



Switch Web

User Manual

Legal Information

©2022 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (<https://www.hikvision.com/>)company website.

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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.

Trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISIONOUR COMPANY 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 HIKVISIONOUR COMPANY 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 HIKVISIONOUR COMPANY 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 HIKVISIONOUR COMPANY 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, HIKVISIONOUR COMPANY 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 MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Preface

Applicable Models

This manual is applicable to switches.

About the Default

- Default administrator account: admin.
- Default IP address: 192.168.1.64.

Contents

Chapter 1 Product Introduction	1
Chapter 2 Activation and Login	2
Chapter 3 Device Management	4
Chapter 4 Network Configuration	7
Chapter 5 Switch Configuration	9
5.1 Port Configuration	9
5.1.1 Configure Property	9
5.1.2 Configure Port Mirroring	10
5.1.3 Configure Port Rate-Limiting	11
5.1.4 Configure Long-Range Mode	11
5.1.5 Configure Storm Control	12
5.1.6 Configure Port Isolation	13
5.2 Configure Link Aggregation	14
5.3 VLAN Configuration	15
5.3.1 Add a VLAN	15
5.3.2 Configure a Port	16
5.4 Configure QoS	17
5.5 Configure LLDP	18
5.6 SNMP Configuration	20
5.6.1 Configure SNMP Proxy	20
5.6.2 SNMP Trap Settings	20
5.7 STP Configuration	21
5.7.1 Global Configuration	21
5.7.2 Configure STP Port	23
5.7.3 STP Status View	24
5.8 PoE Management	24

Chapter 6 System Management	26
6.1 Synchronize the Time	26
6.2 Device Operation	27
6.3 Configure File Export	27
6.4 Configure File Import	28
6.5 Upgrade the Device	28
6.6 Manage Logs	29
6.7 Diagnose the Network	29
6.8 Manage Users	30
6.9 Security Management	30

Chapter 1 Product Introduction

With multiple ports, the layer 2 switch (hereinafter referred to as "the device") is reliable and easy to install and maintain, providing advanced data exchanging on the basis of high-performance access. Through web or client, the switch supports status checking, port management, layer 2 configuration, and other functions. It is suitable for small-scale LAN device access.



Note

The specific functions vary with different models. If there are differences between the figures shown in this manual and your device, the latter prevails.

Chapter 2 Activation and Login

For the first time usage, you must activate the switch and configure the password.

Before You Start

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

Steps



All figures in this manual are for illustration purpose only.

1. Enter the default IP **192.168.1.64** in the browser address bar.

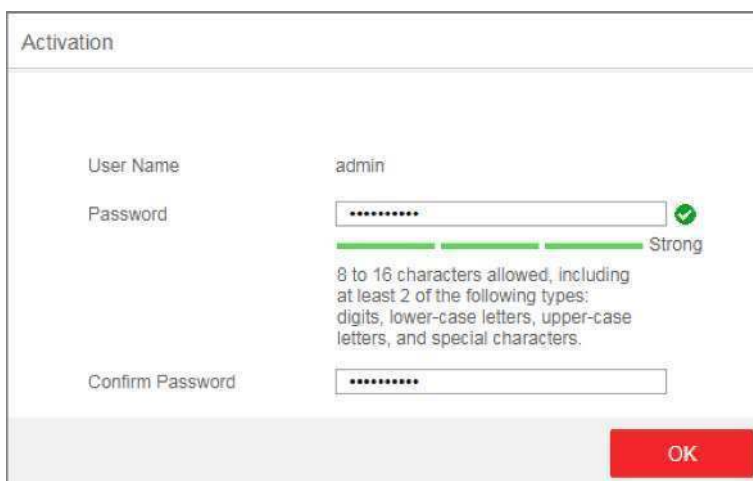


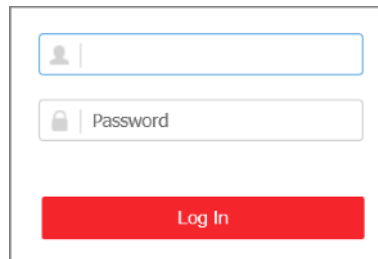
Figure 2-1 Activation



You are recommended to use the newest version of the following browsers: IE 10+, Edge, and Chrome 31+.

2. Configure the password and confirm it.
3. Click **OK**.

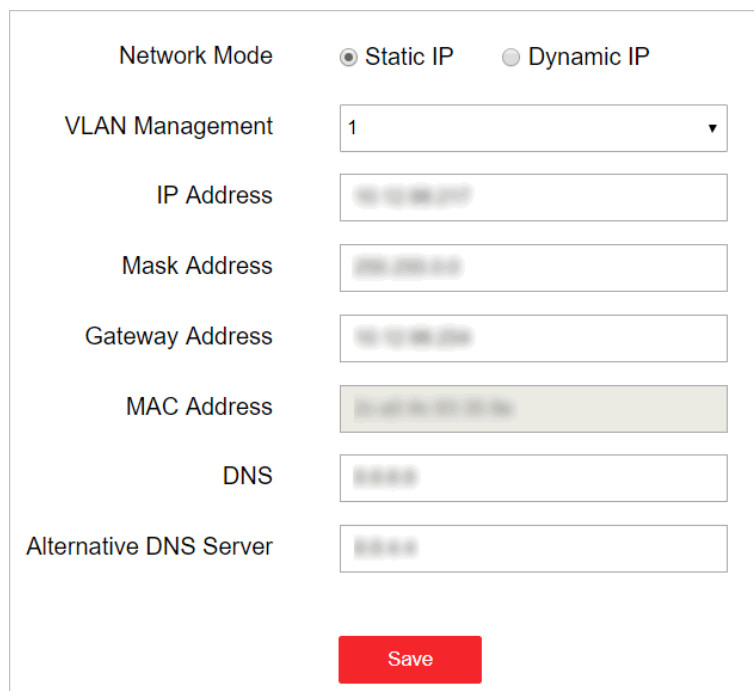
Go to the login page.



A login form with two input fields. The first field is labeled 'User Name' and contains a user icon. The second field is labeled 'Password' and contains a lock icon. Below the fields is a red button labeled 'Log In'.

Figure 2-2 Login

4. Enter the **User Name** and **Password**, and click **Log In**.
5. **Optional:** Change the network configuration.
 - 1) Go to **System Management** → **Network Configuration** → **Basic Config** .



A network configuration form. At the top, there are two radio buttons for 'Network Mode': 'Static IP' (selected) and 'Dynamic IP'. Below this are several input fields: 'VLAN Management' (a dropdown menu showing '1'), 'IP Address' (a text field with a placeholder), 'Mask Address' (a text field with a placeholder), 'Gateway Address' (a text field with a placeholder), 'MAC Address' (a text field with a placeholder), 'DNS' (a text field with a placeholder), and 'Alternative DNS Server' (a text field with a placeholder). At the bottom is a red button labeled 'Save'.

Figure 2-3 Network Configuration

- 2) Change the IP address, mask address, the gateway address, DNS and alternative DNS as needed. You can log in to the switch with the new IP address next time.

