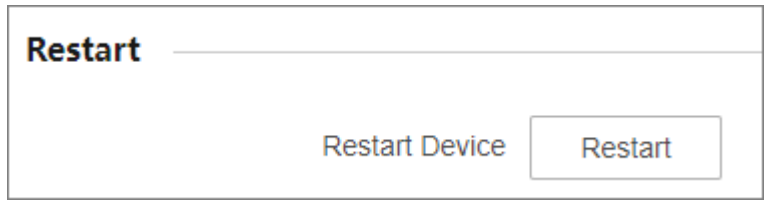


Figure 5-3 Restart

In **Restart**, click **Restart** to remotely restart the switch.

Note

You will enter the login page automatically after the device is restarted.

Upgrade Device

Upload an upgrade file to manually upgrade the switch.

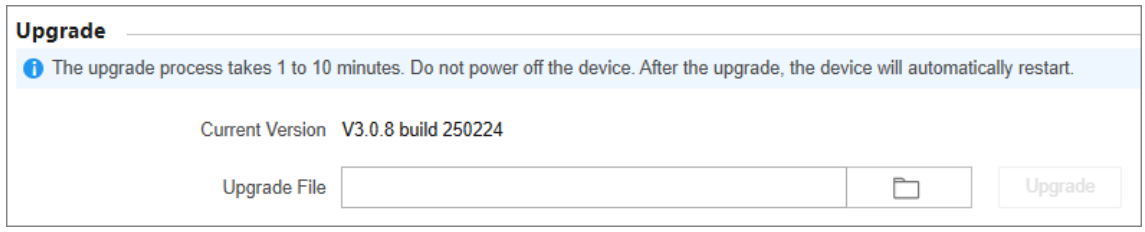


Figure 5-4 Upgrade

1. In **Upgrade**, click to select an upgrade patch file.
2. Click **Upgrade**.

Note

- If upgrading failed or the device cannot function, please contact our technical support engineers.
- The device will restart automatically to enter the login page after upgrade is completed.

Update Device Firmware Through Cloud

Online update requires an active Hik-Connect connection. The device periodically checks for firmware updates (full packages only) through real-time communication with the Hik-Connect server, ensuring version synchronization.

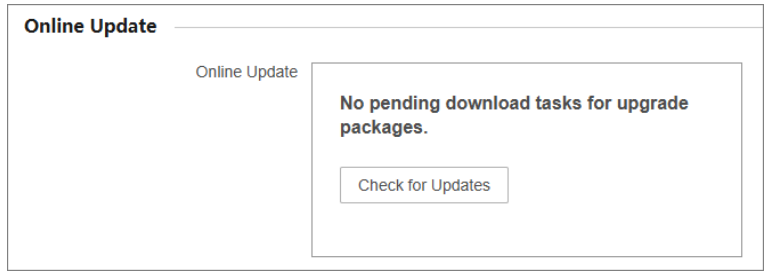


Figure 5-5 Update Online

In **Online Update**, click **Check for Updates**. The system automatically requests the latest firmware version from the Hik-Connect server.

- If a new version is available, a message indicating upgrade to [version XXX] available will show. Follow the prompts to complete online firmware update.
- If the device already runs the latest version, a message indicating already the latest version will show. No online update is required.
- If the device is disconnected from Hik-Connect, a message indicating query failed will show. Make sure that the device is connected to Hik-Connect before checking for updates again.

Note

The difference between online update and manual upgrade lies in network dependency and operation mode. Online update requires the device to maintain connectivity with the cloud platform, which automatically checks for available full packages. In contrast, manual upgrade is network-independent. As long as the upgrade package is obtained, users can perform offline upgrade anytime via local upload, requiring only stable LAN connection between the computer and device, unaffected by cloud platform connection status.

Back Up Device

Export the configuration file for local backup.

Figure 5-6 Back Up

1. In **Backup**, click **Export** to export the configuration file containing device parameters.
2. Set a password and confirm the password for file encryption.

   Note

   Remember the password as it is required when importing device parameters.
3. Click **OK**.

