

A stylized, semi-circular graphic representing a camera lens or sensor array. It features concentric, semi-circular bands in shades of gray and red. On the left side, there are several groups of red rectangular bars of varying lengths, arranged in a semi-circular pattern, resembling a sensor or lens element. A white crosshair is centered on the right side of the graphic, with a vertical line extending from the top to the bottom and a horizontal line extending from the left to the right. The overall design is modern and technical.

**HIKVISION**

**DS-3E1310P-E/DS-3E1318P-E/DS-3E1326P-E**

**User Manual**

**UD.6L0202D2008A01**

**COPYRIGHT ©2016 Hangzhou Hikvision Digital Technology Co., Ltd.**

**ALL RIGHTS RESERVED.**

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be “Hikvision”). This user manual (hereinafter referred to be “the Manual”) cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

## **About this Manual**

This Manual is applicable to DS-3E1310P-E/DS-3E1318P-E/DS-3E1326P-E.

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 in the company website (<http://overseas.hikvision.com/en/>).

Please use this user manual under the guidance of professionals.

## **Trademarks Acknowledgement**

**HIKVISION** and other Hikvision’s trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

## **Legal Disclaimer**

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS 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 OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

# Regulatory Information



## CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.



## FCC Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

Caution!

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.

## IC

CAN ICES-3 (A) /NMB-3 (A)

# Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into “Warnings” and “Cautions”

**Warnings:** Serious injury or death may occur if any of the warnings are neglected.

**Cautions:** Injury or equipment damage may occur if any of the cautions are neglected.

	
<b>Warnings</b> Follow these safeguards to prevent serious injury or death.	<b>Cautions</b> Follow these precautions to prevent potential injury or material damage.



## Warnings

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100~240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

# Preventive and Cautionary Tips

Before connecting and operating your device, please be advised of the following tips:

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Unit is designed for indoor use only.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with an UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

Thank you for purchasing our product. If there is any question or request, please do not hesitate to contact dealer.

The figures in the manual are for reference only.

This manual is applicable to the models listed in the following table.

Model	Description
DS-3E1310P-E	8+2G Web Smart PoE Switch
DS-3E1318P-E	16+2G Web Smart PoE Switch
DS-3E1326P-E	24+2G Web Smart PoE Switch

**Conventions**

Typographical conventions in this User Manual:

Item	Presentation	Example
Button	Shade	“Click the Save button” can be simplified as “Click <b>Save</b> ”.
Menu	Bold	“The menu Basic” can be simplified as <b>Basic</b> .
Continuous Steps	>	Click <b>Wireless &gt; Basic</b>

Symbols in this User Manual:

Item	Meaning
 <b>Note</b>	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
 <b>Tip</b>	This format is used to highlight a procedure that will save time or resources.

# Contents

<b>1 Device Login .....</b>	<b>1</b>
1.1 Login.....	1
1.2 Logout .....	3
1.3 Layout Introduction .....	3
<b>2 System Administration.....</b>	<b>5</b>
2.1 System Info .....	5
2.2 User Management.....	7
2.3 Reset.....	8
2.4 Reboot.....	8
2.5 Firmware Upgrade.....	9
<b>3. Port Management .....</b>	<b>12</b>
3.1 Port Configuration.....	12
3.2 Port Mirroring.....	15
3.2.1 Overview .....	15
3.2.2 Port Mirroring Configuration .....	16
3.2.3 Application Scenarios .....	18
3.3 Port Statistics .....	19
3.4 Rate Limit .....	20
<b>4 Link Aggregation .....</b>	<b>22</b>
4.1 Overview .....	22
4.2 Link Aggregation Configuration .....	22
<b>5 Network Extension .....</b>	<b>24</b>
<b>6 PoE Management.....</b>	<b>26</b>
<b>7 VLAN Management.....</b>	<b>28</b>
7.1 Overview .....	28
7.2 Port VLAN .....	31
7.2.1 Configuration Wizard.....	31
7.2.2 VLAN Port Configuration .....	31
7.2.3 Application Scenarios .....	36

7.3 ONE KEY VLAN .....	38
7.3.1 Configuration Wizard .....	39
7.3.2 ONE KEY VLAN .....	39
7.4 802.1Q VLAN .....	40
7.4.1 Configuration Wizard .....	40
7.4.2 802.1Q VLAN Configuration .....	41
7.4.3 Application Scenarios .....	46
<b>8 Device Management .....</b>	<b>49</b>
8.1 MAC Binding .....	49
8.1.1 Overview .....	49
8.1.2 Configuring MAC Binding .....	50
8.1.3 Application Scenarios .....	51
8.2 QoS .....	54
8.2.1 Overview .....	54
8.2.2 Configuring QoS .....	55
8.3 STP .....	57
8.3.1 Global setting of STP .....	61
8.3.2 Port setting .....	64
8.4 IGSP .....	66
8.5 SNMP .....	68
8.5.1 Overview .....	68
8.5.2 Configure the SNMP .....	69
8.5.3 Application Scenarios .....	74
<b>9 Configuration Management .....</b>	<b>77</b>
9.1 Backup Settings .....	77
9.2 Restore Previous Settings .....	77

# 1 Device Login

## 1.1 Login

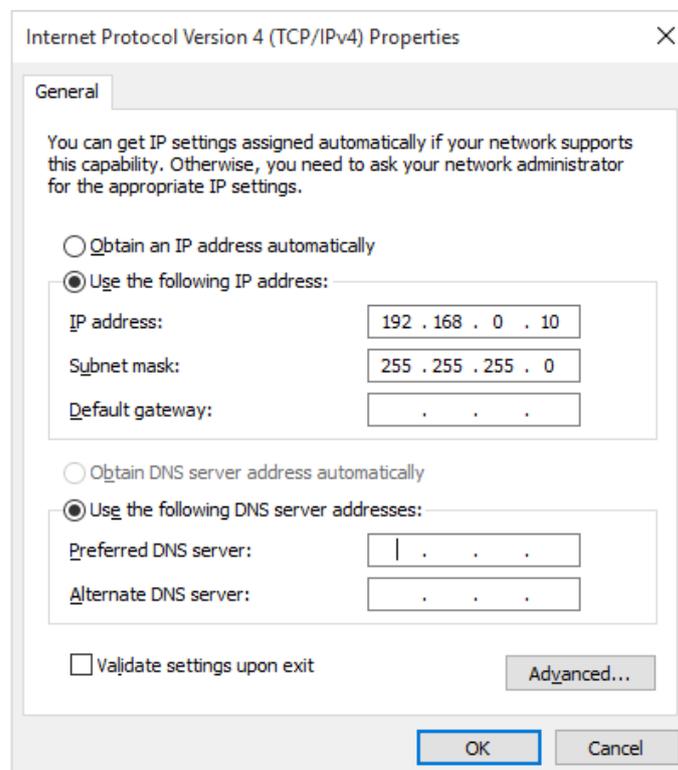
The switch has the function of Web administration. Based on the function, administrators could manage and maintain it in an intuitive way.

The first access to the switch allows you to enter the Web administration page through a web browser by the default login info. The default info of Web login includes:

Login info	Default settings
IP address	192.168.0.1
Username	admin
Password	admin

Log in to the Web administration page: (suppose that the login info is default)

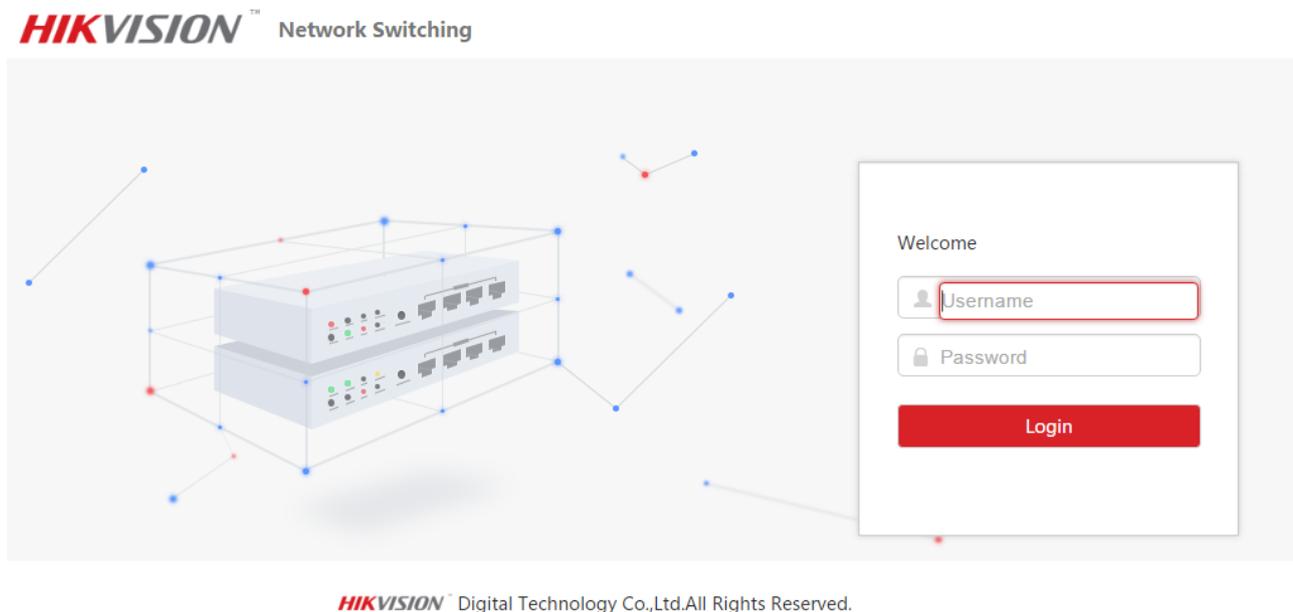
1. Use an Ethernet cable to connect a computer and the RJ45 port of the switch;
2. Set the local IP address as “192.168.0.X” (X is 2~254), sharing the same network segment with but different from the IP address of the switch. Subnet mask is set as 255.255.255.0;



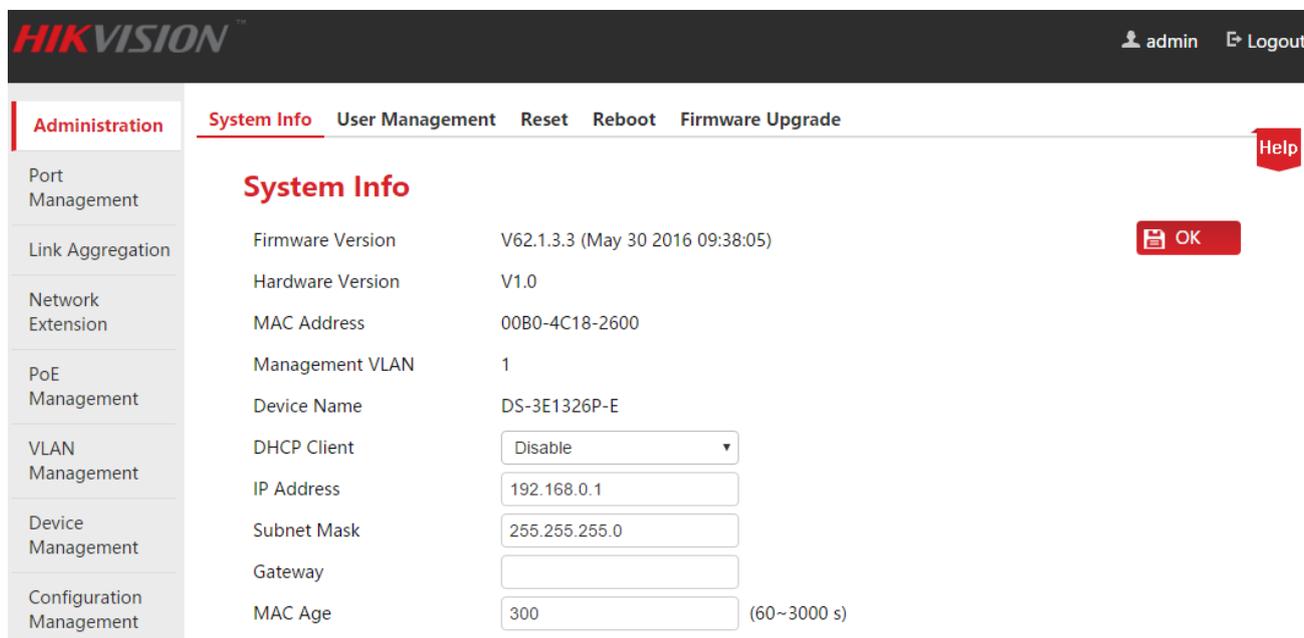
3. Launch a web browser, input IP address of the switch “192.168.0.1”, and then tap Enter on the keyboard;



4. In the Web administration page, input “admin” for username and password respectively, then click **Login**.



5. Upon entering into the Web administration page, you can review or modify configuration of the switch.

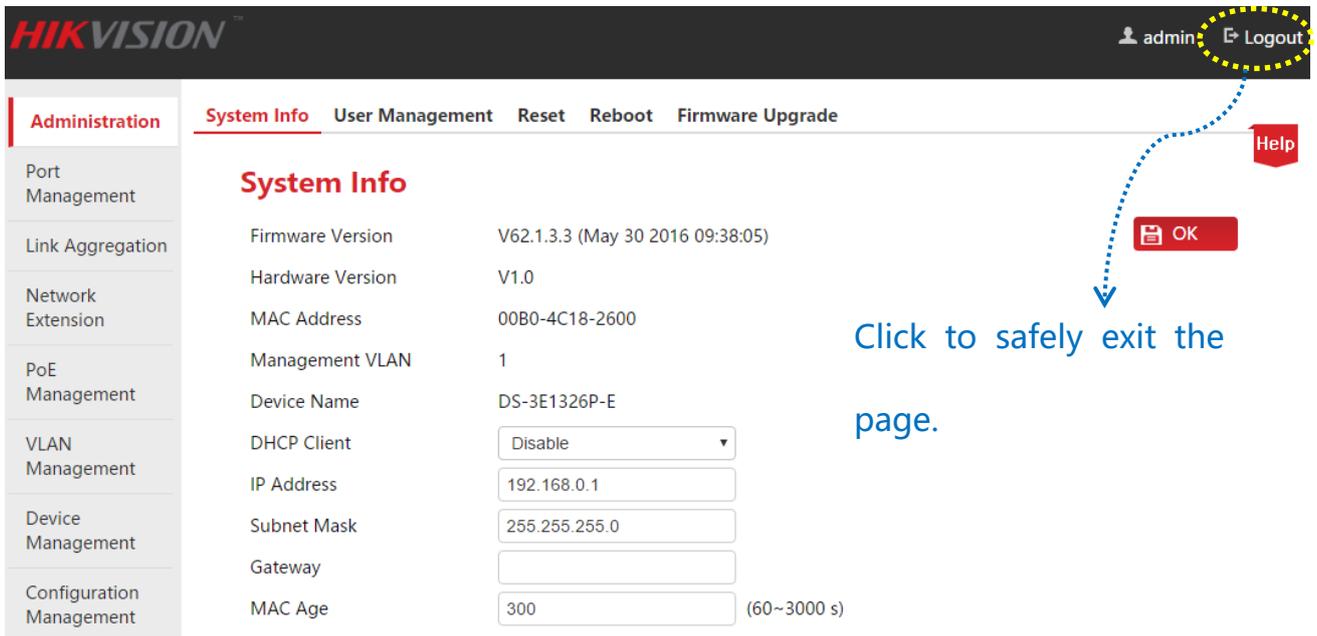


 **Tip**

The Web administrations of 8/16/24-Port 10/100Mbps + 2 Gigabit Web Smart PoE Switches are similar, with just a little difference in port numbers. We take 24-Port 10/100Mbps + 2 Gigabit Web Smart PoE Switch as an example. (Model: DS-3E1326P-E).

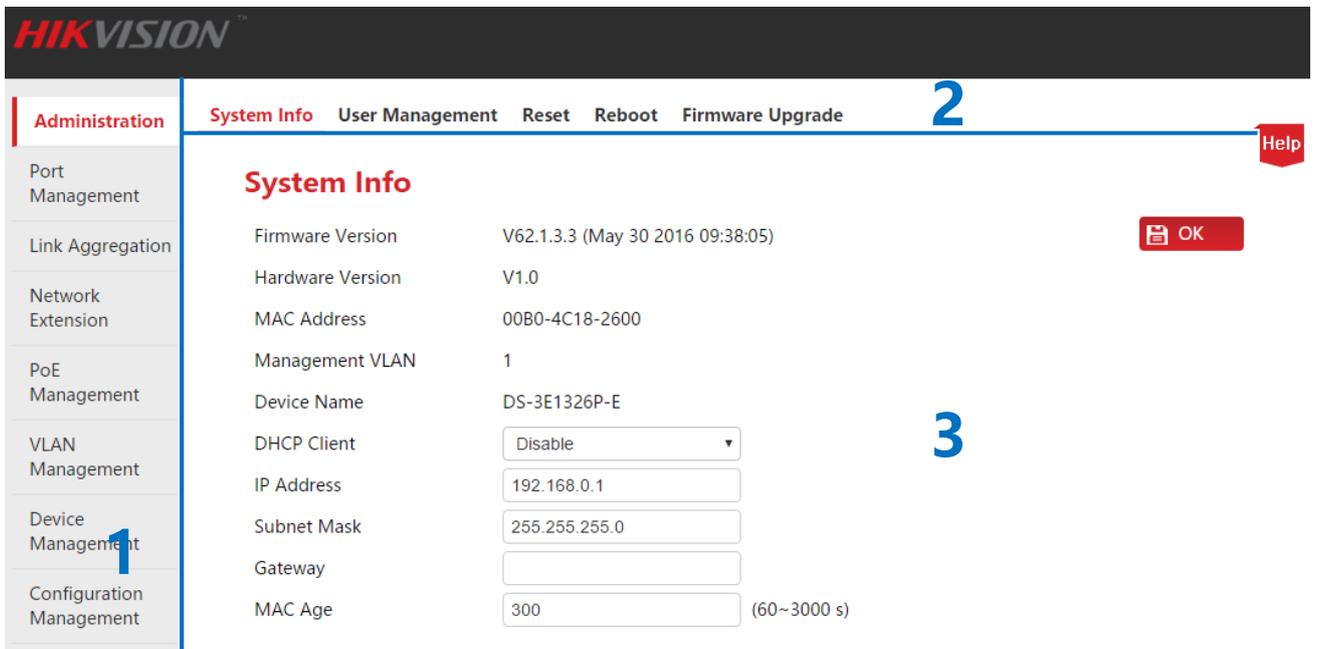
# 1.2 Logout

Click **Logout** at the top right corner of the web administration page and you will safely exit the page.



# 1.3 Layout Introduction

The Web administration page is totally divided into three parts: the first and second-level navigation bar, the third-level navigation bar, configuration zone, as shown below:



S/N	Name	Description
1	The first and second-level navigation bar	The navigation bar takes advantage of navigation tree to arrange Web function menu. It is very easy for users to select the function menu. The selected functions will be displayed in the navigation zone.
2	The third-level navigation bar	
3	Configuration zone	It is designed for users to configure and review the device.

---

 **Tip**

Click  at the top right corner and you can get a view of brief introduction of the page settings.

---

# 2 System Administration

System Administration consists of five parts: [System Info](#), [User Management](#), [Reset](#), [Reboot](#), and [Firmware Upgrade](#).

## 2.1 System Info

Here you can see the basic info of the switch, and configure the IP address or MAC aging time.

Click **Administration** to enter page.

The screenshot shows the HIKVISION web interface for System Administration. The 'Administration' menu is active, and the 'System Info' sub-menu is selected. The page displays the following configuration details:

Parameter	Value
Firmware Version	V62.1.3.3 (May 30 2016 09:38:05)
Hardware Version	V1.0
MAC Address	00B0-4C18-2600
Management VLAN	1
Device Name	DS-3E1326P-E
DHCP Client	Disable
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Gateway	
MAC Age	300 (60~3000 s)

Parameter Description:

Item	Description
Software Version	Display version info and release time.
Hardware Version	Display hardware version info.
MAC address	Display MAC address of the switch.