 Note

You are recommended to change the network configuration to better manage the switch.

Chapter 3 Device Management

After logging in to the device, you can go to **Device Status** to view the device status, including the device information, working status, port status, port statistics, and PoE status.

Device Information

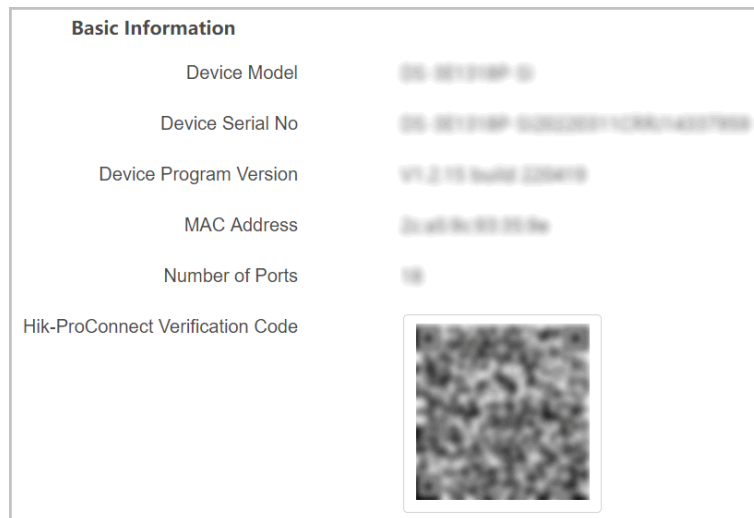


Figure 3-1 Device Information

Working Status

View the working status, including device running time, memory usage, and CPU usage.

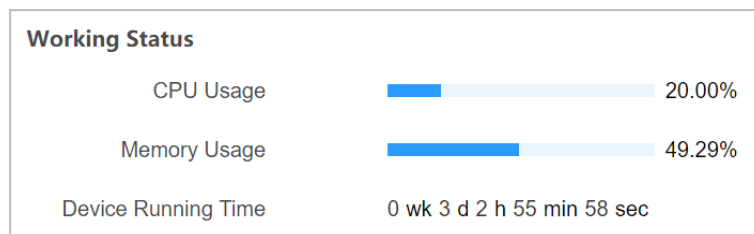


Figure 3-2 Working Status

Port Status

Port Name	Connection Status	Rate	Duplex	Flow Control	Operation
Eth1	Disconnected	-	-	-	⚙️
Eth2	Disconnected	-	-	-	⚙️
Eth3	Disconnected	-	-	-	⚙️
Eth4	Disconnected	-	-	-	⚙️
Eth5	Disconnected	-	-	-	⚙️
Eth6	Connected	100M	Full-Duplex	On	⚙️
Eth7	Disconnected	-	-	-	⚙️
Eth8	Disconnected	-	-	-	⚙️

Figure 3-3 Port Status

View the connection status, rate, duplex, and flow control of all ports.

Port Statistics

Retreshing Rate 30 sec		<button>Reset</button> <button>Refresh</button>						
Port	Number of Bytes Sent	Number of Packets Sent	Sending Rate	Number of Bytes Received	Number of Packets Received	Receiving Rate	Sending Peak Rate	Receiving Peak Rate
Eth1								
Eth2								
Eth3								
Eth4								
Eth5								
Eth6	46,710,709	62,149	17.2Kbps	1,700,972,247	1,991,010	2.7Mbps	9.0Mbps	4.5Mbps
Eth7								
Eth8								

Figure 3-4 Port Statistics

- **Refreshing Rate:** 10 sec, 30 sec, 60 sec, and **Manually Refresh** is available.
- **Refresh:** When you choose **Manually Refresh**, you can click **Refresh** to refresh the statistics.
- **Reset:** You can click **Reset** to clear all the statistics.

PoE Status

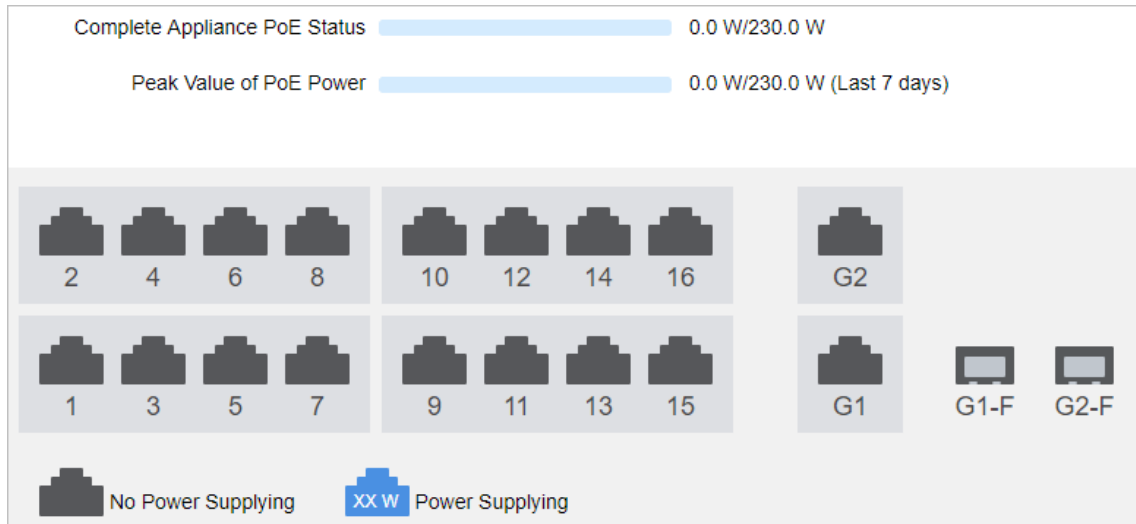


Figure 3-5 PoE Status

View the complete appliance PoE status and the output power of each PoE port.

Chapter 4 Network Configuration

You can click **Cloud Management** on the home page to check Hik-Connect status. Go to **System Management → Network Configuration**, configure the basic parameters of the device, or perform trouble shooting for offline problems.

Cloud Management

Click **Cloud Management** to check device status and detection information, and click **Configure** to set related parameters.

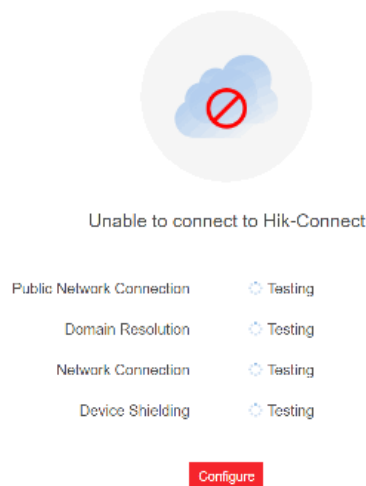


Figure 4-1 Cloud Management

Basic Configuration

Go to **System Management → Network Configuration → Basic Config**, and configure the parameters.

