Smart Managed Switch Web

User Manual

See Far, Go Further

UD33916B

Legal Information

About this Document

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

About this Product

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

Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF

THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Preface

Applicable Models

This manual is applicable to smart managed switches.

About Defaults

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

Note

- The default user name **admin** needs to be activated for first-time login.
- The default IP address of the switch is dynamically assigned.
- 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

1 Introduction 1

2 Activation and Login 1

3 Device Information 3

3.1 Device Overview 3

3.2 Port Status 4

3.3 Network Status 5

4 Network Configuration 7

5 Device Configuration 8

5.1 Port Configuration 8

5.1.1 Configure Port Attributes 8

5.1.2 Configure Link Aggregation 9

5.1.3 Configure Long-Range Mode 10

5.1.4 Configure Port Isolation 10

5.1.5 Configure Port Mirroring 11

5.1.6 Configure High-Priority Port 12

5.2 STP Configuration 12

5.3 LLDP Configuration 14

5.4 VLAN Configuration 14

5.4.1 Add VLAN 14

5.4.2 Configure Port VLAN 15

5.5 PoE Management 16

6 System Management 16

6.1 Time Synchronization 16

6.2 System Maintenance 17

1 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.

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

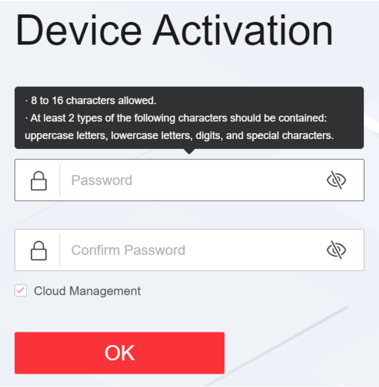
Ensure that your computer and switch are on the same network segment.

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

· 8 to 16 characters allowed.
· At least 2 types of the following characters should be contained: uppercase letters, lowercase letters, digits, and special characters.

Figure 2-1 Activation

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.

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

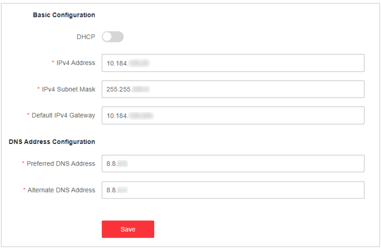
   The Hik-Connect service is enabled.

4. Click **OK**.

   The network configuration page is displayed.

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

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



Basic Configuration

DHCP

* IPv4 Address: 10.184.[redacted]

* IPv4 Subnet Mask: 255.255.[redacted]

* Default IPv4 Gateway: 10.184.[redacted]

DNS Address Configuration

* Preferred DNS Address: 8.8.[redacted]

* Alternate DNS Address: 8.8.[redacted]

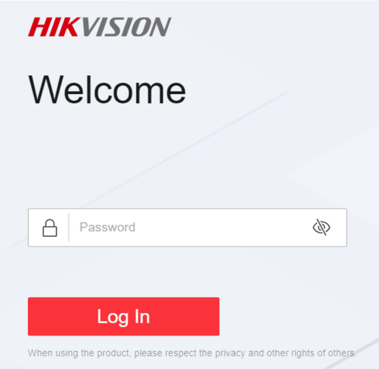
Figure 2-2 Network Configuration

   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 Login

3 Device Information

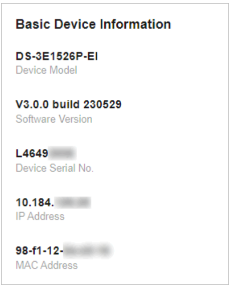
After logging in to the switch web, you can obtain detailed information about the switch, including the device overview information, port status information, and network status information.

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 No., IP address, and MAC address of the switch in the lower right corner of the **Overview** page.



Basic Device Information

DS-3E1526P-EI
Device Model

V3.0.0 build 230529
Software Version

L4649[redacted]
Device Serial No.

10.184.[redacted]
IP Address

98-f1-12-[redacted]
MAC Address

Figure 3-1 Basic Device Information

Device Name

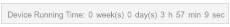
You can view the current device name or click ✎ next to it to customize the device name on the **Overview** page.

DS-3E1106P-EI/M ✎

Figure 3-2 Device Name

Device Running Time

You can also view the running time of the current device in the upper right corner of the **Overview** page.