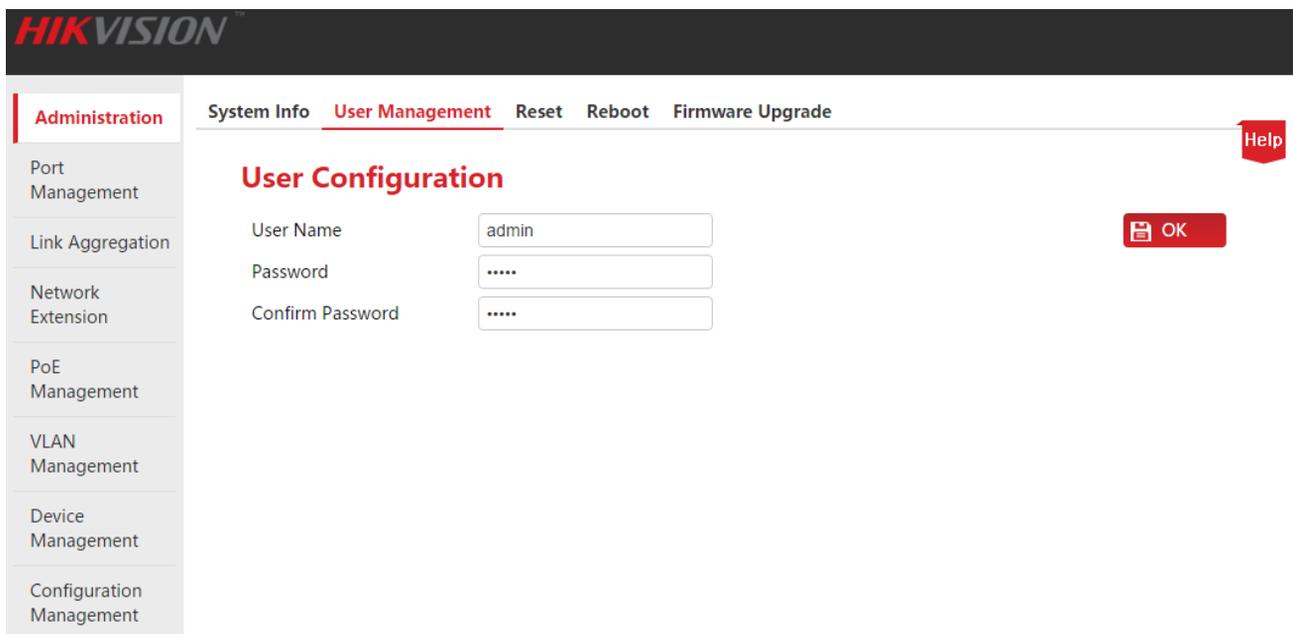
Item	Description
VLAN Management	<p>When VLAN mode is 802.1Q VLAN, the management VLAN of the switch is 1 and unavailable to be modified.</p> <p><b>⚠ Note</b></p> <p>The switch only can be visited when the computer is connected to the management VLAN port member (PVID of the port is 1).</p>
Device Name	<p>The model of the device, e.g, the name of 24-Port 10/100Mbps + 2 Gigabit Web Smart PoE Switch is “DS-3E1326P-E”.</p>
DHCP Client	<p>Enable/Disable DHCP client function.</p> <ul style="list-style-type: none"> <li>• Enable: The switch will automatically acquire IP address, subnet mask and gateway from the DHCP server.</li> <li>• Disable: Manual settings are required for IP address, subnet mask and gateway to manage the device and connect to the Internet.</li> </ul> <p><b>⚠ Note</b></p> <p>When DHCP Client is enabled, you must check the switch’s IP address from DHCP server before your next access to the Web administration and use this IP address to login.</p>
IP address	<p>The IP address of the switch. The default one is 192.168.0.1 and can be modified when DHCP client is disabled.</p> <p>Also, it is the management IP address of the switch which can be used to log in to the Web administration.</p> <p><b>⚠ Note</b></p> <p>Once IP address is altered, it is necessary to change the IP address of the governing computer to keep its network segment consistent with that of new one. And only the new IP address can be used to log in to the Web administration.</p>
Subnet Mask	<p>The subnet mask of the IP address. The default one is 255.255.255.0, and can be modified when DHCP client is disabled.</p>
Gateway	<p>It is the gateway address of the switch by default. It can be modified when DHCP client is disabled.</p>

Item	Description
MAC Time Aging	<p>It is the dynamic MAC aging time and suggested to keep the default value “300s”.</p> <p> <b>Tip</b></p> <p>Less aging time will drive the dynamic MAC address table to refresh more frequently and destination addresses in the received data packages cannot be found. As a result, the switch is only capable of broadcasting these Packages to all ports, at the price of damaging the switch performance.</p> <p>Much aging time will force the dynamic MAC address table to save up more stale addresses until it uses up all address tables. Eventually, the switch fails to refresh them upon changing network.</p>

## 2.2 User Management

Click User Management and you can modify the login User Name and Password, thus to prevent unauthorized users from accessing to the Web administration to change settings and bring about negative effects on your network.

Click **Administration > User Management** to enter the page below.



The screenshot shows the HIKVISION web interface. The top navigation bar includes 'System Info', 'User Management' (selected), 'Reset', 'Reboot', and 'Firmware Upgrade'. A 'Help' icon is in the top right. The left sidebar contains 'Administration' (selected), 'Port Management', 'Link Aggregation', 'Network Extension', 'PoE Management', 'VLAN Management', 'Device Management', and 'Configuration Management'. The main content area is titled 'User Configuration' and contains three input fields: 'User Name' with the value 'admin', 'Password' with masked characters '.....', and 'Confirm Password' with masked characters '.....'. An 'OK' button is located to the right of the password fields.

### Configuration Steps:

**1. User Name:** The character size is 1~15, only made up of letters, digits and underlines, and is started with a letter;

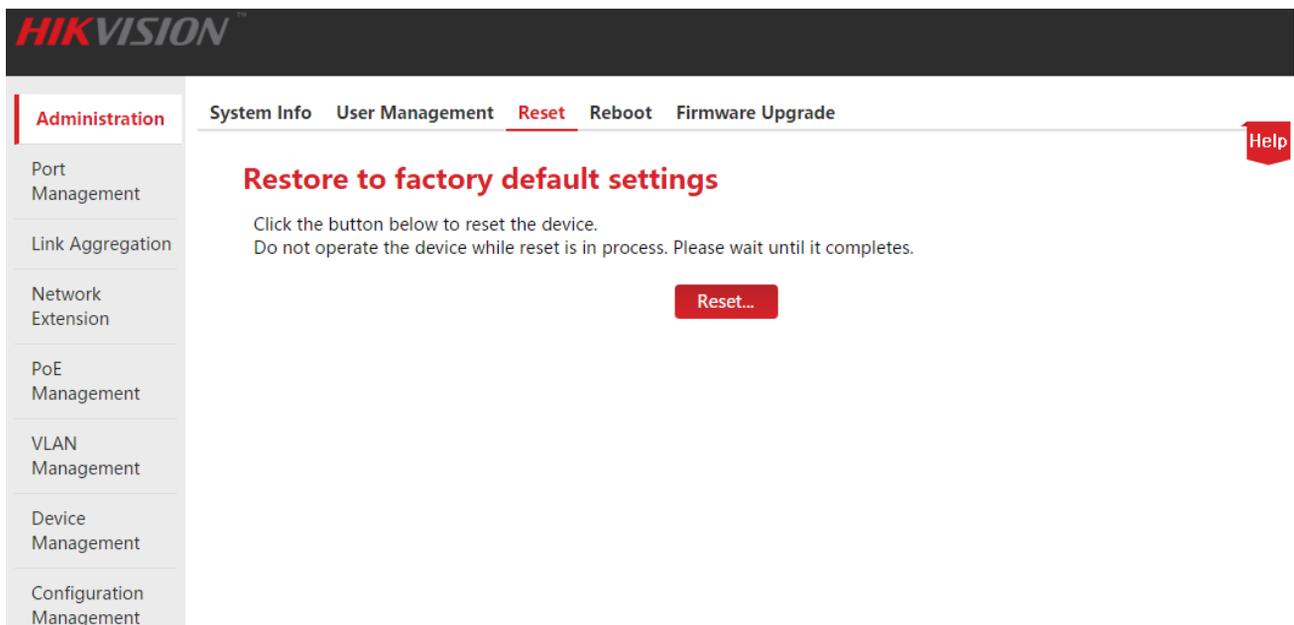
- 2. Password:** The character size is 1~15, only made up of English letters, digits, underlines and hyphens;
- 3. Confirm Password:** Enter the password once again;
- 4. Click .**

The switch will reboot automatically when new user name and password are created. The new user name and password are required for the next access to the Web administration.

## 2.3 Reset

The function of reset is available when you want to clear all configurations and restore the switch to factory default settings.

Click **Administration > Reset** to enter the page below.



In case of forgetting IP login address or user name/password, you can use the **RESET** button to reset the switch. The procedures are shown below:

- 1.** Under power-up state, use a needle-shaped object to press the **RESET** button on the front panel of the switch for 6 seconds;
- 2.** Wait for about 20 seconds until RAN LED is blinking again.

### Tip

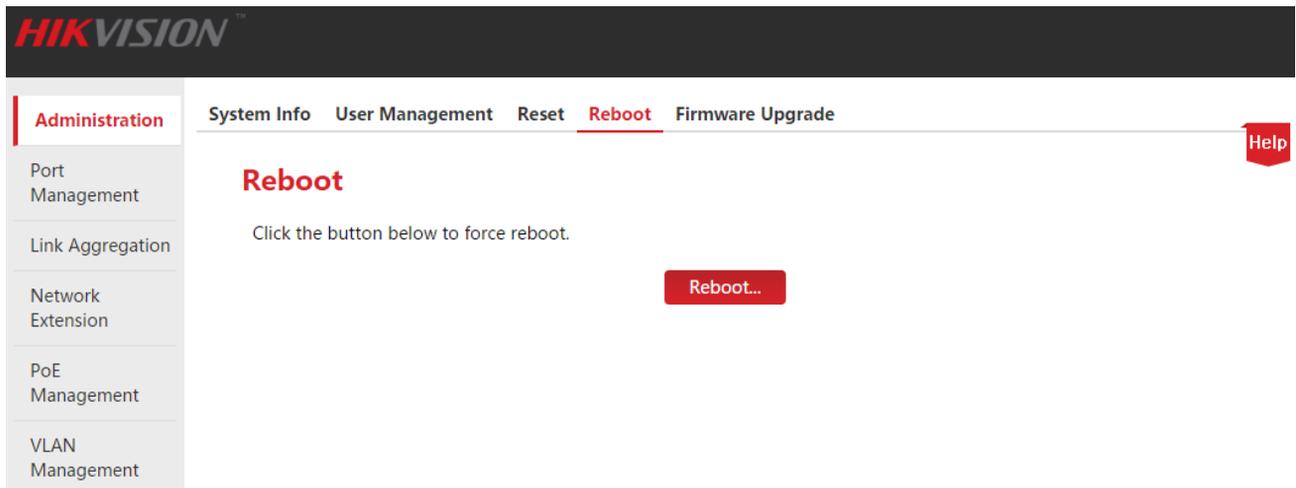
Upon resetting the switch IP address is “192.168.0.1”, user name and password are both “admin”.

## 2.4 Reboot

Reboot the switch to release partial cache, remove unwanted messages, thus to keep it running freely. Sometimes, reboot the switch to solve some problems such as deadlocks,

inability to access to the Web administrator page.

Click **Administration > Reboot** to enter the page below.



### Note

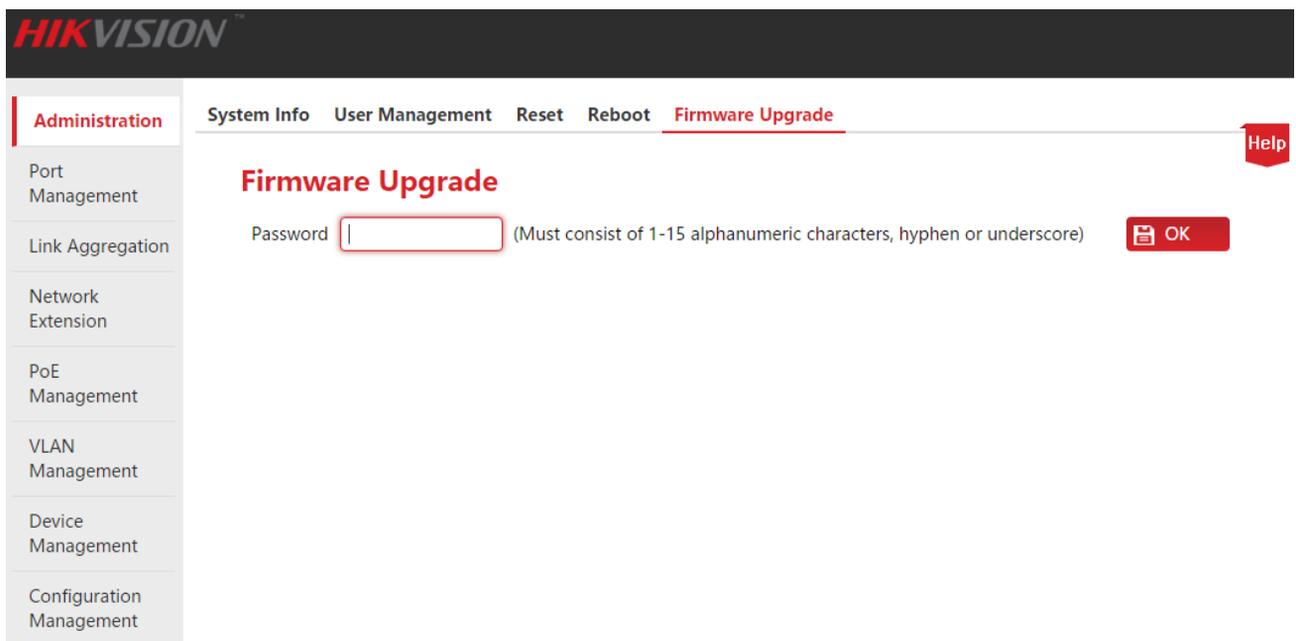
During reboot, please note that powering off will damage the switch.

## 2.5 Firmware Upgrade

Go to HIKVISION official website <http://overseas.hikvision.com/en/> to download the latest firmware corresponding to the switch for more value-added functions and more stable performance.

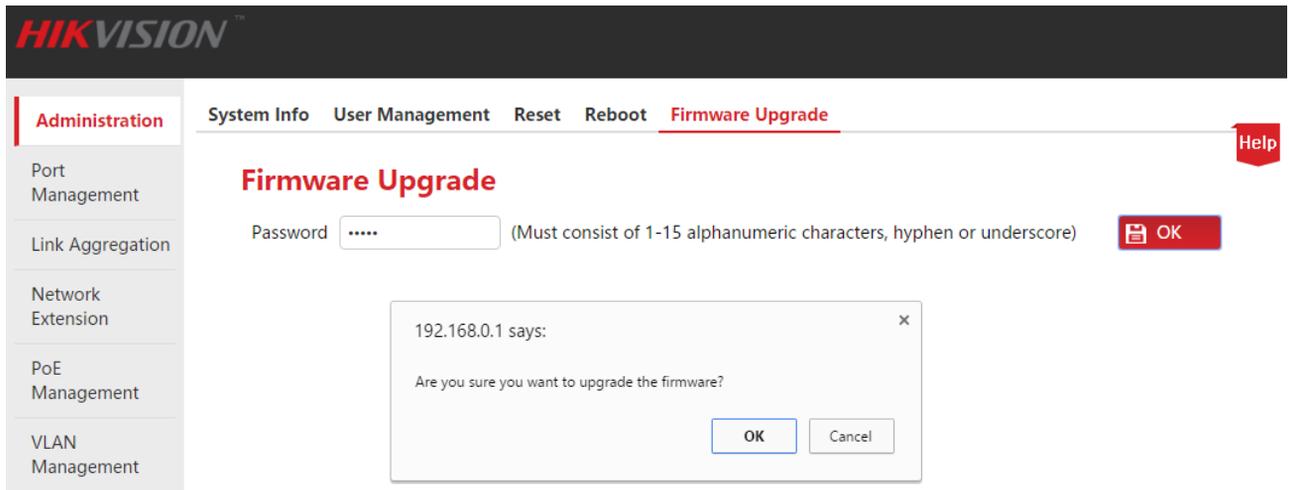
The login password is required to enter prior to firmware upgrade (the default login password is “admin”).

Click **Administration > Firmware Upgrade** to enter the verification page of firmware upgrade.



### How to upgrade software:

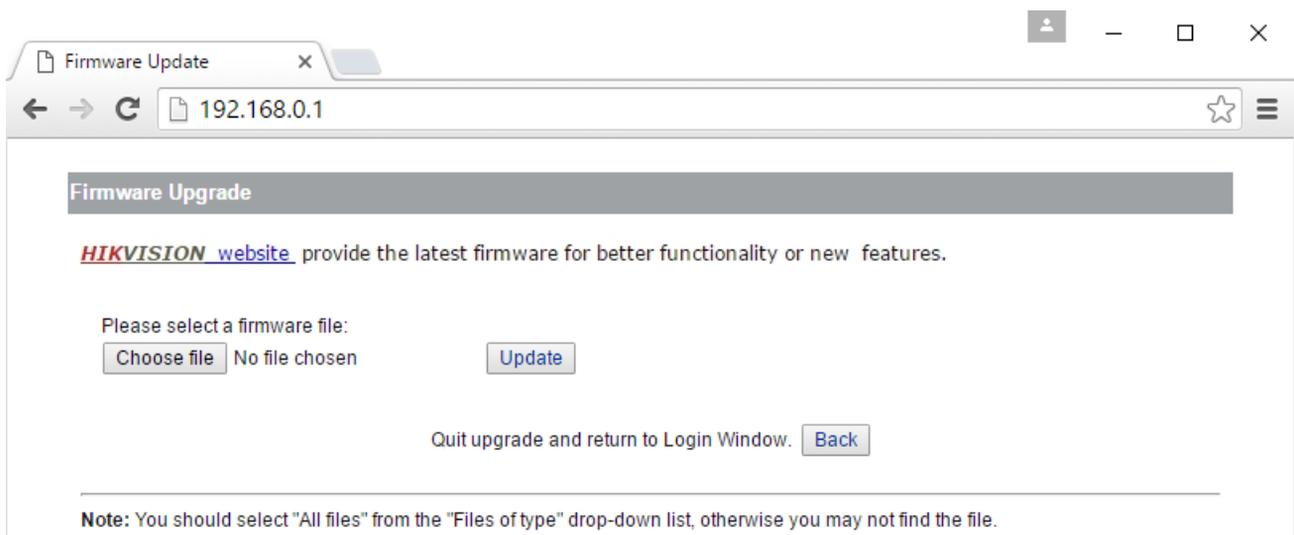
1. Go to <http://overseas.hikvision.com/en/> to download the latest upgrading file corresponding to the switch to the local computer;
2. Log in to Web administration page, then click **Administration > Firmware Upgrade** to enter the verification page of Firmware Upgrade;
3. Input the login password of the Web Administration in the input box after "Password", then click **OK** ;
4. In the pop-up dialog box, click **OK** ;



### **!** Note

During upgrade, please note that powering off will damage the switch. In case of abrupt power outage, please re-upgrade it; if unable to access to the Web Administration after the outage, please contact the technical support for maintenance.

5. In the pop-up Firmware Upgrade page below, click **Choose file** to select an upgrade file from the local computer and load it;
6. Click **Update** ;
7. In the pop-up dialog box, click **OK** ;



 **Note**

No interrupting. Wait for the button  to appear and click  when it turns highlighted. Otherwise, upgrade it again.

---

8. A progress bar is shown. When no progress is left for the progress bar, wait for the following page to appear and upon the button  turning highlighted, click .

# 3. Port Management

Port Management covers four parts: [Port Configuration](#), [Port Mirroring](#), [Statistics](#), and [Rate Limit](#).

## 3.1 Port Configuration

Here you can check and set the basic parameters of all ports. Click **Port Management** to enter the page below.

**Port Configuration**

Enable/Disable:  Speed/Duplex:

Priority:  Flow Control:

Storm Control:  Address Learning:

<input type="checkbox"/>	Port	Link Status	Speed/Duplex	Priority	Flow Control	State	Storm Control	Address Learning
<input type="checkbox"/>	1	100M_FDX	Auto	High	Enable	Enable	Disable	Enable
<input type="checkbox"/>	2	100M_FDX	Auto	High	Enable	Enable	Disable	Enable
<input type="checkbox"/>	3	---	Auto	High	Enable	Enable	Disable	Enable
<input type="checkbox"/>	4	---	Auto	High	Enable	Enable	Disable	Enable
<input type="checkbox"/>	5	---	Auto	High	Enable	Enable	Disable	Enable
<input type="checkbox"/>	6	---	Auto	High	Enable	Enable	Disable	Enable
<input type="checkbox"/>	7	---	Auto	High	Enable	Enable	Disable	Enable
<input type="checkbox"/>	8	100M_FDX	Auto	High	Enable	Enable	Disable	Enable
<input type="checkbox"/>	9	---	Auto	Low	Enable	Enable	Disable	Enable
<input type="checkbox"/>	10	100M_FDX	Auto	Low	Enable	Enable	Disable	Enable

Parameter setting specification:

Item	Description
<input type="checkbox"/>	Check the box in front of the corresponding port number to select that port. Check the box at the top to select all of the ports.
Enable/Disable	<p>Enable/Disable the port.</p> <ul style="list-style-type: none"> <li><b>Enable:</b> Enable the forwarding function of the selected port.</li> <li><b>Disable:</b> Disable the forwarding function of the selected port.</li> </ul>

Item	Description
Enable/Disable (Continued)	<p> <b>Note</b></p> <p>Only when a port is enabled can it forward data properly. Disable an unused port, reopen it when needed, to reduce the power consumption.</p>
Speed/Duplex	<p>Select the transmission speed and mode of the port.</p> <p>FDX refers to Full Duplex, meaning that the port can receive and send messages at the same time; HDX refers to Half Duplex, meaning that the port can either receive or send messages at the same time.</p> <p>Port G1/SFP1 and G2/SFP2 support 1000M/FDX and Auto-negotiation; other ports support 10M/FDX, 10M/HDX, 100M/FDX, 100M/HDX and Auto-negotiation.</p> <p>When the switch is being linked with the terminal network equipment, make sure of the speed and duplex according with the two ports to keep nice communication.</p> <p>Generally, to keep the default setting <b>Auto</b>.The transmission speed and mode will be determined by the auto-negotiation of the local port and the terminal port.</p>
Priority	<p>Select the port priority when setting QoS.</p>
Flow Control	<p>Enable/disable the flow control function of the selected port.</p> <p>When the flow control of the switch and the terminal equipment are all enabled, if some port congestion of the switch occurs, the port will send the pause frame to the terminal equipment that will be suspended to send data after receiving the pause frame; meanwhile, when one port of the switch receives a pause frame, the port also will be paused to send data.</p> <p>By default, the port flow control is enabled.</p> <p> <b>Note</b></p> <p>Enable the flow control to avoid the data packet loss caused by the inconsistency of the sending and receiving rate. Yet that will also affect the communication rate of the data source port and other facilities. Please be careful with this function when linking the network port.</p>

Item	Description
Storm Control	<p>Enable/disable the broadcasting storm control function of the selected port. By default, the storm control is disabled.</p> <p>Broadcast storm means that the broadcasting frame quantities are soaring up due to the continuous transmissions, which brings negative effect on the communication, degrades the system performance and even results in breakdown of the network.</p> <p>While enabling the storm control, the switch will discard the excessive broadcasting messages as the broadcast traffic on the port exceeds the limited value (2000pps), thus reducing the proportion of the broadcast traffic to the limited range.</p>
Address Learning	<p>Enable/disable the address learning function of the selected port.</p> <p>While enabling the address Learning, if no corresponding MAC address in the MAC address table as the switch receives the data package, it will broadcast this package to all ports. The switch will record the corresponding MAC port to the MAC table when the destination host returns some information from one port.</p> <p>The MAC address table keeps the system port corresponding with the MAC address of the host linking with that port.</p> <p> <b>Tip</b></p> <p>While enabling the function <a href="#">MAC Binding</a>, the MAC address learning function of this port will be automatically disabled.</p>

Parameter description of the display list:

Item	Description
Port	Display the port number.
Link State	Display the actual speed and duplex, if not connected or linked failure, it will be shown as “---”.
Speed/Duplex	Display the current speed and duplex of the port.
Priority	Display the priority of the port.
Flow Control	Display the enable/disable state of the port flow control.
State	Display the enable/disable state of the port.

