Smart Managed Switch Web

User Manual

Navigation Page

	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.
- DS-3EXXXX-S and DS-3T series switches with software version V3.1.0 and above support ACL, IPSG, gateway ARP protection, and DHCP snooping configurations, while those with software versions below V3.1.0 do not support the preceding configurations.
- DS-3EXXXX-E series switches do not support ACL, IPSG, gateway ARP protection, and DHCP snooping configurations.
- ZD-S series switches do not support ACL, IPSG, and gateway ARP protections, but support DHCP snooping configuration.

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 the smart managed solar industrial PoE switch.

About Defaults

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

ℹ **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 super IP address cannot be modified. If the switch is directly connected to a PC, the super IP address can be used to access the switch for device management.

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.
ℹ **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

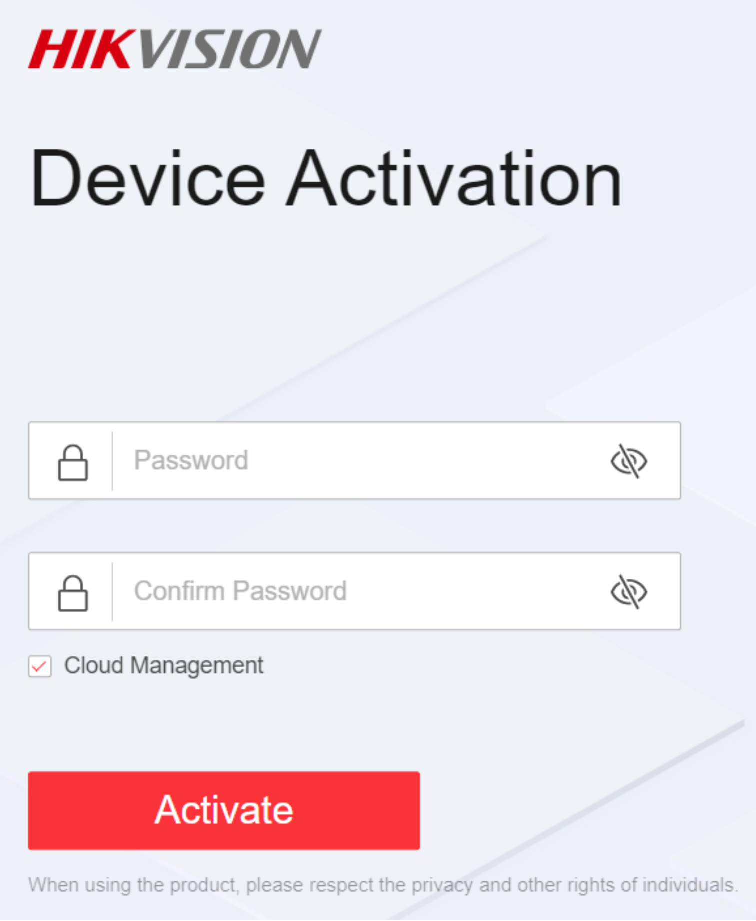
Ensure that your computer and switch are on the same network segment.

Steps

Note

All figures in this manual are for illustration purpose only.

1. Enter the default IP address of the switch in the address bar of a web browser, and press **Enter**.



Device Activation

☑ Cloud Management

When using the product, please respect the privacy and other rights of individuals.

Figure 2-1 Activate Device

Note

- You can obtain the default IP address of the switch 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

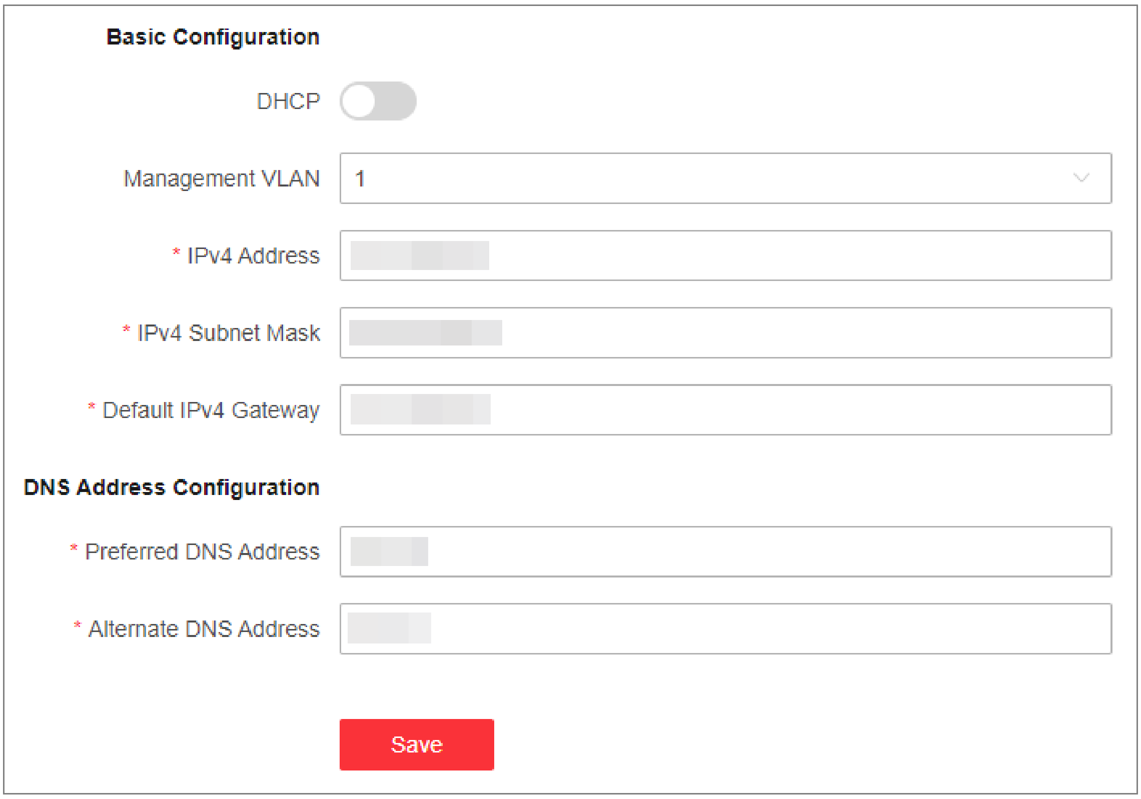
- The password should contain 8 to 16 characters, including at least two types of the following categories: uppercase letters, lowercase letters, digits, and special characters.
- The password cannot contain user name, '123', or 'admin' (case-insensitive), 4 or more consecutively increasing or decreasing 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.

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** .



Basic Configuration

DHCP

Management VLAN: 1

* IPv4 Address

* IPv4 Subnet Mask

* Default IPv4 Gateway

DNS Address Configuration

* Preferred DNS Address

* Alternate DNS Address

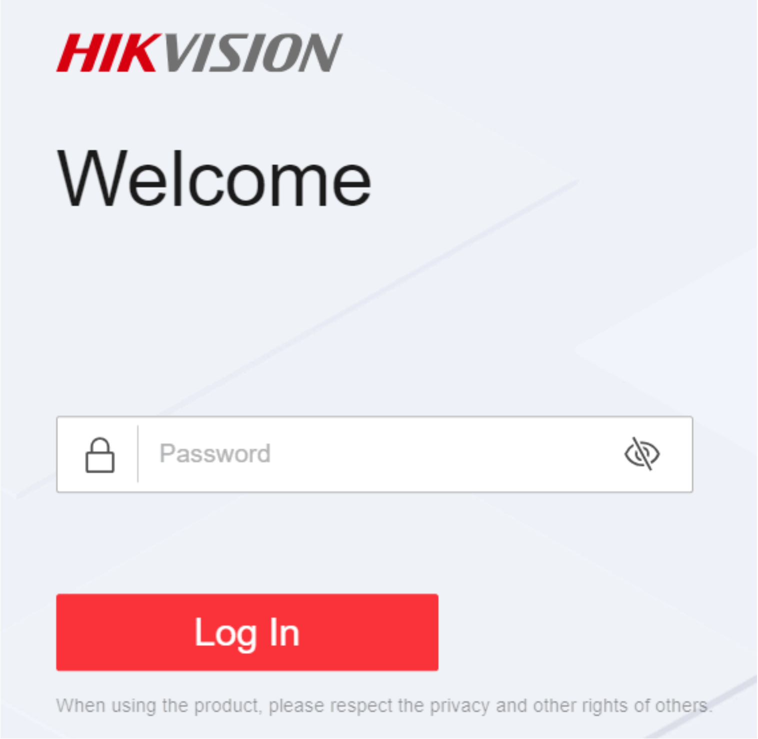
Figure 2-2 Modify Network Parameters

2) Modify the 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.



When using the product, please respect the privacy and other rights of others.

Figure 2-3 Log In

Chapter 3 Device Information

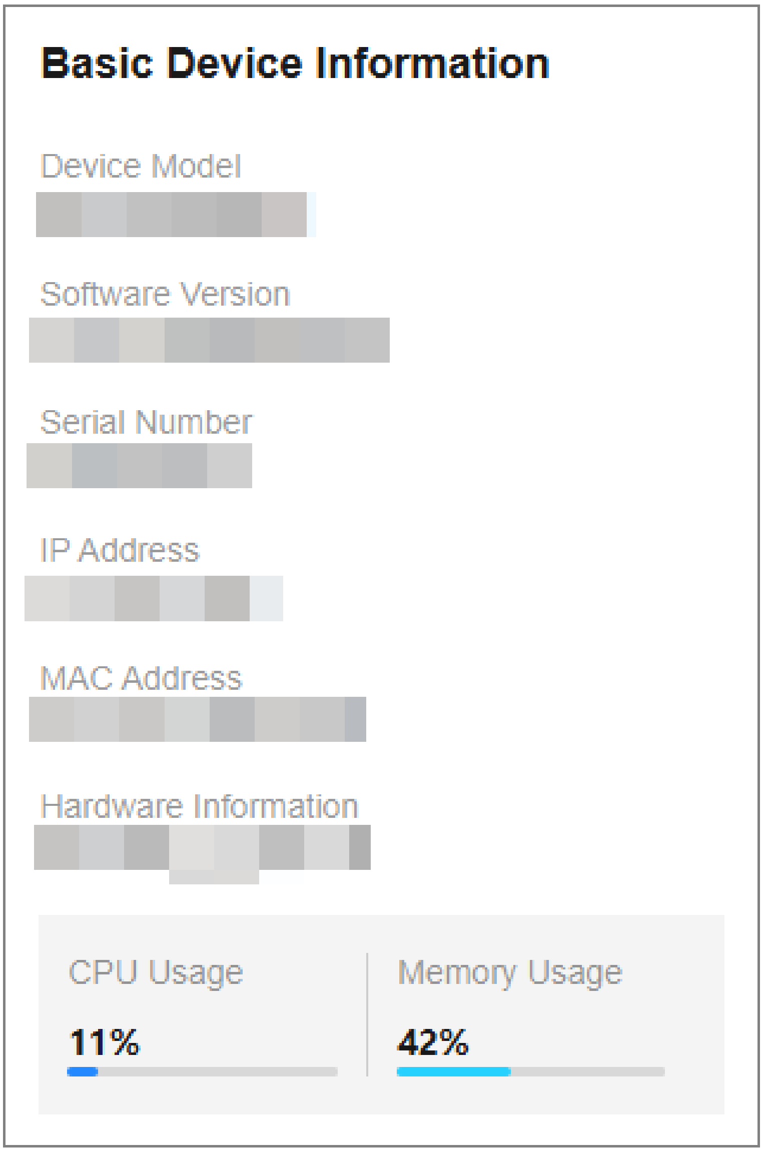
After logging in to the switch web, you can obtain detailed information about the switch, including the device overview information, port status information, and network status information.

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.



Basic Device Information

Device Model

[redacted]

Software Version

[redacted]

Serial Number

[redacted]

IP Address

[redacted]

MAC Address

[redacted]

Hardware Information

[redacted]

CPU Usage

11%

Memory Usage

42%

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

Device Name

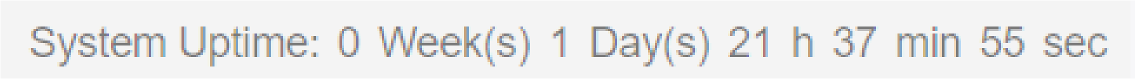
You can view the current device name or click ✎ next to it to customize the device name on the **Overview** page. The default device name is the device model.

DS-3T1306P-SI/HS ✎

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.

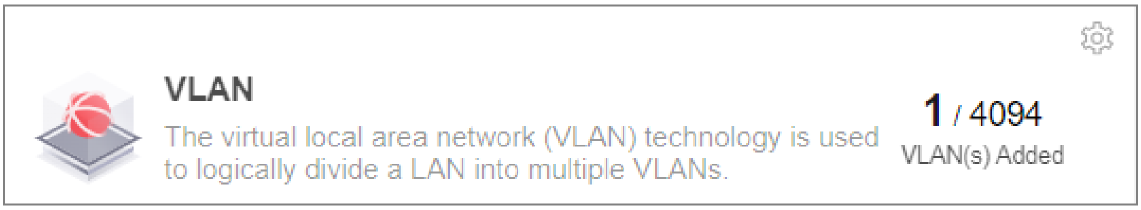


System Uptime: 0 Week(s) 1 Day(s) 21 h 37 min 55 sec

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.



VLAN

The virtual local area network (VLAN) technology is used to logically divide a LAN into multiple VLANs.

1 / 4094

VLAN(s) Added

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.

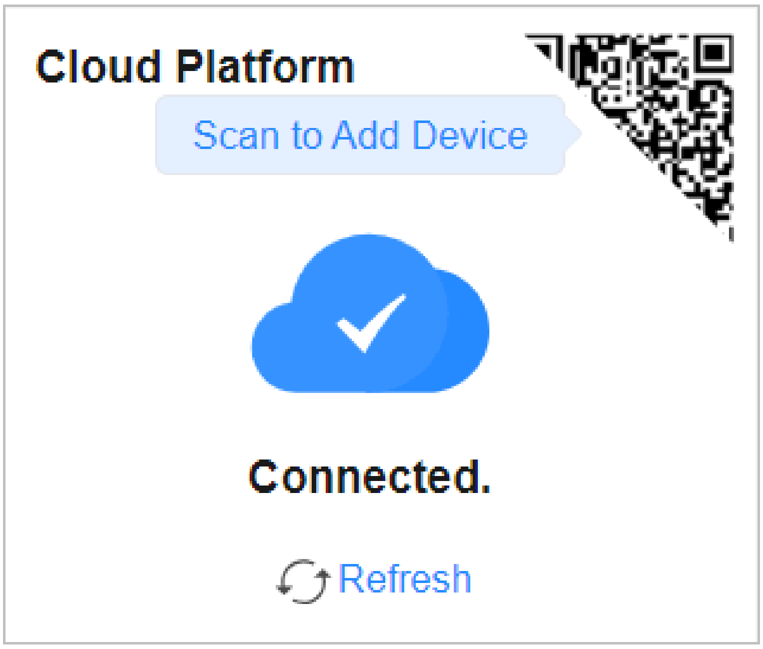


Figure 3-5 View Cloud Platform Connection Status (Connected)

- 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.

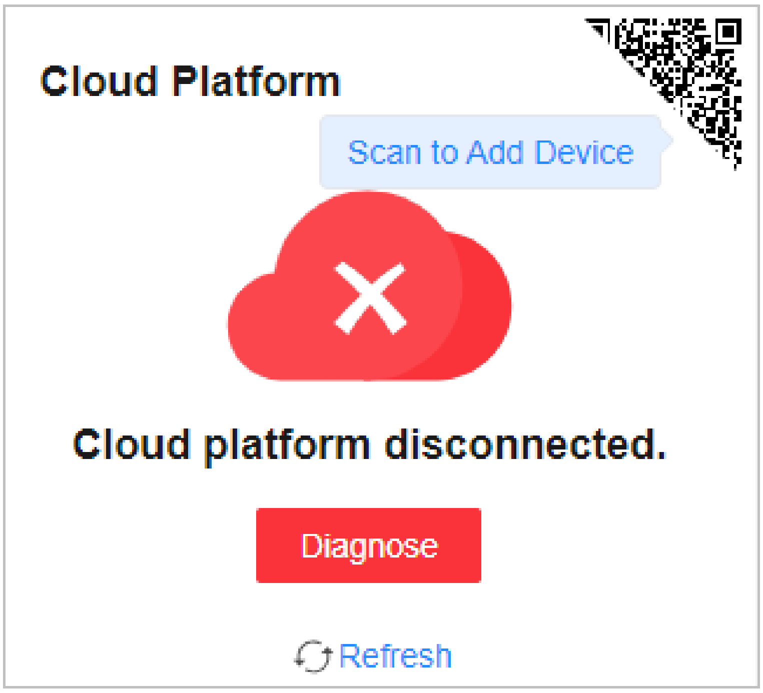


Figure 3-6 View Cloud Platform Connection Status (Disconnected)

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.