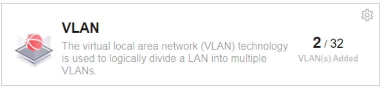


Device Running Time: 0 week(s) 0 day(s) 3 h 57 min 9 sec

Figure 3-3 Device Running Time

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

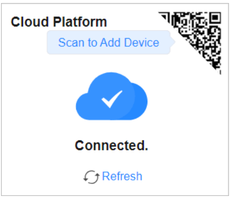
The virtual local area network (VLAN) technology is used to logically divide a LAN into multiple VLANs.

2 / 32

VLAN(s) Added

Figure 3-4 Number of VLANs Added

Cloud Platform Connection Status



Cloud Platform

Scan to Add Device

Connected.

Refresh

Figure 3-5 Cloud Platform Connection Status

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

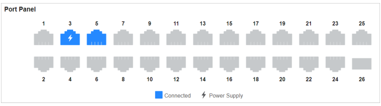
- If the cloud platform is connected, scan the QR code to add the device to Hik-Partner Pro app for remote management.
- If the cloud platform is disconnected, click **Refresh** to reconnect, or click **Diagnose** to find out the cause of the connection failure and go to the cloud platform configuration page as prompted for cloud platform configuration.

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.

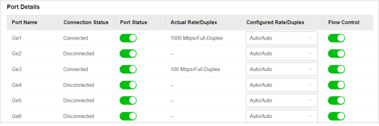


Port Panel

Figure 3-6 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 Details

Port Name	Connection Status	Port Status	Actual Rate/Duplex	Configured Rate/Duplex	Flow Control
Ge1	Connected	●	1000 Mbps/Full-Duplex	Auto/Auto	●
Ge2	Disconnected	●	--	Auto/Auto	●
Ge3	Connected	●	100 Mbps/Full-Duplex	Auto/Auto	●
Ge4	Disconnected	●	--	Auto/Auto	●
Ge5	Disconnected	●	--	Auto/Auto	●
Ge6	Disconnected	●	--	Auto/Auto	●

Figure 3-7 Port Details

Connection Status

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

Port Status

Enable or disable a port. Ports are enabled by default.

Actual Rate/Duplex

The actual rate and duplex mode of a port.

Configured Rate/Duplex

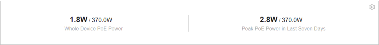
The default value is **Auto/Auto**. You can select different combinations of rates and duplex modes as required.

Flow Control

Enabled by default. 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.



1.8W / 370.0W
Whole Device PoE Power

2.8W / 370.0W
Peak PoE Power in Last Seven Days

Figure 3-8 PoE Power

Note

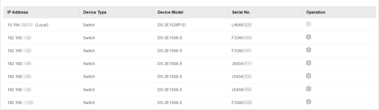
PoE power display is only available for switches supporting PoE.

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

Network Device Discovery is a function that automatically detects transmission devices in the same LAN with the switch and displays information about these devices. Go to **Network Monitoring → Network Device Discovery** , and you can view the device IP address, type, model, and serial No. of the network device(s) found. You can also select a device and click ⚙ in the **Operation** column to go to the web configuration page of the device.

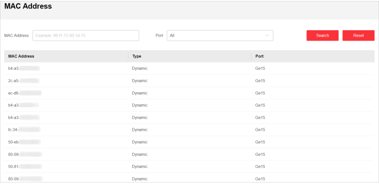


IP Address	Device Type	Device Model	Serial No.	Operation
10.184.[redacted] (Local)	Switch	DS-3E1526P-EI	L4649[redacted]	⚙
192.168.[redacted]	Switch	DS-3E1508-S	F3340[redacted]	⚙
192.168.[redacted]	Switch	DS-3E1508-S	F3340[redacted]	⚙
192.168.[redacted]	Switch	DS-3E1508-S	J5434[redacted]	⚙
192.168.[redacted]	Switch	DS-3E1508-S	J5434[redacted]	⚙
192.168.[redacted]	Switch	DS-3E1508-S	J5434[redacted]	⚙
192.168.[redacted]	Switch	DS-3E1508-S	F3340[redacted]	⚙