Item	Description
Storm Control	Display if the storm control function of the port is enabled.
Address Learning	Display if the address learning function of the port is enabled.

## 3.2 Port Mirroring

### 3.2.1 Overview

The function of port mirroring provided by the switch realizes the data duplication from one or several ports (the source ports) to the specified port (the mirroring destination port). The data monitoring equipment connected with the destination port enables the network administrator to monitor the traffic, analyze the performance and diagnose the fault real-time.

#### 📌 The Basic Concept of Port Mirroring

##### 1. Source Port

As the ports monitored, users are allowed to monitor and analyze the message passing through the source port. All messages' monitoring can be achieved on the condition that the source port is set as a routed port (i.e. the port accessing to the Internet).

##### 2. Mirroring Destination Port

The mirroring destination port, called monitor port as well, monitors and analyzes the messages by forwarding the received ones to the data monitoring equipment.

The speed of mirroring destination port is bound to be not less than all the source ports combined.

##### 3. Sniffer Mode

Three kinds of mirroring port directions are listed below.

- Ingress: The mirroring is specific to the messages received through the source ports.
- Egress: The mirroring aims at the messages sent by the source ports.
- Egress & Ingress: The mirroring aims at messages both received and sent by the source ports.



#### Tip

The duplication of the same data flow is processed only once by the switch. For example, a data flow sent by port 2 and received by port 1 will be mirrored only once to the mirroring destination port.

---

### 📌 The Port Mirroring Type Supported by the Switch

The series of HIKVISION Smart PoE Switches only support local port mirroring, which means the source ports and destination port are on the same switch.

## 3.2.2 Port Mirroring Configuration

Click **Port Management > Port Mirroring** to enter the page below.

The screenshot shows the HIKVISION web interface for configuring port mirroring. The sidebar on the left includes 'Administration', 'Port Management' (selected), 'Link Aggregation', 'Network Extension', 'PoE Management', 'VLAN Management', 'Device Management', and 'Configuration Management'. The main content area is titled 'Mirroring Port' and has tabs for 'Port Configuration', 'Port Mirroring' (active), 'Statistics', and 'Rate Limit'. There is a 'Help' button in the top right. The configuration includes a 'Mirroring Destination Port' dropdown, a 'Sniffer Mode' dropdown (set to 'None'), and an 'OK' button. Below these is a table with 10 rows, each representing a source port (1-10) and a 'Mirroring State' checkbox, all of which are currently unchecked.

Source Port	Mirroring State
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>
9	<input type="checkbox"/>
10	<input type="checkbox"/>

### How to configure port mirroring:

1. Mirroring destination port: Select a port as the destination port;
2. Mirroring state: Check corresponding boxes to make the ports as source ports;
3. Sniffer Mode: Select the direction;
4. Click **OK**.

Parameter Description:

Item	Description
Mirroring Destination Port	Select the mirroring destination port of the switch. The blank is perceived to close the mirroring function. The bandwidth of the sole mirroring destination port is supposed to be more than or equal to the sum of source ports.

Item	Description
Mirroring Destination Port (Continued)	<p> <b>Note</b></p> <ul style="list-style-type: none"> <li>The same port is not allowed to be set as the destination port and the source port at the same time.</li> <li>The source ports can be set after the mirroring destination port is set.</li> <li>The mirroring destination port should be excluded from any aggregation group.</li> <li>Once STP function is enabled, any port cannot be set to mirroring destination port.</li> </ul>
Sniffer Mode	<p>Select the mirroring direction; otherwise, it is regarded as the disabled mirroring function.</p> <ul style="list-style-type: none"> <li>Ingress: Copy the data received by the source ports to the destination port.</li> <li>Egress: Copy the data sent by the source ports to the destination port.</li> <li>Egress &amp; Ingress: Copy both the data received and sent by the source ports to the destination port.</li> </ul> <p> <b>Note</b></p> <p>Package loss arises supposing that the sum of the bandwidth of the source ports is greater than that of the mirroring destination port.</p>
Source Port	<p>Display the port of the switch.</p> <p> <b>Tip</b></p> <p>The port selected as a mirroring destination port is prohibited to be a source one simultaneously.</p>
Mirroring State	<p>Select the source ports of the switch.</p>

## 3.2.3 Application Scenarios

### Networking Demand

The following is an enterprise user's network environment.

- Division 1 accesses switch C through port 1.
- Division 2 accesses switch C through port 2.
- The server is connected to the port 3 of the switch C.

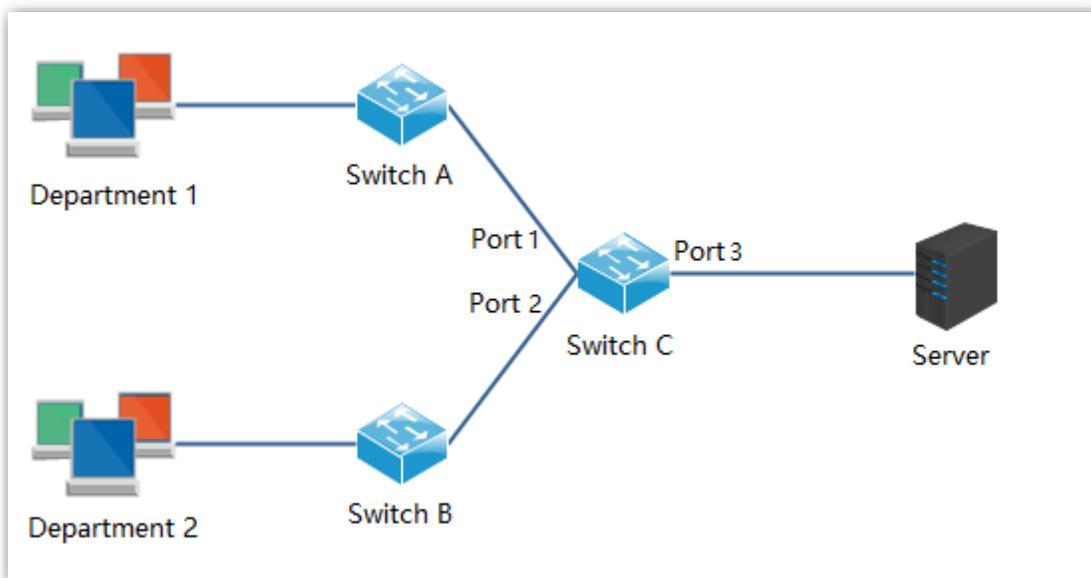
Demand: The monitoring of the messages received and sent by division 1 and division 2 is expected to be implemented through the server.

### Networking Analyses

Specified as follows, the demand is realized by making use of the port mirroring.

- Port 1 and port 2 are selected to be the source ports of mirroring with "Egress & Ingress".
- Port 3 connected with the server is set as the mirroring destination port.

### Networking Diagram



### Configuration Steps

1. Log in to the Web administration page of the switch C, then click **Port Management > Port Mirroring** to enter the setting page;
2. Mirroring Destination Port: select "3";
3. Mirroring State: Check the source port 1 and 2;
4. Sniffer Mode: Select "Egress & Ingress";
5. Click **OK**.

**Mirroring Port**

Mirroring Destination Port: 3

Sniffer Mode: Egress & Ingress

Source Port	Mirroring State
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

### 3.3 Port Statistics

Here you can check and clear the data flow statistics of all ports.

Click **Port Management > Statistics** to enter the page below.

**Port Statistics**

Statistics Mode: TX & RX

Port	TX	RX
1	269642	346630
2	427945	216664
3	0	0
4	0	0
5	0	0
6	12693	11905
7	0	0
8	5871	3764
9	0	0
10	122785	21409

Buttons:

**Clear**

Clear the statistics in the current page and collect statistics again.

**Refresh**

Refresh the statistics in the current page.

Parameter Description:

Item	Description
Statistics Mode	<p>Select the statistics mode.</p> <ul style="list-style-type: none"> <li><b>TX &amp; RX:</b> Display the number of data packages transmitted and received by the port.</li> <li><b>Collision &amp; TX:</b> Display the number of data packages conflicting and transmitted by the port.</li> <li><b>Drop &amp; RX:</b> Display the number of data packages discarded and received by the port.</li> <li><b>CRC Error &amp; RX:</b> Display the number of data packages after CRC testing and received by the port.</li> </ul>

### 3.4 Rate Limit

Here you can set the Tx Rate and Rx Rate of **Downlink Ports**.

Click **Port Management > Rate Limit** to enter the page below.

The screenshot shows the Hikvision web interface for Rate Limit configuration. The navigation menu on the left includes Administration, Port Management (selected), Link Aggregation, Network Extension, PoE Management, VLAN Management, Device Management, and Configuration Management. The main content area is titled 'Rate Limit' and features two dropdown menus for 'Tx Rate(bps)' and 'Rx Rate(bps)', both set to 'Make no change'. There are two buttons: 'OK' and 'Unlimited'. Below these is a table with the following data:

<input type="checkbox"/>	Port	Tx Rate(kbps)	Rx Rate(kbps)	Link Speed
<input type="checkbox"/>	1	--	--	100Mbps
<input type="checkbox"/>	2	--	--	100Mbps
<input type="checkbox"/>	3	--	--	---
<input type="checkbox"/>	4	--	--	---
<input type="checkbox"/>	5	--	--	---
<input type="checkbox"/>	6	--	--	---
<input type="checkbox"/>	7	--	--	---
<input type="checkbox"/>	8	--	--	100Mbps
<input type="checkbox"/>	9	--	--	---

Buttons:

**Unlimited** Clear all sets of Rate Limit. All ports receive and transmit the data frame in an actual link speed.

Parameter Description:

Item	Description
Tx Rate (bps)	Set the data transmitting rate of the selected port.
Rx Rate (bps)	Set the data receiving rate of the selected port.
<input type="checkbox"/>	Check the box in front of the corresponding port number to select that port. Check the box at the top to select all of the ports.

Parameter description of the display list:

Item	Description
Port	<p>Check the box in front of the corresponding port number to set the rate limit.</p> <p>The rate limit is only available for the downlink ports, not available for the uplink ports (G1/SFP1, G2/SFP2).</p>
Tx Rate (kbps)	Display the transmitting rate limit of the port. "--" shows that the port will transmit the data in an actual link speed.
Rx Rate (kbps)	Display the receiving rate limit of the port. "--" shows that the port will receive the data in an actual link speed.
Link Speed	Display the negotiated link speed of the port. If not connected or negotiated failure, it will be shown as "---".

# 4 Link Aggregation

## 4.1 Overview

Link Aggregation means that multiple physical ports are aggregated to a logical group. At the same group, multiple physical links are regarded as one logical link. Link Aggregation makes the load sharing among the ports of the aggregation group possible, which will expand the bandwidth. Meanwhile, the dynamic replication exits among the ports of the same aggregation group, which will improve the link reliability.

At the same group, all ports settings shall be accordant, including STP, VLAN, Address Learning and Port Management. Detailed specifications are as below:

- At the same group, the STP (State, Priority, and Path Cost), VLAN (PVID, Tag Processing Policy) and Port (Enable/Disable status, Speed/Duplex, Priority, Flow Control, Storm Control, Address Learning) shall be consistent in configuration.
- For the ports at the aggregation group, following function settings are not available: Static Port MAC Address Binding, Mirroring Destination Port.
- The port which has enabled the mirroring destination port is not allowed to join the aggregation group.

## 4.2 Link Aggregation Configuration

Click **Link Aggregation** to enter the page below.

The screenshot shows the HIKVISION web interface for Link Aggregation configuration. The left sidebar contains navigation options: Administration, Port Management, Link Aggregation (selected), Network Extension, PoE Management, VLAN Management, Device Management, and Configuration Management. The main content area is titled 'Link Aggregation' and 'Aggregation Algorithm'. A dropdown menu is set to 'SMAC & DMAC'. A table lists three aggregation groups with their member ports and status.

Aggregation Group	Member Ports				Status
1	P1 <input checked="" type="checkbox"/>	P2 <input checked="" type="checkbox"/>	P3 <input checked="" type="checkbox"/>	P4 <input checked="" type="checkbox"/>	<input type="checkbox"/>
2	P5 <input checked="" type="checkbox"/>	P6 <input checked="" type="checkbox"/>	P7 <input checked="" type="checkbox"/>	P8 <input checked="" type="checkbox"/>	<input type="checkbox"/>
3	G1/G1-F <input checked="" type="checkbox"/>	G2/G2-F <input checked="" type="checkbox"/>			<input type="checkbox"/>

## Parameter Description:

Item	Description
Aggregation Algorithm	<p>Select Aggregation Algorithm.</p> <ul style="list-style-type: none"><li>• Port ID: All member ports of the group fulfill the load sharing based on the Port ID of the receiving data.</li><li>• SMAC: All member ports of the group fulfill the load sharing based on the Source MAC Address of the receiving data.</li><li>• DMAC: All member ports of the group fulfill the load sharing based on the Destination MAC Address of the receiving data.</li><li>• SMAC &amp; DMAC: All member ports of the group fulfill the load sharing based on the Source MAC Address + Destination MAC Address of the receiving data.</li></ul>
Aggregation Group	Display the number of the aggregation group.
Member Ports	Display the ports that can join the aggregation group in the switch. Check the box right after the corresponding port number to select that port.
Status	Enable/Disable the aggregation group.

# 5 Network Extension

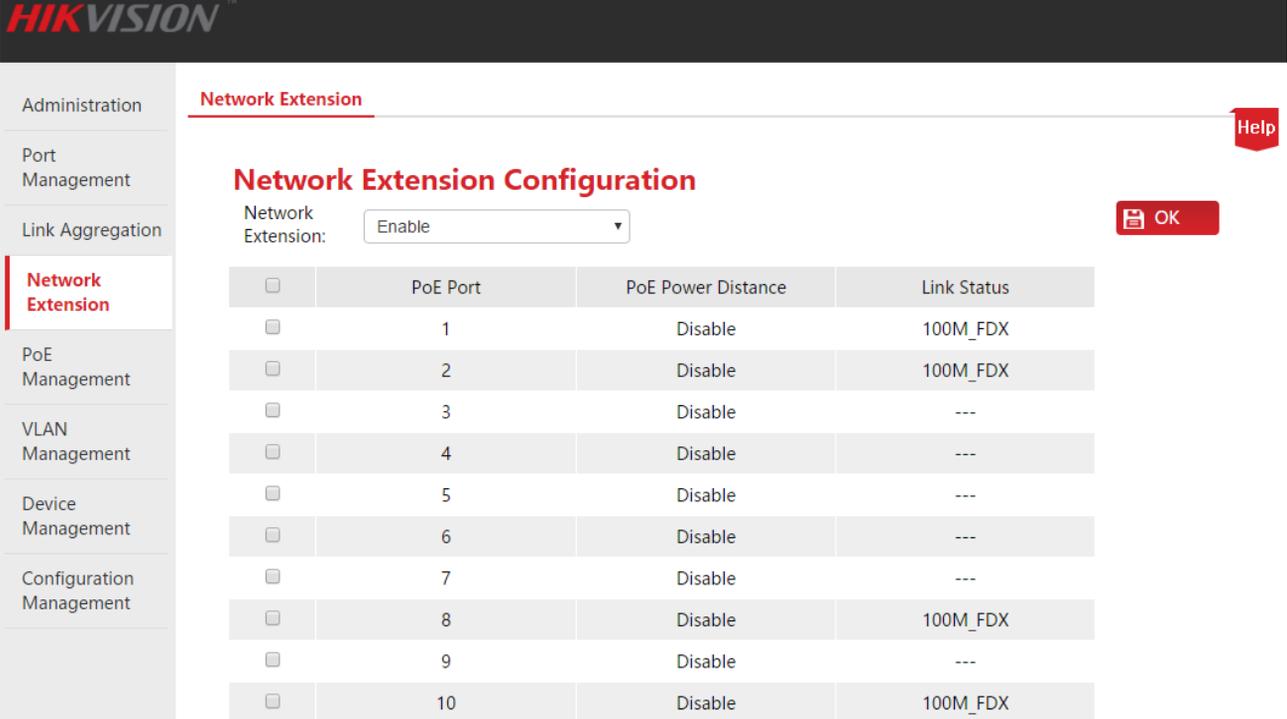
HIKVISION Web Smart PoE switch series offer you the Network Extension, which can extend the data transmission and PoE Power Distance of the **Downlink Ports** to make network deploy more convenient.

The port link speed will be automatically negotiated to 10Mbps once the Port Extension is enabled, at this time, if using the CAT5E cable or above, the data transmission and PoE power distance can break 100 meters and reach 250 meters.

## Note

Please ensure the terminal device port Speed and Duplex as “Auto-negotiation” to avoid link negotiation failure when enabling the Port Extension.

Click **Network Extension** to enter the page below.



<input type="checkbox"/>	PoE Port	PoE Power Distance	Link Status
<input type="checkbox"/>	1	Disable	100M_FDX
<input type="checkbox"/>	2	Disable	100M_FDX
<input type="checkbox"/>	3	Disable	---
<input type="checkbox"/>	4	Disable	---
<input type="checkbox"/>	5	Disable	---
<input type="checkbox"/>	6	Disable	---
<input type="checkbox"/>	7	Disable	---
<input type="checkbox"/>	8	Disable	100M_FDX
<input type="checkbox"/>	9	Disable	---
<input type="checkbox"/>	10	Disable	100M_FDX

## How to enable (or disable) the Port Extension:

- : Check the box in front of the corresponding port number to select that port;
- Network Extension: Click the pull-down menu to select to “Enable” (or “Disable”) the Port Extension;
- Click  to end the setup.

Parameter Description:

Item	Description
Network Extension	Enable/Disable Network Extension function of the selected ports.
<input type="checkbox"/>	<p>Check the box in front of the corresponding port number to select that port. Check the box at the top to select all of the ports.</p> <p> <b>Tip</b></p> <p>Once a port's Network Extension function is enabled, the port only supports 10Mbps Full/Half Duplex communication.</p>
PoE Port	Display the number of the port which can support PoE power.
PoE Power Distance	Display the enable/disable status of the PoE Power Distance.
Link Status	Display the Speed and Duplex of the port. If not connected or negotiated failure, it will be shown as "---".

# 6 PoE Management

All **Downlink Ports** support PoE power supply and conform to IEEE 802.3af and IEEE 802.3at. The switch will automatically supply required PoE power to the powered device which is connected with the PoE port.

Click **PoE Management** to enter the page below. You can check the PoE power status of the current switch and enable/disable the PoE power function of the downlink port as well.



**Tip**

By default, the PoE power function of all switch downlink ports is enabled.

**HIKVISION**

Administration | **Global Settings** | Help

Port Management

Link Aggregation

Network Extension

**PoE Management**

VLAN Management

Device Management

Configuration Management

**PoE Power**

Consumption Power: 1.8W

Remaining Power: 368.2W

OK

**PoE Status**

Make no change

<input type="checkbox"/>	Port	PoE Status	Power Supplied[W]
<input type="checkbox"/>	1	Enable	0.0
<input type="checkbox"/>	2	Enable	1.8
<input type="checkbox"/>	3	Enable	0.0
<input type="checkbox"/>	4	Enable	0.0
<input type="checkbox"/>	5	Enable	0.0
<input type="checkbox"/>	6	Enable	0.0
<input type="checkbox"/>	7	Enable	0.0
<input type="checkbox"/>	8	Enable	0.0

Parameter Description:

Item	Description
PoE status	Enable/Disable the PoE power function of the selected port.
<input type="checkbox"/>	Check the box in front of the corresponding port number to select that port. Check the box at the top to select all of the ports.

Parameter description of the display list:

<b>Item</b>	<b>Description</b>
Consumption Power	Display the total output power of the switch that has been consumed.
Remaining Power	Display the remaining output power of the switch.
Port	Display the downlink port number of the switch.
PoE Status	Display PoE power status of the downlink port (Enable/Disable).
Power Supplied[W]	Display the supplied output power of the downlink port.