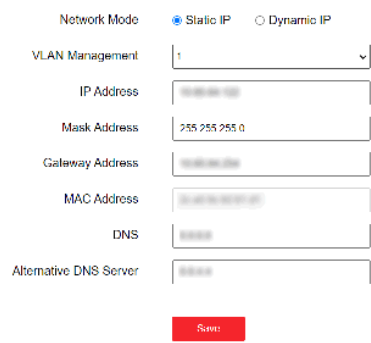
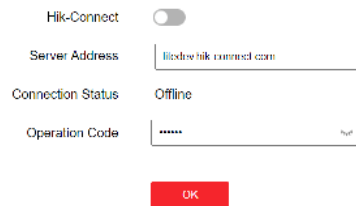


Figure 4-2 Basic Configuration

Hik-Connect Configuration

If "Device Offline" is prompted when you add the device to Hik-ProConnect, you should edit the DNS server address and configure Hik-Connect parameters.

Go to **System Management** → **Network Configuration** → **Hik-Connect Config**, ensure **Hik-Connect** is enabled. You can also check the operation code.



Hik-Connect	☒
Server Address	112.125.81.100:8080
Connection Status	Offline
Operation Code	***** 
OK	

Figure 4-3 Hik-Connect Configuration



Note

It takes a while for reconnecting to Hik-Connect service.

Chapter 5 Switch Configuration

5.1 Port Configuration

5.1.1 Configure Property

The basic parameters can influence the working status of ports. Configure the parameters according to the actual situation.

Steps

1. Go to **Switch Configuration** → **Basic Configuration** → **Property Configuration** .

Port Name	Rate	Duplex	Flow Control	Switch
Plh1	Auto Negotiation	Auto Negotiation	On	On
Plh2	Auto Negotiation	Auto Negotiation	On	On
Plh3	Auto Negotiation	Auto Negotiation	On	On

Figure 5-1 Configure Port Property

2. Select desired port(s) and configure the parameters.

Switch

Enable or disable the port. No data will be transmitted if the port is disabled.

Rate

The speed of data transmission of the port.

Duplex

The duplex mode of the port.

- RJ45 port: **Auto Negotiation** is set by default and cannot be edited.
- SFP fiber optical port: **Auto Negotiation** is set by default. You can also set it as **Full-Duplex**.

Flow Control

Enabling the flow control can prevent data loss in data transmission.

3. Click **OK** to save.

4. **Optional:** Check port properties in **Port Property Configuration List**.

5.1.2 Configure Port Mirroring

Port mirroring monitors network traffic by sending copies of incoming and outgoing packets from the source port to the target port(s).

Steps

1. Go to **Switch Configuration** → **Basic Configuration** → **Port Mirroring**.

Port Mirroring

Normal Port Selected Port

Tips: Select multiple ports at one time for batch configuration.

Port Mirroring: Off Mirror Port: None Mirror Direction: [Dropdown]

OK

Port Name	Port Mirroring	Mirror Direction
Ph1	Off	
Ph2	Off	
Ph3	Off	

Figure 5-2 Configure Port Mirroring

2. Select the desired port(s) as target port(s) to monitor network traffic of the source port, and configure the parameters.

Port Mirroring

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

Mirror Port

Only one port can be set as the mirror port (the source port).

Mirror Direction

Inbound

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

Outbound

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

Inbound and Outbound

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



Note

- If **Port Mirroring** is enabled, at least one port should be selected as the target port.
- If **Mirror Port** is set as **None**, **Port Mirroring** should be disabled.

3. Click **OK** to save.

4. **Optional:** Check mirroring status of different ports in **Port Mirroring List**.

5.1.3 Configure Port Rate-Limiting

Port rate-limiting refers to the limitation of the sending rate and receiving rate of each port. This function is only applicable to Gigabit switches.

Steps

1. Go to **Switch Configuration** → **Basic Configuration** → **Port Rate-Limiting**.

Port Rate-Limiting

Normal Port Selected Port

Tips: Select multiple ports at one time for batch configuration.

Send Limit Rate Control On Receive Limit Rate Control On

Upper Limit of Sending Rate Limit 1000 Mbps Upper Limit of Receiving Rate Limit 1000 Mbps

Port Rate-Limiting List

Port Name	Sending Rate-Limiting	Upper Limit of Sending Rate Value(...)	Receiving Rate-Limiting	Upper Limit of Receiving Rate Value...
Gc1	Off	1000	Off	1000

Figure 5-3 Configure Port Rate-Limiting

2. Select desired port(s), and configure the parameters.

Send Limit Rate Control

Enable or disable sending rate limit of the selected port(s).

Upper Limit of Sending Rate Limit

Set the upper limit of sending rate.

Receive Limit Rate Control

Enable or disable sending rate limit of the selected port(s).

Upper Limit of Receiving Rate Limit

Set the upper limit of receiving rate.

3. Click **OK** to save.

You can check rate limiting information of different ports in **Port Rate-Limiting List**.

5.1.4 Configure Long-Range Mode

When long-range mode is enabled, the transmission distance of the port can reach 300 meters, and the rate is 10 Mbps.

Steps

1. Go to **Switch Configuration → Basic Configuration → Long-Range Mode** .

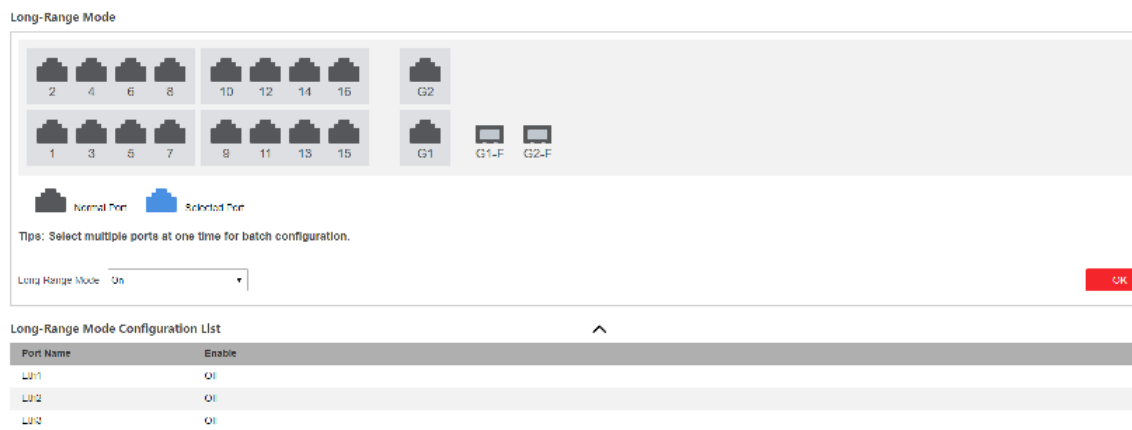


Figure 5-4 Configure Long-Range Mode

2. Select the desired port(s), and enable or disable **Long-Range Mode**.
3. Click **OK** to save.
4. **Optional:** Check long range status of different ports in **Long-Range Mode Configuration List**.