Figure 3-9 Network Device Discovery

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

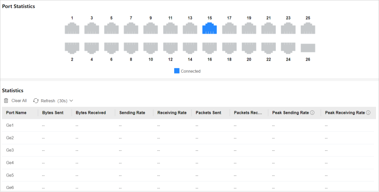
MAC Address: Example: 98-f1-12-00-1d-75   Port: All

MAC Address	Type	Port
b4-a3-[redacted]	Dynamic	Ge15
2c-a5-[redacted]	Dynamic	Ge15
ec-d6-[redacted]	Dynamic	Ge15
b4-a3-[redacted]	Dynamic	Ge15
b4-a3-[redacted]	Dynamic	Ge15
fc-34-[redacted]	Dynamic	Ge15
50-eb-[redacted]	Dynamic	Ge15
80-09-[redacted]	Dynamic	Ge15
50-81-[redacted]	Dynamic	Ge15
80-09-[redacted]	Dynamic	Ge15

Figure 3-10 Port MAC Address

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.



Port Statistics

Statistics

Port Name	Bytes Sent	Bytes Received	Sending Rate	Receiving Rate	Packets Sent	Packets Rec...	Peak Sending Rate ⓘ	Peak Receiving Rate ⓘ
Ge1	--	--	--	--	--	--	--	--
Ge2	--	--	--	--	--	--	--	--
Ge3	--	--	--	--	--	--	--	--
Ge4	--	--	--	--	--	--	--	--
Ge5	--	--	--	--	--	--	--	--
Ge6	--	--	--	--	--	--	--	--

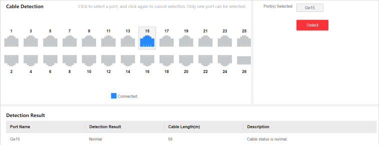
Figure 3-11 Port Statistics

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.

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 to select a port, and click again to cancel selection. Only one port can be selected.

Port(s) Selected: Ge15

Detection Result

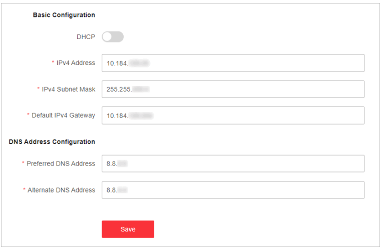
Port Name	Detection Result	Cable Length(m)	Description
Ge15	Normal	58	Cable status is normal.

Figure 3-12 Cable Status Detection

4 Network Configuration

You can click on the home page to check Hik-Connect connection status, or go to **System → Network Configuration** for network configuration, cloud platform configuration, and SADP configuration.

Network Configuration



Basic Configuration

DHCP: off

* IPv4 Address: 10.184.[redacted]

* IPv4 Subnet Mask: 255.255.[redacted]

* Default IPv4 Gateway: 10.184.[redacted]

DNS Address Configuration

* Preferred DNS Address: 8.8.[redacted]

* Alternate DNS Address: 8.8.[redacted]

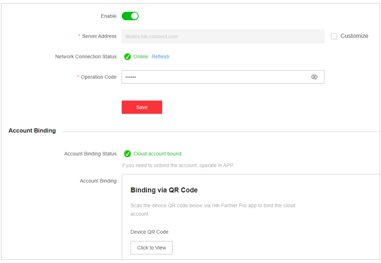
Figure 4-1 Network Configuration

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.

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 → 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: ●

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

Network Connection Status: ✓ Online Refresh

* Operation Code: ••••••

Account Binding

Account Binding Status: ✓ Cloud account bound.

If you need to unbind the account, operate in APP.

Account Binding: Binding via QR Code

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

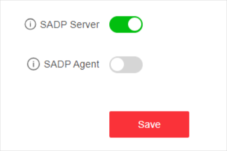
Device QR Code

Figure 4-2 Cloud Platform Configuration

Note

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

SADP Configuration



SADP Server: ●

SADP Agent: ○

Figure 4-3 SADP Configuration

Enable **SADP Server** or **SADP Agent** as required.

Note

- After SADP server is enabled, devices supporting SADP can be searched and information about the devices is displayed.
- After SADP agent is enabled, query requests are sent to the LAN periodically (every minute) for network topology drawing.