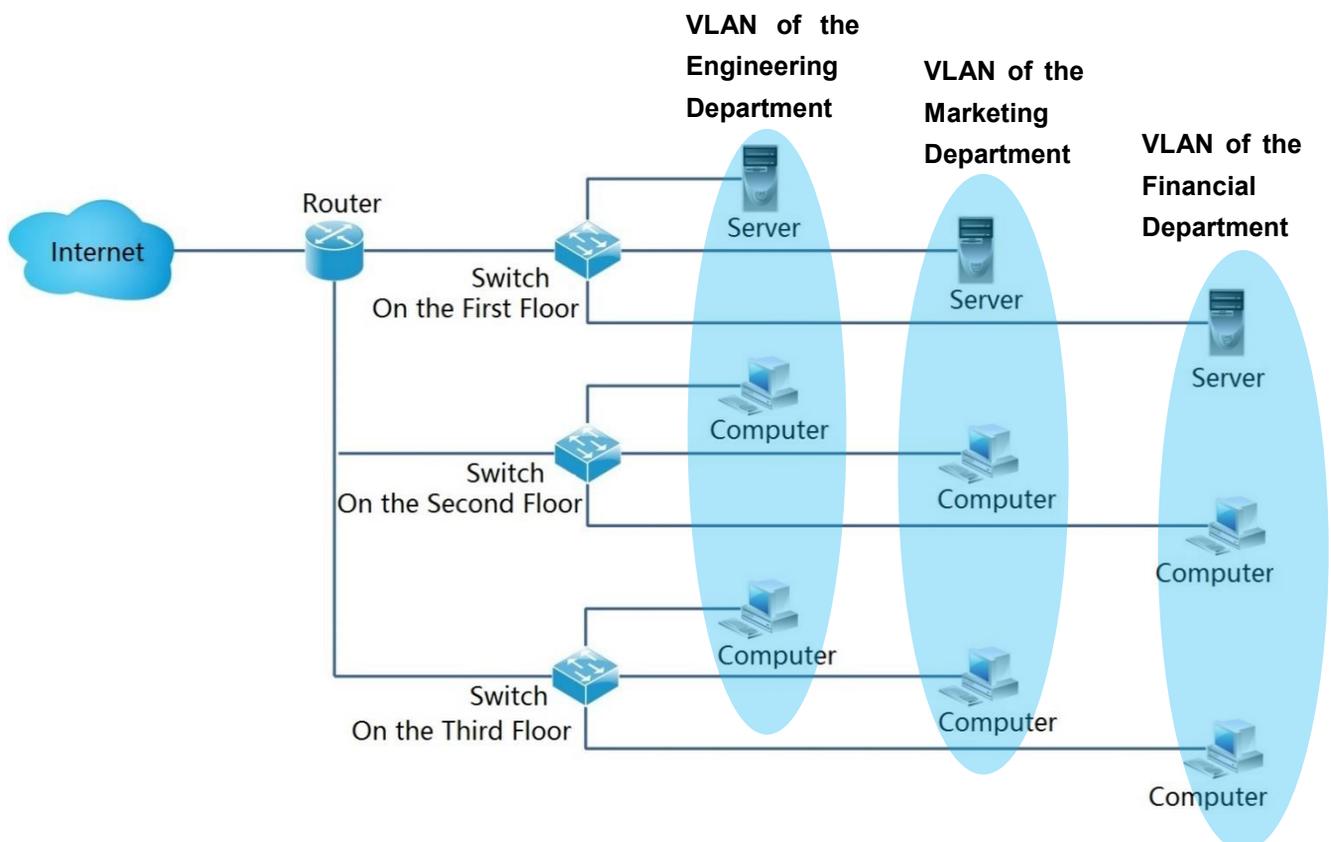
# 7 VLAN Management

## 7.1 Overview

In the traditional shared media Ethernet and Switched Ethernet, all the users are in the same broadcast domain. The growing number of the broadcast packet with the more and more in-network computers leads to the great increase of the data traffic among all intranet devices, which influence the network performance. The possible broadcast storm brought by the continuous extension of the network is likely to make the entire network unavailable.

VLAN (Virtual Local Area Network), is a data exchange technology in the realized virtual work group, by the means of splitting the devices in local area network into multiple network segments logically instead of physically. The technology logically divides one local area network into several ones—VLAN. Free from the limitation of the geographical location, the VLAN intra-group hosts of the same broadcast domain achieve the mutual exchange normally, just as connected in the same network segment. The hosts of the different VLAN are obliged to exchange through a router or a layer 3 switch that supports VLAN function rather than communicate directly, as a result of interlock broadcast isolation.

The following diagram shows how to use VLAN:



The followings are the advantages of VLAN:

- Improve the network performance. This technology confines the broadcast packages in a local area network within a single VLAN to save the network bandwidth and improve the capacity.

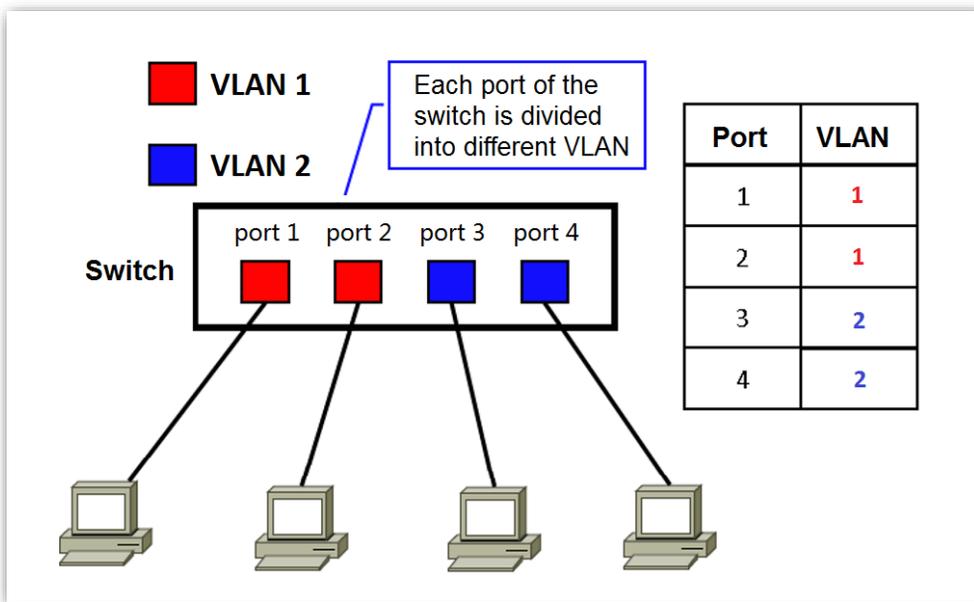
- Reduce the investment on devices. VLAN technology realizes the achievable control of network management cost, instead of increase of that in the traditional broadcast storm isolation using router.
- Simplify network management. The VLAN establishes virtual work groups across the geographical network. As long as locating geographically in the range of the virtual local area network, the user is capable of accessing to the network without altering the configuration.
- Ensure the network security. The mutual communication between the distinct VLAN hosts is not permitted to conduct directly, instead, it is realized exclusively through a router or a layer 3 switch that supports VLAN function. And that strengthens the security between the different departments in an enterprise network.

Three VLAN modes are supported by HIKVISION Smart PoE Switch series: Port VLAN, ONE-KEY VLAN and 802.1Q VLAN.

### 👉 Port VLAN

Port VLAN function is based on physical ports and is only supported on the same switch. In this case, physical ports in the same VLAN on the same switch can communicate with each other.

As shown below, the 4 ports of one switch are divided into 2 different VLAN: Port 1 and 2 into VLAN 1, and port 3 and 4 into VLAN 2.



The communication between the VLAN ports divided into the identical VLAN is permitted only. Therefore in the above example, port 1 can communicate with port 2 solely, the same as port 3 and 4.

### ➤ ONE-KEY VLAN

ONE-KEY VLAN divides VLAN in view of port essentially.

Enabling ONE-KEY VLAN function makes every downlink port of switch and the uplink port (G1/SEP1 and G2/SEP2) into one respective VLAN automatically. The communication is allowed to happen between downlink and uplink ports, but not within the downlink ports to assure security network effectively.

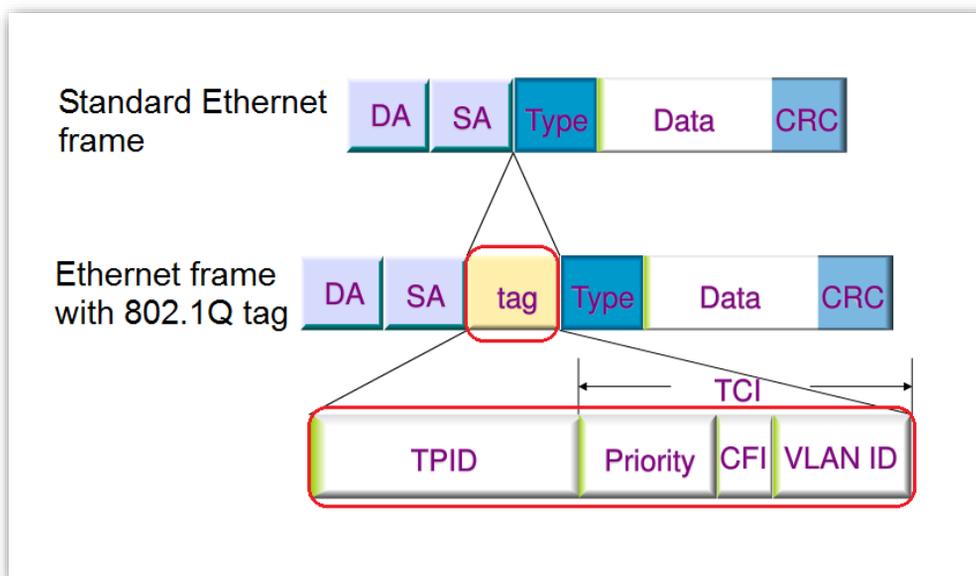
#### ⚠ Note

- Prior to enabling “ONE KEY VLAN”, please link the port G1/SFP1, G2/SFP2 to the central switching device.
- This mode is suggested to be enabled in case of the DHCP conflict resulting from the wireless router connected privately to the switch.

### ➤ 802.1Q VLAN

The VLAN interworking of different manufacturers’ equipment is ensured by the 802.1Q standard issued by IEEE in 1999 for defining the VLAN international standard.

As required in 802.1Q protocol, one 4 bytes 802.1Q VLAN tag is bound to be wrapped behind the destination MAC address and the source MAC address of the Ethernet frame for identifying the relevant information of VLAN. As shown below, the Ethernet frame with 802.1Q tag is produced by adding an 802.1Q VLAN tag behind the destination MAC address and the source MAC address of the standard Ethernet frame.



The information in the 802.1Q tag is specified as following:

Field	Specification
TPID	Identify the data frame with the 802.1Q VLAN Tag. This field’s length is 2 bytes, or 16 bit. IEEE 802.1Q protocol defines the value of it to be 0x8100.

Field	Specification
Priority	Identify the priority of data frame and send the high priority data packets in advance when the switch is blocked. The value range of this 3 bits field is <0~7> with 7 displaying the highest priority and 0 the lowest.
CFI	Identify whether the MAC address is wrapped in a standard format. The field length is 1 bit. The standard format wrap of MAC address is indicated by 0, otherwise by 1. The default value of the Ethernet switch is 0.
VID	VLAN ID is used to identify the message belonging to 802.1Q VLAN. The value range of this 12 bit field is <0~4095>, more accurately, that of VID is <1~4094> for 0 and 4095 is barely used.

## 7.2 Port VLAN

### 7.2.1 Configuration Wizard

The following is concerned with how to configure the port VLAN of HIKVISION Web Smart PoE switch and configuration tasks:

Steps	Configuration Tasks	Specification
1	<a href="#">7.2.2.1 VLAN Mode Toggle</a>	Optional. VLAN mode is port VLAN by default.
2	<a href="#">7.2.2.2 VLAN Division</a>	<b>Mandatory.</b> No VLAN division by default.

### 7.2.2 VLAN Port Configuration

Please toggle VLAN Mode before division of VLAN.

#### 7.2.2.1 VLAN Mode Toggle

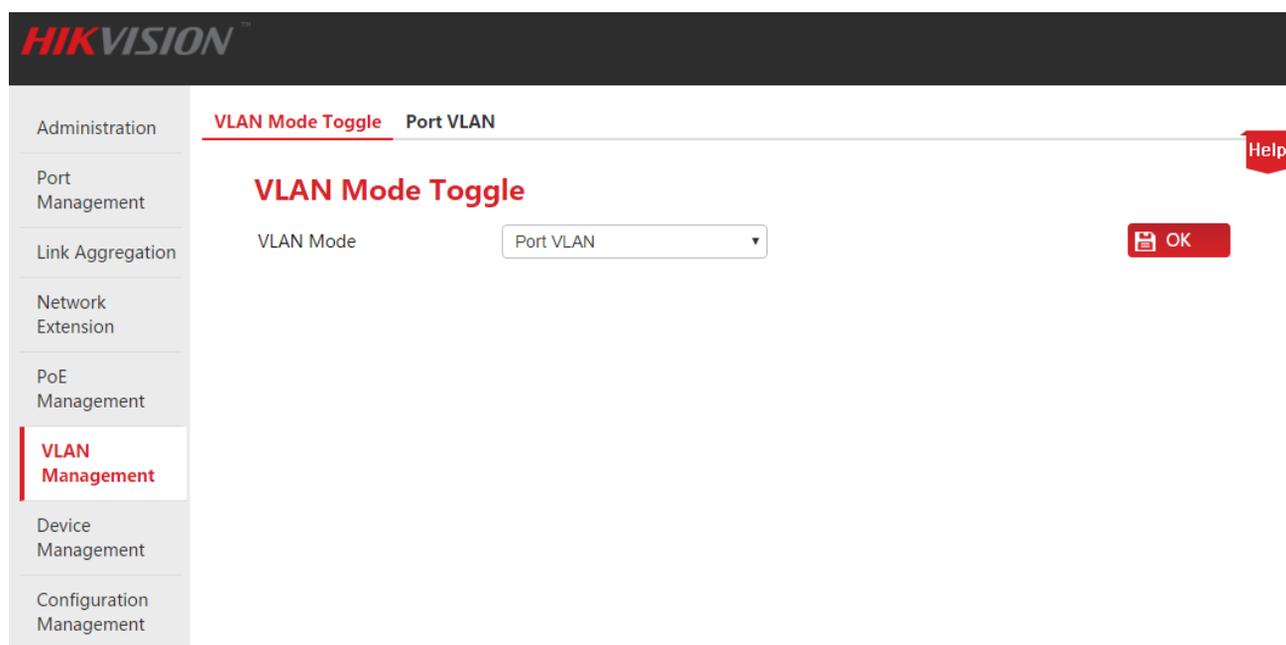
Toggle the VLAN mode to port VLAN.

#### Configuration Steps:

1. Log in to the Web administration and then go to **VLAN Management** page;

2. VLAN Mode: Select “Port VLAN”;

3. Click **OK**.



### 7.2.2.2 VLAN Division

This part takes the form of example to describe how to add, delete and modify port VLAN and how to restore VLAN port configuration to the factory settings.

#### Add Port VLAN

Suppose to add the port 2, 3, G1/SFP1, G2/SFP2 to VLAN2.

#### Configuration Steps:

1. Log in to the Web administration and go to **VLAN Management > Port VLAN** page;
2. Select: Check the  before Port No. to select the port to be set;

#### Tip

Check the  at the top to select all of ports.

3. VLAN List: In the following input box, enter the VLAN ID of the selected ports in Step 2;

**VLAN Port Configuration**

Select	Port List	VLAN List	Option
<input type="checkbox"/>	2-3,25-26	2	+Add -Del
<input type="checkbox"/>	1	1	Mod
<input checked="" type="checkbox"/>	2	1	Mod
<input checked="" type="checkbox"/>	3	1	Mod
<input type="checkbox"/>	4	1	Mod
<input checked="" type="checkbox"/>	G1/G1-F	1	Mod
<input checked="" type="checkbox"/>	G2/G2-F	1	Mod

\*Because of layout, the sample picture doesn't display middle ports.

4. Operate: Click **+Add** to end the setup. The outcome is shown in the page below.

**VLAN Port Configuration**

Select	Port List	VLAN List	Option
<input type="checkbox"/>			+Add -Del
<input type="checkbox"/>	1	1	Mod
<input type="checkbox"/>	2	1-2	Mod
<input type="checkbox"/>	3	1-2	Mod
<input type="checkbox"/>	4	1	Mod
<input type="checkbox"/>	G1/G1-F	1-2	Mod
<input type="checkbox"/>	G2/G2-F	1-2	Mod

\*Because of layout, the sample picture doesn't display middle ports.

### Delete Port VLAN

As shown in the example of [Add Port VLAN](#), the port 2 and 3 are still in the VLAN 1. So if it intends to make the port 2 and 3 only communicated with the uplink port G1/SFP1 and G2/SFP2 and isolated from other downlink ports, it is required to delete these two ports from VLAN 1.

### Configuration Steps:

1. Log in to the Web administration and go to **VLAN Management > Port VLAN** page;
2. Select: Check the  before Port No. to select the port to be set;

3. VLAN List: In the following input box, enter the VLAN ID to be deleted;

**HIKVISION**

Administration | VLAN Mode Toggle **Port VLAN** Help

Port Management | **VLAN Port Configuration** Default

Select	Port List	VLAN List	Option
<input type="checkbox"/>	2-3	<input type="text" value="1"/>	<span>+Add</span> <span>-Del</span>
<input type="checkbox"/>	1	1	<span>Mod</span>
<input checked="" type="checkbox"/>	2	1-2	<span>Mod</span>
<input checked="" type="checkbox"/>	3	1-2	<span>Mod</span>
<input type="checkbox"/>	4	1	<span>Mod</span>
<input type="checkbox"/>	5	1	<span>Mod</span>
<input type="checkbox"/>	6	1	<span>Mod</span>
<input type="checkbox"/>	7	1	<span>Mod</span>
<input type="checkbox"/>	8	1	<span>Mod</span>

4. Operate: Click -Del to end the setup. The outcome is shown in the page below.

**HIKVISION**

Administration | VLAN Mode Toggle **Port VLAN** Help

Port Management | **VLAN Port Configuration** Default

Select	Port List	VLAN List	Option
<input type="checkbox"/>		<input type="text"/>	<span>+Add</span> <span>-Del</span>
<input type="checkbox"/>	1	1	<span>Mod</span>
<input checked="" type="checkbox"/>	2	2	<span>Mod</span>
<input type="checkbox"/>	3	2	<span>Mod</span>
<input type="checkbox"/>	4	1	<span>Mod</span>
<input type="checkbox"/>	5	1	<span>Mod</span>
<input type="checkbox"/>	6	1	<span>Mod</span>
<input type="checkbox"/>	7	1	<span>Mod</span>
<input type="checkbox"/>	8	1	<span>Mod</span>
<input type="checkbox"/>	9	1	<span>Mod</span>

### Modify Port VLAN

Suppose to modify port 4 from VLAN 1 to VLAN2.

#### Configuration Steps:

1. Log in to the Web administration and go to **VLAN Management > Port VLAN** page;
2. Operate: Click Mod corresponding to the port number;

**3.** Enter the page of VLAN modification;

- In case of deletion, please select the VLAN to be deleted from “Member VLANs” and click .
- In case of addition, please select the VLAN to be added from “Available VLANs” and click .

 **Tip**

The VLAN deleted will be displayed in the “Available VLANs”, and the VLAN added will be displayed in the “Member VLANs”.

**4.** Click  to end the setup. The outcome is shown in the page below.

**HIKVISION**

Administration | **VLAN Mode Toggle** | Port VLAN | Help

**VLAN Port Configuration** | Default

Select	Port List	VLAN List	Option
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="+Add"/> <input type="button" value="-Del"/>
<input type="checkbox"/>	1	1	<input type="button" value="Mod"/>
<input type="checkbox"/>	2	2	<input type="button" value="Mod"/>
<input type="checkbox"/>	3	2	<input type="button" value="Mod"/>
<input type="checkbox"/>	4	2	<input type="button" value="Mod"/>
<input type="checkbox"/>	5	1	<input type="button" value="Mod"/>
<input type="checkbox"/>	6	1	<input type="button" value="Mod"/>
<input type="checkbox"/>	7	1	<input type="button" value="Mod"/>
<input type="checkbox"/>	8	1	<input type="button" value="Mod"/>

### Restore VLAN Port Configuration to the State of Factory default settings

This function is available when port VLAN is intended to be restored to the state of factory default settings with other configurations remained the same.

#### Configuration Steps:

1. Log in to the Web administration and go to **VLAN Management > Port VLAN** page;
2. Click .

Upon completion, port VLAN will be restored to the factory settings, i.e. all ports are in the VLAN1.