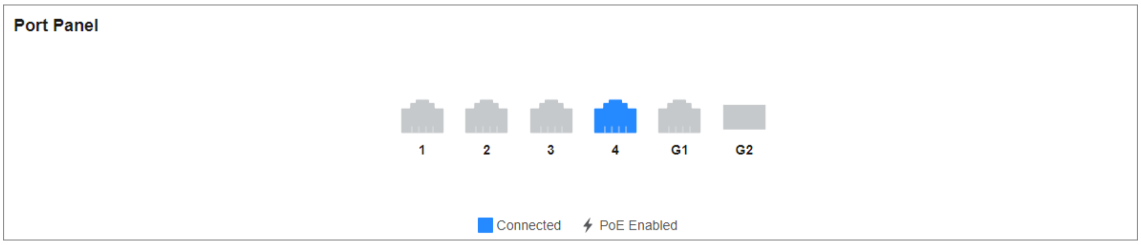
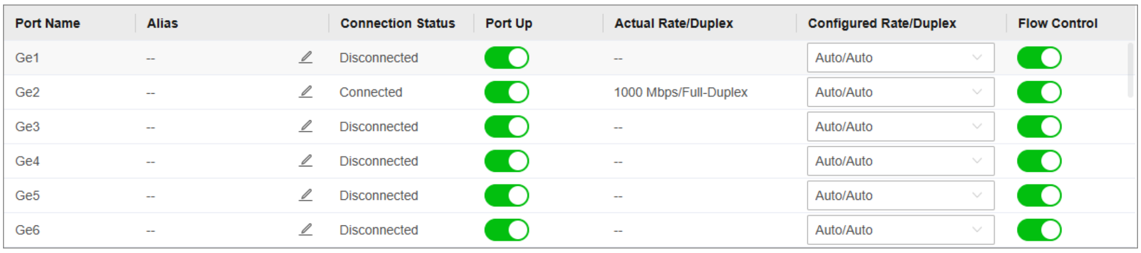


Figure 3-7 View Port Panel

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

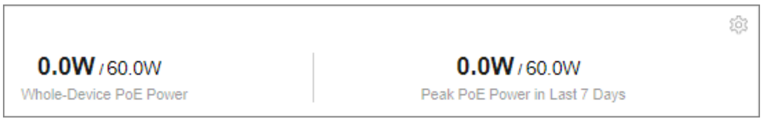
Configure the rate and duplex mode of a port. The default value is **Auto/Auto**. You can select different combinations of rates and duplex modes as required.

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.



0.0W / 60.0W

Whole-Device PoE Power

0.0W / 60.0W

Peak PoE Power in Last 7 Days

Figure 3-9 View PoE Power

Note

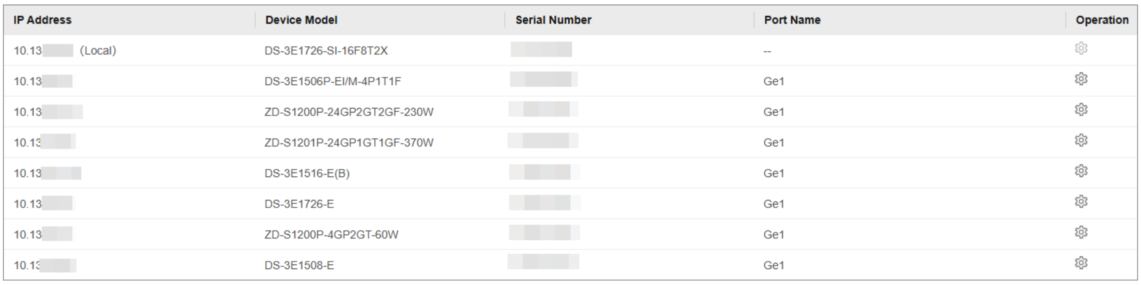
PoE power display is only available for switches supporting PoE.

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

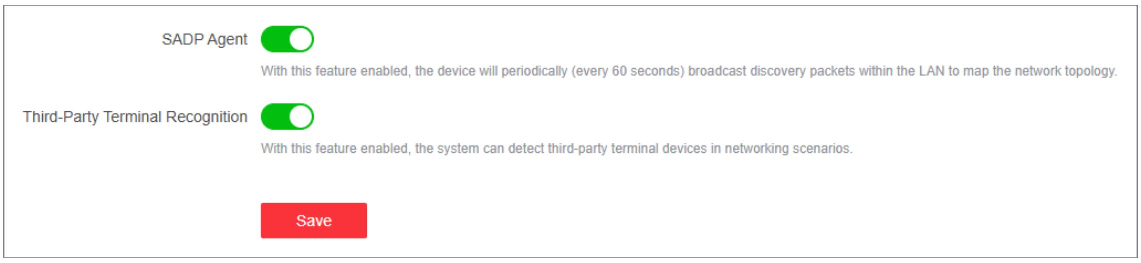
Device Discovery automatically detects and identifies network devices and terminal devices within the same LAN as the switch. Go to **Network Monitoring → Device Discovery → Device Discovery** , and you can view the IP address, device model, serial number, and connected switch port of the detected device(s). 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[redacted] (Local)	DS-3E1726-SI-16F8T2X	[redacted]	--	⚙
10.13[redacted]	DS-3E1506P-EI/M-4P1T1F	[redacted]	Ge1	⚙
10.13[redacted]	ZD-S1200P-24GP2GT2GF-230W	[redacted]	Ge1	⚙
10.13[redacted]	ZD-S1201P-24GP1GT1GF-370W	[redacted]	Ge1	⚙
10.13[redacted]	DS-3E1516-E(B)	[redacted]	Ge1	⚙
10.13[redacted]	DS-3E1726-E	[redacted]	Ge1	⚙
10.13[redacted]	ZD-S1200P-4GP2GT-60W	[redacted]	Ge1	⚙
10.13[redacted]	DS-3E1508-E	[redacted]	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.



SADP Agent ●

With this feature enabled, the device will periodically (every 60 seconds) broadcast discovery packets within the LAN to map the network topology.

Third-Party Terminal Recognition ●

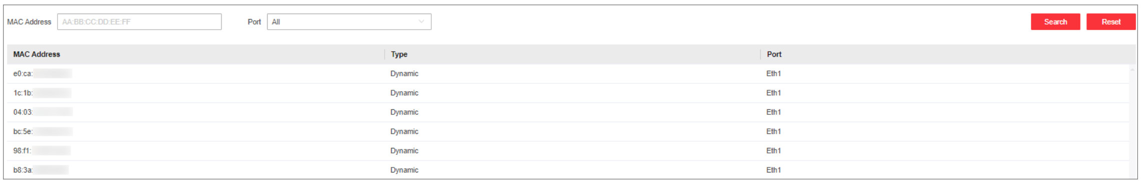
With this feature enabled, the system can detect third-party terminal devices in networking scenarios.

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.



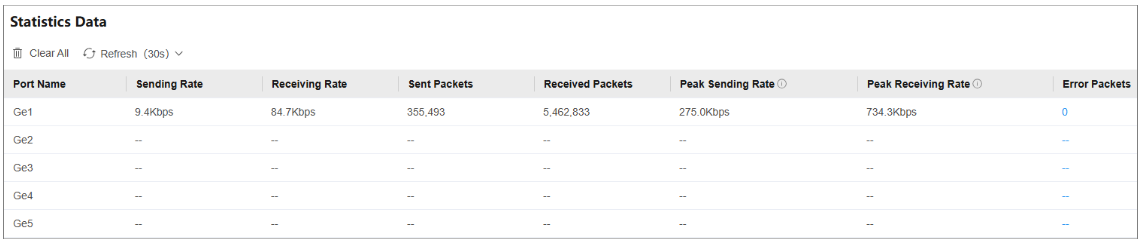
MAC Address AA:BB:CC:DD:EE:FF Port All

MAC Address	Type	Port
e0:ca:[redacted]	Dynamic	Eth1
1c:1b:[redacted]	Dynamic	Eth1
04:03:[redacted]	Dynamic	Eth1
bc:5e:[redacted]	Dynamic	Eth1
98:f1:[redacted]	Dynamic	Eth1
b8:3a:[redacted]	Dynamic	Eth1

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.



Statistics Data

Port Name	Sending Rate	Receiving Rate	Sent Packets	Received Packets	Peak Sending Rate	Peak Receiving Rate	Error Packets
Ge1	9.4Kbps	84.7Kbps	355,493	5,462,833	275.0Kbps	734.3Kbps	0
Ge2	--	--	--	--	--	--	--
Ge3	--	--	--	--	--	--	--
Ge4	--	--	--	--	--	--	--
Ge5	--	--	--	--	--	--	--

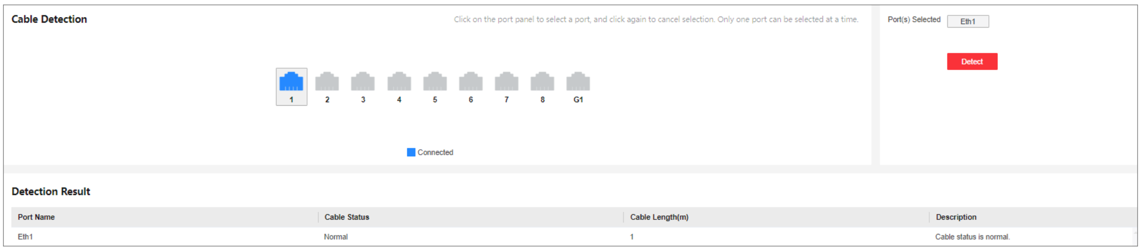
Figure 3-13 View Port Statistics

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 error packets, the number of CRC error packets, the number of flow control frames, and the number of dropped packets.

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.



Cable Detection

Click on the port panel to select a port, and click again to cancel selection. Only one port can be selected at a time.

Port(s) Selected: Eth1

Detection Result

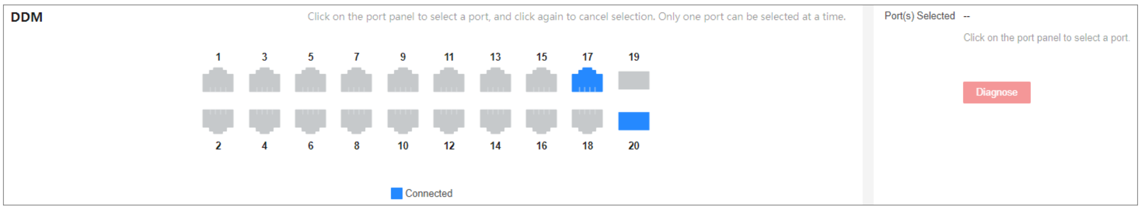
Port Name	Cable Status	Cable Length(m)	Description
Eth1	Normal	1	Cable status is normal.

Figure 3-14 Detect Cable Status

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** .



DDM

Click on the port panel to select a port, and click again to cancel selection. Only one port can be selected at a time.

Port(s) Selected --

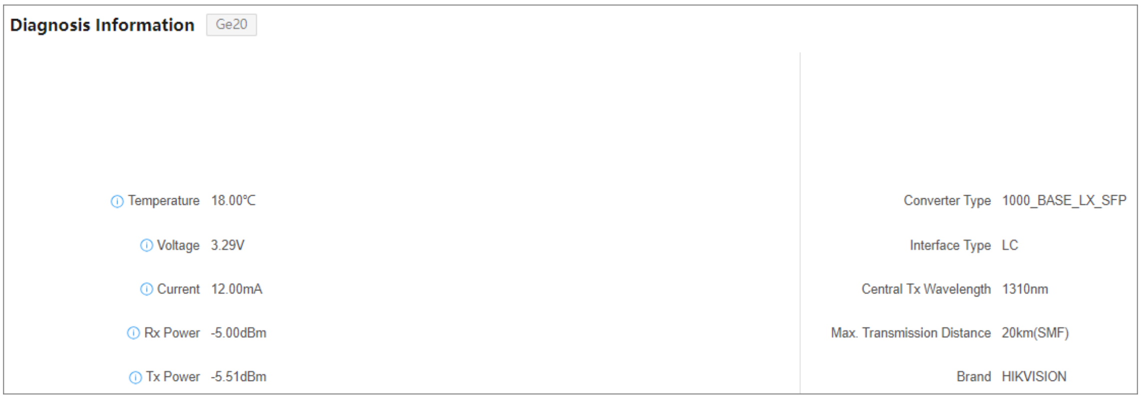
Click on the port panel to select a port.

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.



Diagnosis Information Ge20

Temperature	18.00℃
Voltage	3.29V
Current	12.00mA
Rx Power	-5.00dBm
Tx Power	-5.51dBm
Converter Type	1000_BASE_LX_SFP
Interface Type	LC
Central Tx Wavelength	1310nm
Max. Transmission Distance	20km(SMF)
Brand	HIKVISION

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

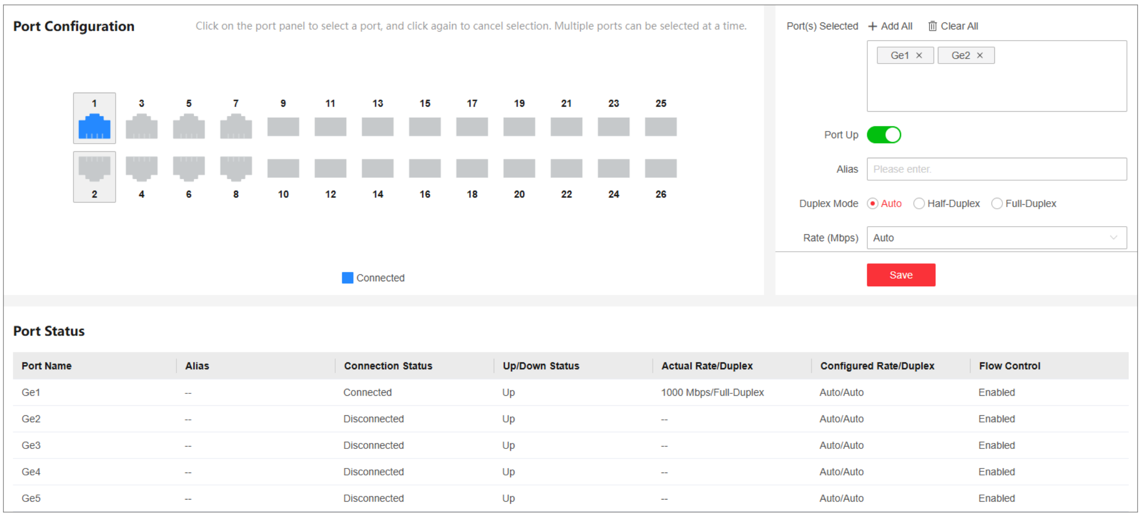
4.1 Port Configuration

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** .



Port Configuration

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

🟦 Connected

Port(s) Selected + Add All 🗑 Clear All

Ge1 × Ge2 ×

Port Up ●

Alias Please enter.

Duplex Mode ● Auto ○ Half-Duplex ○ Full-Duplex

Rate (Mbps) Auto

Save

Port Status

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

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.

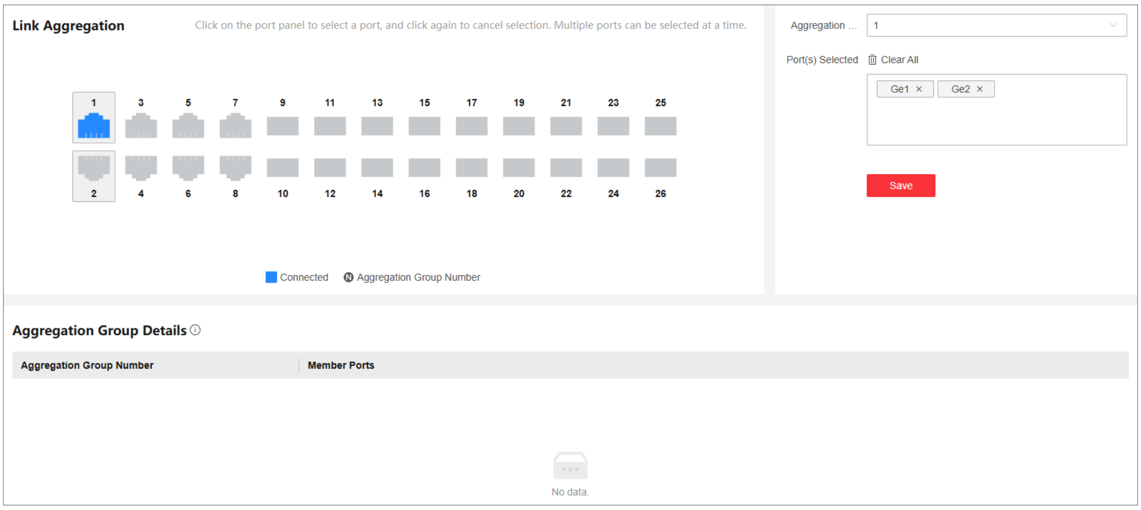
3. Click **Save**.
4. **Optional:** View the port attributes in the port status list.

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** .



Link Aggregation

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

Aggregation ... 1

Port(s) Selected Clear All

Ge1 × Ge2 ×

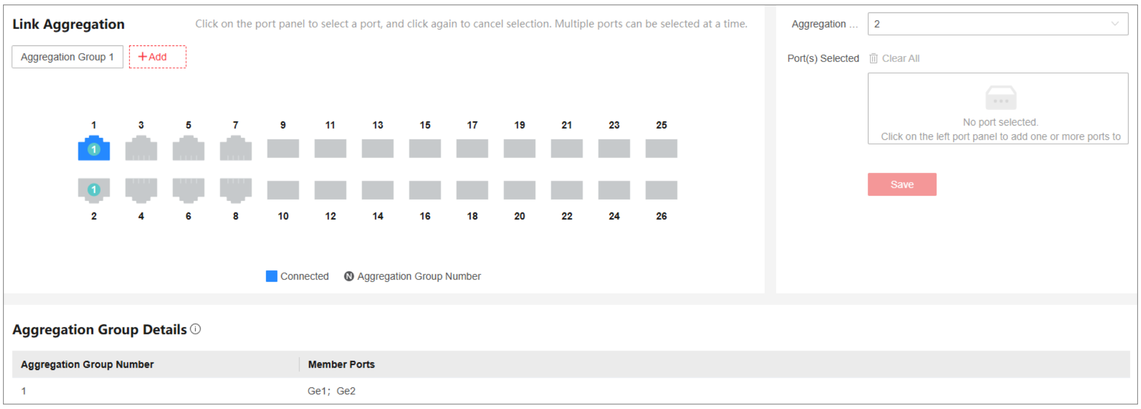
Save

Aggregation Group Details

Aggregation Group Number	Member Ports

No data.