Reset Device

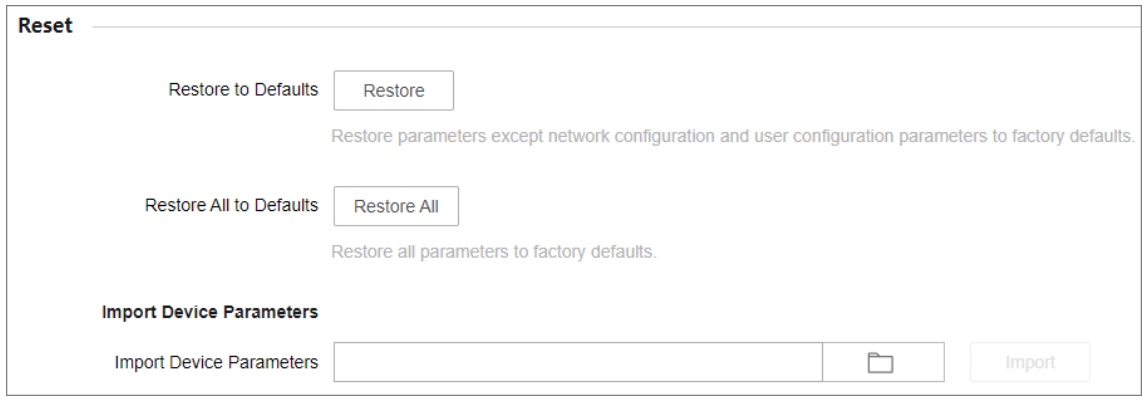


Figure 5-7 Reset

- **Restore to Defaults**: Click **Restore** to restore parameters except network configuration and user configuration parameters to factory defaults.
- **Restore All to Defaults**: Click **Restore All** to restore all parameters to factory defaults.

Note

- The device parameters cannot be recovered once being restored to factory defaults.
- The device will restart automatically after being restored to factory defaults.

- **Import Device Parameters**: Click to select the configuration file containing device parameters, click **Import**, enter the password for file decryption, and then click **OK** to import the configuration file for fast device configuration.

Note

The device will restart automatically to enter the login page after the configuration file is imported.

Export Diagnostic Information

Export diagnostic information for troubleshooting, system optimization, security auditing, and remote technical support.

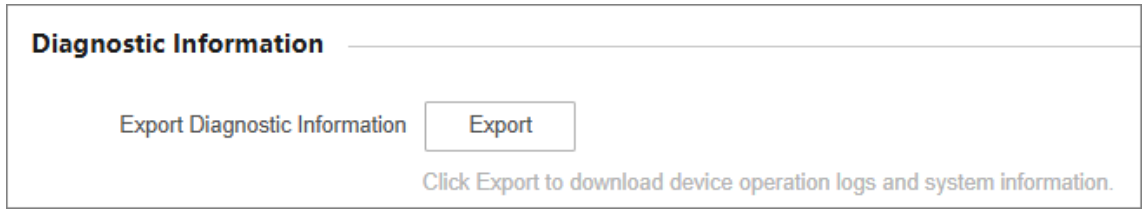


Figure 5-8 Export Diagnostic Information

In **Diagnostic Information**, 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.

5.3 Network Configuration

Network Configuration

1. Go to **System Management → Network Configuration → Network Configuration** .
2. Set the management VLAN, IPv4 address, IPv4 subnet mask, default IPv4 gateway, preferred DNS address, and alternate DNS address as required, or enable **DHCP** for automatic IP address assignment.