5.1.5 Configure Storm Control

Storm control prevents the ports from being disrupted by a broadcast storm. Both errors in the protocol-stack implementation and mistakes in network configuration can cause a storm. The storm congests the network and degrades the network performance. This function is only applicable to Gigabit switches.

Steps

1. Go to **Switch Configuration → Basic Configuration → Storm Control** .

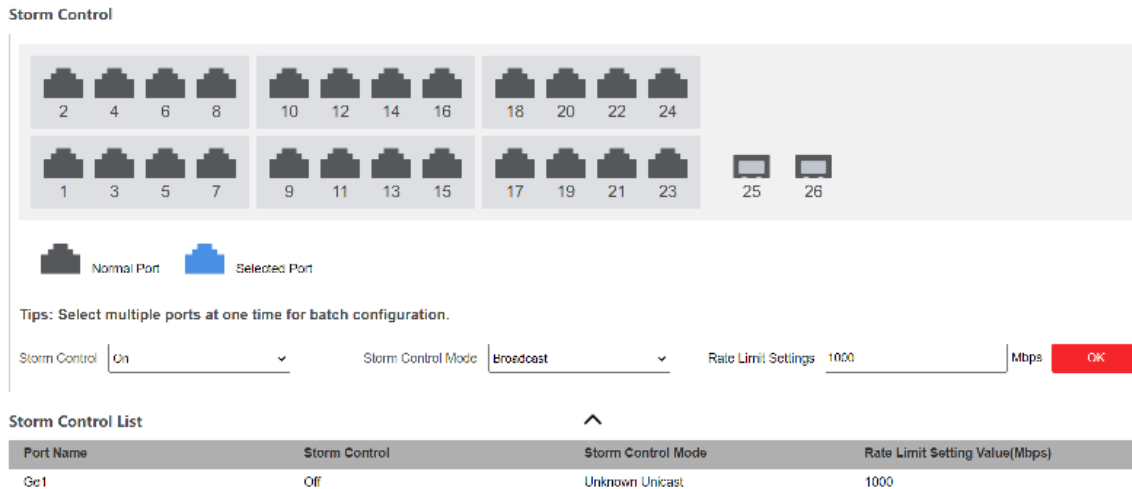


Figure 5-5 Storm Control

2. Select the desired port(s), and configure the parameters.

Storm Control

Enable or disable storm control of the selected port(s).

Storm Control Mode

Broadcast

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

Multicast

The data packets are sent to the specified devices.

Unknown Unicast

The data packets are sent to the specified device.

Rate Limit Settings

Set the rate limit of the selected port(s).

3. Click **OK** to save.

5.1.6 Configure Port Isolation

Add multiple ports to a isolation group, and ports in the same isolation group cannot communicate with each other.

Steps

1. Go to **Switch Configuration → Basic Configuration → Port Isolation** .

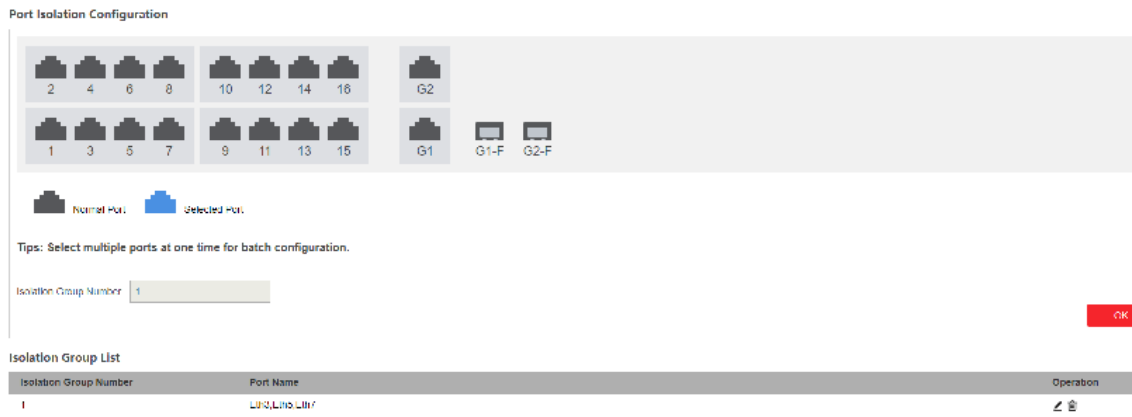


Figure 5-6 Configure Port Isolation

2. Select the desired ports.
3. Click **OK** to add the selected port into a isolation group.
4. **Optional:** Edit the isolation group.
 - 1) Click of the desired isolation group.
 - 2) Select or deselect the desired port(s) to add to or delete from the group.
 - 3) Click **OK** to save.
5. **Optional:** Click to delete the isolation group.

5.2 Configure Link Aggregation

Link aggregation is used to aggregate physical ports to create a logical channel. Link aggregation provides higher transmission speed and wider bandwidth.

Steps

1. Go to **Switch Configuration → Basic Configuration → Link Aggregation**.



Figure 5-7 Configure Link Aggregation

Load Balancing Mode

Source and Destination MAC is set by default.

2. Select the desired ports to add.

Note

- Only the selectable ports can be added.
- This function is not applicable to all combos. Please refer to the actual conditions.
- 2 to 4 ports are allowed for each link aggregation group:
- Ports in the same aggregation group should be configured as the same value, including rate, duplex, flow control, VLAN, and long-range.

3. Set **Aggregation Group Number**, and click **OK**.

Note

The numbers of aggregation group depends on the actual conditions of the mode.

4. **Optional:** Edit the aggregation group.
 - 1) Click  of the desired isolation group.
 - 2) Select or deselect the desired port(s) to add to or delete from the group.
 - 3) Click **OK** to save.
5. **Optional:** Click  to delete the aggregation group.

5.3 VLAN Configuration

A Virtual Local Area Network (VLAN) is a group of devices located on different LAN segments, and they are configured to communicate as if they were attached to the same wire. LANs are based on logical connections instead of physical connections, which is flexible for device connection.

5.3.1 Add a VLAN

Steps

1. Go to **Switch Configuration → Basic Configuration → VLAN → 802.1Q VLAN**.
2. Click **Add**.

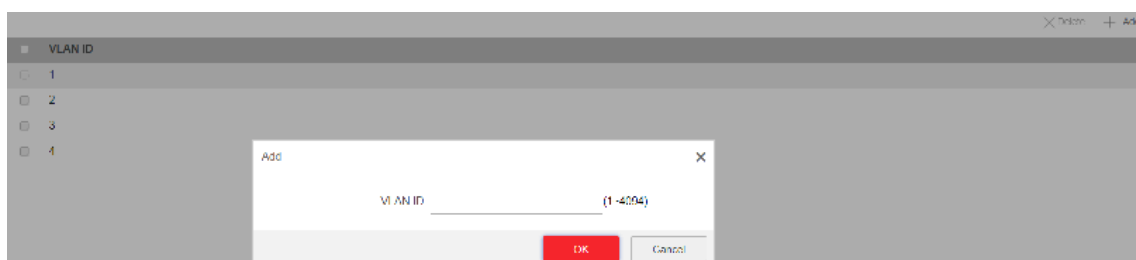


Figure 5-8 Add a VLAN

3. Enter a VLAN ID.



Note

- A maximum of 128 VLANs are supported.
- The range is from 1 to 4094.