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



Link Aggregation

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

Aggregation Group 1 | +Add

🟦 Connected | Ⓝ Aggregation Group Number

Aggregation ... 2

Port(s) Selected | Clear All

No port selected.

Click on the left port panel to add one or more ports to

Save

Aggregation Group Details

Aggregation Group Number	Member Ports
1	Ge1; Ge2

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.

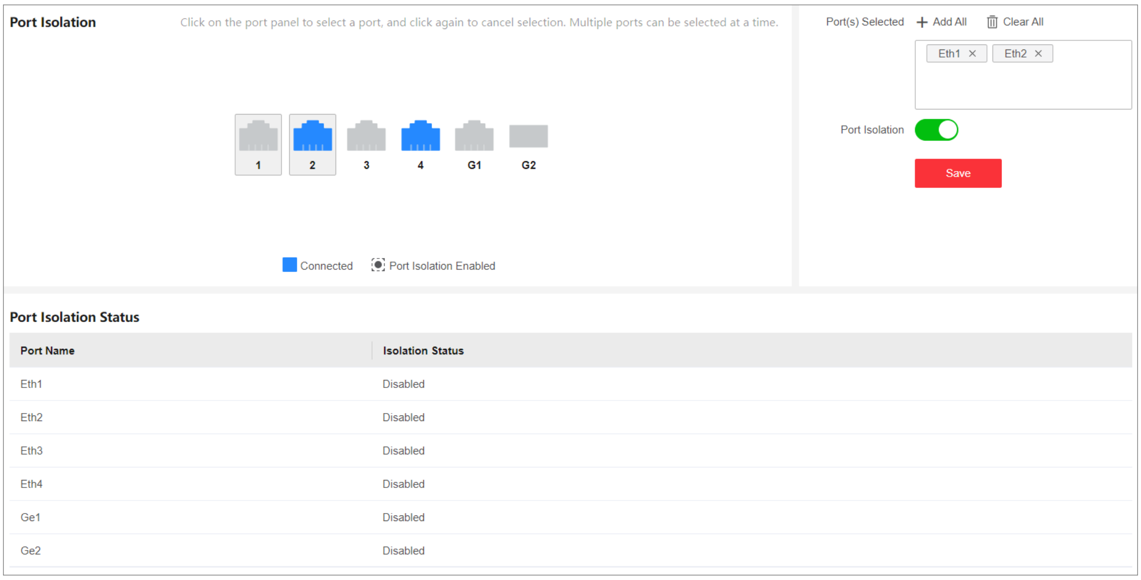
5. Click **Save**.
6. **Optional:** Edit the aggregation group.
   1) Click an existing aggregation group, for example, "Aggregation Group 1".
   2) Select the desired port(s) on the left port panel to add to the group, or deselect the desired port(s) on the right to delete from the group.
   3) Click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



Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

Port Isolation Status

Port Name	Isolation Status
Eth1	Disabled
Eth2	Disabled
Eth3	Disabled
Eth4	Disabled
Ge1	Disabled
Ge2	Disabled

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.

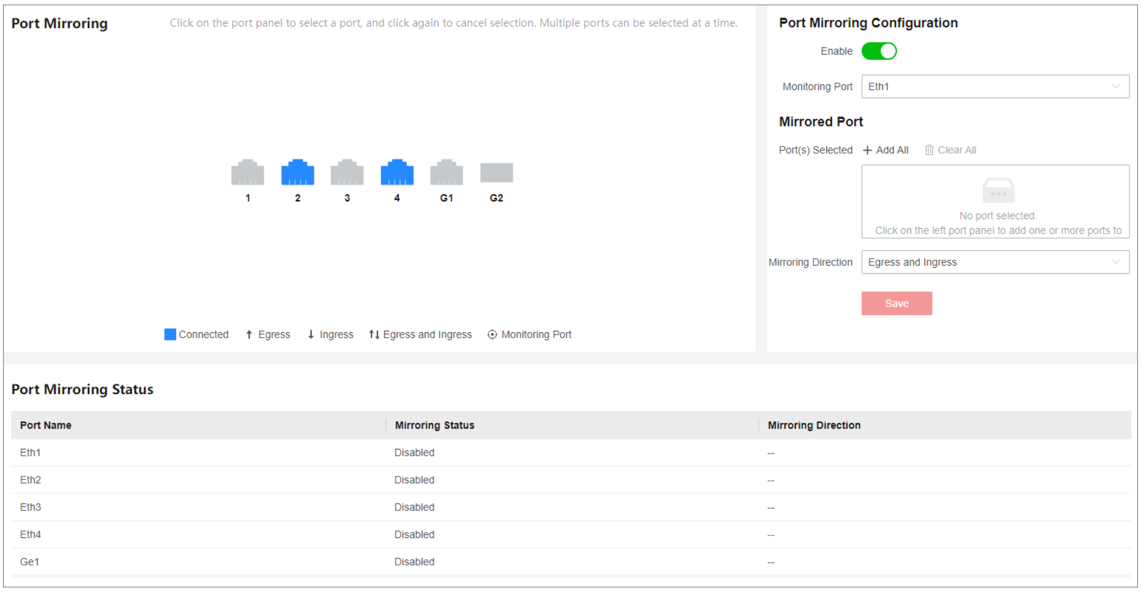
3. Enable or disable **Port Isolation** as required.
4. Click **Save**.
5. **Optional:** View the port isolation status of each port in the **Port Isolation Status** list.

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** .



Port Mirroring

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

Port Mirroring Configuration

Enable: ●

Monitoring Port: Eth1

Mirrored Port

Port(s) Selected + Add All 🗑 Clear All

No port selected.
Click on the left port panel to add one or more ports to

Mirroring Direction: Egress and Ingress

Port Mirroring Status

Port Name	Mirroring Status	Mirroring Direction
Eth1	Disabled	--
Eth2	Disabled	--
Eth3	Disabled	--
Eth4	Disabled	--
Ge1	Disabled	--

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.

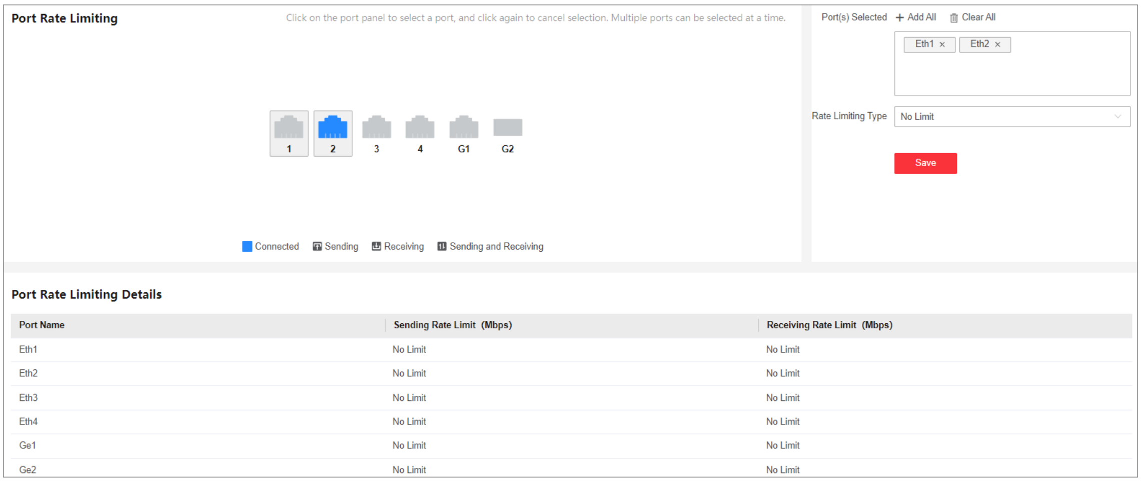
4. **Optional:** View the mirroring status of each port in the **Port Mirroring Status** list.

4.1.5 Configure Port Rate Limiting

Port rate limiting refers to limitation of a port's sending and receiving rates. This function is only applicable to Gigabit switches.

Steps

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



Port Rate Limiting

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

Port(s) Selected + Add All 🗑 Clear All

Eth1 × Eth2 ×

Rate Limiting Type: No Limit

Port Rate Limiting Details

Port Name	Sending Rate Limit (Mbps)	Receiving Rate Limit (Mbps)
Eth1	No Limit	No Limit
Eth2	No Limit	No Limit
Eth3	No Limit	No Limit
Eth4	No Limit	No Limit
Ge1	No Limit	No Limit
Ge2	No Limit	No Limit

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**. The value ranges from 1 to 1000(Mbps).

Receiving Rate Limit(Mbps)

Set the upper limit of receiving rate when **Rate Limiting Type** is **Receiving** or **Sending/ Receiving**. The value ranges from 1 to 1000(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 function is only applicable to Gigabit switches.

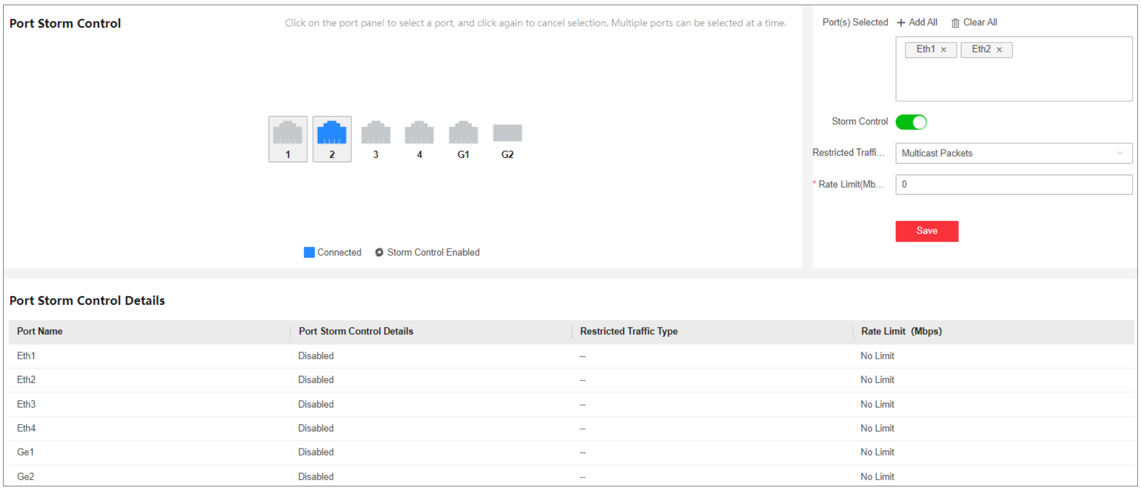
Steps

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:



Port Storm Control

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

Port(s) Selected + Add All 🗑 Clear All

Eth1 × Eth2 ×

Storm Control: on

Restricted Traffi...: Multicast Packets

* Rate Limit(Mb...: 0

Save

Port Storm Control Details

Port Name	Port Storm Control Details	Restricted Traffic Type	Rate Limit (Mbps)
Eth1	Disabled	--	No Limit
Eth2	Disabled	--	No Limit
Eth3	Disabled	--	No Limit
Eth4	Disabled	--	No Limit
Ge1	Disabled	--	No Limit
Ge2	Disabled	--	No Limit

Figure 4-7 Configure Global 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.

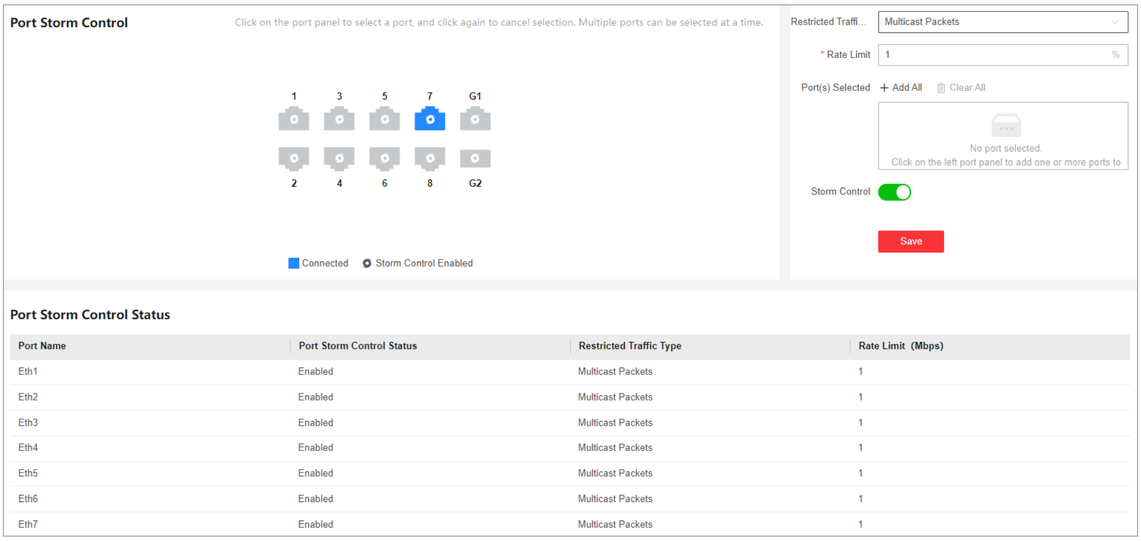
Unknown Unicast Packets

The data packets are sent to the specified device.

Rate Limit(Mbps)

Set the rate limit of the selected port(s), which ranges from 1 Mbps to 1000 Mbps.

- Port-Based Storm Control:



Port Storm Control

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

Restricted Traffi... Multicast Packets

* Rate Limit 1 %

Port(s) Selected + Add All Clear All

No port selected.
Click on the left port panel to add one or more ports to

Storm Control

Port Storm Control Status

Port Name	Port Storm Control Status	Restricted Traffic Type	Rate Limit (Mbps)
Eth1	Enabled	Multicast Packets	1
Eth2	Enabled	Multicast Packets	1
Eth3	Enabled	Multicast Packets	1
Eth4	Enabled	Multicast Packets	1
Eth5	Enabled	Multicast Packets	1
Eth6	Enabled	Multicast Packets	1
Eth7	Enabled	Multicast Packets	1

Figure 4-8 Configure Port-Based 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), which ranges from 1% to 100%.

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).

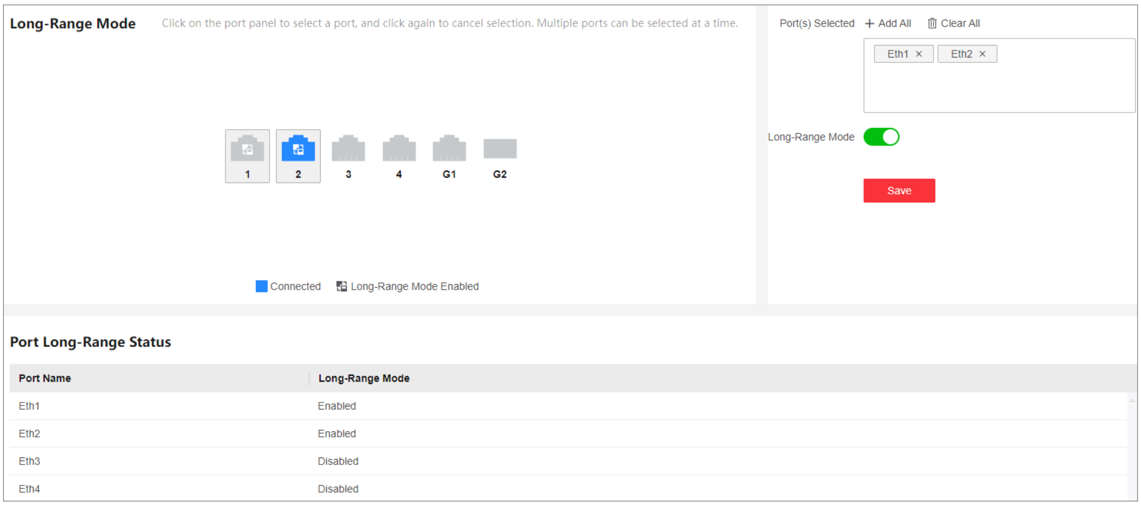
3. Click **Save**.
4. **Optional:** View the storm control status of each port in the **Port Storm Control Status** list.

4.1.7 Configure Long-Range Mode

The transmission distance of a port with long-range mode enabled can reach 300 meters at a rate of 10 Mbps.