5 Device Configuration

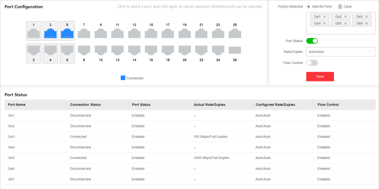
5.1 Port Configuration

5.1.1 Configure Port Attributes

The basic attributes can influence the working status of a port. Configure the parameters as required.

Steps

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



Port Configuration

Click to select a port, and click again to cancel selection. Multiple ports can be selected.

🟦 Connected

Port(s) Selected + Add All Ports 🗑 Clear

Ge1 × Ge2 × Ge3 × Ge4 × Ge5 × Ge6 ×

Port Status: ●

Rate/Duplex: Auto/Auto

Flow Control: ○

Port Status

Port Name	Connection Status	Port Status	Actual Rate/Duplex	Configured Rate/Duplex	Flow Control
Ge1	Disconnected	Enabled	--	Auto/Auto	Enabled
Ge2	Disconnected	Enabled	--	Auto/Auto	Enabled
Ge3	Connected	Enabled	100 Mbps/Full-Duplex	Auto/Auto	Enabled
Ge4	Disconnected	Enabled	--	Auto/Auto	Enabled
Ge5	Connected	Enabled	1000 Mbps/Full-Duplex	Auto/Auto	Enabled
Ge6	Disconnected	Enabled	--	Auto/Auto	Enabled
Ge7	Disconnected	Enabled	--	Auto/Auto	Enabled

Figure 5-1 Configure Port Attributes

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

Port Status

Enable or disable the selected port(s). Once a port is disabled, no data will be transmitted on it.

Rate/Duplex

The data transmission speed of a port or the duplex mode of a port. The configurable rates or duplex modes of ports 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.

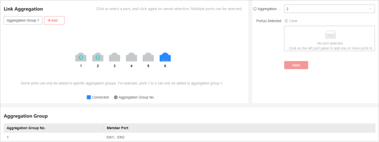
5.1.2 Configure Link Aggregation

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** .

2. Click +Add .



Link Aggregation

Click to select a port, and click again to cancel selection. Multiple ports can be selected.

Some ports can only be added to specific aggregation groups. For example, ports 1 to 4 can only be added to aggregation group 1.

🟦 Connected ⓝ Aggregation Group No.

ⓘ Aggregation ...: 2

Port(s) Selected 🗑 Clear

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

Aggregation Group

Aggregation Group No.	Member Port
1	Eth1; Eth2

Figure 5-2 Configure Link Aggregation

3. 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. For example, ports 1 to 4 can only be added to aggregation group 1. Please refer to the actual situation.
- The rate, duplex mode, flow control, and long-range mode configurations of ports in one aggregation group should be the same.

4. Set **Aggregation Group No.**.

Note

The number of aggregation groups allowed varies.

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.

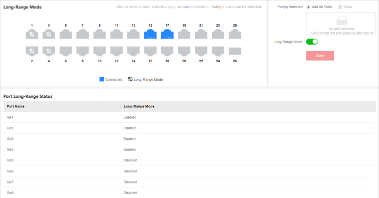
8. Optional: View the member ports of each aggregation group in the list below.

5.1.3 Configure Long-Range Mode

After the long-range mode is enabled for a port, the transmission distance of the port can reach 300 meters at a rate of 10 Mbps.

Steps

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



Click to select a port, and click again to cancel selection. Multiple ports can be selected.

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

Port Long-Range Status

Port Name	Long-Range Mode
Ge1	Enabled
Ge2	Enabled
Ge3	Enabled
Ge4	Enabled
Ge5	Disabled
Ge6	Disabled
Ge7	Disabled
Ge8	Disabled

Figure 5-3 Configure Long-Range Mode

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

Note

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

3. Enable or disable **Long-Range Mode** on the right as required.

4. Click **Save**.

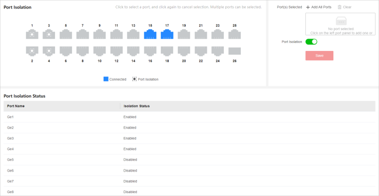
5. Optional: View the long-range statuses of different ports in the **Port Long-Range Status** list.

5.1.4 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 **L2 Configuration → Port Isolation** .



Port Isolation

Click to select a port, and click again to cancel selection. Multiple ports can be selected.