## 7.2.3 Application Scenarios

### Networking Demand

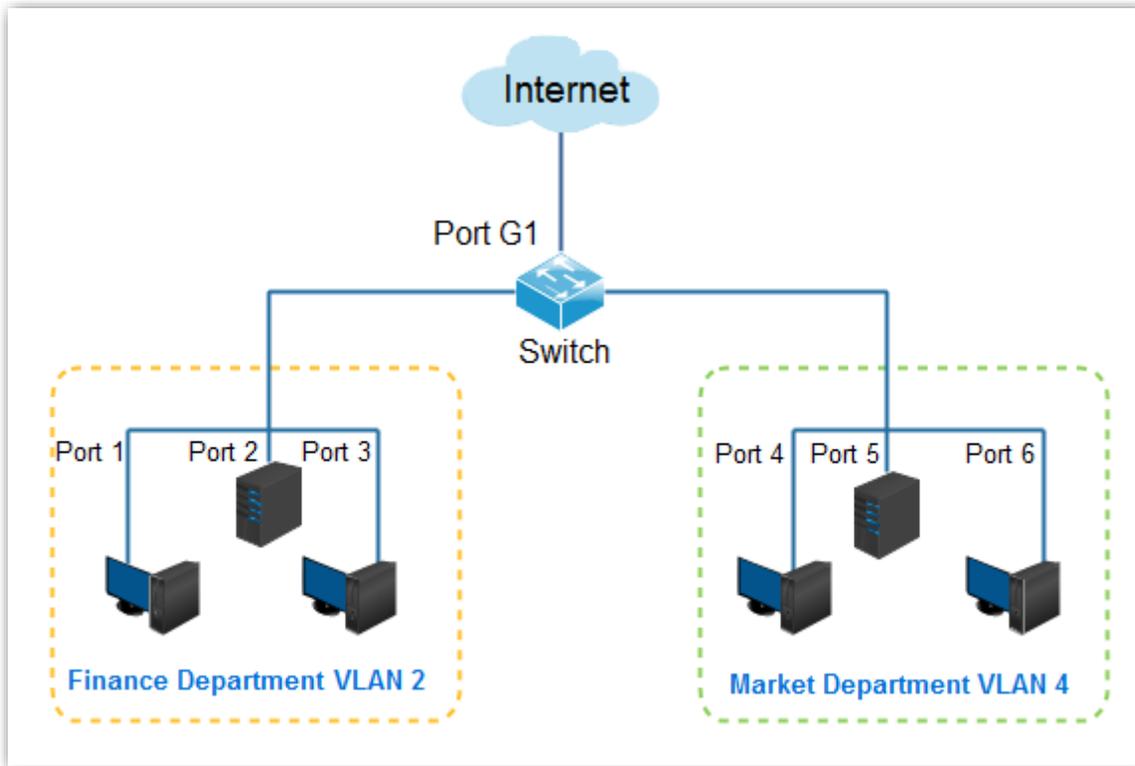
The finance department and market department of a company would like to realize: Intercommunication is made within them but prohibited between them. All personnel of both departments shall access to the Internet.

### Networking analysis

Set port VLAN:

- VLAN2 for the finance department and VLAN4 for the market department.
- VLAN2 and VLAN4 for the port connected to the Internet.

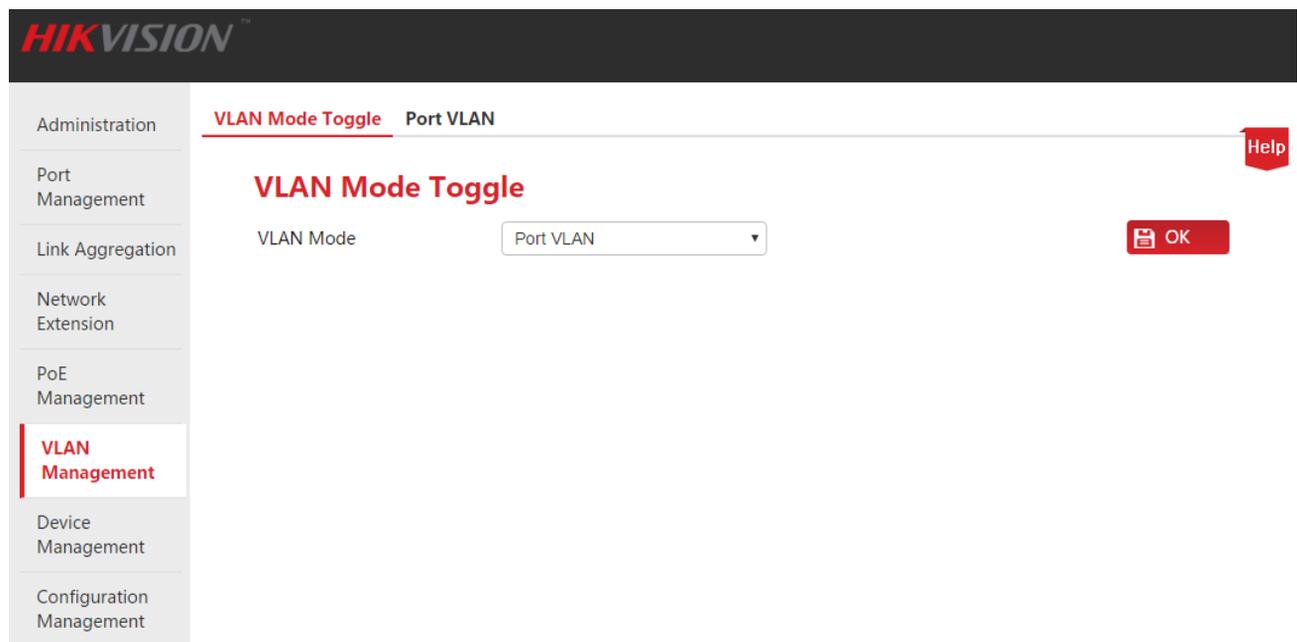
## Networking Drawing



## Configuration Steps

First, toggle VLAN Mode to the Port VLAN.

1. Log in to the Web administration and then go to **VLAN Management** page;
2. VLAN Mode: Select **Port VLAN**;
3. Click **OK**.



**Second, division VLAN.**

1. Go to **VLAN Management > Port VLAN** page;
2. Select the port 1, 2, 3, G1/SFP1, enter 2 in the input box below the VLAN List and then click **+Add**;
3. Select the port 4, 5, 6, G1/SFP1, enter 4 in the input box below the VLAN List and then click **+Add**;
4. Select the port 1, 2, 3, 4, 5, 6, G1/SFP1, enter 1 in the input box below the VLAN List and then click **-Del**;

**VLAN Port Configuration**

Select	Port List	VLAN List	Option
<input type="checkbox"/>			<b>+Add</b> <b>-Del</b>
<input type="checkbox"/>	1	2	Mod
<input type="checkbox"/>	2	2	Mod
<input type="checkbox"/>	3	2	Mod
<input type="checkbox"/>	4	4	Mod
<input type="checkbox"/>	5	4	Mod
<input type="checkbox"/>	6	4	Mod
<input type="checkbox"/>	G1/G1-F	2,4	Mod
<input type="checkbox"/>	G2/G2-F	1	Mod

**\*Because of layout, the sample picture display no middle ports.**

**Verify Configuration**

Intercommunication is made within departments but prohibited between them. All personnel shall access to the Internet.

**7.3 ONE KEY VLAN**

**!Note**

- Prior to enabling “ONE KEY VLAN”, please link the port G1/SFP1, G2/SFP2 to the central switching device.
- This mode is suggested to be initiated in case of the DHCP conflict resulting from the wireless router connected privately to the switch.

## 7.3.1 Configuration Wizard

The following is concerned with how to configure the ONE KEY VLAN of HIKVISION smart PoE switch and configuration tasks:

Steps	Configuration Tasks	Specification
1	<a href="#">7.3.2.1 VLAN Mode Toggle</a>	<b>Mandatory.</b> VLAN mode is port VLAN by default.
2	<a href="#">7.3.2.2 View Results of VLAN Division</a>	Optional.

## 7.3.2 ONE KEY VLAN

Please toggle VLAN Mode before viewing results of VLAN division.

### 7.3.2.1 VLAN Mode Toggle

When VLAN Mode is toggled to the ONE KEY VLAN, the system will automatically divide each downlink port and uplink port (Port G1/SFP1 and port G2/SFP2) as a separate VLAN.

#### Configuration Steps:

1. Log in to the Web administration and then go to **VLAN Management** page;
2. Select **ONE KEY VLAN** for VLAN Mode;
3. Click **OK**.

The screenshot displays the HIKVISION web management interface. The top navigation bar includes the HIKVISION logo and a 'Help' button. The left sidebar contains a menu with the following items: Administration, Port Management, Link Aggregation, Network Extension, PoE Management, **VLAN Management** (highlighted in red), Device Management, and Configuration Management. The main content area shows the 'VLAN Mode Toggle' configuration page. At the top of this page, there are two tabs: 'VLAN Mode Toggle' (selected) and 'Port VLAN'. The 'VLAN Mode' is currently set to 'ONE KEY VLAN' in a dropdown menu. A red 'OK' button is visible in the bottom right corner of the configuration area.

### 7.3.2.2 View Results of VLAN Division

Click **VLAN Management** > **Port VLAN** to view the results of VLAN division.

The screenshot shows the HIKVISION web interface for VLAN Port Configuration. The left sidebar contains navigation options: Administration, Port Management, Link Aggregation, Network Extension, PoE Management, **VLAN Management** (highlighted), Device Management, and Configuration Management. The main area is titled 'VLAN Port Configuration' and includes a 'VLAN Mode Toggle' set to 'Port VLAN'. A 'Default' button and a 'Help' icon are also visible. The central table lists 24 ports and two aggregated port ranges, each with a 'Select' checkbox, 'Port List', 'VLAN List', and 'Option' (Mod) column.

Select	Port List	VLAN List	Option
<input type="checkbox"/>			+Add -Del
<input type="checkbox"/>	1	1	Mod
<input type="checkbox"/>	2	2	Mod
<input type="checkbox"/>	3	3	Mod
<input type="checkbox"/>	4	4	Mod
<input type="checkbox"/>	5	5	Mod
<input type="checkbox"/>	6	6	Mod
<input type="checkbox"/>	7	7	Mod
<input type="checkbox"/>	8	8	Mod
<input type="checkbox"/>	9	9	Mod
<input type="checkbox"/>	10	10	Mod
<input type="checkbox"/>	11	11	Mod
<input type="checkbox"/>	12	12	Mod
<input type="checkbox"/>	13	13	Mod
<input type="checkbox"/>	14	14	Mod
<input type="checkbox"/>	15	15	Mod
<input type="checkbox"/>	16	16	Mod
<input type="checkbox"/>	17	17	Mod
<input type="checkbox"/>	18	18	Mod
<input type="checkbox"/>	19	19	Mod
<input type="checkbox"/>	20	20	Mod
<input type="checkbox"/>	21	21	Mod
<input type="checkbox"/>	22	22	Mod
<input type="checkbox"/>	23	23	Mod
<input type="checkbox"/>	24	24	Mod
<input type="checkbox"/>	G1/G1-F	1-24	Mod
<input type="checkbox"/>	G2/G2-F	1-24	Mod

## 7.4 802.1Q VLAN

### 7.4.1 Configuration Wizard

The following is concerned with how to configure 802.1Q VLAN of HIKVISION smart PoE switch and configuration tasks:

Steps	Configuration Tasks	Specification
1	<a href="#">7.4.2.1 VLAN Mode Toggle</a>	<b>Mandatory.</b> VLAN mode is port VLAN by default.
2	<a href="#">7.4.2.2 VLAN Division</a>	<b>Mandatory.</b> All ports are in VLAN1 by default.
3	<a href="#">7.4.2.3 Port Attribute Setting</a>	<b>Mandatory.</b> By default, all ports' PVID is set to 1 and tag processing policy is "Ignore".

## 7.4.2 802.1Q VLAN Configuration

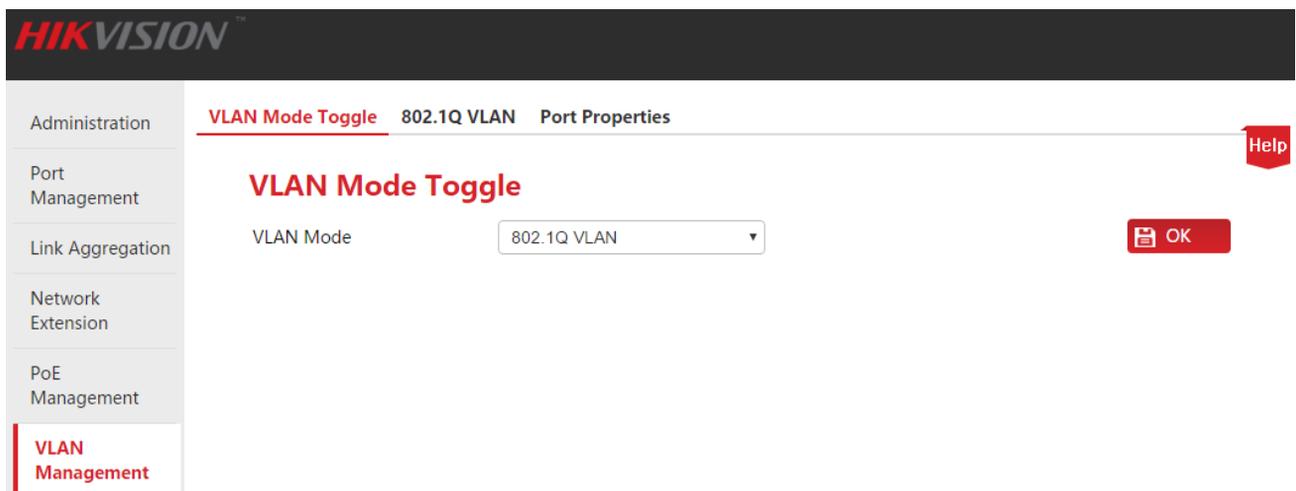
Please toggle VLAN Mode to 802.1Q VLAN before starting other settings in this part.

### 7.4.2.1 VLAN Mode Toggle

Toggle the VLAN mode to 802.1Q VLAN.

#### Configuration Steps:

1. Log in to the Web administration and then go to **VLAN Management** page;
2. Select **802.1Q VLAN** for VLAN Mode;
3. Click **OK**.



### 7.4.2.2 VLAN Division

This part takes the form of example to describe how to add, delete and modify 802.1Q VLAN.

### Add 802.1Q VLAN

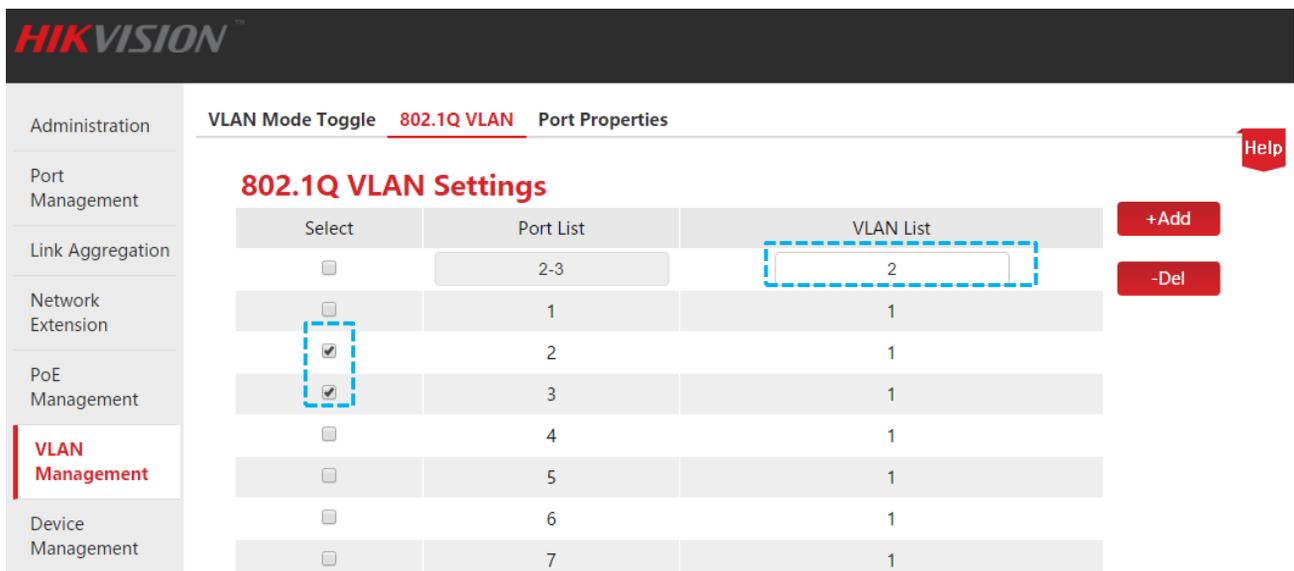
Suppose to add the port 2, 3 to VLAN2.

#### Configuration Steps:

1. Log in to the Web administration and go to **VLAN Management > 802.1Q VLAN** page;
2. Select: Check the  before Port No. to select the port to be set;
3. VLAN List: In the following input box, enter the VLAN ID of the selected ports in **Step 2**;

#### Tip

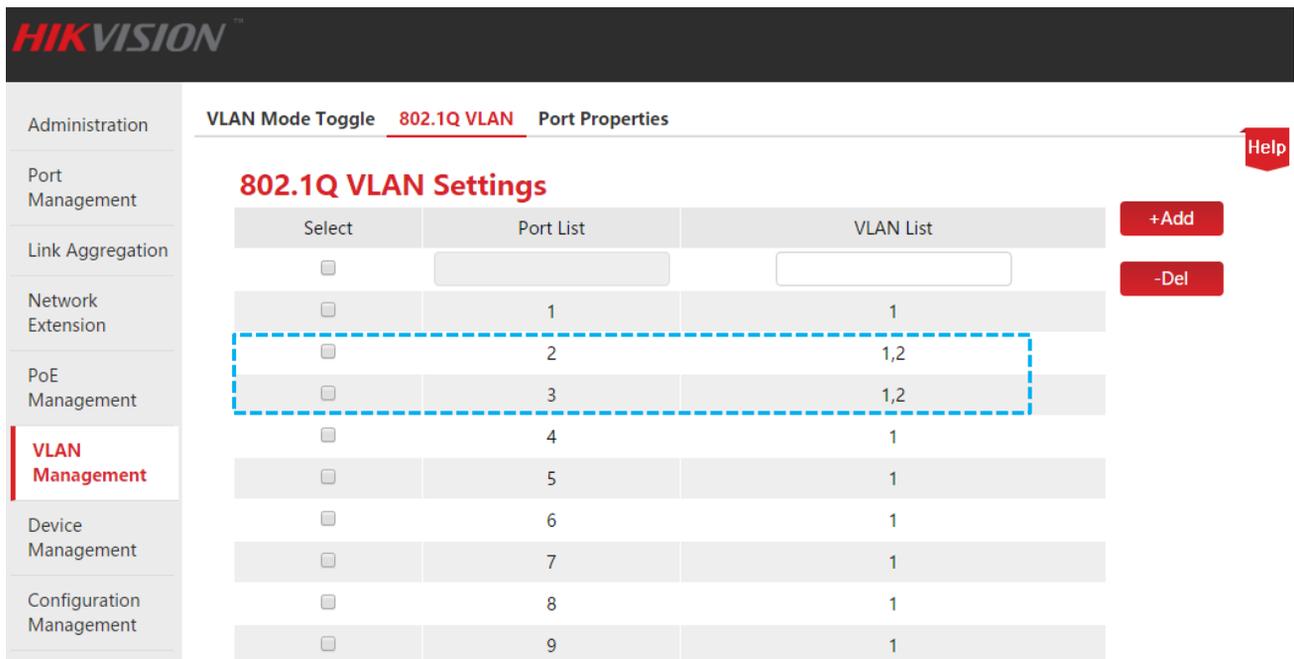
- Check the  at the top to select all of ports.
- Every port can be added into several VLANs, but each time you can only add one VLAN.



The screenshot shows the HIKVISION web interface for 802.1Q VLAN Settings. The left sidebar contains navigation options: Administration, Port Management, Link Aggregation, Network Extension, PoE Management, VLAN Management (highlighted), and Device Management. The main content area has tabs for VLAN Mode Toggle, 802.1Q VLAN, and Port Properties. A table lists ports 1 through 7. The 'Select' column has checkboxes, with ports 2 and 3 checked. The 'Port List' column shows '2-3' for the first row and individual numbers for others. The 'VLAN List' column has an input field for port 2 containing the value '2'. '+Add' and '-Del' buttons are on the right. A 'Help' button is in the top right corner.

Select	Port List	VLAN List
<input type="checkbox"/>	2-3	2
<input type="checkbox"/>	1	1
<input checked="" type="checkbox"/>	2	1
<input checked="" type="checkbox"/>	3	1
<input type="checkbox"/>	4	1
<input type="checkbox"/>	5	1
<input type="checkbox"/>	6	1
<input type="checkbox"/>	7	1

4. Click **+Add** to end the setup. The outcome is shown in the page below.



The screenshot shows the HIKVISION web interface after the configuration. The table now shows ports 2 and 3 with the VLAN List set to '1,2'. The '+Add' button is highlighted in red. The rest of the interface remains the same as in the previous screenshot.

Select	Port List	VLAN List
<input type="checkbox"/>		
<input type="checkbox"/>	1	1
<input checked="" type="checkbox"/>	2	1,2
<input checked="" type="checkbox"/>	3	1,2
<input type="checkbox"/>	4	1
<input type="checkbox"/>	5	1
<input type="checkbox"/>	6	1
<input type="checkbox"/>	7	1
<input type="checkbox"/>	8	1
<input type="checkbox"/>	9	1

### Delete 802.1Q VLAN

Suppose to delete the port 3 in the above-mentioned [Add 802.1Q VLAN](#) from VLAN2.

#### Configuration Steps:

1. Log in to the Web administration and go to **VLAN Management > 802.1Q VLAN** page;
2. Select: Check the  before Port No. to select the port to be set;
3. VLAN List: In the following input box, enter the VLAN ID to be deleted;



Tip

VLAN 1 is the default VLAN ID and must be reserved.