4. Click **OK** to save.

5. **Optional:** You can also delete a VLAN by clicking **Delete**.



Note

You cannot delete the VLAN 1, because VLAN 1 is the Management VLAN.

5.3.2 Configure a Port

Steps

1. Select a port to configure on the **Port Configuration** page.



Port Name	VLAN Type	PVID	Accessible VLAN
Eth1	TRUNK	2	2 1
Eth2	ACCESS	3	3
Eth3	ACCESS	1	1
Eth4	ACCESS	1	1

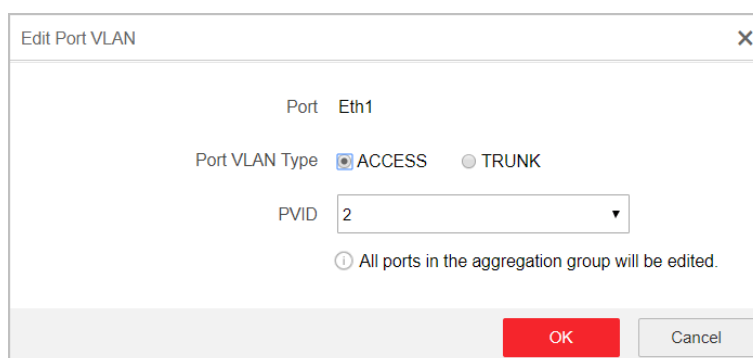
Figure 5-9 Configure a Port

2. Click **Edit**.

3. Configure the port VLAN.

- Access Port

- An access port transports traffic to and from only the specified VLAN, usually the default VLAN, VLAN 1.
- Select **Port VLAN Type** as **ACCESS**, and select the **PVID**.



Port Eth1

Port VLAN Type ☒ ACCESS ☐ TRUNK

PVID

① All ports in the aggregation group will be edited.

OK Cancel

Figure 5-10 Edit an Access Port VLAN



Note

All ports in the same aggregation group will be edited automatically at the same time.

- Trunk Port

- A trunk port is a port that is assigned to carry traffic for all the VLANs.
- Select **Port VLAN Type** as **TRUNK**, select the **PVID**, and enter the **VLAN** that are allowed to be accessed.

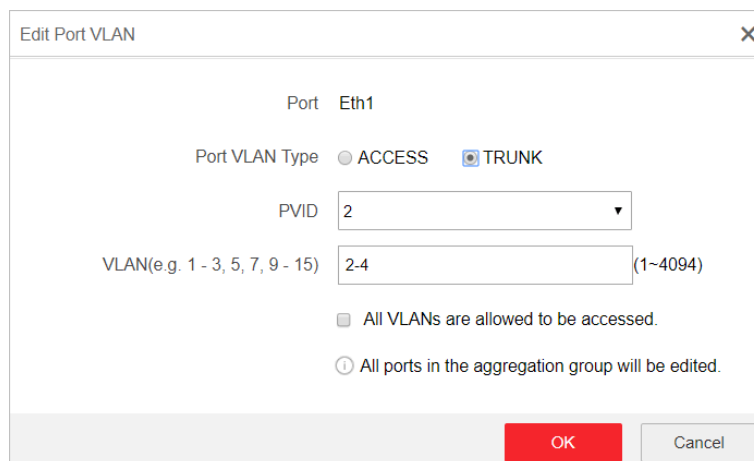


Figure 5-11 Edit a Trunk Port VLAN

Note

- All ports in the same aggregation group will be edited automatically at the same time.
- You can check **All VLANs are allowed to be accessed.** to assign the port to all the VLANs.

4. Click **OK**.

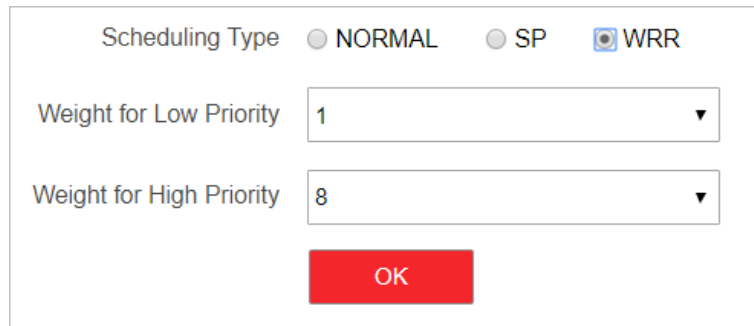
5. Click **OK** to save.

5.4 Configure QoS

Quality of Service (QoS) includes the transmission bandwidth, delay, packet loss rate and etc. Increasing network bandwidth, decreasing network delay, and reducing packet losses can improve QoS in network service. You can configure the scheduling mode and port priority of QoS.

Steps

1. Go to **Switch Configuration → Basic Configuration → QoS → Scheduling Mode** to select a scheduling type.



The figure shows a configuration window for Scheduling Type. It has three radio buttons: NORMAL, SP, and WRR. WRR is selected. Below the radio buttons are two dropdown menus: 'Weight for Low Priority' with the value '1' and 'Weight for High Priority' with the value '8'. At the bottom is a red 'OK' button.

Figure 5-12 Scheduling Mode

NORMAL

First In First Out (FIFO) mode. Transmit the message coming in first. QoS is not enabled.

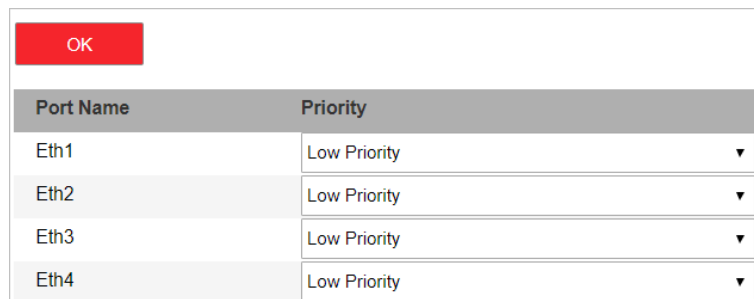
SP

Strict Priority mode. Transmit the message according to the actual priority configuration.

WRR

Weighted Round Robin mode. Transmit the message according to the respective weight for low priority and high priority.

2. Configure the port priority in **Port Priority**.



The figure shows a configuration window for Port Priority. It has a red 'OK' button at the top left. Below it is a table with two columns: 'Port Name' and 'Priority'.

Port Name	Priority
Eth1	Low Priority ▼
Eth2	Low Priority ▼
Eth3	Low Priority ▼
Eth4	Low Priority ▼

Figure 5-13 Port Priority

3. Click **OK** to save.

5.5 Configure LLDP

Link Layer Discovery Protocol (LLDP) is type of data link layer protocol defined by IEEE Std 802.1AB standard. Network devices can send link layer discovery protocol data units (LLDPDU) to inform other devices of their status within the same LAN. It can help to recognize system topology and detect the improper configuration in a LAN.