Steps

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



Long-Range Mode Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

Port(s) Selected + Add All 🗑 Clear All

Eth1 × Eth2 ×

Long-Range Mode ●

Save

Port Long-Range Status

Port Name	Long-Range Mode
Eth1	Enabled
Eth2	Enabled
Eth3	Disabled
Eth4	Disabled

Figure 4-9 Configure Long-Range Mode

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

4.1.8 Configure High-Priority Port

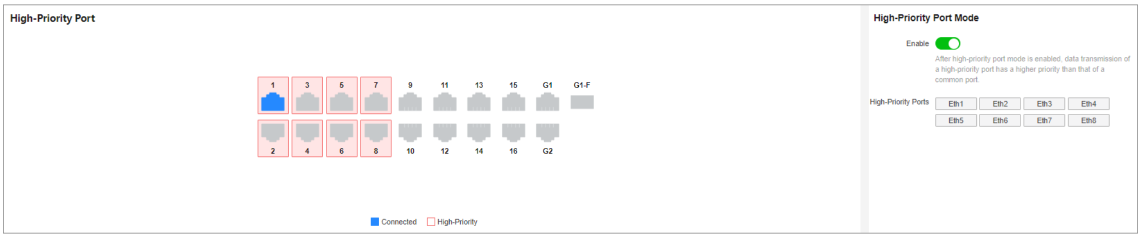
High-priority ports are identified by a red area on the device front panel. In the case of uplink congestion, the data of ports in this area is preferentially transmitted.

Steps

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

Note

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



Enable: on

After high-priority port mode is enabled, data transmission of a high-priority port has a higher priority than that of a common port.

High-Priority Ports: Eth1 Eth2 Eth3 Eth4 Eth5 Eth6 Eth7 Eth8

Figure 4-10 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.

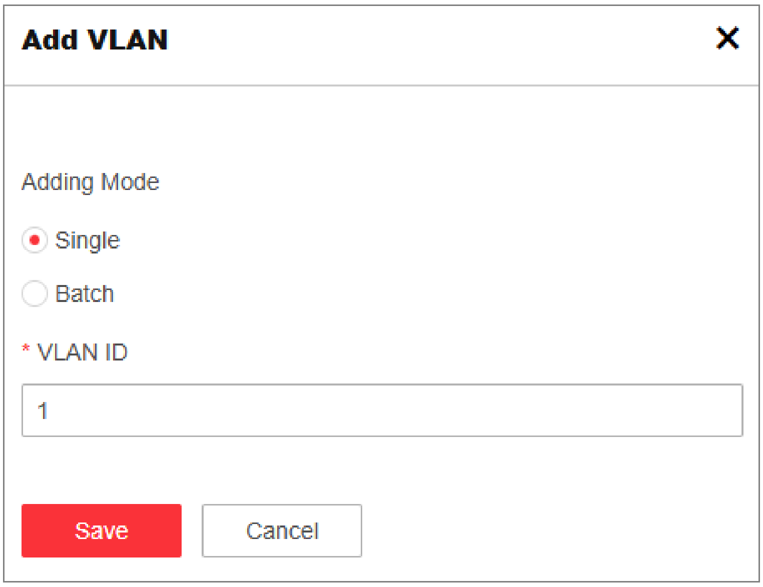
4.2 VLAN Configuration

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.



Add VLAN

Adding Mode

● Single

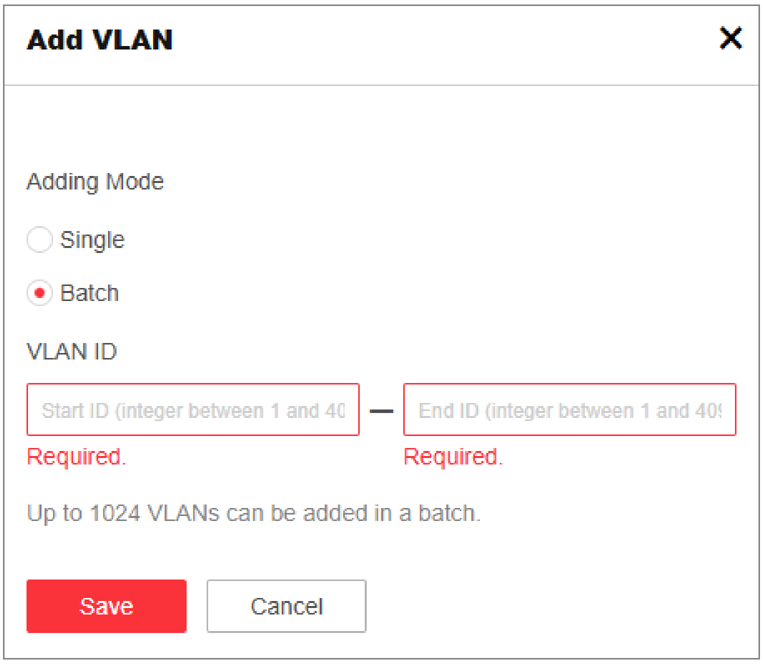
○ Batch

* VLAN ID

1

Figure 4-11 Add a Single VLAN

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



Add VLAN

Adding Mode

○ Single

● Batch

VLAN ID

Start ID (integer between 1 and 40 — End ID (integer between 1 and 40

Required. Required.

Up to 1024 VLANs can be added in a batch.

Figure 4-12 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

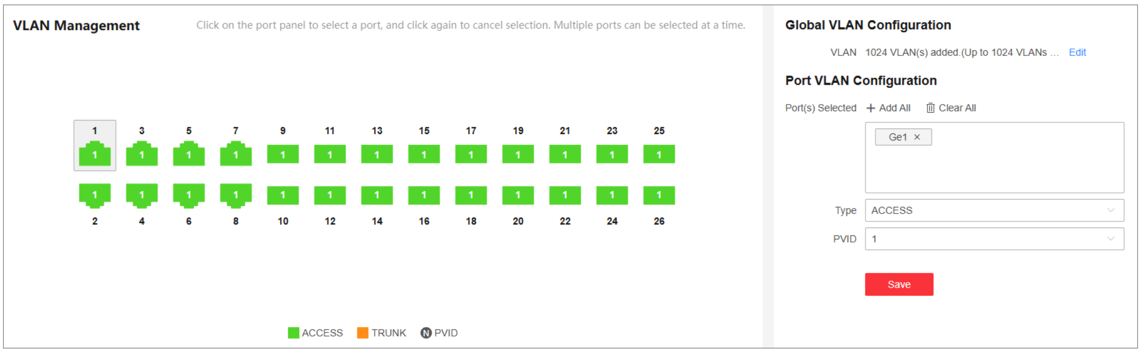
Steps

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.



VLAN Management

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

Global VLAN Configuration

VLAN 1024 VLAN(s) added.(Up to 1024 VLANs ... Edit

Port VLAN Configuration

Port(s) Selected + Add All 🗑 Clear All

Ge1 ×

Type ACCESS

PVID 1

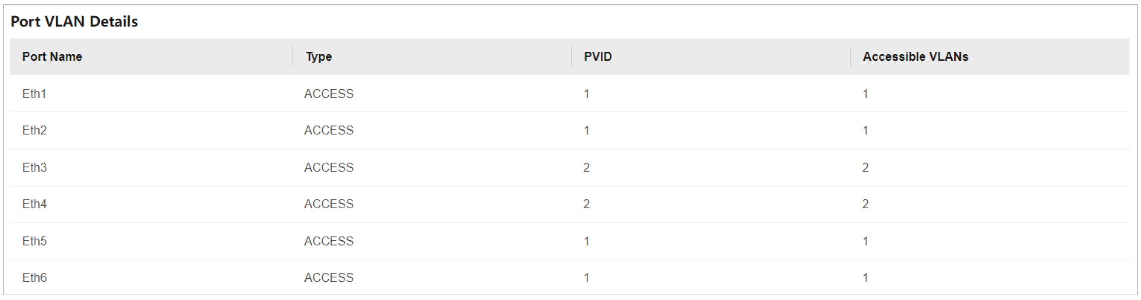
Save

Figure 4-13 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

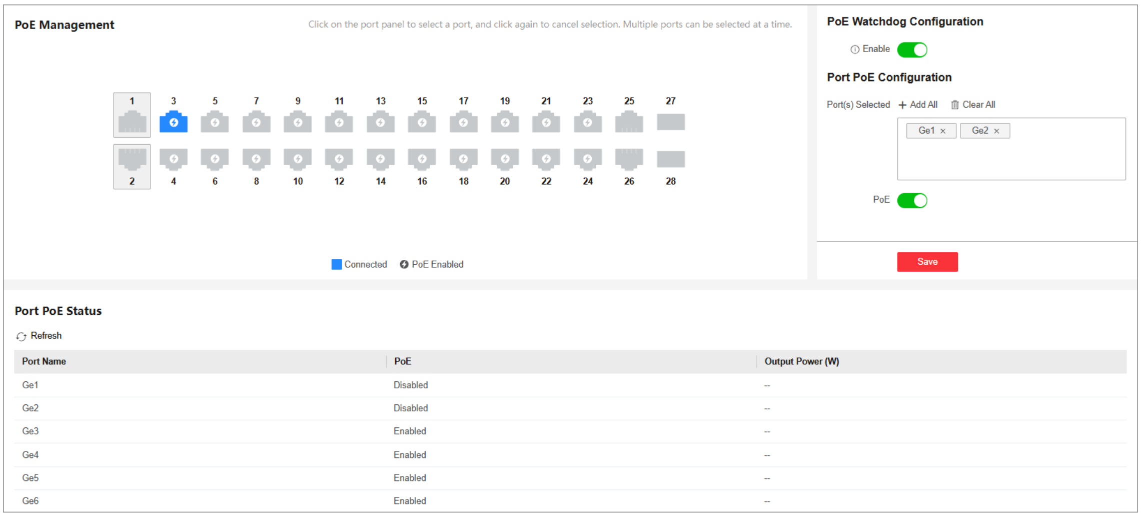
Port Name	Type	PVID	Accessible VLANs
Eth1	ACCESS	1	1
Eth2	ACCESS	1	1
Eth3	ACCESS	2	2
Eth4	ACCESS	2	2
Eth5	ACCESS	1	1
Eth6	ACCESS	1	1

Figure 4-14 Port VLAN Details

4.3 PoE Configuration

Note

PoE configuration, exclusively available on PoE switches, comprises three modules: PoE watchdog configuration, port-level PoE configuration, and power saving plan configuration.



PoE Management

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

PoE Watchdog Configuration

Enable: on

Port PoE Configuration

Port(s) Selected: Ge1 × Ge2 ×

PoE: on

Port PoE Status

Port Name	PoE	Output Power (W)
Ge1	Disabled	--
Ge2	Disabled	--
Ge3	Enabled	--
Ge4	Enabled	--
Ge5	Enabled	--
Ge6	Enabled	--

Figure 4-15 Configure PoE Watchdog and Port-Level PoE

PoE Watchdog Configuration

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

Port PoE Configuration

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

1. Click **PoE Management → PoE Management** .
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.

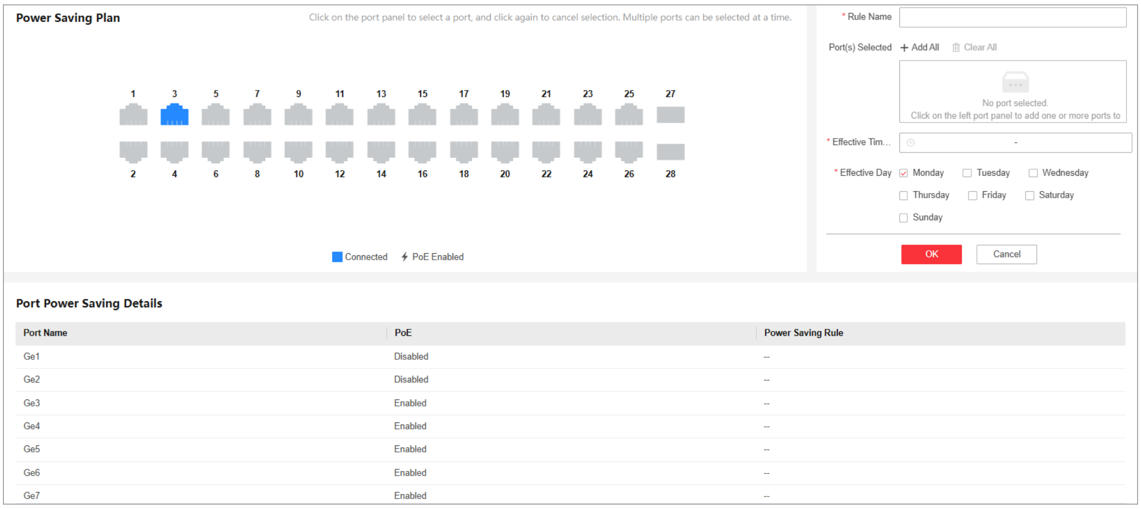
3. Enable **PoE** to supply power to the PD(s) connected to the port(s).
4. Enable **PD Compatibility Mode** as required.

Note

- Enabling this mode can improve compatibility for unsupported IPC(s) and AP(s), but may decrease PD detection sensitivity of PoE ports. You can enable this mode if some PD(s) fail to be powered by the switch so that PD(s) not compliant with normal PoE standards can also be detected by PoE port(s).
- **PD Compatibility Mode** is a model-specific feature, available only on some devices. Actual support depends on hardware specifications.

5. Click **Save**.
6. View the PoE enabling status, output power, etc. of PoE ports(s) in the **Port PoE Status** list. For devices supporting PD compatibility mode, you may additionally monitor PD compatibility mode enabling status and power supply status.

Power Saving Plan Configuration


Power Saving Plan
Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.
1
3
5
7
9
11
13
15
17
19
21
23
25
27
2
4
6
8
10
12
14
16
18
20
22
24
26
28
Connected
PoE Enabled

* Rule Name

Port(s) Selected + Add All 🗑 Clear All

No port selected.
Click on the left port panel to add one or more ports to

* Effective Tim... -

* Effective Day ☑ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

OK Cancel

Port Power Saving Details

Port Name	PoE	Power Saving Rule
Ge1	Disabled	--
Ge2	Disabled	--
Ge3	Enabled	--
Ge4	Enabled	--
Ge5	Enabled	--
Ge6	Enabled	--
Ge7	Enabled	--

Figure 4-16 Configure Power Saving Plan

Note

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

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

   Note

   By default, no power saving plan is configured.

2. In **Rule Configuration**, click **Add**.
3. Set **Rule Name**, for example, ***Daytime***.
4. 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

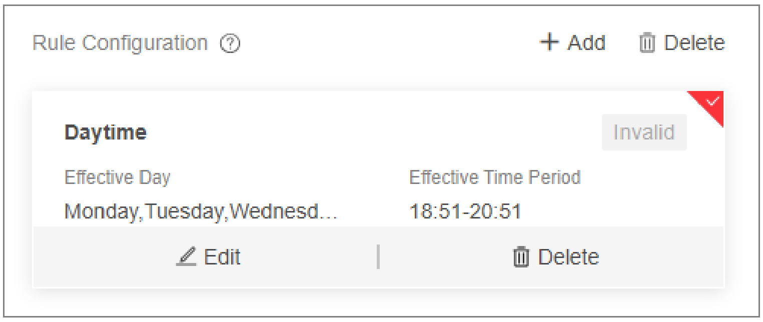
   The start time should be earlier than the end time.

6. Set **Effective Day** to specify on which day(s) of the week the newly added rule will take effect.
7. Click **OK**.
8. 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. Select a power saving rule, and click **Edit** or **Delete** to edit or delete the rule.



Rule Configuration

Daytime — Invalid

Effective Day: Monday,Tuesday,Wednesd...

Effective Time Period: 18:51-20:51

Figure 4-17 Edit/Delete Rule

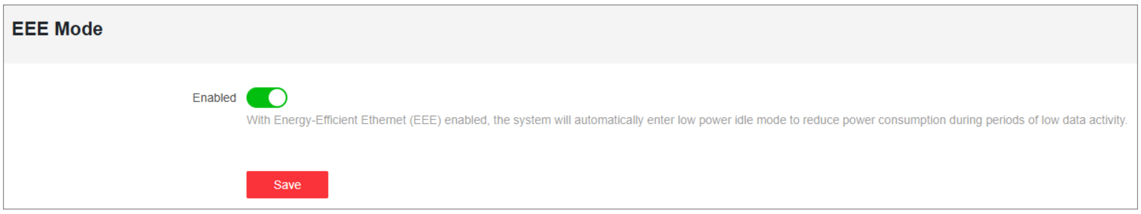
Note

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.



EEE Mode

Enabled: ●

With Energy-Efficient Ethernet (EEE) enabled, the system will automatically enter low power idle mode to reduce power consumption during periods of low data activity.