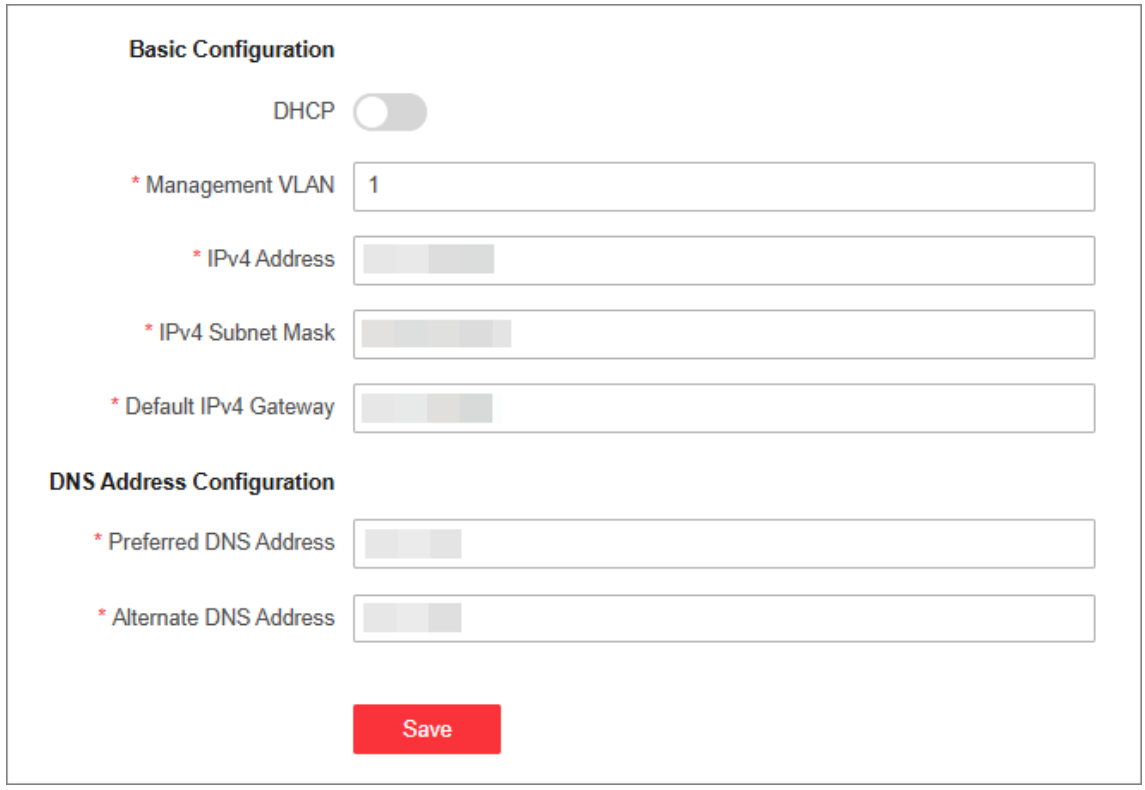


Figure 5-9 Configure Network

Cloud Platform Configuration

If the device is displayed as offline when you add it to Hik-Partner Pro, you need to modify the DNS server address and configure Hik-Connect parameters.

Go to **System Management → Network Configuration → Cloud Platform Configuration** , and ensure that Hik-Connect is enabled. You can also check the operation code, and bind the device to your cloud account on Hik-Partner Pro app.