Port(s) Selected + Add All Ports Clear

Port Isolation: enabled

Port Isolation Status

Port Name	Isolation Status
Ge1	Enabled
Ge2	Enabled
Ge3	Enabled
Ge4	Enabled
Ge5	Disabled
Ge6	Disabled
Ge7	Disabled
Ge8	Disabled

Figure 5-4 Configure Port Isolation

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

Note

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

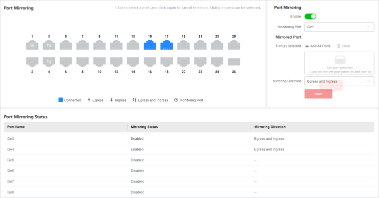
3. Enable or disable **Port Isolation** on the right as required.
4. Click **Save**.
5. **Optional:** View the port isolation statuses of different ports in the **Port Isolation Status** list.

5.1.5 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 to select a port, and click again to cancel selection. Multiple ports can be selected.

Port Mirroring

Enable: enabled

Monitoring Port: Ge1

Mirrored Port

Port(s) Selected + Add All Ports Clear

Mirroring Direction: Egress and Ingress

Port Mirroring Status

Port Name	Mirroring Status	Mirroring Direction
Ge3	Enabled	Egress and Ingress
Ge4	Enabled	Egress and Ingress
Ge5	Disabled	--
Ge6	Disabled	--
Ge7	Disabled	--
Ge8	Disabled	--

Figure 5-5 Configure Port Mirroring

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

Note

You can also click + Add All Ports or Clear 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.

---

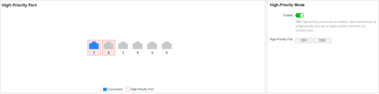
4. **Optional:** View the mirroring statuses of different ports in the **Port Mirroring Status** list.

5.1.6 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 **Quality of Service → High-Priority Port** .



High-Priority Port

High-Priority Mode

Enable

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 Port: Eth1 Eth2

Figure 5-6 Configure High-Priority Port

Note

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

---

2. In **High-Priority 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.

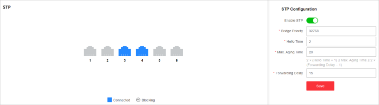
All high-priority ports of the switch are enabled, with a higher data transmission priority than common ports.

5.2 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 Configuration

Enable STP: on

* Bridge Priority: 32768

* Hello Time: 2

* Max. Aging Time: 20

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

* Forwarding Delay: 15

Figure 5-7 STP Configuration

2. In **STP Configuration**, toggle on **Enable STP**.

3. Set STP parameters as required.

Table 5-1 STP Parameters

Parameter	Description
Bridge Priority	• The value ranges from 0 to 61440, in an increment of 4096. The default value is 32,768. 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

Parameter	Description
	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 status of each port or the global status of STP settings.

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.

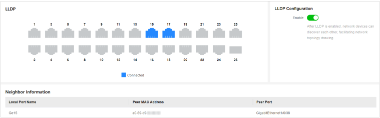
5.3 LLDP Configuration

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 drawing.

Neighbor Information

Local Port Name	Peer MAC Address	Peer Port
Ge15	a0-69-d9-[redacted]	GigabitEthernet1/0/38

Figure 5-8 LLDP Configuration

Note

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

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

5.4 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.

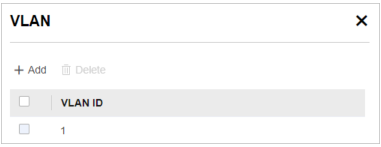
5.4.1 Add VLAN

Steps

1. Click **VLAN Management** in the left navigation pane.

2. In **VLAN Configuration**, click **Edit**.

3. Click **Add**.



VLAN ✕

+ Add 🗑 Delete

□	VLAN ID
□	1

Figure 5-9 Add VLAN(s)

4. Select an adding mode.

- **Single**: Only one VLAN is added at a time.
- **Batch**: Multiple VLANs are added in a batch.

5. Set **VLAN ID**.

- **Single**: Enter a VLAN ID. The VLAN ID should be an integer between 1 to 4094.
- **Batch**: Enter the start VLAN ID and end VLAN ID. The VLAN ID should be an integer between 1 to 4094, and the end VLAN ID should be greater than the start VLAN ID.