Figure 4-18 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

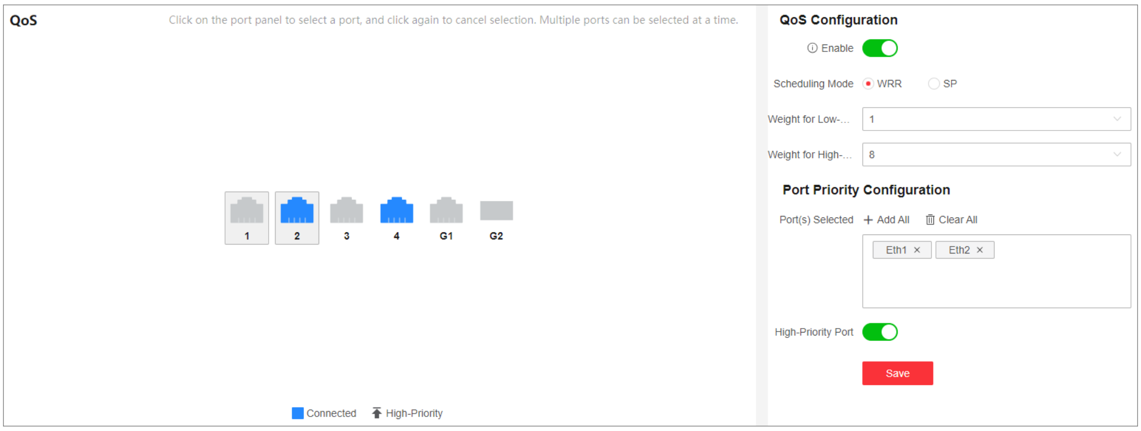
Quality of Service (QoS) is a technology used to solve issues such as network congestion, delay, jitter, and packet loss. In the case of limited bandwidth resources, QoS allocates appropriate bandwidth for various services and preferentially forwards applications such as voice, video, and important data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



QoS

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

QoS Configuration

Enable: on

Scheduling Mode: ● WRR ○ SP

Weight for Low-...: 1

Weight for High-...: 8

Port Priority Configuration

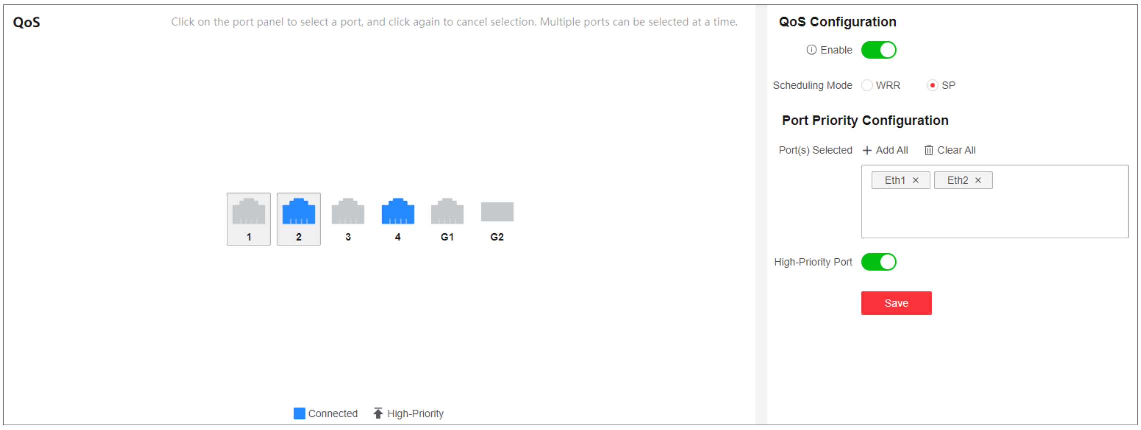
Port(s) Selected: Eth1 × Eth2 ×

High-Priority Port: on

Figure 4-19 Select WRR Mode

SP

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



QoS

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

QoS Configuration

Enable: on

Scheduling Mode: ○ WRR ● SP

Port Priority Configuration

Port(s) Selected: Eth1 × Eth2 ×

High-Priority Port: on

Figure 4-20 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.

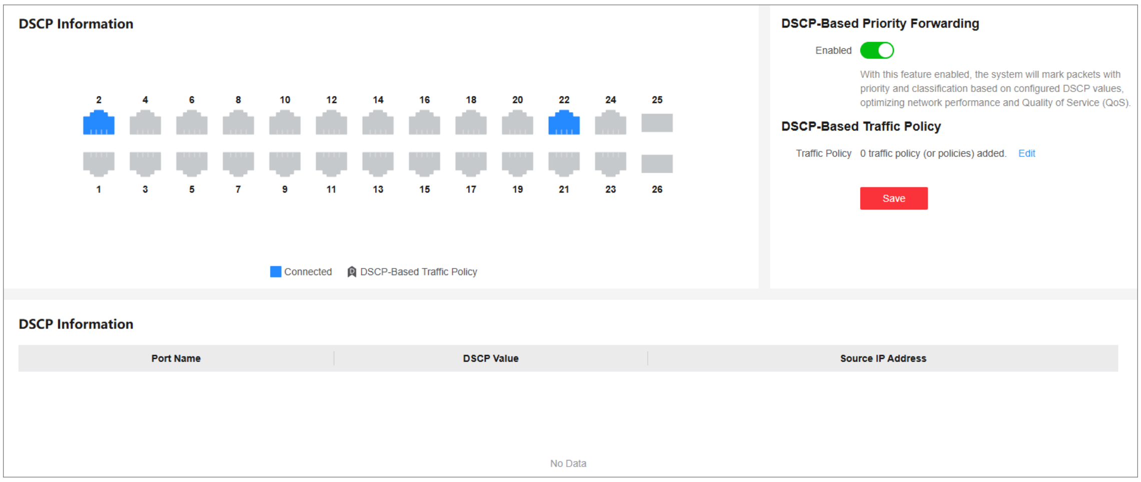
5. Enable **High-Priority Port** to set the selected port(s) as high-priority port(s).
6. Click **Save**.

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.



DSCP Information

🟦 Connected 🔒 DSCP-Based Traffic Policy

DSCP-Based Priority Forwarding

Enabled ●

With this feature enabled, the system will mark packets with priority and classification based on configured DSCP values, optimizing network performance and Quality of Service (QoS).

DSCP-Based Traffic Policy

Traffic Policy 0 traffic policy (or policies) added. Edit

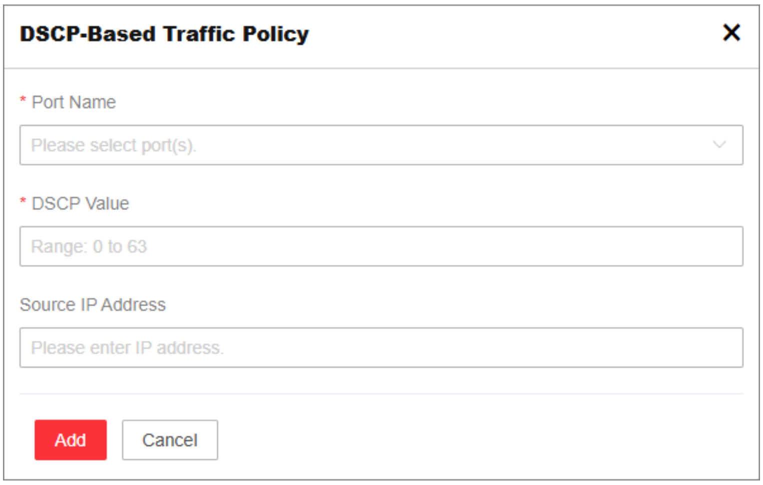
DSCP Information

Port Name	DSCP Value	Source IP Address

No Data

Figure 4-21 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.



DSCP-Based Traffic Policy

* Port Name

Please select port(s).

* DSCP Value

Range: 0 to 63

Source IP Address

Please enter IP address.

Figure 4-22 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.

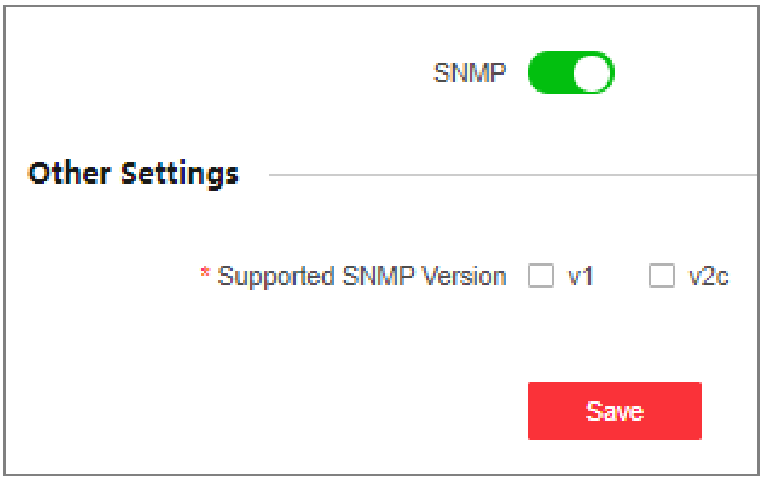
8. **Optional:** View the existing or newly added traffic policies in the **DSCP Information** list.

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.



SNMP

Other Settings

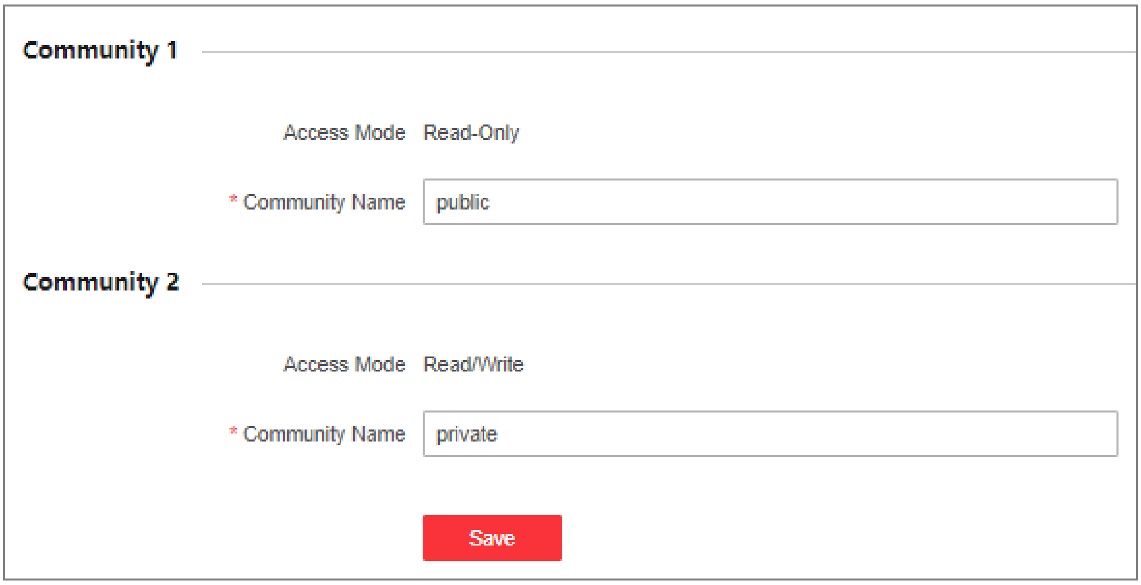
* Supported SNMP Version □ v1 □ v2c

Figure 4-23 Configure Basic SNMP Parameters

4.7.2 Configure SNMP Community

Steps

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



Community 1

Access Mode Read-Only

* Community Name public

Community 2

Access Mode Read/Write

* Community Name private

Figure 4-24 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.

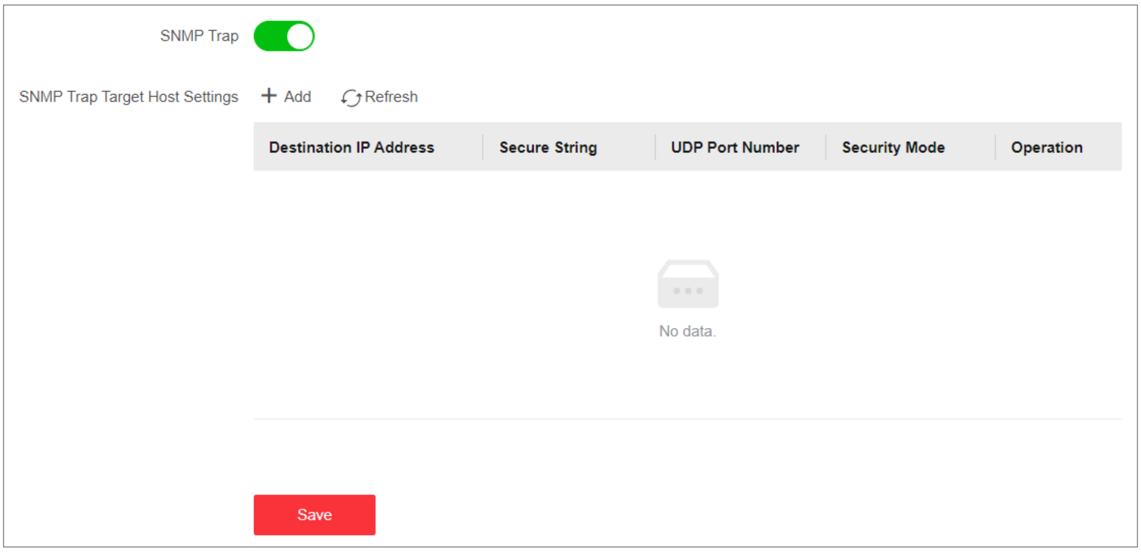
   - **Ready-Only**: The community has a read-only permission to access the NMS. The default community name is **public**.
   - **Read/Write**: The community has a read/write permission to access the NMS. The default community name is **private**.

3. Click **Save**.

4.7.3 Configure SNMP Trap Target Host

Steps

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



SNMP Trap

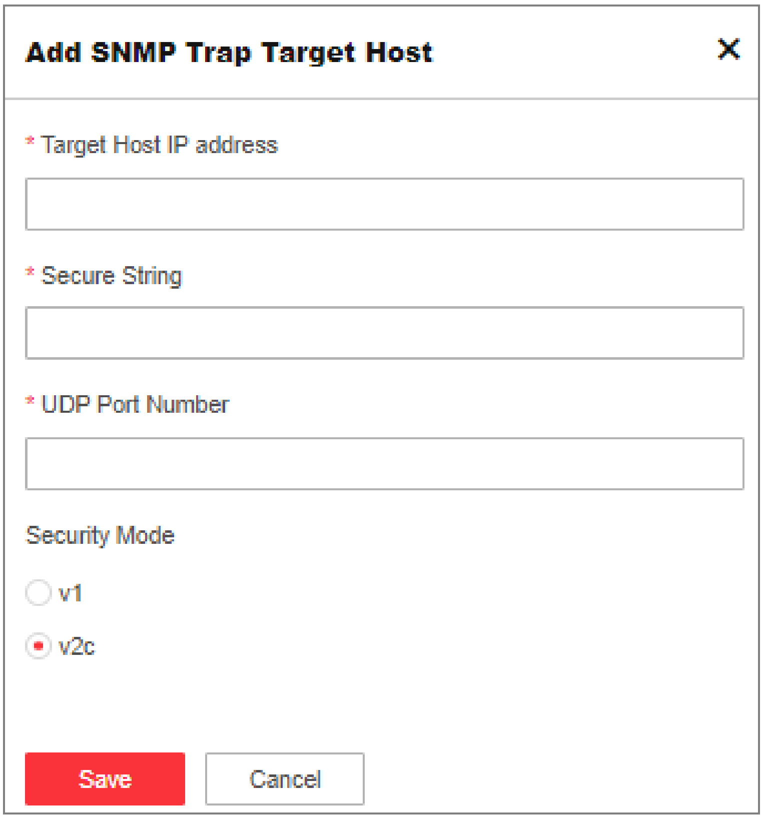
SNMP Trap Target Host Settings

Destination IP Address	Secure String	UDP Port Number	Security Mode	Operation

No data.

Figure 4-25 Configure SNMP Trap Target Host

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



Add SNMP Trap Target Host

* Target Host IP address

* Secure String

* UDP Port Number

Security Mode

○ v1

● v2c

Figure 4-26 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**.

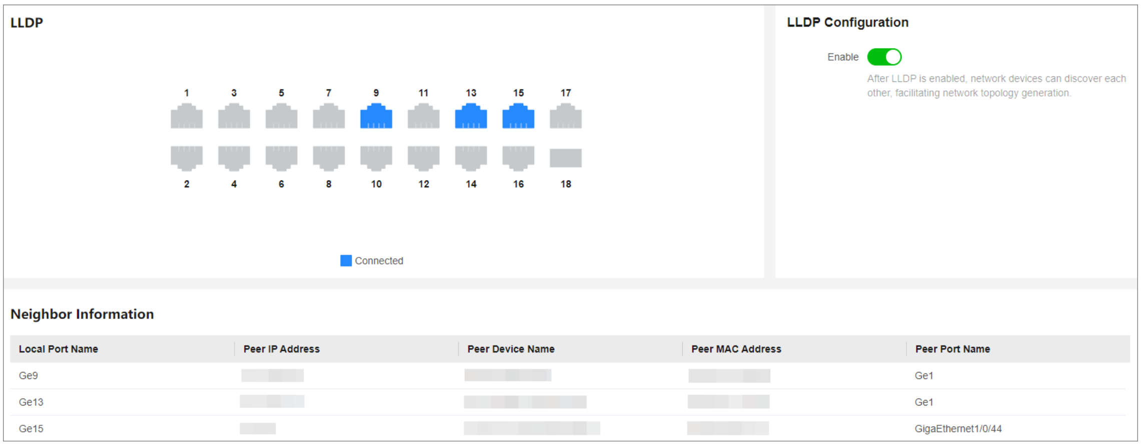
4. Click **Save**.
5. **Optional:** View the details about of existing SNMP trap target hosts. Alternatively, edit or delete the desired target host in the SNMP trap target host list.

4.8 LLDP Configuration

Link Layer Discovery Protocol (LLDP) is a layer 2 neighbor discovery protocol that allows devices to advertise device information to their directly connected peers/neighbors. With LLDP enabled, network devices can send LLDP data units (LLDPDUs) to inform other devices of their status. LLDP helps to draw network topology and detect improper configurations in a network.