Administration | VLAN Mode Toggle | **802.1Q VLAN** | Port Properties | Help

### 802.1Q VLAN Settings

Select	Port List	VLAN List	+Add	-Del
<input type="checkbox"/>	3	2		
<input type="checkbox"/>	1	1		
<input type="checkbox"/>	2	1,2		
<input checked="" type="checkbox"/>	3	1,2		
<input type="checkbox"/>	4	1		
<input type="checkbox"/>	5	1		
<input type="checkbox"/>	6	1		
<input type="checkbox"/>	7	1		

4. Click **-Del** to end the setup. The outcome is shown in the page below.

Administration | VLAN Mode Toggle | **802.1Q VLAN** | Port Properties | Help

### 802.1Q VLAN Settings

Select	Port List	VLAN List	+Add	-Del
<input type="checkbox"/>				
<input type="checkbox"/>	1	1		
<input type="checkbox"/>	2	1,2		
<input type="checkbox"/>	3	1		
<input type="checkbox"/>	4	1		
<input type="checkbox"/>	5	1		
<input type="checkbox"/>	6	1		
<input type="checkbox"/>	7	1		
<input type="checkbox"/>	8	1		
<input type="checkbox"/>	9	1		

## Modify 802.1Q VLAN

Direct modification of 802.1Q VLAN is prohibited. If the VLAN is incorrect, you can delete it and then add the correct VLAN.



### Tip

- At most 31 groups can be created for 802.1Q VLAN.
- Cross-switch VLAN isolation is possible for 802.1Q VLAN.
- All ports invariably belong to VLAN1. You can set the ports' Port Properties to realize VLAN isolation.

### 7.4.2.3 Port Properties Setting

To realize VLAN isolation by 802.1Q VLAN, it is also required to set 802.1Q VLAN Port Properties.

#### Configuration Steps:

1. Log in to the Web administration and go to **VLAN Management > Port Properties** page;

The screenshot shows the HIKVISION web interface for configuring 802.1Q VLAN Port Properties. The page title is "802.1Q VLAN Port Setting". At the top, there are tabs for "VLAN Mode Toggle", "802.1Q VLAN", and "Port Properties". Below the tabs, there are two dropdown menus: "PVID" set to "1" and "Tag Processing Policy" set to "Ignore". An "OK" button is located to the right of these dropdowns. The main content is a table with the following structure:

<input type="checkbox"/>	PORT	PVID	Tag Processing Policy
<input type="checkbox"/>	1	1	--
<input type="checkbox"/>	2	1	--
<input type="checkbox"/>	3	1	--
<input type="checkbox"/>	4	1	--
<input type="checkbox"/>	5	1	--
<input type="checkbox"/>	6	1	--
<input type="checkbox"/>	7	1	--
<input type="checkbox"/>	8	1	--
<input type="checkbox"/>	9	1	--
<input type="checkbox"/>	10	1	--

#### Parameter Description:

Item	Description
<input type="checkbox"/>	Click <input type="checkbox"/> to select the port to be set for 802.1Q VLAN Port Properties. Check the <input type="checkbox"/> at the top to select all ports; check the port in front of the Port No. to select the corresponding one.

Item	Description
PVID	<p>PVID is the default VLAN ID for the port, thus giving a default VLAN affiliation to the data package without VLAN Tag.</p> <p>PVID of each port can be various, but the PVID to be selected must be the existing one. The value of PVID is 1 by default.</p>
Tag Processing Policy	<p>Set ports how to send data and process data received.</p> <p><b>Ignore:</b> In case of the data package received without Tag, the data package to be sent will also has no Tag, and vice versa.</p> <p><b>Add Tag:</b> In case of the data package received without Tag, the data package to be sent will be added PVID of the receiving port; in case of the data package received with Tag, the data package to be sent will preserve the Tag.</p> <p><b>Remove Tag:</b> In case of the data package received without Tag, the data package to be sent will also has no Tag; in case of the data package received with Tag, the data package to be sent will remove the Tag.</p>

Data receiving and processing modes of ports are shown below:

Type of Data Package Received	Data Processing Mode
Receiving Tagged Packets	Packets will be forwarded to other ports in the corresponding VLAN according to VID in the Tag.
Receiving Untagged Packets	Packets will be forwarded to other ports in the corresponding VLAN according to PVID on this port.

2. By referring to the above-mentioned Parameter Description, set PVID and Tag processing policy on the port according to the need. Click **OK** to finish the settings.

### Tip

- The MAC table of the switch in 802.1Q VLAN is a share learning mode, namely, MAC addresses learned in different VLANs are the same entry in the MAC table.
- PVID on a port may not belong to a VLAN ID set on this port. When a VLAN ID corresponding to PVID on the port is deleted, PVID will be automatically changed to the default value of 1.

## 7.4.3 Application Scenarios

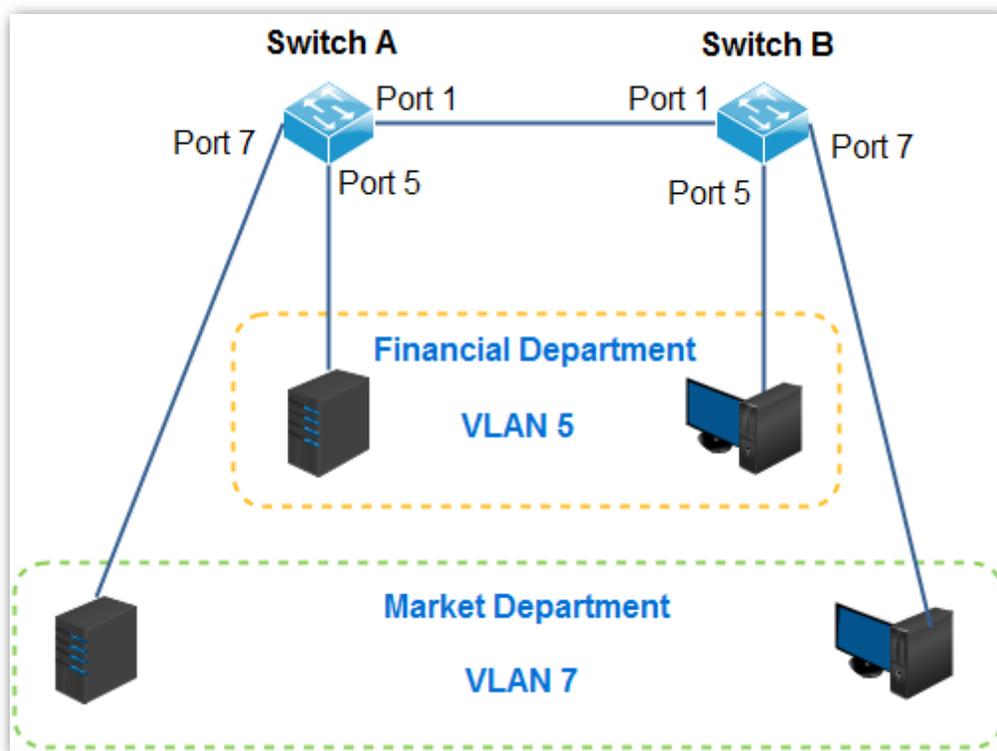
### Networking Requirements

Workers in the financial and market departments of a company work on the second floor, but the servers for both departments are located on the third floor. The following requirements must be met now: Each department can internally intercommunicate and access its server. Intercommunication between the departments cannot be performed.

### Networking Analysis

- Use two switches. Set an 802.1Q VLAN on the switches.
- Add two VLANs on the switches. All devices of financial department belong to VLAN 5, and all devices of market department belong to VLAN 7.
- The ports that connect the switches are added to VLAN 5 and VLAN 7.

### Networking Diagram

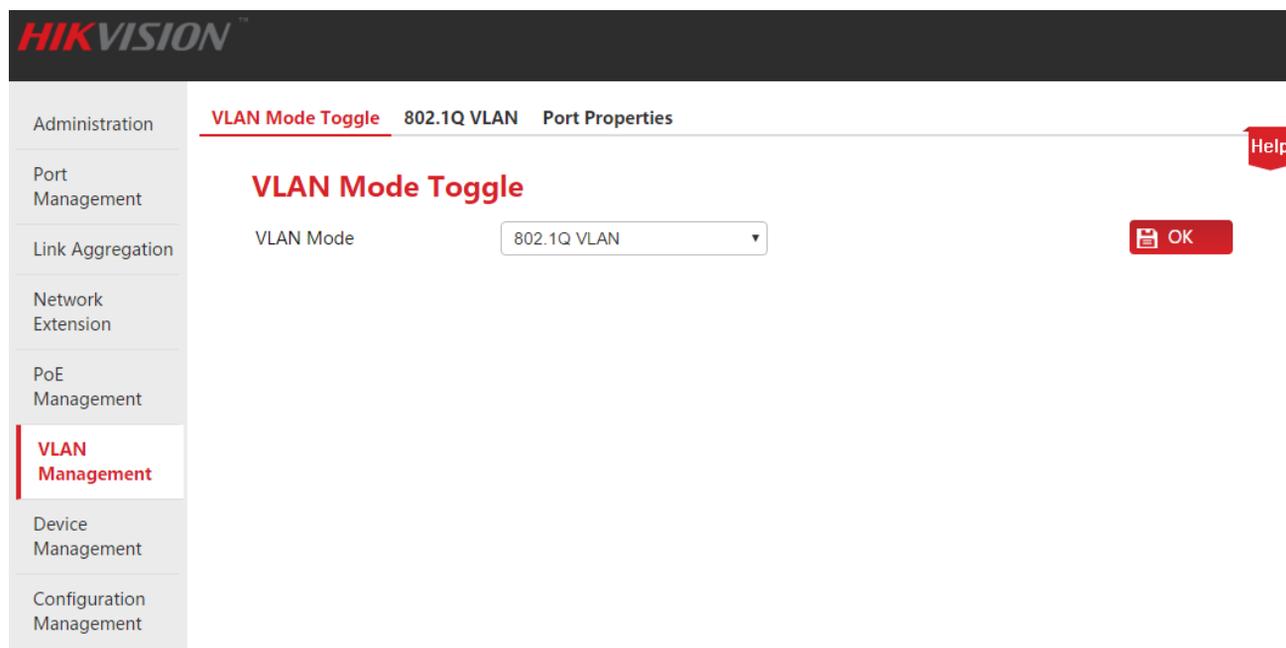


### Configuration Steps

First, set Switch A.

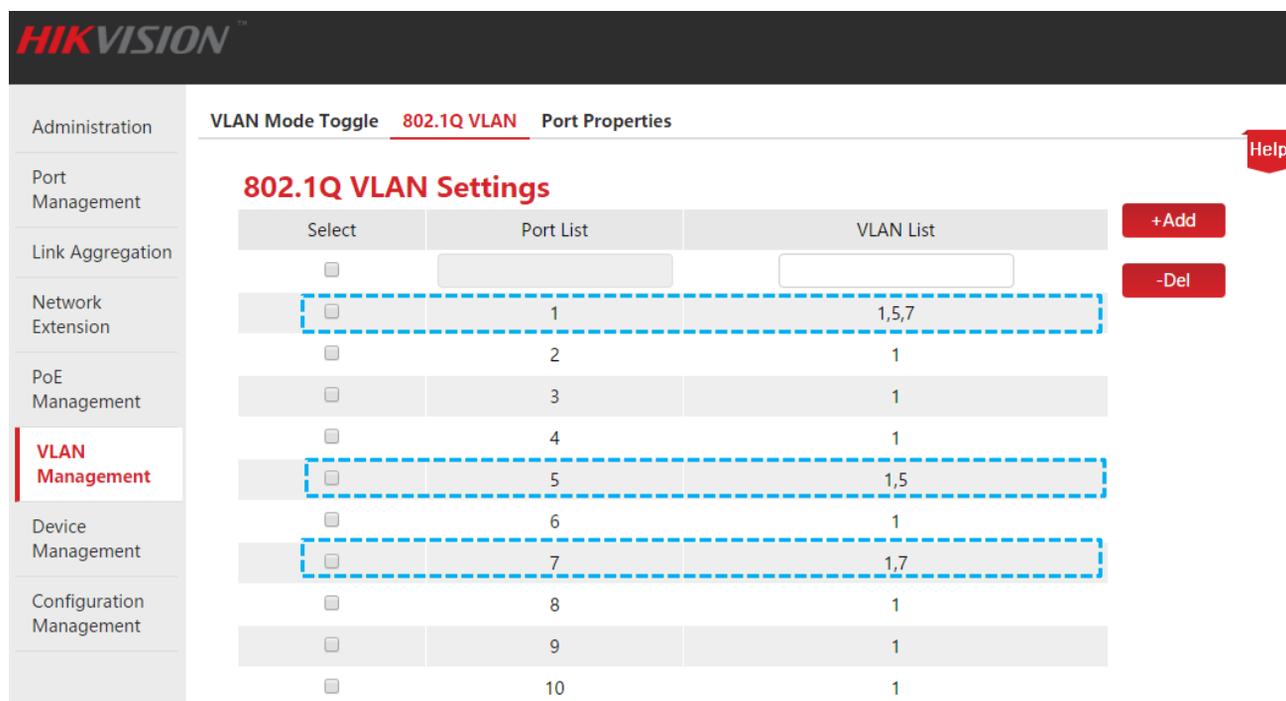
**Step 1:** Switch the VLAN mode to **802.1Q VLAN**.

1. Log in to the Web administration and then go to **VLAN Management** page;
2. VLAN mode: Select **802.1Q VLAN**;
3. Click **OK**.



**Step 2: Partition VLAN.**

1. Go to the **VLAN Management > 802.1Q VLAN** page;
2. Select Ports 1 and 5, enter 5 in the input box below VLAN List, and click **+Add**;
3. Select Ports 1 and 7, enter 7 in the input box below VLAN List, and click **+Add**.



**Step 3: Set port properties.**

1. Go to the **VLAN Management > Port Properties** page;
2. Select Port 5, set PVID to 5 and Tag Processing Policy to **Remove Tag (Rm)**, click **OK**;
3. Select Port 7, set PVID to 7 and Tag Processing Policy to **Remove Tag (Rm)**, click **OK**;
4. Select Port 1, set PVID to 1 and Tag Processing Policy to **Add Tag**, click **OK**.

**802.1Q VLAN Port Setting**

PVID:  Tag Processing Policy:

<input type="checkbox"/>	PORT	PVID	Tag Processing Policy
<input type="checkbox"/>	1	1	Add Tag
<input type="checkbox"/>	2	1	--
<input type="checkbox"/>	3	1	--
<input type="checkbox"/>	4	1	--
<input type="checkbox"/>	5	5	Rm Tag
<input type="checkbox"/>	6	1	--
<input type="checkbox"/>	7	7	Rm Tag
<input type="checkbox"/>	8	1	--
<input type="checkbox"/>	9	1	--

**Second, set Switch B.**

The setting procedure for Switch B is the same as that for Switch A.

**Verify Configuration**

Employees can access the server for their own department, but not the server for the other department.

# 8 Device Management

---

This section helps you enhance the switch's traffic forwarding capacity and manage the switch efficiently. The following five parts are included:

[MAC Binding](#): Perform static MAC address binding of the switch ports.

[QoS](#): Provide different service quality for various network applications according to their different requirements.

[STP](#): Eliminate physical loop in data link layer, avoid broadcast storm and provide link backup redundancy.

[IGMP](#): Manage and control multicast groups to save network bandwidth, to ensure better multicast security and to make each host's separate billing convenient.

[SNMP](#): Manage the switch efficiently.

## 8.1 MAC Binding

### 8.1.1 Overview

MAC Binding provides two functions:

- If a MAC address is bound to a port, the device with the MAC address can only access the network through this port instead of ports.
- If several MAC addresses are bound to a port, this port only allows the device with these MAC addresses instead of other devices to get through.

Through the MAC binding function, a single port only allows the designated users to use network resources to ensure network security and user authority and effectively prevent unauthorized users from gaining data by cheating and performing loiter net.



Ports whose MAC binding is enabled will automatically disable the address learning function.

Bound MAC addresses can be manually added and deleted and will not be aged over time.

---

## 8.1.2 Configuring MAC Binding

Click **Device Management** to enter the configuration page.

Specification of parameter setting:

Item	Description
Select port	Select a port to configure MAC Binding.
Static MAC Address 1	Enter an access device MAC address bound to this port. The switch supports binding up to three access devices (MAC addresses are different).   <b>Note</b> Broadcast or multicast address binding is not allowed.
Static MAC Address 2	
Static MAC Address 3	
Binding	Enable/Disable the MAC binding function of this port.   <b>Tip</b> <ul style="list-style-type: none"> <li>Ports whose MAC binding function is enabled will disable the address learning function.</li> <li>After the MAC binding function is enabled, the switch only allows a designated device to access the network through this port.</li> </ul>

After the settings are finished, click **OK**, and the system will automatically display the

setting information in the list below. You can view the list and check whether the setting information is correct.

Specification of parameters in the display list:

Item	Description
Port	Display port numbers of the switch.
Status	Display the status of MAC Binding function of this port.
Static MAC Address Bound MAC 1/2/3	Display an access device MAC address bound to this port.

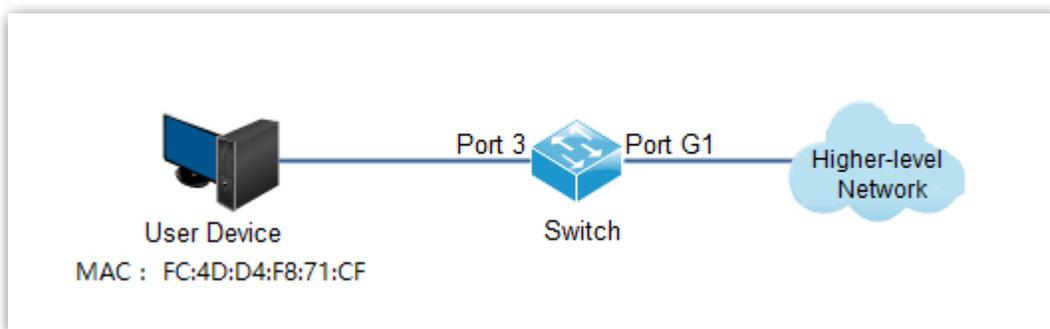
## 8.1.3 Application Scenarios

### 8.1.3.1 Adding MAC Binding

#### Networking Requirements

The MAC address of the user device is FC:4D:D4:F8:71:CF. Connect it to port 3 of the switch. Bind this user device to port 3 of the switch to prevent other unauthorized users from performing loiter net and gaining data from other ports by pretending to an authorized user's MAC address.

#### Networking Diagram



#### Configuration Steps

1. Log in to the web administration page of the switch and go to the **Device Management > MAC Binding Page**;
2. Click the Select Port drop-down menu and select "3";
3. Enter the user device MAC address "FC4DD4F871CF" in the **Static MAC Address 1** column;

4. Click the **Binding** drop-down menu and select **Enable**;

**MAC Binding**

Select Port: 3 | Static MAC Address 1: FC4DD4F871CF | Static MAC Address 2: | Static MAC Address 3: | Binding: Enable

Port	Status	Static MAC Address		
		Bound MAC 1	Bound MAC 2	Bound MAC 3
1	Disable	--	--	--
2	Disable	--	--	--
3	Disable	--	--	--
4	Disable	--	--	--
5	Disable	--	--	--

5. Click **OK** to end the setup. The outcome is shown in the page below.

**MAC Binding**

Select Port: 3 | Static MAC Address 1: FC:4D:D4:F8:71:CF | Static MAC Address 2: | Static MAC Address 3: | Binding: Enable

Port	Status	Static MAC Address		
		Bound MAC 1	Bound MAC 2	Bound MAC 3
1	Disable	--	--	--
2	Disable	--	--	--
3	Enable	FC:4D:D4:F8:71:CF	--	--
4	Disable	--	--	--
5	Disable	--	--	--

**Verify Configuration**

After the settings are finished, only the device with MAC address "FC:4D:D4:F8:71:CF" among all user devices connected to Port 3 can access the higher-level network. If the device with MAC address "FC:4D:D4:F8:71:CF" is connected to other ports of the switch, this device cannot access the higher-level network.

**8.1.3.1 Cancel MAC Binding**

**Networking Requirements**

Cancel MAC address binding of Port 3 added in the above-mentioned example.

### Configuration Steps

1. Log in to the web administration page of the switch and go to the **Device Management > MAC Binding** Page;
2. Click the **Select Port** drop-down menu, select **3**, Click the **Binding** drop-down menu, and select **Disable**;
3. Click **OK** to end the setup.

### Verify Configuration

The device in this example can connect to other ports to access the network.

## 8.2 QoS

### 8.2.1 Overview

Traditional IP network mainly involves business, like www, FTP, E-mail, etc. It can deliver packets to the destination but ensures no guarantee of forwarding delay, jitter, packet loss rate and reliability.

As IP technology develops rapidly and all kinds of new business, such as distance education, teleconference, VOD, etc. emerge, IP network has turned into a multi-service bearer network from a pure data network. Thus, QoS appears.

Briefly speaking, QoS provides network applications with different quality of service, like provide dedicated bandwidth, decrease transmission delay and jitter, reduce packet loss rate, etc.

#### 📌 How QoS works

This switch provides the simple QoS function. By setting a port priority, the system first discard packets on low-priority ports during network congestion to ensure transmission of packets on high-priority ports. The switch has a total of two priority queues. Queue Low is of low priority. Queue High is of high priority. The Priority Modes supported by the switch are First in First Out (FIFO), Strict Priority (SP), and Weighted Round Robin (WRR). By default, it is FIFO.