Note

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

6. Click **Save**.

7. Optional: Select the desired VLAN(s) and click **Delete** to delete a VLAN.

Note

The default VLAN 1 cannot be deleted.

5.4.2 Configure Port VLAN

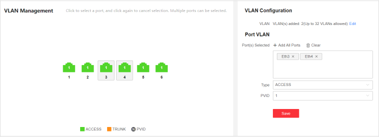
Steps

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

Note

- You can also click + Add All Ports or 🗑 Clear 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 to select a port, and click again to cancel selection. Multiple ports can be selected.

VLAN Configuration

VLAN VLAN(s) added: 2(Up to 32 VLANs allowed) Edit

Port VLAN

Port(s) Selected + Add All Ports 🗑 Clear

Eth3 × Eth4 ×

Type ACCESS

PVID 1

Save

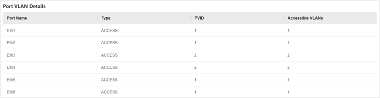
Figure 5-10 Configure Port VLAN

- **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.



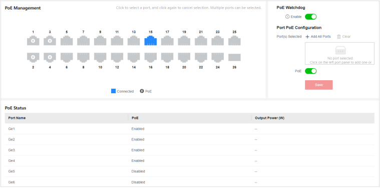
Port VLAN Details

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 5-11 Port VLAN Details

5.5 PoE Management

Click **PoE Management** in the left navigation pane.



PoE Management

Click to select a port, and click again to cancel selection. Multiple ports can be selected.

PoE Watchdog

Enable: on

Port PoE Configuration

Port(s) Selected + Add All Ports Clear

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

PoE: on

Save

PoE Status

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

Figure 5-12 PoE Management

PoE Watchdog

Enable PoE watchdog to auto-detect and restart IP cameras that do not respond.

Port PoE Configuration

Select the desired port(s) on the left port panel and enable PoE to supply power to the powered device(s) connected.

Note

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

PoE Status

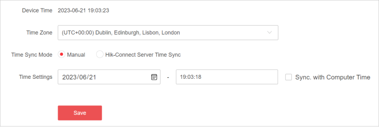
View the PoE enabling status and output power of PoE ports in the **PoE Status** list.

6 System Management

6.1 Time Synchronization

Steps

1. Go to **System → Time Configuration** .


Device Time 2023-06-21 19:03:23

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

Time Sync Mode ● Manual ○ Hik-Connect Server Time Sync

Time Settings 2023/06/21 - 19:03:18 □ Sync. with Computer Time

Figure 6-1 Time Synchronization

2. Set **Time Zone**.

3. Set **Time Sync Mode**.

- **Manual**: Click 📅 to manually set the date and time, or check **Sync. with Computer Time** to synchronize the device time.
- **Hik-Connect Server Time Sync**: Use the Hik-Connect server for automatic time calibration and synchronization.

4. Click **Save**.

6.2 System Maintenance

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

Restart Device

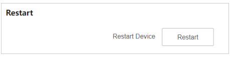


Figure 6-2 Device Restart

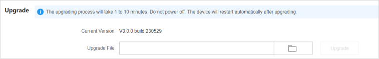
In **Restart**, click **Restart** to remotely restart the switch.

Note

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

Upgrade Device

Upload an upgrade file to upgrade the switch.


Upgrade

The upgrading process will take 1 to 10 minutes. Do not power off. The device will restart automatically after upgrading.

Current Version V3.0.0 build 230529

Figure 6-3 Device 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.

Back Up Device

Export the configuration file for local backup.

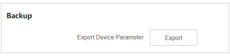


Figure 6-4 Device Backup

1. In **Backup**, click **Export** to export the configuration file containing device parameters.

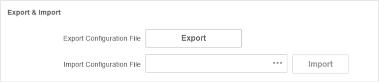


Figure 6-5 Export Device Parameters

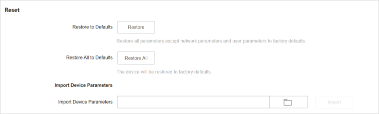
2. Set a password and confirm the password for file encryption.

Note

Remember the password as it is required when importing device parameters.

3. Click **OK**.

Reset Device



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

The device will be restored to factory defaults.

Figure 6-6 Device Reset

- **Restore to Defaults**: Click **Restore** to restore all parameters except network parameters and user 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.