Steps

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



LLDP

LLDP Configuration

Enable ●

After LLDP is enabled, network devices can discover each other, facilitating network topology generation.

Neighbor Information

Local Port Name	Peer IP Address	Peer Device Name	Peer MAC Address	Peer Port Name
Ge9	[redacted]	[redacted]	[redacted]	Ge1
Ge13	[redacted]	[redacted]	[redacted]	Ge1
Ge15	[redacted]	[redacted]	[redacted]	GigaEthernet1/0/44

Figure 4-27 Configure LLDP

Note

After LLDP is enabled, network devices can discover each other, facilitating network topology drawing.

3. **Optional:** View the local port(s), peer device(s), IP and MAC addresses of peer device(s), and peer port(s) in the **Neighbor Information** list.

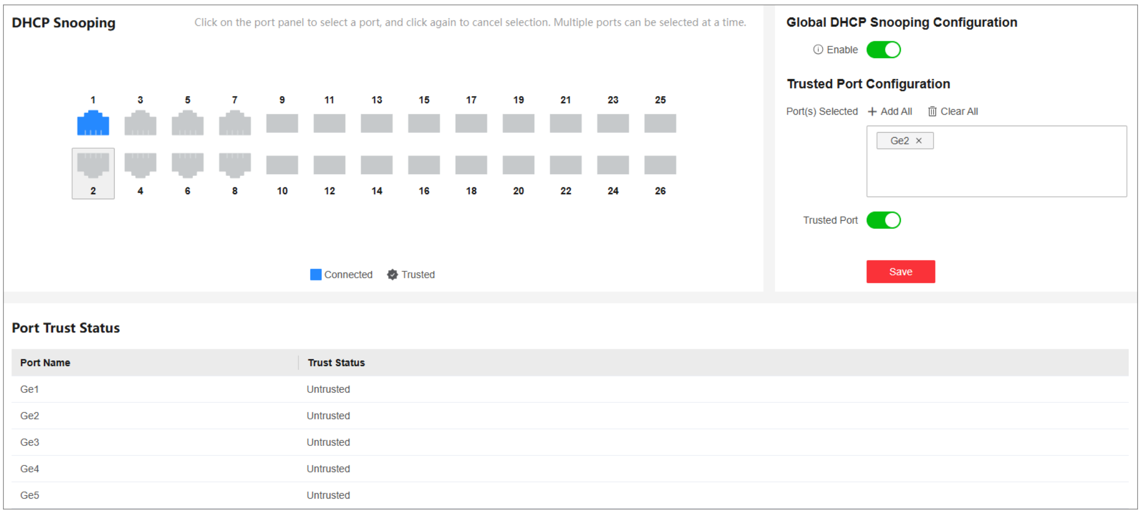
4.9 Security Configuration

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** .



DHCP Snooping

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

Global DHCP Snooping Configuration

ⓘ Enable ●

Trusted Port Configuration

Port(s) Selected + Add All 🗑 Clear All

Trusted Port ●

Port Trust Status

Port Name	Trust Status
Ge1	Untrusted
Ge2	Untrusted
Ge3	Untrusted
Ge4	Untrusted
Ge5	Untrusted

Figure 4-28 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.

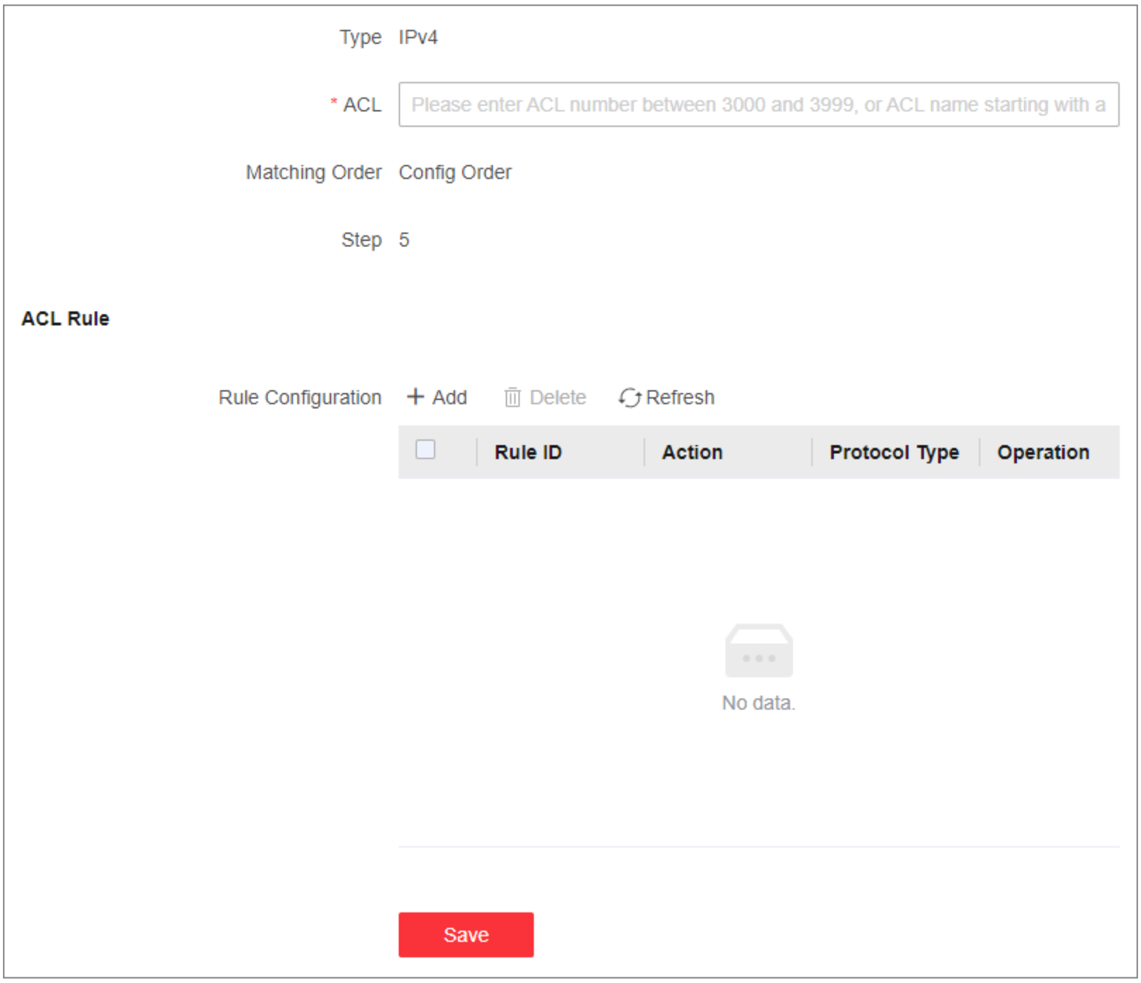
Note

- 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**.



Type IPv4

* ACL Please enter ACL number between 3000 and 3999, or ACL name starting with a

Matching Order Config Order

Step 5

ACL Rule

Rule Configuration + Add Delete Refresh

□	Rule ID	Action	Protocol Type	Operation

No data.

Figure 4-29 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.

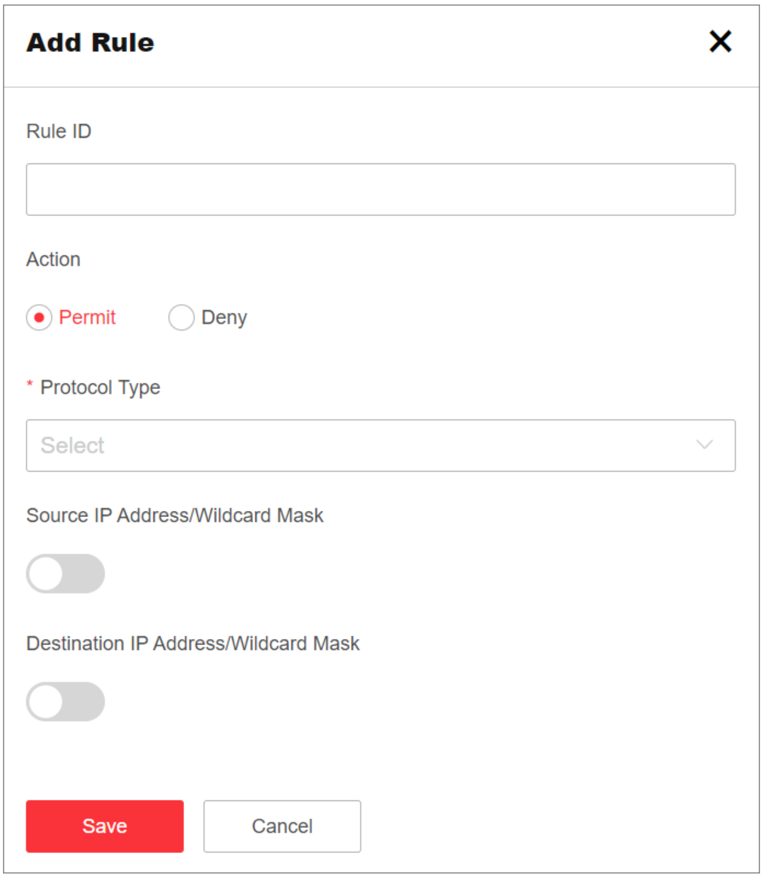
Matching Order

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**.



Add Rule

Rule ID

Action

● Permit ○ Deny

* Protocol Type

Select

Source IP Address/Wildcard Mask

Destination IP Address/Wildcard Mask

Figure 4-30 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.
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.

Parameter	Description
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.

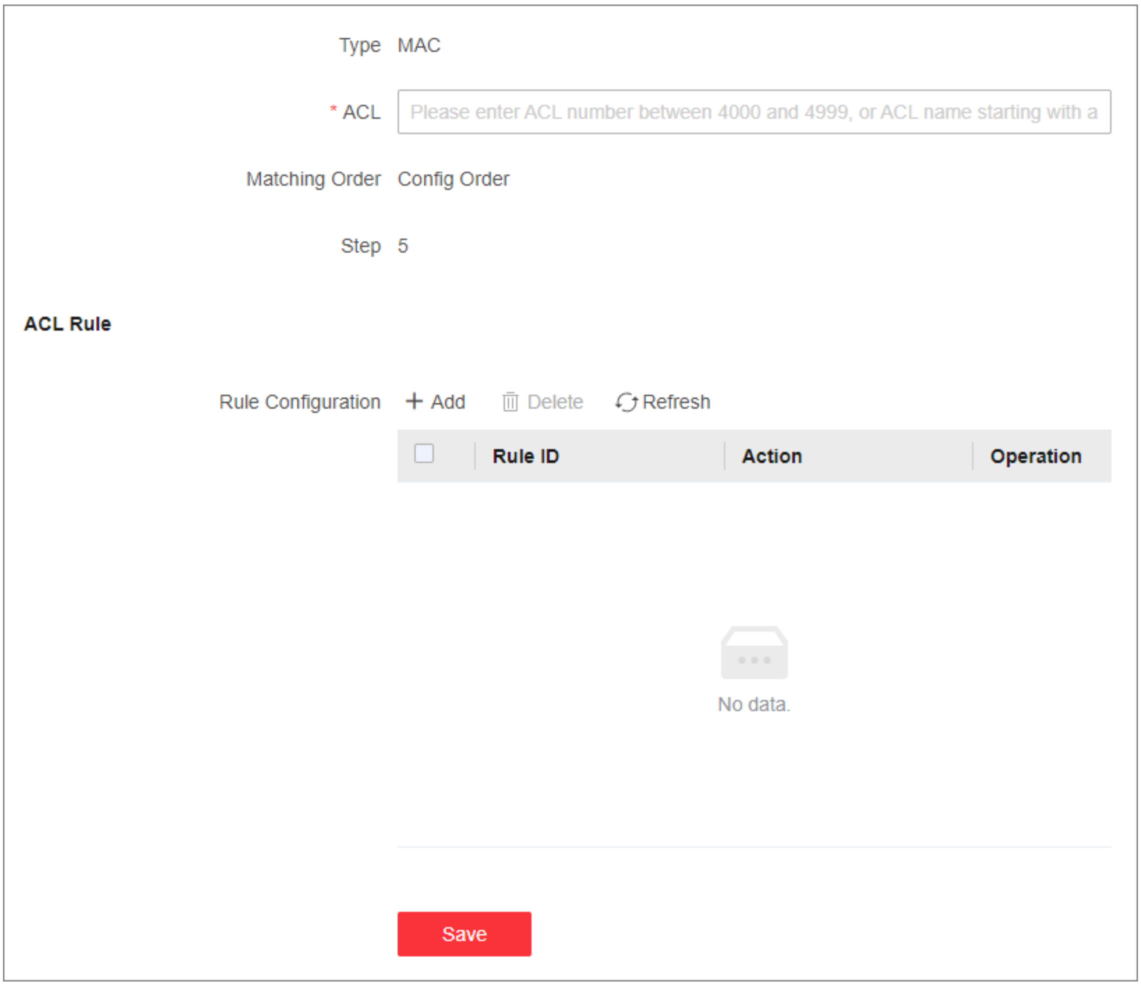
c. Click **Save**.

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**.



Type MAC

* ACL Please enter ACL number between 4000 and 4999, or ACL name starting with a

Matching Order Config Order

Step 5

ACL Rule

Rule Configuration + Add Delete Refresh

□	Rule ID	Action	Operation

No data.

Save

Figure 4-31 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

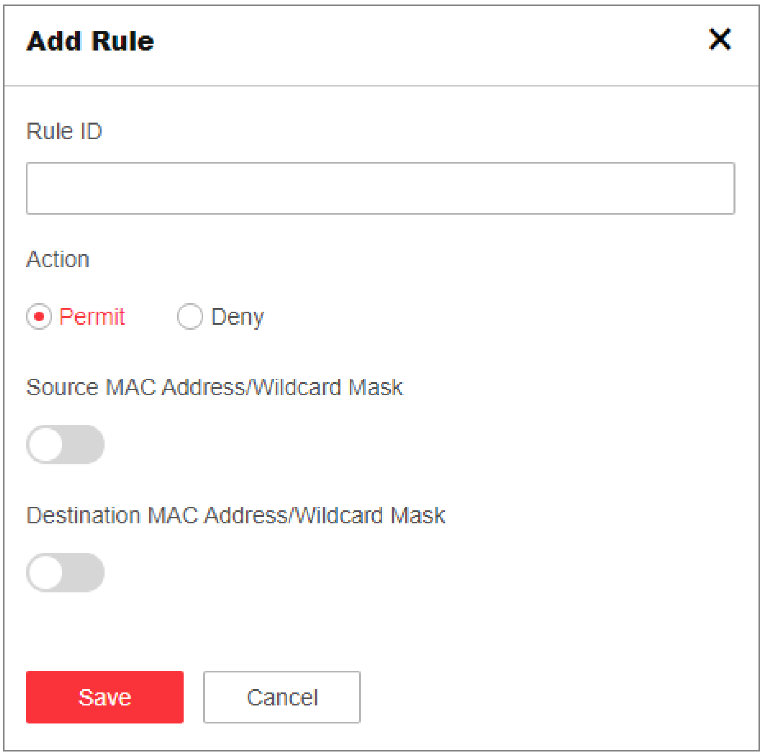
The matching order of ACL rules is **Config Order** by default, which is unconfigurable. The system matches packets against ACL rules in ascending order of rule IDs. The rule with the smallest ID is processed first.

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**.



Add Rule

Rule ID

Action

● Permit ○ Deny

Source MAC Address/Wildcard Mask

Destination MAC Address/Wildcard Mask

Figure 4-32 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**.

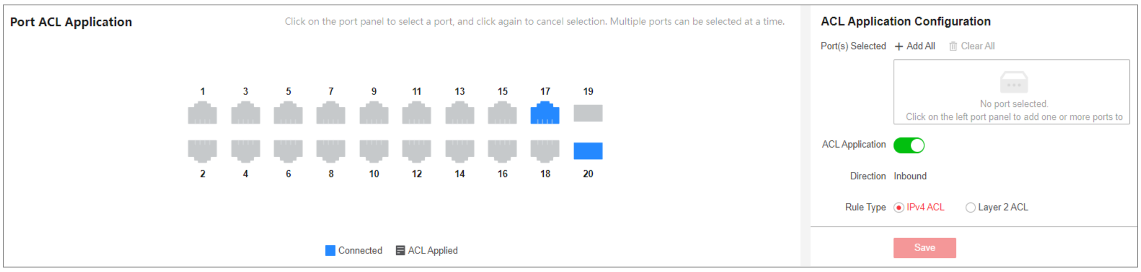
d. View, edit, or delete the configured ACL rule(s) in the ACL rule list.

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** .



Port ACL Application

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

ACL Application Configuration

Port(s) Selected

No port selected.
Click on the left port panel to add one or more ports to

ACL Application: on

Direction: Inbound

Rule Type: ● IPv4 ACL ○ Layer 2 ACL

Figure 4-33 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**.