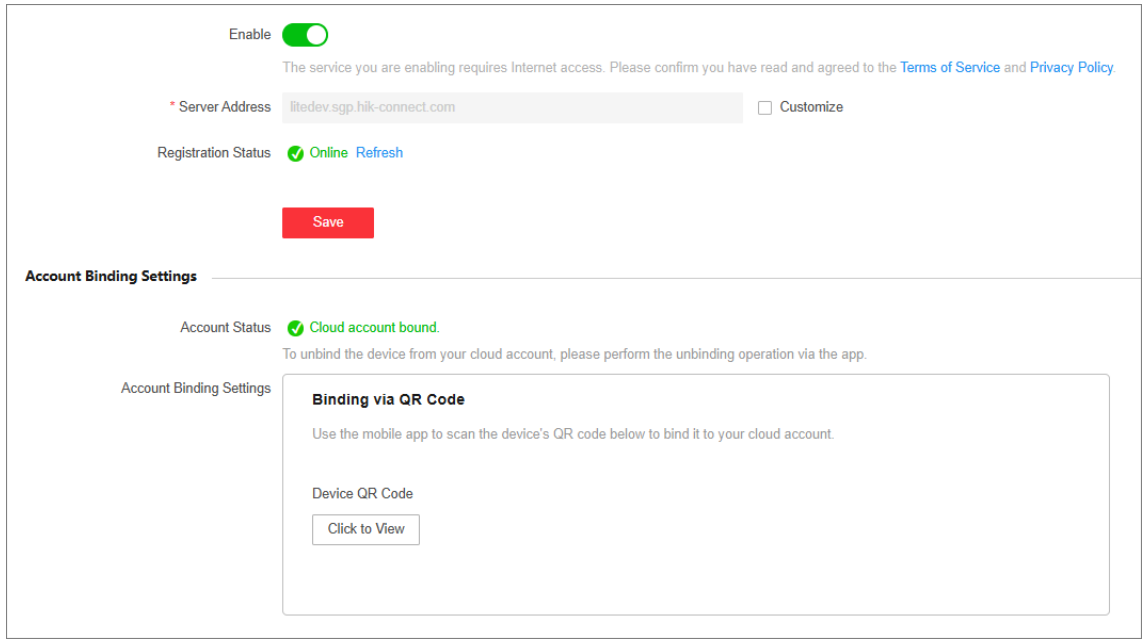


Figure 5-10 Configure Cloud Platform

Note

It takes several minutes for reconnecting to Hik-Connect service.

Remote Management

Go to **System Management → Network Configuration → Remote Management** for remote device management via HTTP, HTTPS, SSH, or Telnet.

Note

The supported remote management methods may vary by device. For example, some devices (such as type-A devices shown in the figure below) support HTTP, HTTPS, and SSH, while others (such as type-B devices shown in the figure below) support HTTP and Telnet. Additionally, the configurable parameters may also differ. Please refer to the actual interface for accurate information.

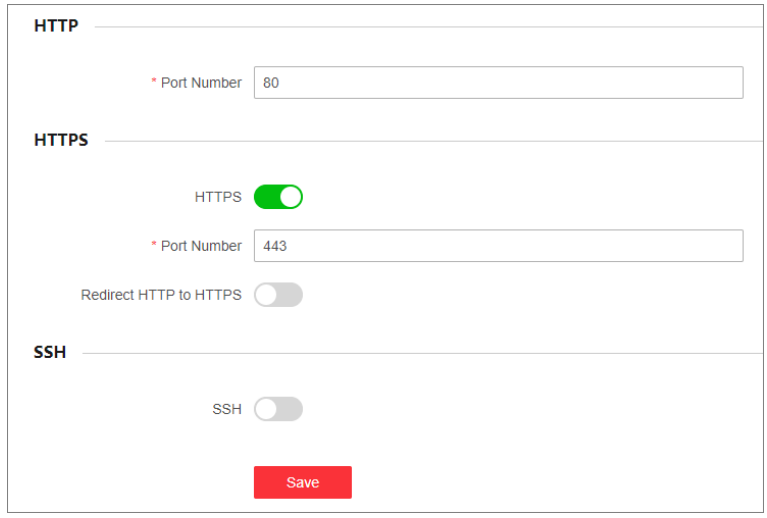


Figure 5-11 Manage Device Remotely (Type-A Device)

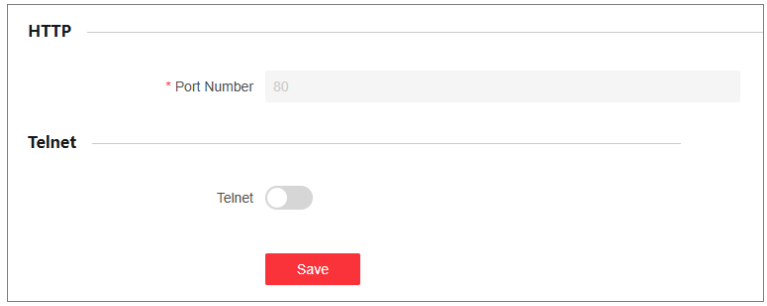


Figure 5-12 Manage Device Remotely (Type-B Device)

- **HTTP**:
  - For type-A devices, you can modify the port number and click **Save** to save the modification. The HTTP port number must be an integer between 2000 and 65535, with a default value of 80.
  - For type-B devices, the port number is fixed at 80 and cannot be changed.
- **HTTPS**: Set the parameters as required and click **Save**.

  HTTPS

  Enable or disable HTTPS.

  Port Number

  If HTTPS is enabled, set the HTTPS port number.

  Note

  The HTTPS port number should be an integer between 2000 to 65535, or 443 by default.