#### 📌 Priority Mode

##### 1. FIFO

FIFO is that packets that are received first are forwarded first. It applies to most network applications such as email and FTP.

##### 2. Strict Priority Mode

Strict Priority Queuing is specially designed to meet the demands of critical services or applications. When congestion occurs on the network, the system will ask for service preferentially to reduce response delay.

Then under SP algorithm, the port strictly prioritizes packets from higher priority queue over those from lower priority queue. Namely, packets in the queue with lower priority are sent only when the queue with higher priority is empty. Thus High-priority packets are always processed before those of less priority. Medium-priority packets are always processed before low-priority packets. The lowest priority queue would be serviced only when highest priority queues had no packets buffered.

The disadvantage of SP queue is that: if there are packets in the queues with higher priority for a long time in congestion, the packets in the queues with lower priority will be “starved to

death” because they are not served.

### 3. Weighted Round Robin Mode (WRR)

WRR-Mode: Weighted Round Robin Mode. In this mode, packets in all the queues are sent in order based on the weight value for each queue and every queue can be assured of a certain service time. Assuming there are 2 egress queues on the port. The two weight values (namely,  $w_2$  and  $w_1$ ) indicate the proportion of resources assigned to the two queues respectively. On a 100M port, if you set the weight values of WRR queue-scheduling algorithm to 7 and 5 (correspond to  $w_2$  and  $w_1$  respectively). Then the queue with the lowest priority can be ensured of, at least, 30 Mbps bandwidth, thus WRR queue overcomes the disadvantage of SP queue that the packets in the queues with lower priority cannot get service for a long time.

In WRR mode, though the queues are scheduled in order, the service time for each queue is not fixed, that is to say, if a queue is empty, the next queue will be scheduled. In this way, the bandwidth resources are made full use of.

## 8.2.2 Configuring QoS

Click **Device Management > QoS** to enter the configuration page.

The screenshot shows the HIKVISION web interface for QoS configuration. The left sidebar contains a navigation menu with the following items: Administration, Port Management, Link Aggregation, Network Extension, PoE Management, VLAN Management, Device Management (highlighted in red), MAC, and QoS. The main content area is titled 'QoS' and 'Priority Mode'. A dropdown menu is set to 'SP (Strict Priority)'. There is an 'OK' button and a 'Help' icon.

### QoS Configuration Steps:

1. Priority Mode: Select a QoS mode. If WRR is selected, you must also set Low weight and High weight. Note that the proportion of High must be greater than that of Low. This series of switches support a proportion of 1-7.
2. Click **OK** to finish QoS mode selection;



3. Click **Port Management > Port Configuration** and select a port (Assume that you select Port 9 in this example). Set its **Priority** to **High**, and the corresponding port will be in the high-priority queue.

<input type="checkbox"/>	Port	Link Status	Speed/Duplex	Priority	Flow Control	State	Storm Control	Address Learning
<input type="checkbox"/>	1	100M_FDX	Auto	High	Enable	Enable	Disable	Enable
<input type="checkbox"/>	2	100M_FDX	Auto	High	Enable	Enable	Disable	Enable
<input type="checkbox"/>	3	---	Auto	High	Enable	Enable	Disable	Enable
<input type="checkbox"/>	4	---	Auto	High	Enable	Enable	Disable	Enable
<input type="checkbox"/>	5	---	Auto	High	Enable	Enable	Disable	Enable
<input type="checkbox"/>	6	---	Auto	High	Enable	Enable	Disable	Enable
<input type="checkbox"/>	7	---	Auto	High	Enable	Enable	Disable	Enable
<input type="checkbox"/>	8	---	Auto	High	Enable	Enable	Disable	Enable
<input checked="" type="checkbox"/>	9	100M_FDX	Auto	Low	Enable	Enable	Disable	Enable
<input type="checkbox"/>	10	100M_FDX	Auto	Low	Enable	Enable	Disable	Enable

**Qos Configuration specification**

If the QoS mode is SP, set Port 1 to High and Port 2 to Low in Priority. When both ports send packets to the same port at the same time, this port will let packets from Port 1 pass, followed by packets from Port 2.

If WRR is selected, set weights to High=7 and Low=1 respectively. When both ports send packets to the same port at the same time, this port will send packets in a traffic proportion of 7:1.

## 8.3 STP

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links.

Spanning Tree Protocol (STP) is standardized as IEEE 802.1D. As the name suggests, it creates a spanning tree within a network of connected layer-2 bridges (typically Ethernet switches), and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes.

### 📌 STP protocol packets

To implement spanning tree function, switches in the network transfer BPDU (Bridge Protocol Data Unit) between each other to exchange information. BPDUs carry the information that is needed for switches to figure out the spanning tree.

The network topology is determined by BPDU transmission among devices. There are two types of BPDUs in the original STP specification

- Configuration BPDU: Used for Spanning Tree computation and spanning tree topology maintenance.
- Topology Change Notification (TCN) BPDU: Used to announce changes in the network topology

### 📌 Basic concepts of STP

#### 1. Bridge ID

The bridge ID contains both numbers combined together - Bridge priority + MAC, in which the bridge priority is a configurable parameter. The smaller the bridge ID is, the higher the bridge priority is. The root bridge is the bridge with the lowest bridge ID.

#### 2. Root Bridge

There is only one Root Bridge in the networking, so the concepts of Root Bridge was introduced in the STP. There is only one Root Bridge in the structure of whole network, and it is changeable as the network topology changes, thus the Root Bridge is not stable.

Initially, all devices regard themselves as the root bridge and generate their own configuration BPDUs and send them out periodically. When the network topology becomes stable, only the root bridge device will send configuration BPDUs out and other devices will forward these BPDUs.

#### 3. Root Port

The root bridge port is the port that has the lowest path cost from this bridge to the Root Bridge and forwards packets to the root. There is only one root port on the non-root bridge device and no root port on the root bridge devices.

#### 4. Designated Bridge and Designated Port

**Designated bridge:** As for a device, it is the device that connects to and forwards BPDUs to the host. As for a LAN, it is the device that forwards BPDUs to the network segment.

In every network segment, the device with the smallest path cost to the root bridge will be selected as the designated bridge. When all switches have the same root path cost, the device with the lowest network bridge ID will be selected as the designated bridge.

**Designated port:** As for a device, it is the port that forwards BPDUs to the host. As for a LAN, it is the port that forwards BPDUs to the network segment.

#### 5. Path cost

The parameter for choosing the link path by STP. By calculating the path cost, STP chooses the better links and blocks the redundant links so as to disbranch the ring-network to form a tree-topological ring-free network.

#### ➤ BPDU Priority in STP mode

BPDUs with a smaller root bridge ID have a higher priority. If the root bridge IDs are identical, then compare the root path cost as follows: root path cost in BPDU plus the path cost corresponding to that port, assume that the sum of the both is  $S$ , the BPDU with a smaller  $S$  has a relatively high priority.

If the root path costs are also identical, then compare the IDs of designated bridge, IDs of designated port ID, and the IDs of ports receiving the BPDU successively, and the BPDU with smaller values mentioned above has a relatively high priority.

#### ➤ STP Computing Process

##### 1. Initial Status

Initially, each switch regards itself as the root, and generates a configuration BPDU for each port on it as a root, with the root path cost being 0, the ID of the designated bridge being that of the switch, and the designated port being itself.

##### 2. BPDU Comparison

Each switch sends out configuration BPDUs and receives a configuration BPDU on one of its ports from another switch. The following table shows the comparing operations.

Step	Content
1	<p>If the priority of the BPDU received on the port is lower than that of the BPDU of the port itself, the switch discards the BPDU and does not change the BPDU of the port.</p> <p>If the priority of the BPDU is higher than that of the BPDU of the port itself, the switch replaces the BPDU of the port with the received one.</p>
2	The switch selects the best BPDU by comparing BPDUs on all ports.

### 3. Select the root bridge

The root bridge is selected by BPDU comparing. The switch with the smallest root ID will be chosen as the root bridge.

### 4. Select the root port and designated port

The operation is taken in the following way:

Step	Content
1	Non-Root Bridge will receive the port of the best BPDU as the root port.
2	<p>Using the root port BPDU and the root path cost, the switch generates a designated port BPDU for each of its ports.</p> <ul style="list-style-type: none"> <li>• Root ID is replaced with that of the root port;</li> <li>• Root path is replaced with the sum of the root path cost of the root port and the path cost between this port and the root port;</li> <li>• The ID of the designated bridge is replaced with that of the switch;</li> <li>• The ID of the designated port is replaced with that of the port.</li> </ul>
3	<p>The switch compares the resulting BPDU with the BPDU of the desired port whose role you want to determine.</p> <ul style="list-style-type: none"> <li>• If the resulting BPDU takes the precedence over the BPDU of the port, the port is chosen as the designated port and the BPDU of this port is replaced with the resulting BPDU. The port regularly sends out the resulting BPDU;</li> <li>• If the BPDU of this port takes the precedence over the resulting BPDU, the BPDU of this port is not replaced and the port is blocked. The port only can receive BPDUs.</li> </ul>



#### Tip

In an STP with stable topology, only the root port and designated port can forward data, and the other ports are blocked. The blocked ports can only receive BPDUs.

### 👉 STP Timer

#### 1. Hello Time

It specifies the interval to send BPDU packets. It is used to test the links. Hello Time ranges from 1 to 10 seconds.

#### 2. Max Age

If the BPDU packet is not received after the Max Age, the switch will send the BPDU packet to all the other switches, and recalculate the spanning tree. Max Age ranges from 6 to 40 seconds.

### 3. Forward Delay

It means the delay time that the removing of the switch port status. Max Age ranges from 4 to 30 seconds.

When the STP regeneration caused by network malfunction occurs, the STP structure will get some corresponding change. However, the recomputed new BPDU cannot be immediately spread over the entire network. Allowing a newly selected root port and designated port to start forwarding data immediately might give rise to transient loop. Therefore, STP adopts a kind of state transition mechanism, such that the newly selected root port and designated port cannot enter into their forwarding status before a 2-times forwarding delay expires; the forwarding delay can ensure that the new BPDU is already spread over the entire network.

#### 📌 RSTP(rapid spanning tree protocol)

RSTP (Rapid Spanning Tree Protocol) made improvements on the STP, and achieved a rapid convergence of network topologies. Its “rapidness” reflects in such a fact that when a port is selected to serve as root port and designated port, the delay time before it enters into forwarding status is greatly reduced under a certain condition, so as to reduce the time for the network to achieve its final topology stabilization (conventional STP needs approximately 50 seconds, while RSTP need approximately 1 second only).

The pre-conditions for implementing rapid status transition of root port and designated port in the RSTP are given below:

- Root port: Old root port on the device already stopped forwarding data, and upstream designated port already started forwarding the data.
- Designated port: Designated port is an edge port or designated port that is connected to a point-to-point link. If the device the designated port is connected to edge port, the device directly enter into the forwarding status; if the designated port is connected to a point-to-point link, the device shakes hands with a downstream device, gets a response, and immediately enters into the forwarding status.

#### 📌 Basic concept of RSTP

##### 1. Edge port

Edge port is a designated port that can be set, it can be directly connected to a loop-free network port, and it is directly connected to the terminal devices (user side) in most cases. A port designated as edge port can rapidly transit to its forwarding status, and it does not have to experience the listen-in and learning status. An edge port receiving a BPDU message will become a non-edge port and an ordinary spanning tree port to participate in the computation of spanning tree.

##### 2. Point-to-point link

Point-to-point link is a link for direct connection between two switches.

## 8.3.1 Global setting of STP

Click the **Device Management > STP** to access the configuration page.

### 📌 Global setting

It is used to configure and view the global properties of spanning tree functions of the switch.

## Parameter Description:

Item	Description
STVI version	<p>Enable/Disable the STP functions of the switch, and directly select the spanning tree mode of switch at enabling:</p> <ul style="list-style-type: none"> <li>• Disable: Disable the spanning tree functions.</li> <li>• STP: Enable the compatibility mode of spanning tree.</li> <li>• RSTP: Enable the compatibility mode of rapid spanning tree.</li> </ul>
Priority	<p>Set the priority of the switch.</p> <p>Priority is an important reference to determine whether the switch will be selected to work as root bridge, and switch with higher priority will be selected to work as root bridge under equivalent conditions. The lower the value, the higher the priority. Priority is 32768 by default.</p>
Hello Time	<p>Set the time interval to 2 seconds by default for the switch to send BPDU.</p>
Max Age	<p>Set the maximum survival time of BPDU message when it is stored on the switch. The default is 20 seconds.</p> <p>Maximum aging time must meet the following requirements:</p> <ul style="list-style-type: none"> <li>• Maximum aging time <math>\geq 2 * (\text{Hello Time} + 1)</math></li> <li>• Maximum aging time <math>\leq 2 * (\text{forwarding delay time} - 1)</math></li> </ul>
Forward Delay	<p>Set the delay time of port status transition of the switch when a change in network topology takes place. The default is 15 seconds.</p>

### Loopback Detection

## Loopback Detection

Loopback Detection Disable ▼

Auto-Wakeup Disable ▼

Wakeup Time Interval 10 s ▼

**⚠ Note**

- When the spanning tree functions are disabled, the loopback detection function, auto awakening and awakening time interval cannot be set.
- When the spanning tree function is enabled and the loopback detection function is disabled, the auto wake-up function gets invalid. Auto wake-up function can get valid only when both the STP function and loopback detection function are enabled.

Parameter Description:

Item	Description
Loopback Detection	<p>Enable/Disable the loopback detection function.</p> <p>After the function is enabled, if the port receives a BPDU message forwarded by the port, the downstream equipment is considered as giving rise to a loop, and the port is also set to Discard status.</p>
Auto-Wakeup	<p>Enable/Disable the auto-wakeup function.</p> <ul style="list-style-type: none"> <li>• Enable: When the wake-up time interval expires, the Discard port enters into its Forwarding status and conducts detection over again.</li> <li>• Disable: When the port enters into its Discard status, the port requires manual turn-on.</li> </ul>
Wakeup Time Interval	<p>Set the wakeup time interval.</p> <p>If the auto-wakeup is enabled, the Discard port enters into its Forwarding status and conducts detection over again when the wake-up time interval expires.</p>

**➤ Specify Root Bridge**

View the current root bridge status.

**Specify Root Bridge**

Bridge ID	32768:00B0-4C18-2600
Root Bridge ID	32768:0090-4C0F-F0BE
Hello Time	2
Max Age	20
Forward Delay	0

Parameter Description:

Item	Description
Bridge ID	Display the bridge ID of current switch, and comprise the system priority and MAC address of the switch.
Root Bridge ID	In the entire network spanning tree, it is selected to serve as a bridge ID of root bridge device.
Hello Time	Display the Hello Time value of Root bridge setting.
Max Age	Display the value of maximum aging time of root bridge setting.
Forward Delay	Display the value of forwarding delay of root bridge setting.

### 8.3.2 Port setting

The port priority and path cost can be set herein, and the information on the roles and status of switch ports can be inquired.

Click the **Device Management > STP > Port configuration** to access the page.

**HIKVISION**

Administration | **Global Settings** | **Port Configuration** | Help

**STP Port Configuration** [OK]

Select Port:  Priority:  (0~240) Path Cost(0=Auto):  (0~200000000)

Port	Role	State	Link Status	Path Cost	Priority	Loopback Status
1	Designated	Forwarding	100M_FDX	Auto:200000	128	--
2	Designated	Forwarding	100M_FDX	Auto:200000	128	--
3	--	Disable	--	Auto:0	128	--
4	--	Disable	--	Auto:0	128	--
5	--	Disable	--	Auto:0	128	--
6	--	Disable	--	Auto:0	128	--
7	--	Disable	--	Auto:0	128	--
8	Designated	Forwarding	100M_FDX	Auto:200000	128	--
9	--	Disable	--	Auto:0	128	--
10	Designated	Forwarding	100M_FDX	Auto:200000	128	--
11	--	Disable	--	Auto:0	128	--

Specification of parameter setting:

Item	Description
Select port	Select the port to be set.
Priority	Set the port priority, effective values are integral multiples of 16, and the lower the value, the higher the priority.  Port priority is an important reference to determine whether the ports connected to port will be selected to work as root ports. Ports on downstream device connected to a port with a higher priority will be selected to work as root port under equivalent conditions
Path cost (0=AUTO)	Set the path cost of port.

Specification of list parameters:

Item	Description
Port	Display the serial number of ports of the switch.
Role	Display the role of port: Root, Designed, Alternate, Backup and --. "--" indicates that the port is not connected or that the STP function of switch is disabled.
State	Display the status of the port: Forwarding, Learning, Listening, Blocking, Discard, and Disable.
Link Status	Display the rate and duplexing mode of the port. Where, "--" indicates that the port is not connected or negotiation fails.
Path Cost	Display the path cost of the port.
Priority	Display the priority of the port.
Loopback Status	Display whether loop takes place in the downstream device of the port; if yes, display "Active", if not, display "--".

## 8.4 IGSP

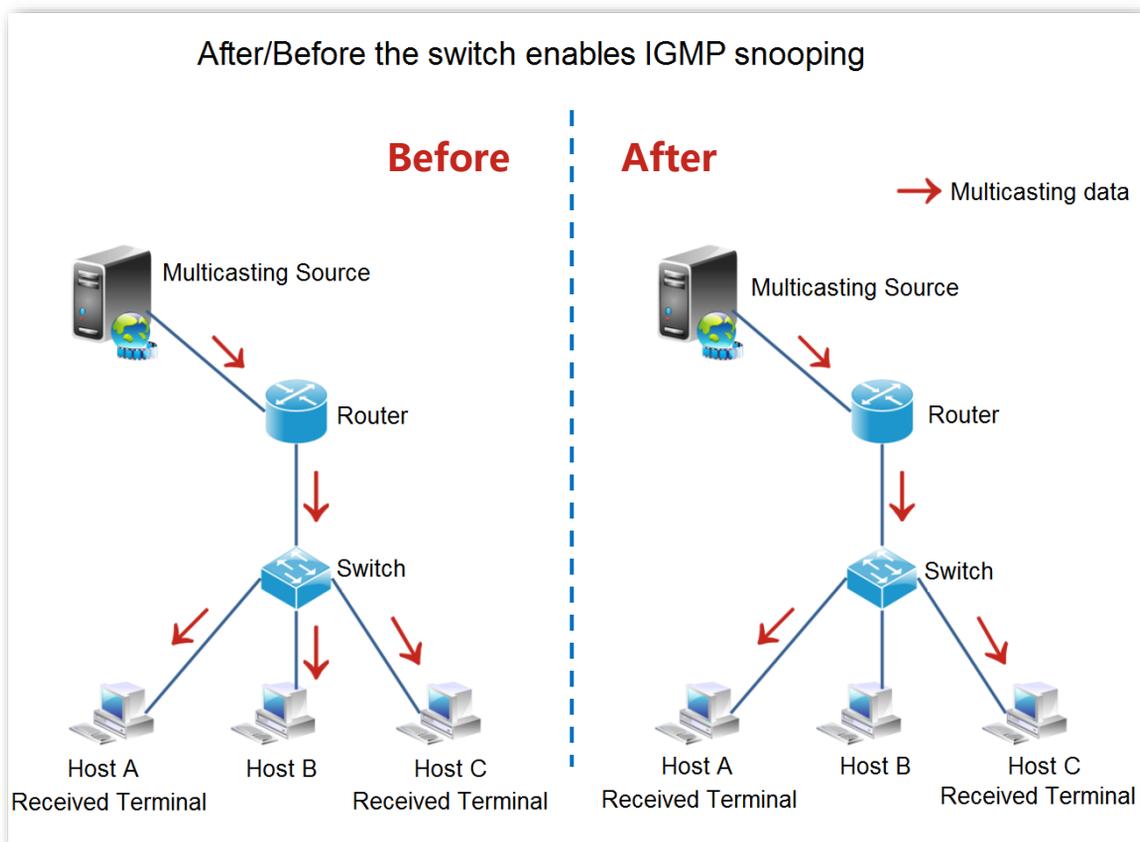
IGSP (Internet Group Management Protocol Snooping, IGMP Snooping) is a multicasting constraint mechanism running on the layer-2 device, and it is used to manage and control the multicasting groups.

The layer-2 device running the IGMP Snooping analyzes the received IGMP messages, establishes mapping relationship for the ports and MAC multicasting addresses, and forwards multicasting data as per such mapping relationships.

When the layer-2 device is not running IGMP snooping multicasting data are broadcast on layer 2. After layer-2 device runs IGMP snooping, the multicasting data of known multicasting groups will not be broadcast on layer 2, instead the data will be multicast to the designated receiver; however, the unknown multicasting data will still be broadcast on layer 2.

Primary function of IGMP snooping is to finish dynamic registration of layer-2 multicasting on the switch. To implement layer-2 multicasting by enabling IGMP snooping, IGMP shall be implemented on both the host and router, the switch is just to dynamically maintain the layer-2 multicasting group by snooping the IGMP messages of different types transmitted by host and router; in addition, the multicasting registration on the local switch will not be spread into other switches as a general rule. Only the ports joining the multicasting group can receive the multicasting data stream so as to reduce the network flow and save the network bandwidth.

A comparison diagram (after/before the switch enables IGMP snooping) is given below.



Click the **Device Management > IGSP** to access the IGMP Snooping configuration page, and the user can enable/disable the snooping function of the switch herein.