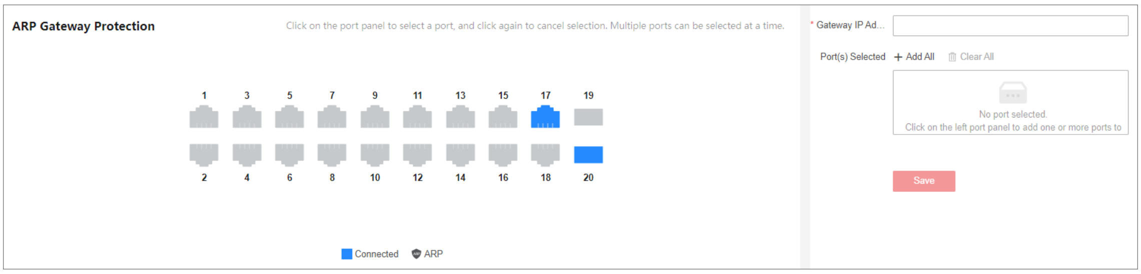
   The ports to which ACL rules have been applied are displayed on the port panel.
6. **Optional:** View details about the ports to which ACL rules have been applied in the **Port ACL Application Details** list.

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** .



ARP Gateway Protection

Click on the port panel to select a port, and click again to cancel selection. Multiple ports can be selected at a time.

No port selected.
Click on the left port panel to add one or more ports to

Figure 4-34 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**.

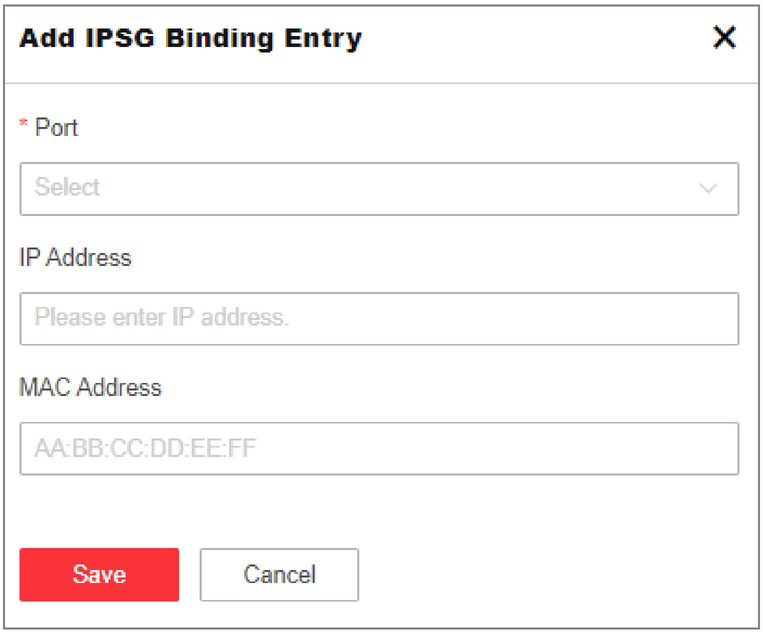
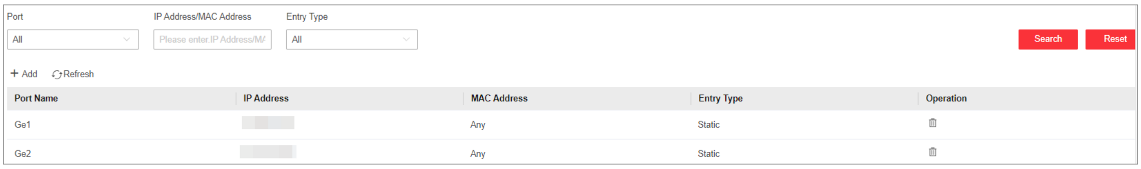


Figure 4-35 Add Static Binding Entry

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.



Port: All

IP Address/MAC Address: Please enter IP Address/M/

Entry Type: All

Search Reset

+ Add Refresh

Port Name	IP Address	MAC Address	Entry Type	Operation
Ge1	[redacted]	Any	Static	🗑
Ge2	[redacted]	Any	Static	🗑

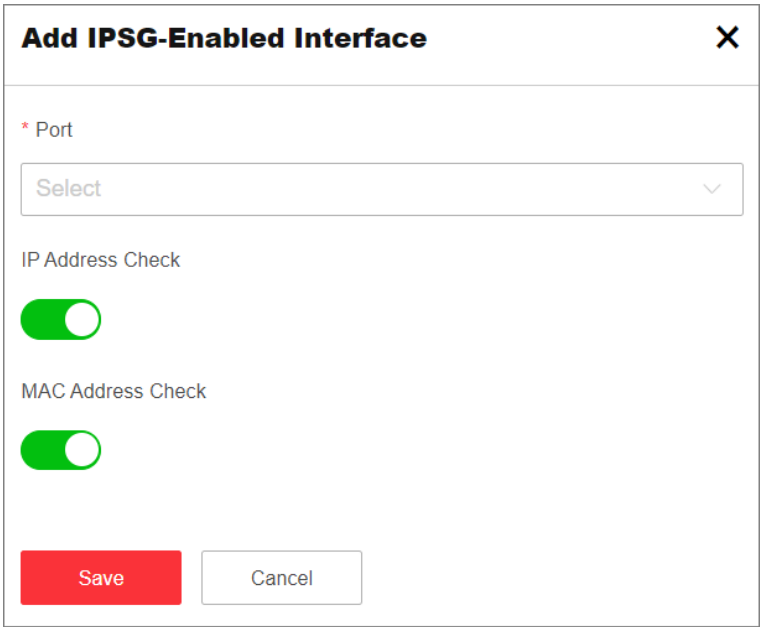
Figure 4-36 Search/Delete Binding Entry

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**.



Add IPSG-Enabled Interface

* Port

Select

IP Address Check

MAC Address Check

Figure 4-37 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.

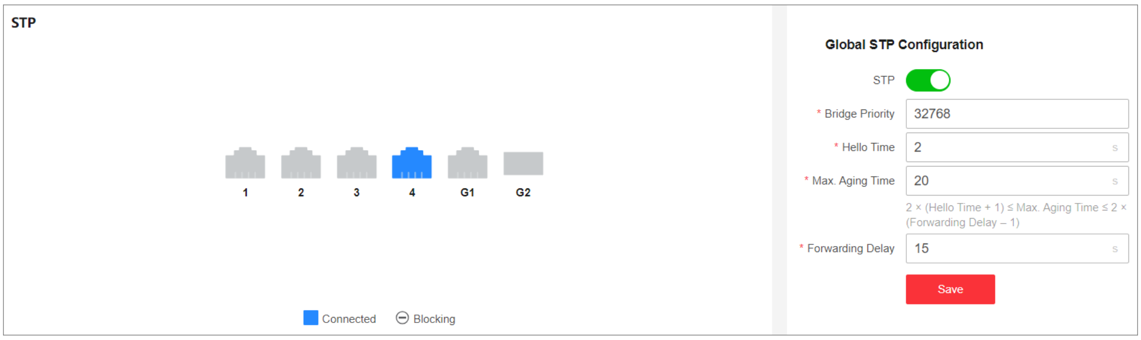
4.10 Loop Prevention Configuration

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** .



STP: enabled

* Bridge Priority: 32768

* Hello Time: 2 s

* Max. Aging Time: 20 s

2 × (Hello Time + 1) ≤ Max. Aging Time ≤ 2 × (Forwarding Delay – 1)

* Forwarding Delay: 15 s

Figure 4-38 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

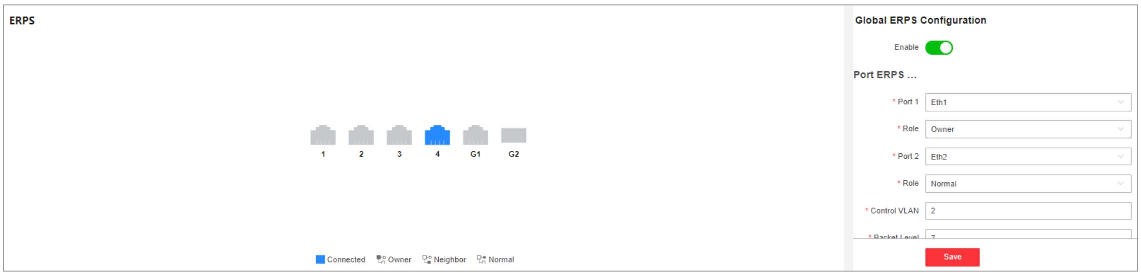
- The **Port Status** information includes the port name, path cost, port role, and port status.
- The **STP Status** information includes the bridge ID, root bridge ID, as well as hello time, Max. aging time, and forwarding delay of the root bridge.

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** .



Global ERPS Configuration

Enable: ●

Port ERPS ...

* Port 1: Eth1

* Role: Owner

* Port 2: Eth2

* Role: Normal

* Control VLAN: 2

* Packet Level: 7

Figure 4-39 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.

Parameter	Description
	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.

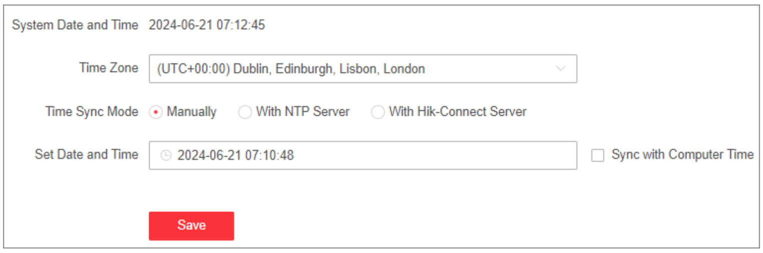
5. Click **Save**.
6. **Optional:** View the ERPS node status and port status in the **ERPS Status** list.

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.



System Date and Time 2024-06-21 07:12:45

Time Zone (UTC+00:00) Dublin, Edinburgh, Lisbon, London

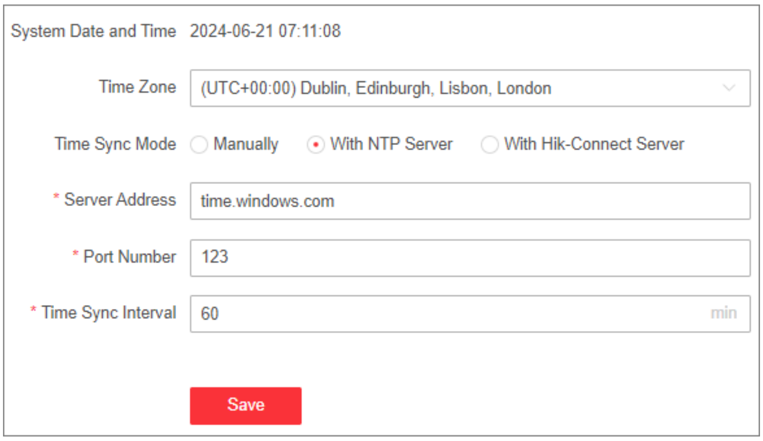
Time Sync Mode ● Manually ○ With NTP Server ○ With Hik-Connect Server

Set Date and Time 2024-06-21 07:10:48 □ Sync with Computer Time

Save

Figure 5-1 Configure Time Manually

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



System Date and Time 2024-06-21 07:11:08

Time Zone (UTC+00:00) Dublin, Edinburgh, Lisbon, London

Time Sync Mode ○ Manually ● With NTP Server ○ With Hik-Connect Server

* Server Address time.windows.com

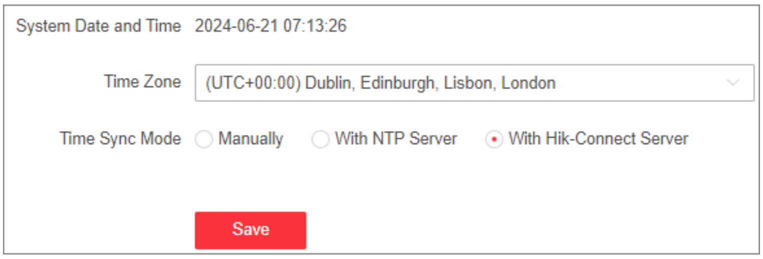
* Port Number 123

* Time Sync Interval 60 min

Save

Figure 5-2 Configure Time with NTP Server

   - **With Hik-Connect Server**: Use the Hik-Connect server for automatic time calibration and synchronization. You do not need to configure any parameters.



System Date and Time 2024-06-21 07:13:26

Time Zone (UTC+00:00) Dublin, Edinburgh, Lisbon, London

Time Sync Mode ○ Manually ○ With NTP Server ● With Hik-Connect Server

Figure 5-3 Configure Time with Hik-Connect Server

Note

Some device models do not support time synchronization with the NTP server. Please refer to the actual situation.

4. Click **Save**.

5.2 System Maintenance

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

Restart Device

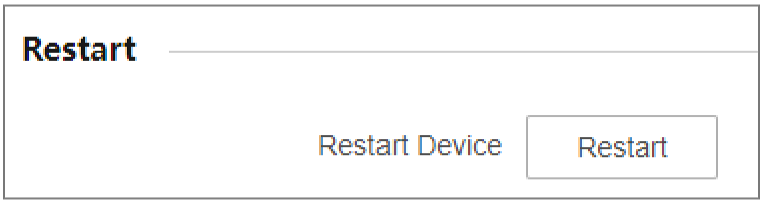


Figure 5-4 Restart

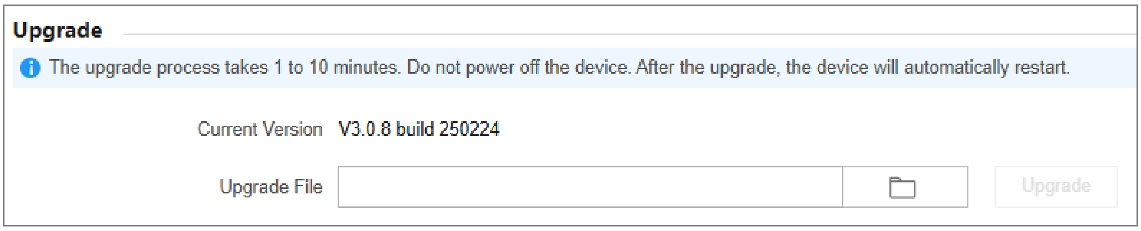
In **Restart**, click **Restart** to remotely restart the switch.

Note

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

Upgrade Device

Upload an upgrade file to manually upgrade the switch.



Upgrade

The upgrade process takes 1 to 10 minutes. Do not power off the device. After the upgrade, the device will automatically restart.

Current Version V3.0.8 build 250224

Upgrade File

Figure 5-5 Upgrade

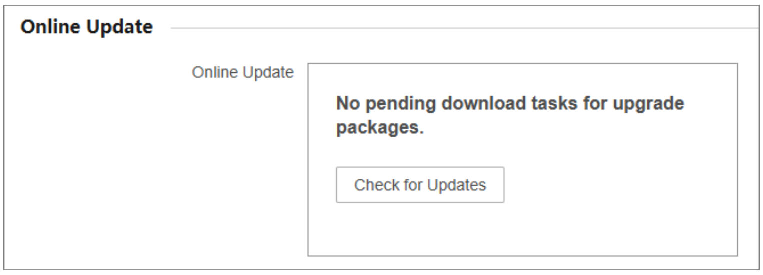
1. In **Upgrade**, click 🗀 to select an upgrade patch file.
2. Click **Upgrade**.

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.



Online Update

Online Update

No pending download tasks for upgrade packages.

Figure 5-6 Update Online

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

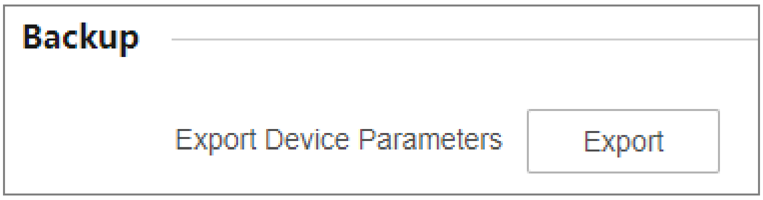
- If a new version is available, a message indicating upgrade to [version XXX] available will show. Follow the prompts to complete online firmware update.
- If the device already runs the latest version, a message indicating already the latest version will show. No online update is required.
- If the 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.



Backup

Export Device Parameters

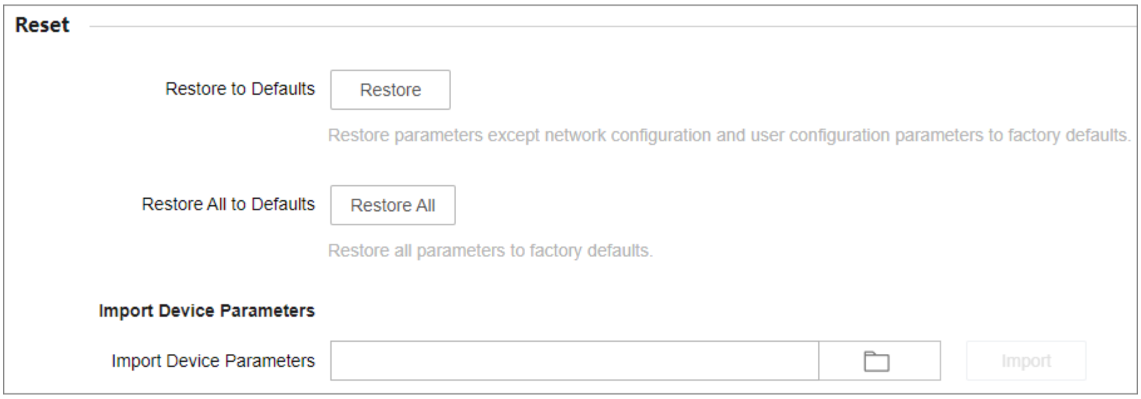
Figure 5-7 Back Up

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



Reset

Restore to Defaults

Restore parameters except network configuration and user configuration parameters to factory defaults.