  Redirect HTTP to HTTPS

Enable or disable **Redirect HTTP to HTTPS**.

Note

If **Redirect HTTP to HTTPS** is enabled, traffic accessed through port 80 will be automatically redirected to port 443.

- **SSH**: Once enabled, SSH offers secure remote management via an encrypted command-line interface, enabling safe configuration, monitoring, and maintenance tasks.

Note

SSH is reserved for technical support to perform fault diagnosis and is not accessible to end users.

- **Telnet**: Once enabled, Telnet allows remote device management through a command-line interface, facilitating configuration, monitoring, and maintenance operations over a network.

Note

Telnet is suitable only for low-risk internal networks due to its lack of encryption.

SADP Configuration

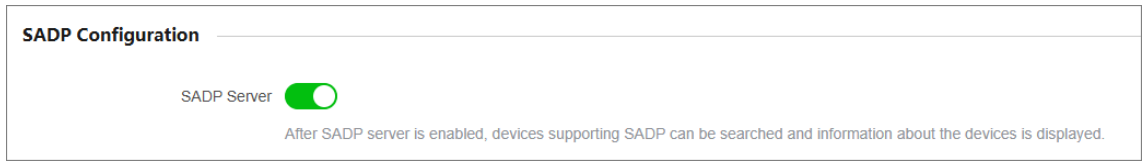


Figure 5-13 Configure SADP Server

Go to **System Management → Network Configuration → Network Service** , and enable **SADP Server** as required. If SADP server is enabled, devices supporting SADP can be searched and information about the devices will be displayed.

Standard Switching Mode Configuration

This feature is enabled by default. If you want to disable it, go to **System Management → Network Configuration → Network Service** and toggle off **Enable** in **Standard Switching Mode**. If network service is disabled, the device will automatically restart and function only as an unmanaged switch with its previous configuration cleared.

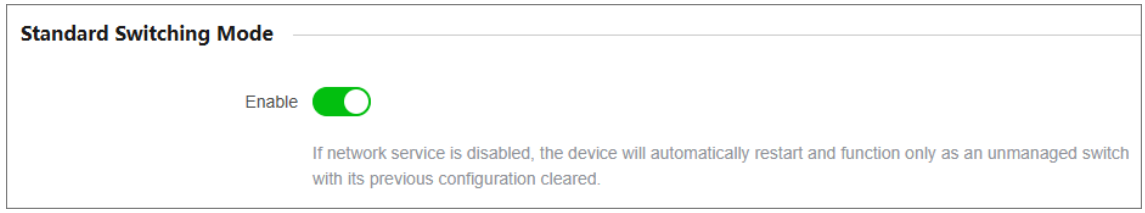


Figure 5-14 Configure Network Service

Note

An unmanaged switch is also referred to as a plug-and-play switch. As the name "plug-and-play" implies, it requires minimal configuration. Users can simply connect the network cables from different devices to the ports of the switch, and it will automatically start working. There is no need for complex setup processes or detailed network knowledge.

Super IP Address Configuration

The Super IP address provides a stable, fixed access point that enables users to easily access the switch's management interface for configuration or management operations—eliminating the need to memorize or search for more complicated actual addresses.
The Super IP feature is enabled by default, allowing any device directly connected to the switch to access its web management interface using the Super IP address. If the feature is disabled, it becomes unavailable for use. The default Super IP address is 10.180.190.200, and it can also be customized to suit your network configuration requirements.