Go to **Switch Configuration → L2 Configuration → LLDP Configuration** .

Basic Settings

Enabling LLDP makes the device discoverable.

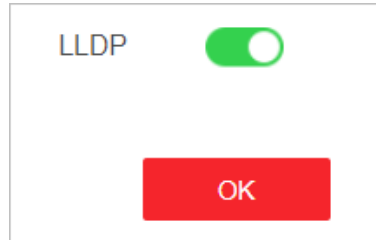


Figure 5-14 Basic Settings

LLDP Port Settings

Configure the port to send or receive LLDP messages.

- If **Send LLDP Message** is enabled, the port can be discovered by the peer device.
- If **Receive LLDP Message** is enabled, the port can discover the peer device.

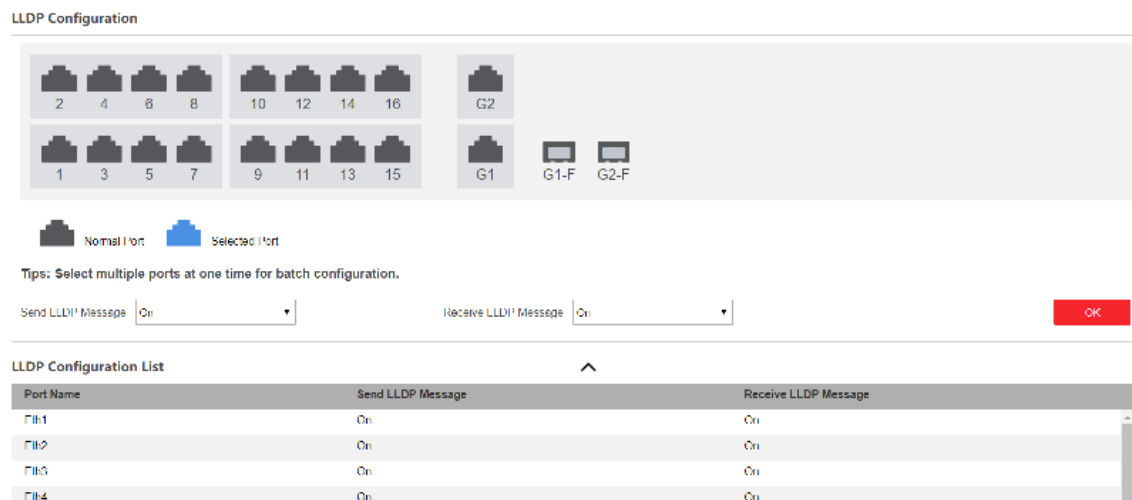


Figure 5-15 LLDP Port Settings

Neighbor Information

Check local port, MAC address of peer device, and peer port.

Local Port	Peer MAC Address	Peer Port
Eth6	2c:a5:9c:9a:3b:75	Ge9
Eth8	2c:a5:9c:9a:3b:75	Ge5

Figure 5-16 Neighbor Information

5.6 SNMP Configuration

Simple Network Management Protocol (SNMP) is a widely used application-layer communication protocol for monitoring network performance. SNMP network is composed of the Network Management System (NMS) and the Agent. NMS is the SNMP manager, and Agent sends Traps to NMS.

5.6.1 Configure SNMP Proxy

Steps

1. Go to **Switch Configuration → L2 Configuration → SNMP Configuration → SNMP Proxy Settings**.



The interface shows the 'SNMP' toggle switch turned on. Below it is a table with two columns: 'Community Name' and 'Access Mode'. The table has two rows: 'public' with 'Read Only' and 'private' with 'Read/Write'. An 'OK' button is in the top right corner.

Community Name	Access Mode
public	Read Only
private	Read/Write

Figure 5-17 Proxy Settings

2. Enable **SNMP**.
3. Define the **Community Name**.

Community Name

The community name is an authentication mechanism, similar to a password. It is used to limit the data transmission between NMS and Agent.

- **Read-Only Community Name:** The Community name accessible to NMS with read permission. The default is **public**.
- **Read/Write Community Name:** The Community name accessible to NMS with read and write permission. The default is **private**.

4. Click **OK** to save.

5.6.2 SNMP Trap Settings

Steps

1. Enable **Trap** on the **SNMP Trap Settings** page.
2. Click **Add** to add a trap.

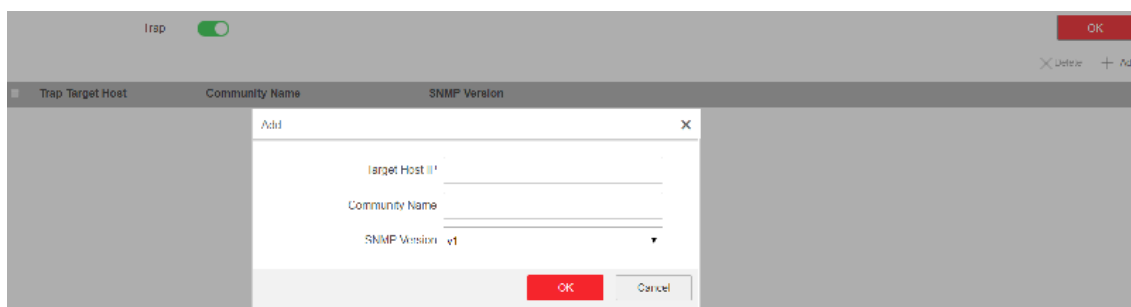


Figure 5-18 Trap Settings

3. Click **OK**.
4. Click **OK** to save.
5. **Optional:** You can check the trap and click **Delete** to delete a trap.

5.7 STP Configuration

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

5.7.1 Global Configuration

Steps

1. Go to **Switch Configuration → L2 Configuration → STP Configuration → Global Configuration**.
2. Check **Enable STP**.

① The maximum aging time must meet the following conditions:

Maximum Aging Time $\geq 2 \times (\text{Hello Time} + 1)$

Maximum Aging Time $\leq 2 \times (\text{Forwarding Delay} - 1)$

Enable STP ☒

STP Mode RSTP

Bridge Priority 32768 ✓

Hello Time 2 S ✓

Maximum Aging Time 20 S ✓

Forwarding Delay 15 S ✓

OK

Figure 5-19 Global Configuration

3. Configure the parameters.

Table 5-1 Parameters of STP

Parameter	Description
STP Mode	STP: Spanning-tree protocol. RSTP: Rapid spanning-tree protocol. RSTP provides faster spanning tree convergence after a topology change.
Bridge Priority	The lower the number is, the higher the priority is. The range is from 0 to 61,440 seconds, in increments of 4096; the default is 32,768. Valid values are 0, 4096, 12288, 16384 ... and 61440. A switch with higher bridge priority is more likely to become a root bridge.
Hello Time	The time between each BPDU that is sent on a port, which is used for port link diagnosis. The range is from 1 to 10 seconds. The default is 2 seconds.
Maximum Aging Time	The maximum length of time that passes before a bridge port saves its configuration BPDU information. The range is from 6 to 40 seconds. The default is 20 seconds.