Restore All to Defaults

Restore all parameters to factory defaults.

Import Device Parameters

Import Device Parameters

Figure 5-8 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.

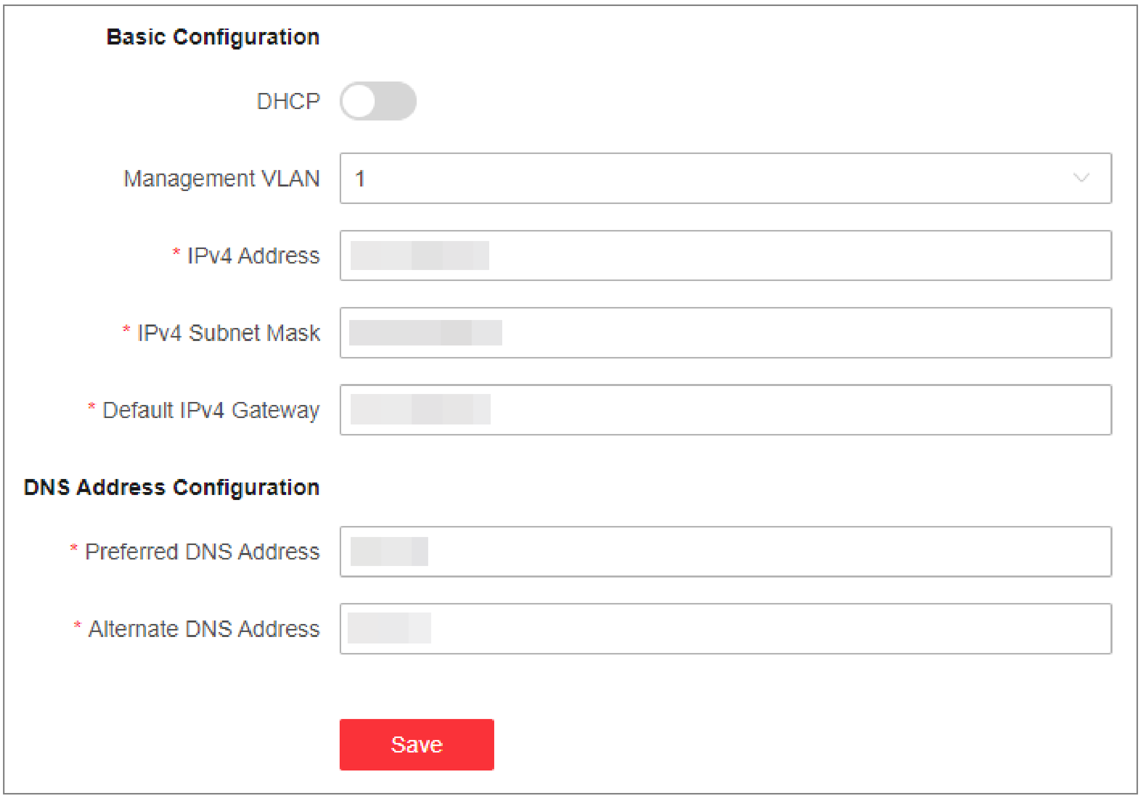
Note

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

5.3 Network Configuration

Network Configuration

1. Go to **System Management → Network Configuration → Network Configuration** .
2. Select a management VLAN, and set the 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.



Basic Configuration

DHCP: off

Management VLAN: 1

* IPv4 Address: [redacted]

* IPv4 Subnet Mask: [redacted]

* Default IPv4 Gateway: [redacted]

DNS Address Configuration

* Preferred DNS Address: [redacted]

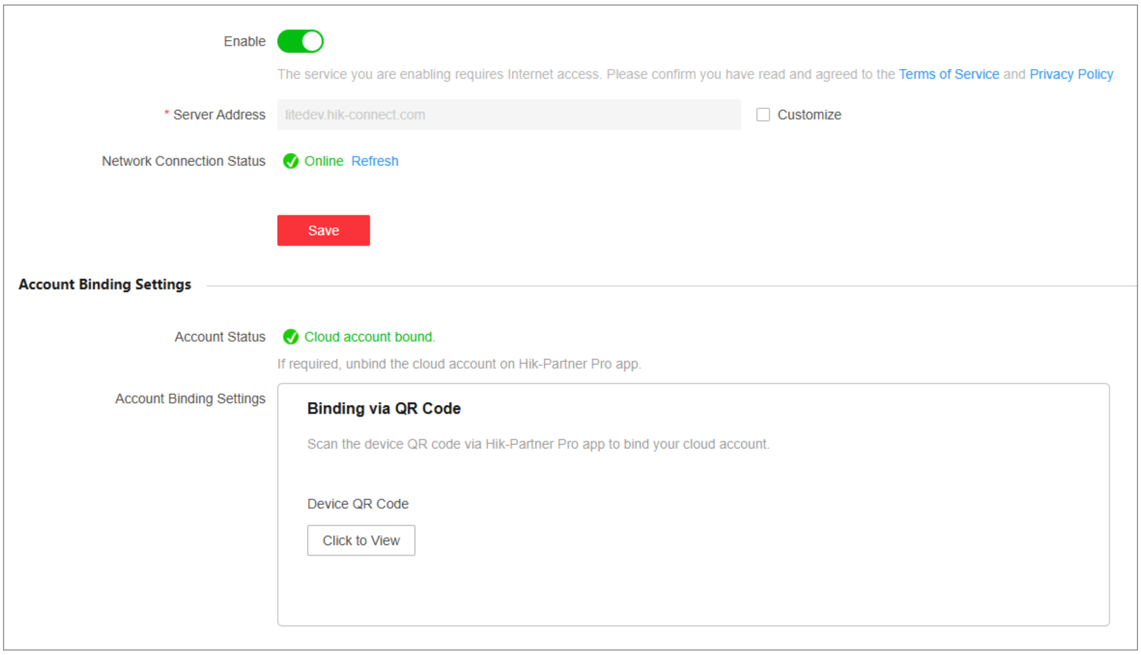
* Alternate DNS Address: [redacted]

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.



Enable ●

The service you are enabling requires Internet access. Please confirm you have read and agreed to the Terms of Service and Privacy Policy.

* Server Address: litedev.hik-connect.com □ Customize

Network Connection Status: ✓ Online Refresh

Save

Account Binding Settings

Account Status: ✓ Cloud account bound.

If required, unbind the cloud account on Hik-Partner Pro app.

Account Binding Settings

Binding via QR Code

Scan the device QR code via Hik-Partner Pro app to bind your cloud account.

Device QR Code

Click to View

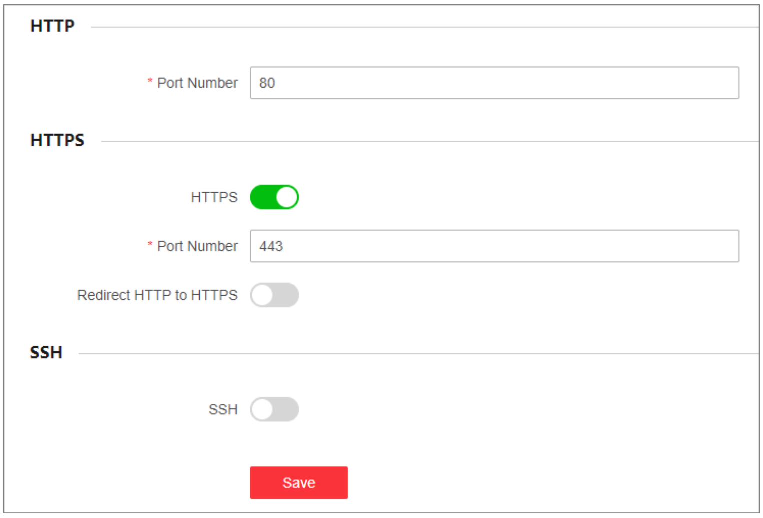
Figure 5-10 Configure Cloud Platform

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 or HTTPS.



HTTP

* Port Number: 80

HTTPS

HTTPS: ●

* Port Number: 443

Redirect HTTP to HTTPS: ○

SSH

SSH: ○

Save

Figure 5-11 Manage Device Remotely

- **HTTP**: Set **Port Number** and click **Save**.

  Note

  The HTTP port number should be an integer between 2000 and 65535, or 80 by default.

- **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

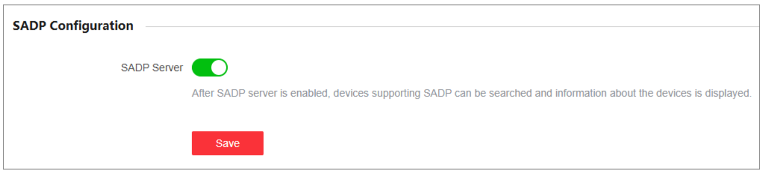
  Enable or disable **Redirect HTTP to HTTPS**.

  Note

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

- **SSH**: SSH is used for fault locating by technical support, and is not available to users.

SADP Configuration



SADP Configuration

SADP Server

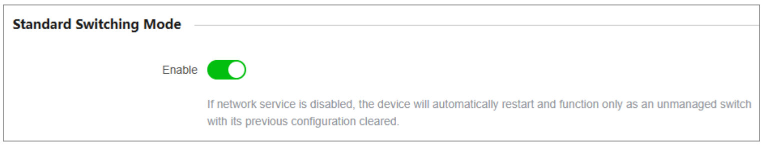
After SADP server is enabled, devices supporting SADP can be searched and information about the devices is displayed.

Figure 5-12 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.



Standard Switching Mode

Enable ●

If network service is disabled, the device will automatically restart and function only as an unmanaged switch with its previous configuration cleared.

Figure 5-13 Configure Network Service

Note

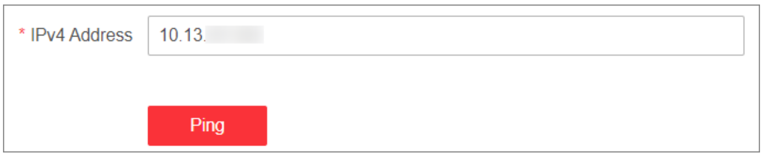
An unmanaged switch is also referred to as a plug-and-play switch. As the name "plug-and-play" implies, it requires minimal configuration. Users can simply connect the network cables from different devices to the ports of the switch, and it will automatically start working. There is no need for complex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

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** .



* IPv4 Address: 10.13.[redacted]

Figure 5-14 Ping

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

Note

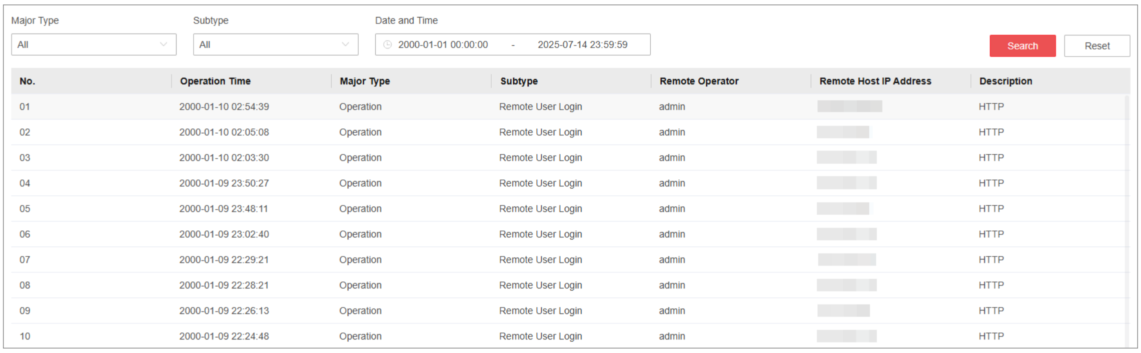
The network diagnosis result is displayed in the **Ping Result** area.

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

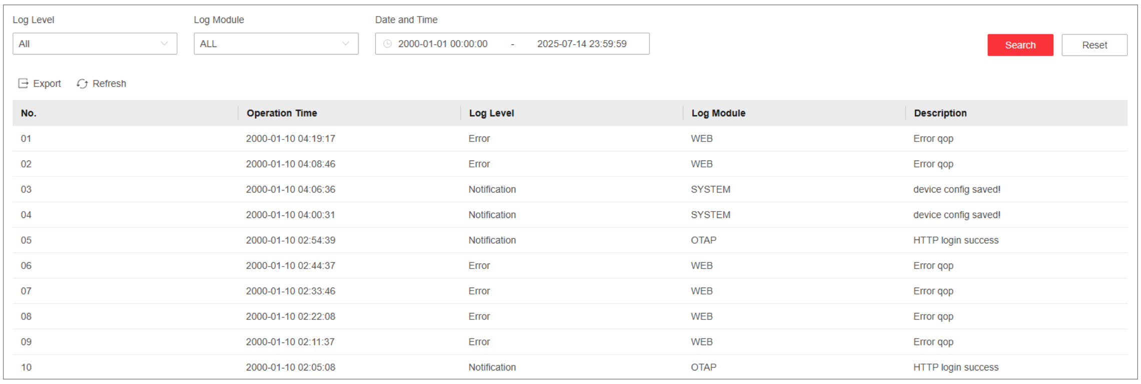
1. Go to **System Management → System Maintenance → Security Audit Log** or **System Management → System Maintenance → Device Operation Log** .



Major Type: All
Subtype: All
Date and Time: 2000-01-01 00:00:00 - 2025-07-14 23:59:59

No.	Operation Time	Major Type	Subtype	Remote Operator	Remote Host IP Address	Description
01	2000-01-10 02:54:39	Operation	Remote User Login	admin	[redacted]	HTTP
02	2000-01-10 02:05:08	Operation	Remote User Login	admin	[redacted]	HTTP
03	2000-01-10 02:03:30	Operation	Remote User Login	admin	[redacted]	HTTP
04	2000-01-09 23:50:27	Operation	Remote User Login	admin	[redacted]	HTTP
05	2000-01-09 23:48:11	Operation	Remote User Login	admin	[redacted]	HTTP
06	2000-01-09 23:02:40	Operation	Remote User Login	admin	[redacted]	HTTP
07	2000-01-09 22:29:21	Operation	Remote User Login	admin	[redacted]	HTTP
08	2000-01-09 22:28:21	Operation	Remote User Login	admin	[redacted]	HTTP
09	2000-01-09 22:26:13	Operation	Remote User Login	admin	[redacted]	HTTP
10	2000-01-09 22:24:48	Operation	Remote User Login	admin	[redacted]	HTTP

Figure 5-15 Manage Security Audit Logs (Only for Admin Users)



Log Level: All
Log Module: ALL
Date and Time: 2000-01-01 00:00:00 - 2025-07-14 23:59:59

No.	Operation Time	Log Level	Log Module	Description
01	2000-01-10 04:19:17	Error	WEB	Error qop
02	2000-01-10 04:08:46	Error	WEB	Error qop
03	2000-01-10 04:06:36	Notification	SYSTEM	device config saved!
04	2000-01-10 04:00:31	Notification	SYSTEM	device config saved!
05	2000-01-10 02:54:39	Notification	OTAP	HTTP login success
06	2000-01-10 02:44:37	Error	WEB	Error qop
07	2000-01-10 02:33:46	Error	WEB	Error qop
08	2000-01-10 02:22:08	Error	WEB	Error qop
09	2000-01-10 02:11:37	Error	WEB	Error qop
10	2000-01-10 02:05:08	Notification	OTAP	HTTP login success

Figure 5-16 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

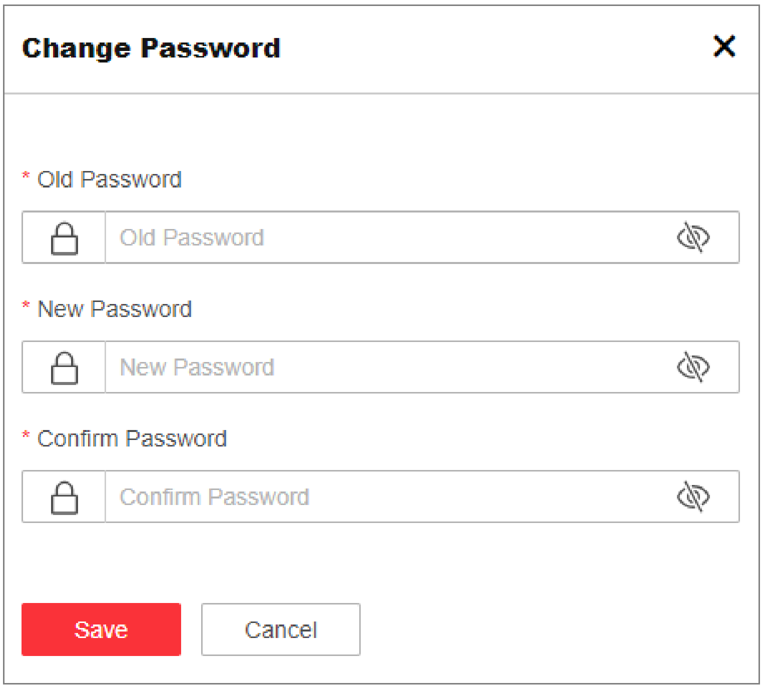
Device operation logs can be exported as a TXT file. A prompt will pop up after logs are exported successfully.

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.



Change Password

* Old Password

Old Password

* New Password

New Password

* Confirm Password

Confirm Password

Figure 5-17 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.

3. Click **Save**.

See Far, Go Further