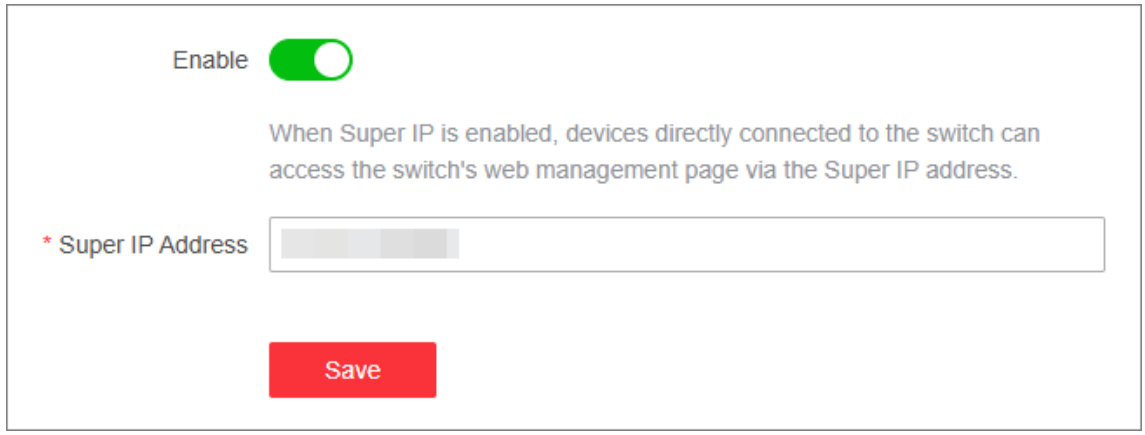


Figure 5-15 Configure Super IP Address

Note

- The super IP address and the device's local IP address cannot be configured in the same subnet.
- After the super IP feature is disabled and then enabled again, the default super IP address remains 10.180.190.200.
- Modifying or updating the Super IP address may cause temporary network conflicts or service interruptions. Proper planning and validation are recommended to minimize risks and ensure a smooth configuration process.

5.4 Network Diagnosis

Ping is a function that helps to diagnose network connectivity and quickly locate network faults.

Steps

1. Click **Network Monitoring → Ping** .

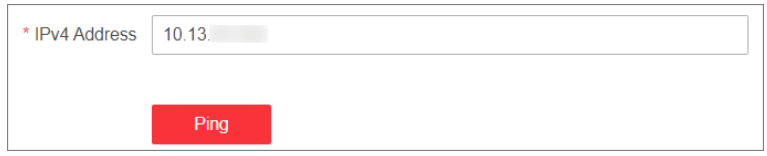


Figure 5-16 Ping

2. Enter a network server address in the **IPv4 address** field.
3. Click **Ping**.

Note

The network diagnosis result is displayed in the **Ping Result** area.

5.5 Log Management

This 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.

Steps

1. Go to **System Management → System Maintenance → Security Audit Log** or **System Management → System Maintenance → Device Operation Log** .

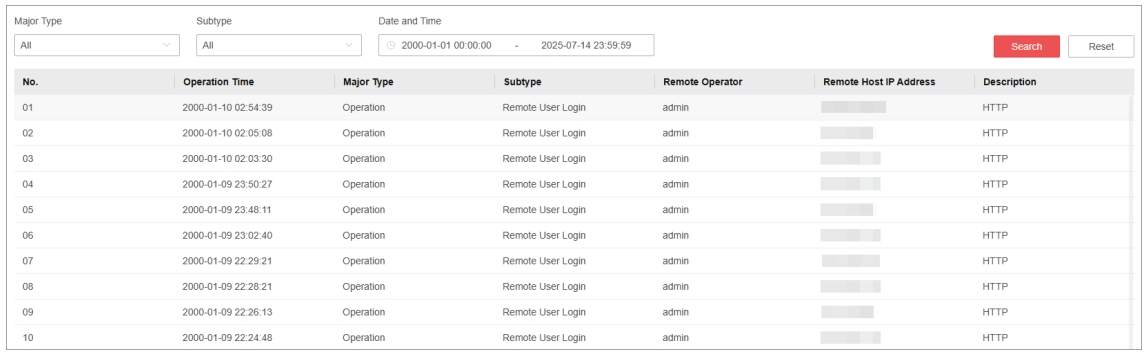


Figure 5-17 Manage Security Audit Logs (Only for Admin Users)