Parameter	Description
	 Note The maximum aging time must meet the following conditions: • Maximum Aging Time $\geq$ (Hello Time + 1) • Maximum Aging Time $\leq$ (Forwarding Delay - 1)
Forwarding Delay	The time interval that is spent in the listening and learning state when the topology changes. The range is from 4 to 30 seconds. The default is 15 seconds.

4. Click **Save**.

5.7.2 Configure STP Port

If a loop occurs, you can set port priority, so that the spanning tree can select the port with the highest priority to forward data.

Steps

1. The port is enabled by default on the **STP Port Configuration** page.

Port Name	Port	Port Priority
Eth1		128
Eth2		128
Eth3		128
Eth4		128

Figure 5-20 Port Priority

2. Configure the **Port Priority**.

Port Priority

- The lower the number is, the higher the priority is, the more probably the port becomes the root port.
- The range is from 0 to 240, in increments of 16; the default is 128. Valid values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240.

Note

If the priority of the port is the same, spanning tree uses the port ID to select a port as the root port.

3. Click **Save**.

5.7.3 STP Status View

You can check the global status of STP settings and the status of each port.

Go to **Switch Configuration → L2 Configuration → STP Configuration → STP Status** .

Global Status	
Bridge ID:	0000000000000000
Root Bridge ID:	0.00.00.00.00.00
Root Bridge Hello Time:	0
Root Bridge Maximum Aging Time:	0
Root Bridge Forwarding Delay:	0

Port Status			
Port Name	Path Cost	Port Role	Port Status

Figure 5-21 STP Status

5.8 PoE Management

Go to **Switch Configuration → Basic Configuration → PoE Management** .

PoE Management

2 4 6 8

10 12 14 16

G2

1 3 5 7

9 11 13 15

G1

G1-F

G2-F

Normal Port

Selected Port

Tip: Select multiple ports at one time for batch configuration.

PoE Status Control

On

OK

PoE Management List

Port Name	Status
Eth1	On
Eth2	On
Eth3	On
Eth4	On

Figure 5-22 PoE Management

PoE Settings

You can enable PoE to supply power for the powered devices (PDs).

Note

Enabling or disabling PoE has no influences on data transmission of the port.

PoE Watchdog

You can enable PoE watchdog to auto-detect and restart cameras that do not respond.

Chapter 6 System Management

6.1 Synchronize the Time

Steps

1. Go to **System Management** → **System Settings** → **Time Settings** .

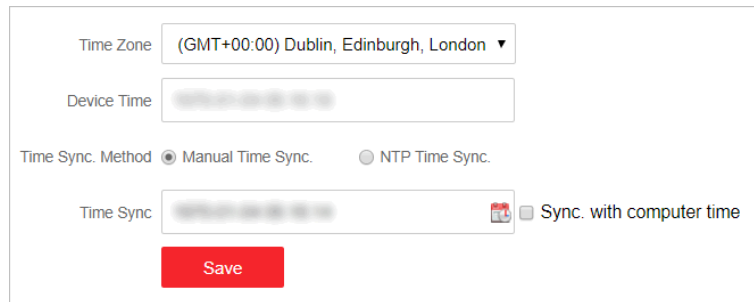


Figure 6-1 Time Settings

2. Select **Time Zone**.
3. Select **Time Sync. Method**.
4. Set time synchronization mode.
 - **Manual Time Sync.:** Click  or check **Sync. with computer time** to synchronize the device time.

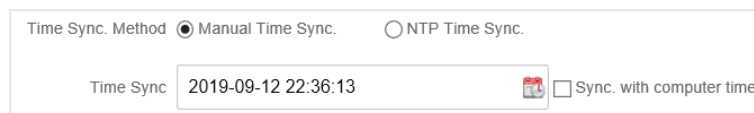


Figure 6-2 Manual Sync

- **NTP Time Sync.:** Enter the **NTP Server Address**, and set the time sync. interval.

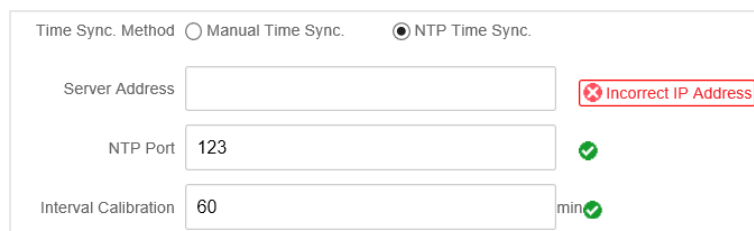


Figure 6-3 NTP Sync

5. Click **Save**.

6.2 Device Operation

When the device malfunctions or fails to work properly, you can go to **System Management** → **System Maintenance** → **Device Operation** to restart or restore the device.



Figure 6-4 Device Operation



Note

Enter the login page automatically after you restart or restore the switch.

Restart

Click **Restart** to remotely restart the switch.

Restore

- **Simply Restore**: Except network configuration and user parameters, all of the other parameters are restored to the default settings.
- **Completely Restore**: Completely restore the parameters to default settings.



Caution

Parameters cannot be recovered after the device is restored to default settings.

6.3 Configure File Export

You can export the configuration file for local backup.

Steps

1. Go to **System Management** → **System Maintenance** → **Export & Import** .
2. Click **Export**.
3. Set a password for the exported configuration file.

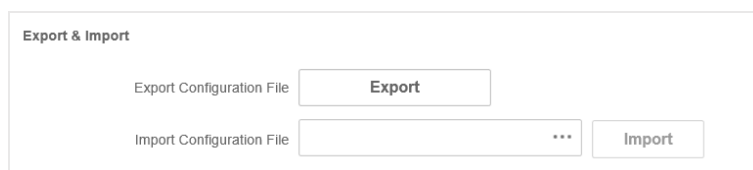


Figure 6-5 Export Configuration file



Note

Password is required when importing the configuration files.

4. Click **OK**.

6.4 Configure File Import

You can import the configuration file to configure the system easily.

Steps

1. Go to **System Management → System Maintenance → Export & Import**.

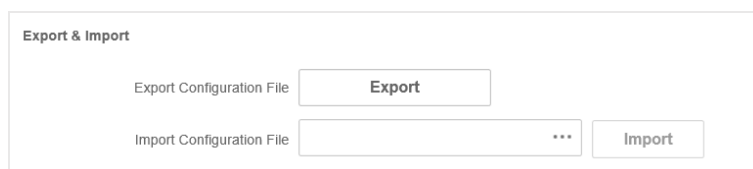


Figure 6-6 Export Configuration file

2. Click ... to select the configuration file.
3. Click **Import**.

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

6.5 Upgrade the Device

You can upload the upgrade file to upgrade your switch.

Steps

1. Go to **System Management → System Maintenance → Device Upgrade**.



Figure 6-7 Upgrade

2. Click ... to select an upgrade patch.

3. Click **Upgrade**.



Note

If upgrading failed or the device cannot function, please contact our technical support engineers.

Result

The device will restart automatically to enter the login page when upgrade finished.

6.6 Manage Logs

System operation logs can be searched and exported for backup.

Steps

1. Go to **System Management → Log Management**.

The screenshot shows the Log Management interface. At the top, there are search filters: 'Major Type' set to 'All Types', 'Minor Type' set to 'All Types', 'Start Time' set to '2022-03-11 00:00:00', and 'End Time' set to '2022-03-22 23:59:59'. There are 'Search' and 'Export' buttons. Below the filters is a table with the following data:

No.	Operation Time	Major Type	Minor Type	Remote Operator	Remote Host Address	Description
1	2022-03-11 16:28:01	Operation	Remote Logout	admin	10.12.98.19	(SUK)
2	2022-03-11 16:28:01	Operation	Remote Login	admin	10.12.98.19	(SUK)
3	2022-03-11 16:28:12	Operation	Remote Login	admin	10.12.98.19	(SAI*)
4	2022-03-11 16:28:20	Operation	Remote Login	admin	10.12.98.19	(SUK)

Figure 6-8 Log Management

2. Set search conditions, including **Major Type**, **Minor Type**, **Start Time** and **End Time**.

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.



Note

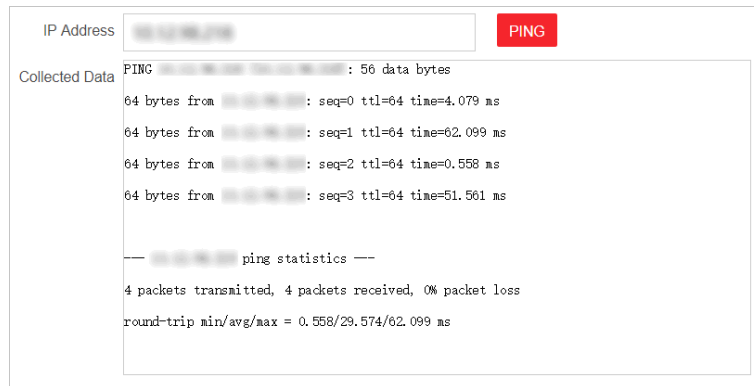
Logs can be exported in Excel. A prompt window will pop up when the logs are exported successfully.

6.7 Diagnose the Network

With network diagnostics, troubleshooting engineers can locate network faults quickly.

Steps

1. Go to **System Management → System Tools → Network Diagnostics**.



The screenshot shows a web interface for network diagnostics. At the top, there is a text input field labeled 'IP Address' containing the value '192.168.1.100'. To the right of this field is a red button labeled 'PING'. Below the input field, the 'Collected Data' section displays the results of a PING command. The text shows 'PING 192.168.1.100: 56 data bytes' followed by four lines of response data: '64 bytes from 192.168.1.100: seq=0 ttl=64 time=4.079 ms', '64 bytes from 192.168.1.100: seq=1 ttl=64 time=62.099 ms', '64 bytes from 192.168.1.100: seq=2 ttl=64 time=0.558 ms', and '64 bytes from 192.168.1.100: seq=3 ttl=64 time=51.561 ms'. Below this, a separator line is followed by 'ping statistics ---', then '4 packets transmitted, 4 packets received, 0% packet loss', and finally 'round-trip min/avg/max = 0.558/29.574/62.099 ms'.

Figure 6-9 Network Diagnostics

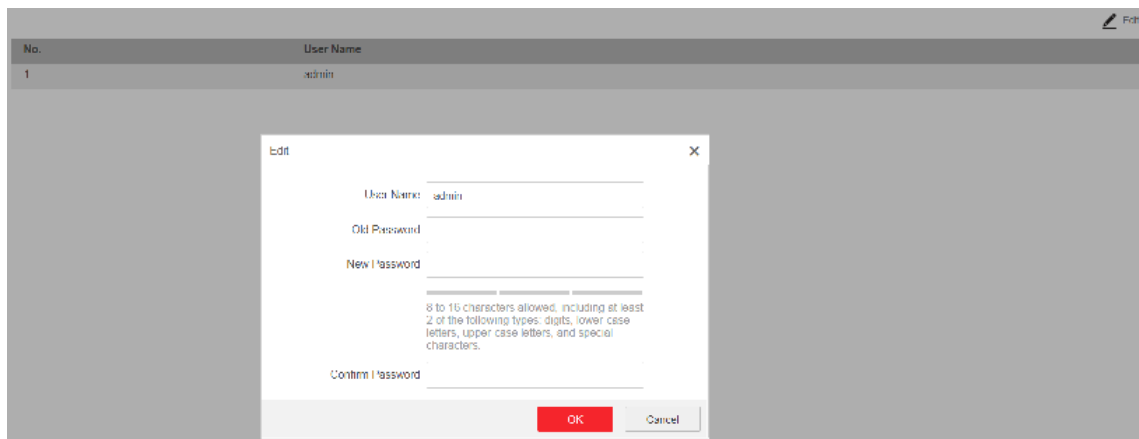
2. Enter the IP address of the server, and click **PING**.

6.8 Manage Users

Regularly change the password to improve the security of the device.

Steps

1. Go to **System Management → User Management**.
2. Click **Edit**.



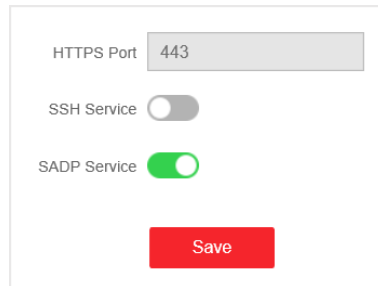
The screenshot shows a web interface with a table of users. The table has two columns: 'No.' and 'User Name'. The first row shows '1' and 'admin'. Below the table, there is a modal dialog box titled 'Edit' with a close button 'X'. The dialog box contains four input fields: 'User Name' (pre-filled with 'admin'), 'Old Password', 'New Password', and 'Confirm Password'. Below the 'New Password' field, there is a text box with the password requirements: '8 to 16 characters allowed, including at least 2 of the following types: digits, lower case letters, upper case letters, and special characters.' At the bottom of the dialog box are two buttons: 'OK' (red) and 'Cancel'.

Figure 6-10 User Management

3. Enter the old password.
4. Enter a new password and confirm it.
5. Click **OK**.

6.9 Security Management

SSH



The screenshot shows a web interface for security management. It contains three settings: 'HTTPS Port' with a value of '443', 'SSH Service' which is disabled (indicated by a grey toggle switch), and 'SADP Service' which is enabled (indicated by a green toggle switch). A red 'Save' button is located at the bottom of the settings area.

Figure 6-11 Security Management

The device supports SSH security service. SSH can prevent the information leakage in the remote management of the device. SSH is disabled by default.



Note

The user name of SSH is **root**, and the password is the device login password.

SADP

After enabling SADP, you can activate the device, change the password and the network information, and etc. SADP is enabled by default.



See Far, Go Further