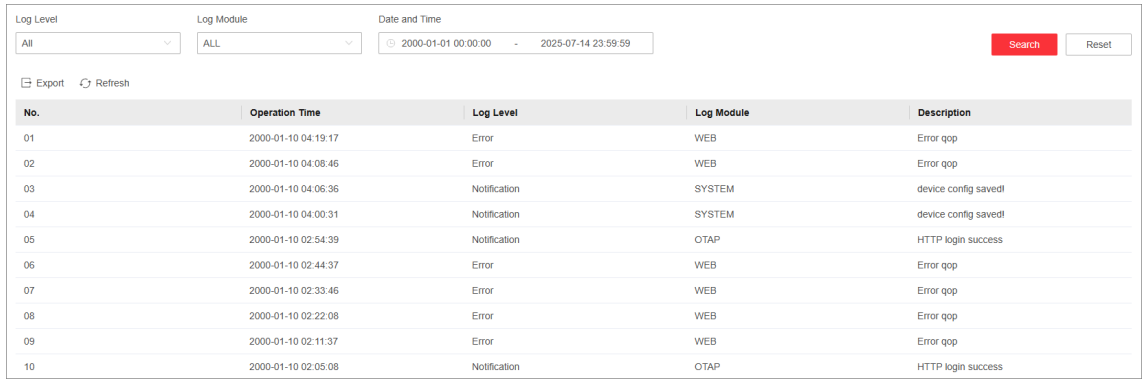


Figure 5-18 Manage Device Operation Logs (For All Users)

2. Set search conditions, including **Major Type**, **Subtype**, and **Date and Time** for security audit logs, or **Log Level**, **Log Module** and **Date and Time** for device operation logs.
3. Click **Search**.

Note

A maximum of 1024 search results can be displayed. Please narrow down the search scope if there are too many search results.

4. **Optional:** Click **Export** to export all the search results of device operation logs.

Note

Device operation logs can be exported as a TXT file. A prompt will pop up after logs are exported successfully.

5.6 Password Modification

Changing password periodically is a crucial step to ensure your device's security.

Steps

1. Click in the upper right corner of the web page.

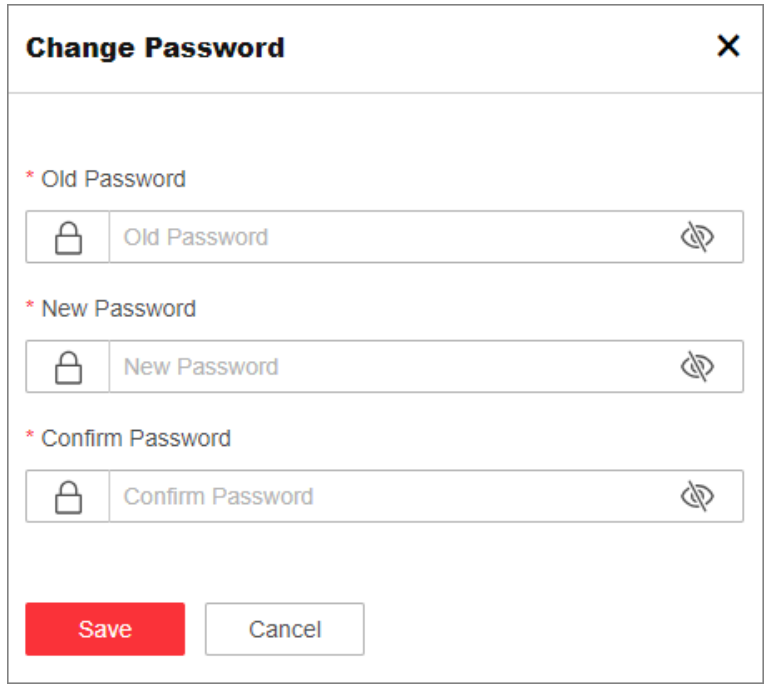


Figure 5-19 Change Password

2. Set **Old Password**, **New Password**, and **Confirm Password** in turn.

Note

- The password should contain 8 to 16 characters, including at least two types of the following categories: uppercase letters, lowercase letters, digits, and special characters.
- The password cannot contain user name, '123', or 'admin' (case-insensitive), 4 or more consecutively increasing or decreasing digits (such as '1234' and '4321'), or 4 or more identical characters (such as '1111' and 'aaaa').
- The password cannot contain only 'hik', 'hkws', or 'hikvision' (case insensitive).
- The password cannot be a common risky password.
- Remember to store your password securely. If you forget it, you can reset the password using the SADP tool or restore the device to factory settings via the reset button. Please note that resetting will erase all device configurations, so proceed with caution.

3. Click **Save**.


See Far, Go Further