The screenshot displays the HIKVISION web management interface. On the left is a vertical navigation menu with the following items: Administration, Port Management, Link Aggregation, Network Extension, PoE Management, VLAN Management, **Device Management** (highlighted with a red bar), MAC, QoS, STP, **IGSP**, and SNMP. The main content area is titled 'IGMP Snooping' and features a sub-label 'IGMP Snooping' followed by a dropdown menu currently showing 'Disable'. To the right of the dropdown is a red 'OK' button with a save icon. In the top right corner of the main area, there is a red 'Help' icon. The HIKVISION logo is visible at the top left of the interface.

## 8.5 SNMP

### 8.5.1 Overview

SNMP (Simple Network Management Protocol) is the network management protocol applied most widely in the current TCP/IP network. Based on the SNMP, a management workstation can remotely manage all network devices supporting such a protocol, including monitoring the network state, modifying the network device configuration, and receiving the network event warnings.

SNMP can shield the physical differentiation of different devices, implement automated management of devices manufactured by different manufacturers, and is especially applicable to the small-size, rapid and low-cost environments.

#### 📌 Management framework of SNMP

SNMP management framework includes three component parts: SNMP administrator, SNMP agent and MIB base (Management Information Base).

- **SNMP administrator:** a system that controls and monitors network nodes using SNMP protocol. Where, the most common SNMP administrator in network environment is referred to as network management system (NMS). A network management system can indicate either a server specially set up to carry out network management, or an application program installed on a certain network device to implement the management functions.
- **SNMP agent:** a software module installed on a managed device to manage the management information data of the managed device and to report the management data to a SNMP management system when necessary.
- **MIB base:** a collection of managed objects. It defines a series of properties of the managed object: name, access authority and data type of the object. Each SNMP agent has its own MIB. SNMP administrator can carry out read/write operation on the objects listed in the MIB as per the authority.

SNMP administrator is the administrator of SNMP network, SNMP agent is the manager of the SNMP network, and the both exchange management information through SNMP protocol.

#### 📌 Basic operation of SNMP

In this switch, SNMP provides the following three basic operations to implement the exchange between the SNMP administrator and SNMP agent:

- **Get operation:** SNMP administrator uses the operation to inquire the values of one or more objects of the SNMP agent;
- **Set operation:** SNMP administrator uses the operation to reset the values of one or more object inside the MIB base;

- Trap operation: SNMP agent uses the operation to aggressively send a warning message to the SNMP administrator (for example: rebooting of a managed device).

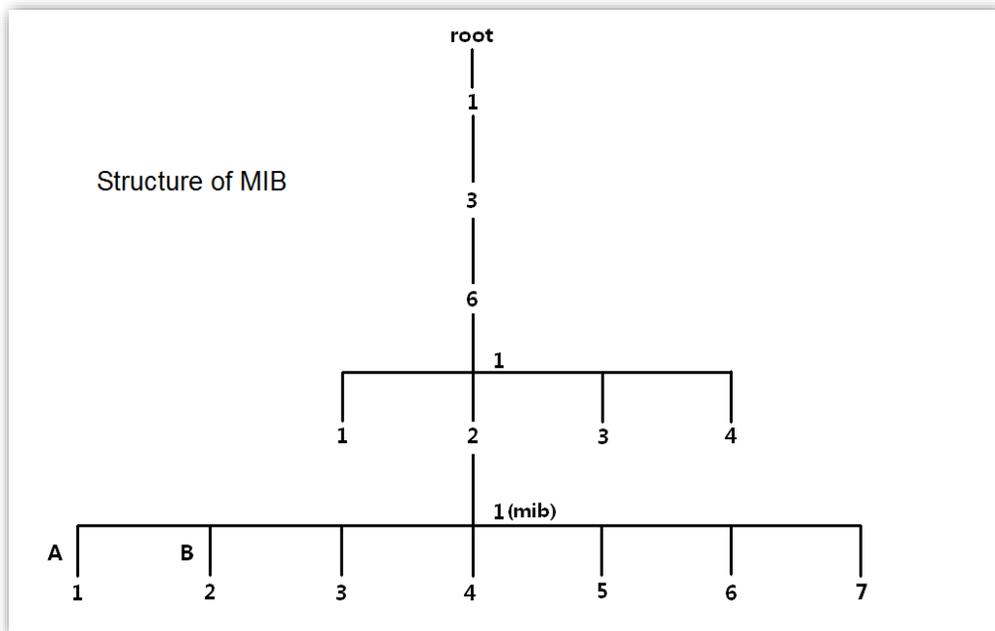
👉 **SNMP protocol version**

The switch is compatible with the versions such as SNMP v1 and SNMP v2c and allows group name authentication. SNMP group name is used to define the relationship between SNMP NMS and SNMP administrator. If the group name carried by SNMP message is not approved by the device, the message will be discarded. The group name functions as a password, and is used to restrict the SNMP administrator to access the SNMP agent.

SNMP v2c not only is compatible with SNMP v1, but also has expanded the functions of SNMP v1: It provides more operation types (GetBulk and InformRequest); supports more data types (such as Counter64); and provides richer error codes for even more meticulous error discrimination.

👉 **Brief introduction to the MIB base**

MIB is organized with a tree topology. Each tree node indicates a managed object, which can be uniquely identified by a numeral string starting from root and indicating the path; the numeral string is referred to as OID (Object Identifier). The structure of MIB is shown in the figure. As shown in Figure, OID of A is (1.3.6.1.2.1.1), while OID of B is (1.3.6.1.2.1.2).



## 8.5.2 Configure the SNMP

### 8.5.2.1 Configuration guidance

The SNMP configuration tasks of HIKVISION smart PoE switch series are given below:

Procedure	Configure the tasks	Specification
1	<a href="#">Enable the SNMP functions</a>	<b>Mandatory.</b> SNMP agent function of the switch is disabled by default.
2	<a href="#">Set the SNMP Community String</a>	Optional. The Read only community string of switch is “public” by default, and the Read & Write community string is “private”.
3	<a href="#">Set the SNMP Trap</a>	Optional. SNMP Trap function of the switch is disabled by default. If the switch is not required to aggressively report to SNMP administrator in case of failure or error, it is unnecessary to carry out this procedure.

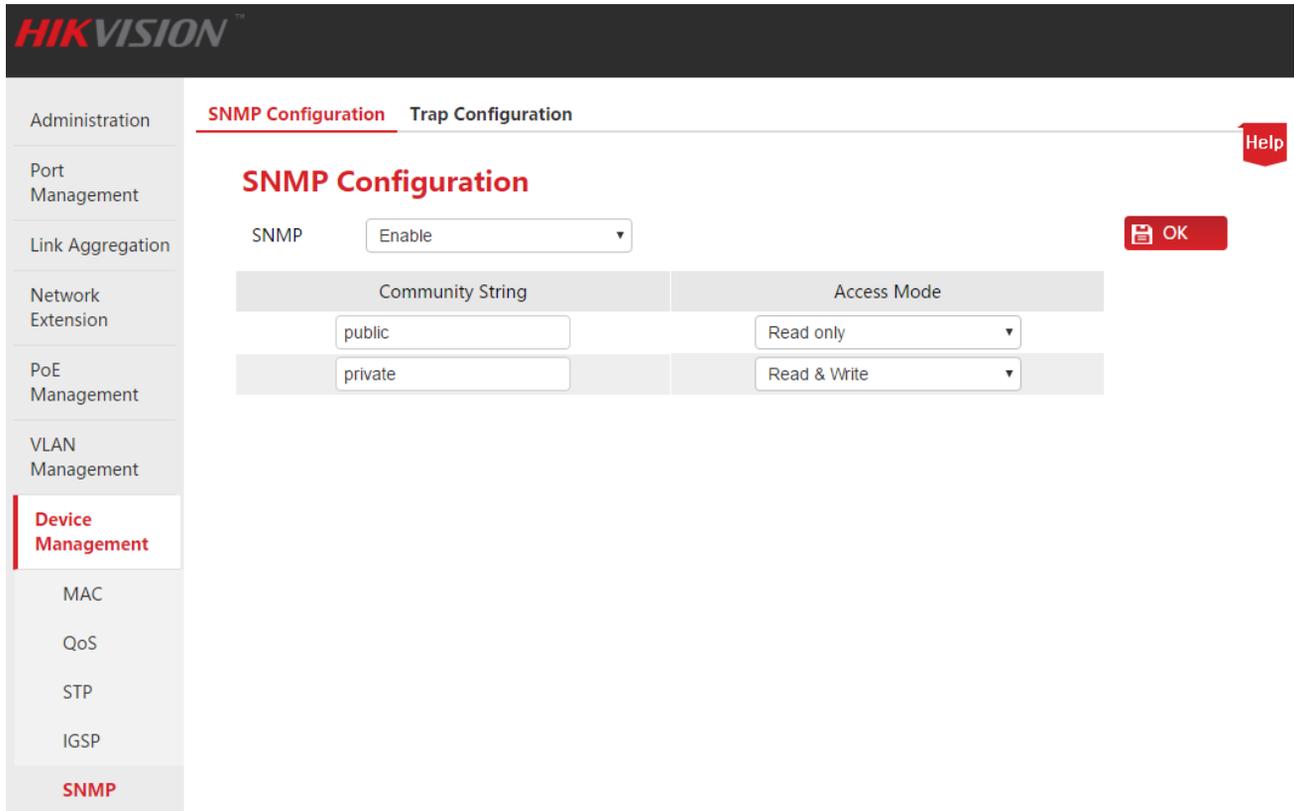
### 8.5.2.2 Configure the tasks

Please enable the SNMP function prior to other operations described in this section.

#### Enable the SNMP functions

##### Configuration Steps:

1. Log in to the Web network management of the switch, and then go to **Device management > SNMP** configuration page;
2. SNMP: Click the drop-down box, and select the **Enable**;
3. Click **OK**.



### Set the SNMP Community String

On the assumption that read-only group name is to be changed to “Jack”, and read/write group name is to be changed to “Jack 123”.

#### Configuration Steps:

1. Log in to the Web network management of the switch, and then go to **Device Management** > **SNMP** configuration page;
2. Community String: Click the input box below the group name column, and modify the Community String for Read only access mode and Read & Write access mode;



3. Click **OK**.

The screenshot shows the HIKVISION web interface for SNMP Configuration. The sidebar on the left includes options like Administration, Port Management, Link Aggregation, Network Extension, PoE Management, VLAN Management, Device Management (highlighted), MAC, QoS, STP, IGSP, and SNMP. The main content area displays the 'SNMP Configuration' page with a toggle set to 'Enable', a table for 'Community String' and 'Access Mode', and an 'OK' button.

Parameter Description:

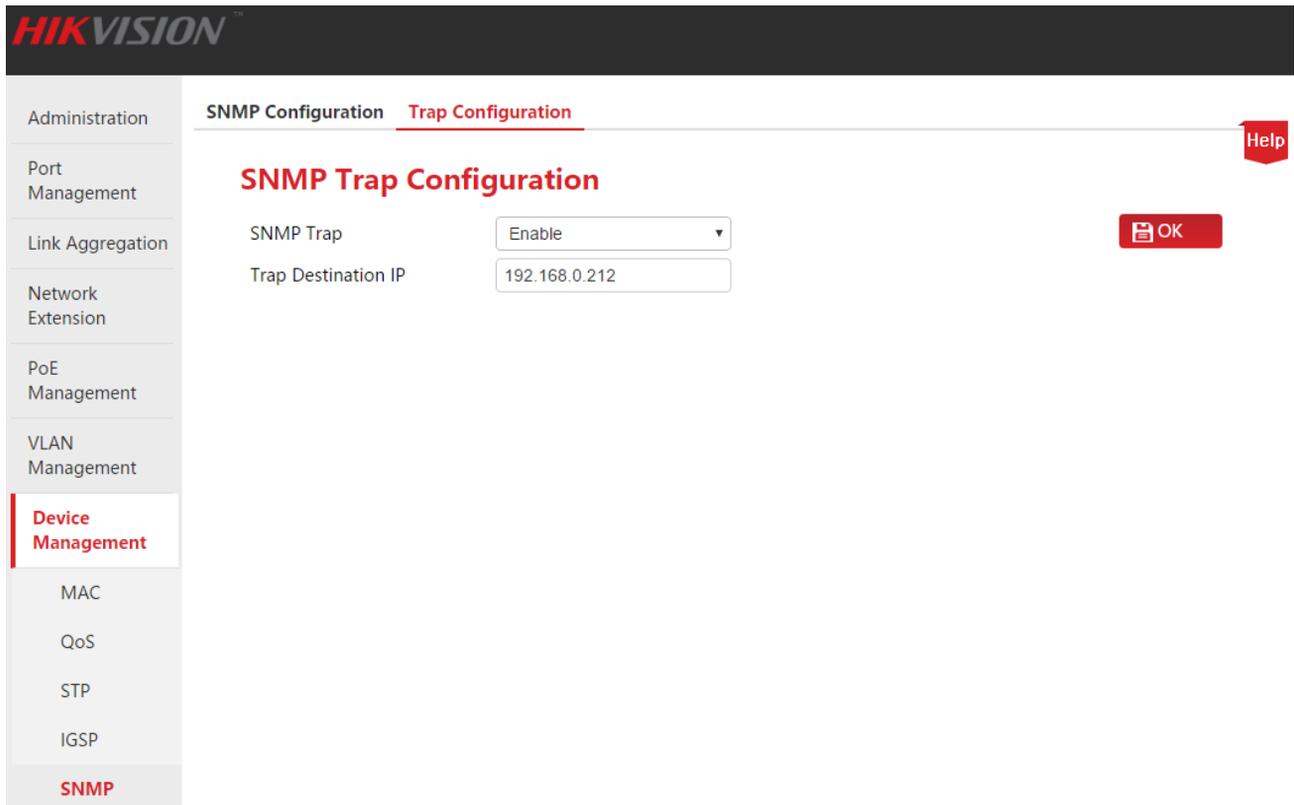
Item	Description
SNMP	Enable/Disable the SNMP agent function of the switch.
Community String	<p>Set the community string. The community string of “read-only” access mode is “public” by default, and the community string of “read/write” access mode is “private” by default.</p> <p>The length of a community string shall comprise 1~15 characters, in which no Chinese characters, single spaces, quotation marks and the following special characters within the following quotation marks (“/”, “&lt;”, “&gt;”, “ ”, “?”) are allowed to occur.</p>
Access Mode	<p>Select the access authority for the group for MIB views, and two types namely “read only” and “Read &amp; Write” are available.</p> <ul style="list-style-type: none"> <li>• Read only: Group has read-only authority for MIB views.</li> <li>• Read &amp; Write: Group has read-and-write authority for MIB views.</li> </ul>

**Set the SNMP Trap**

Trap function allows switch to transmit information aggressively to the SNMP administrator to report some emergency events. For the configuration steps give below, we assume that the IP address of SNMP administrator is 192.168.0.212.

**Configuration Steps:**

1. Log in to the Web network management of the switch, and then go to **Device Management > SNMP > Trap Configuration** page;
2. SNMP Trap: Click the drop-down box, and select the **Enable**;
3. Trap Destination IP: Enter the IP address of SNMP administrator;
4. Click **OK**.



Parameter Description:

Item	Description
SNMP Trap	Enable/Disable the SNMP Trap function of the switch. The default is disabled.
Trap Destination IP	<p>Enable the Trap function, and set the Trap destination IP address.</p> <p>In case an emergency milestone occurs on the switch, transmitting Trap information will be transmitted to the SNMP administrator on the host in which the Trap destination IP address is available.</p> <p> <b>Tip</b></p> <p>Trap destination IP address can only be set to a legal single-machine address falling within the same network segment as the switch, and no exceptional IP address can enable the Trap function.</p>

## 8.5.3 Application Scenarios

### Networking requirements

- The switch shall be connected to the SNMP administrator through Ethernet, the IP address of switch is 192.168.0.1/24, and the IP address of SNMP administrator is 192.168.0.212/24.
- SNMP administrator monitors and manages the switch through SNMP v1 or SNMP v2c, and the switch can aggressively report to the SNMP administrator in case a fault or error takes place.

### Networking assumption

Read only key is “Jack”, and Read & Write key is “Jack 123”.

### Networking diagram



### Configuration Steps

First, configure the switch.

**Step 1:** Enable the SNMP function of switch, and configure the SNMP community string.

1. Log in to the Web network management of the switch, and then go to **Device Management > SNMP** configuration page;
2. SNMP: Click the drop-down box, and select the **Enable**;
3. Community String: Read only group name is to be changed to “Jack”, and Read & Write community string is to be changed to “Jack123”;
4. Click **OK**.

The screenshot shows the HIKVISION web interface. On the left, a navigation sidebar lists various management categories: Administration, Port Management, Link Aggregation, Network Extension, PoE Management, VLAN Management, Device Management (highlighted), MAC, QoS, STP, IGSP, and SNMP. The main content area is titled 'SNMP Configuration' and has two tabs: 'SNMP Configuration' (active) and 'Trap Configuration'. The 'SNMP' status is set to 'Enable'. Below this, there are two rows of configuration options. The first row has 'Community String' set to 'Jack' and 'Access Mode' set to 'Read only'. The second row has 'Community String' set to 'Jack123' and 'Access Mode' set to 'Read & Write'. An 'OK' button is located in the top right corner of the configuration area.

**Step 2:** Allow the switch to aggressively report a fault or error message to the SNMP administrator

1. Go to **Device Management > SNMP > Trap Configuration** page;
2. SNMP Trap: Click the drop-down box, and select the **Enable**;
3. Trap Destination IP: Enter the IP address “192.168.0.212” of SNMP administrator;
4. Click **OK**.

The screenshot shows the HIKVISION web interface. On the left, a navigation sidebar lists various management categories: Administration, Port Management, Link Aggregation, Network Extension, PoE Management, VLAN Management, Device Management (highlighted), MAC, QoS, STP, IGSP, and SNMP. The main content area is titled 'SNMP Trap Configuration' and has two tabs: 'SNMP Configuration' and 'Trap Configuration' (active). The 'SNMP Trap' status is set to 'Enable'. Below this, there is a 'Trap Destination IP' field containing the value '192.168.0.212'. An 'OK' button is located in the top right corner of the configuration area.

**Second, configure the SNMP administrator.**

On the SNMP management software of SNMP v1 /v2c version, set the “Read only community string” and “Read & Write community string”, and notice that they shall be kept in line with the switch configuration. Refer to the manual supporting SNMP management software for specific methods.

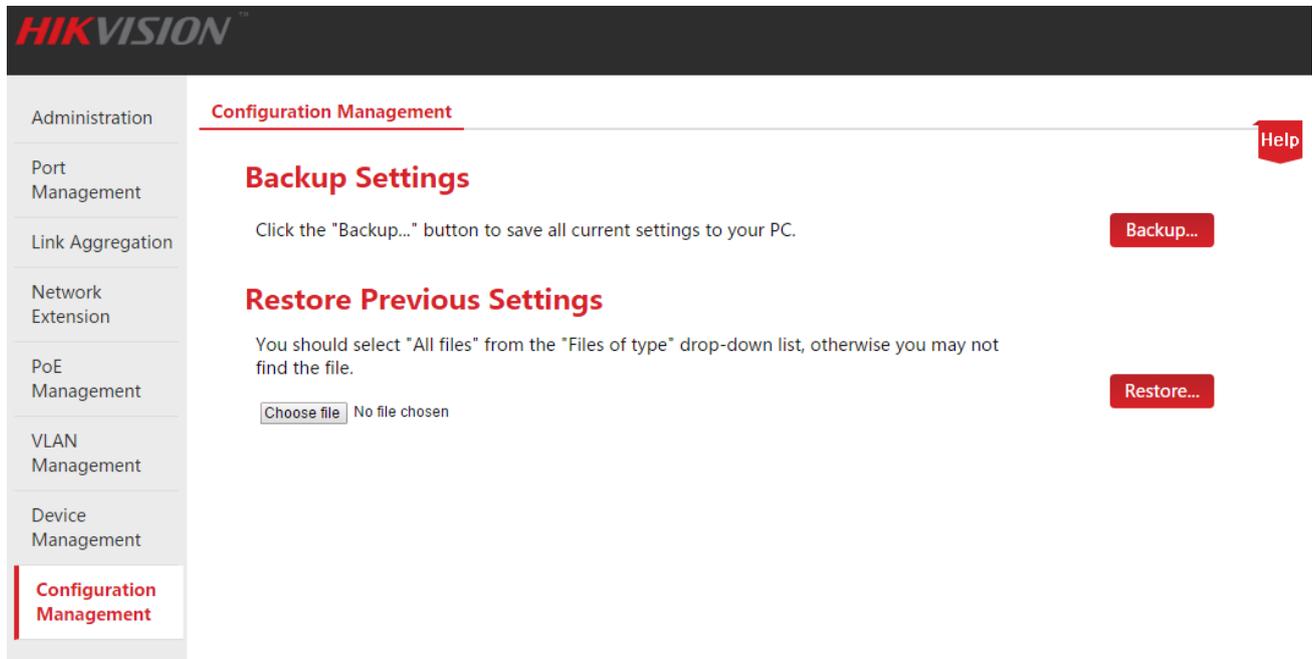
**Verify configuration**

When the above-mentioned setting is finished, SNMP administrator can establish SNMP connection with the SNMP agent on the switch, and inquire and set the values of some parameters through the MIB nodes.

If a fault or error occurs on the switch, SNMP administrator can see corresponding warning message.

# 9 Configuration Management

To back-up/restore the configuration here, click the **Configuration Management** to access the page.



The screenshot displays the HIKVISION web interface for Configuration Management. On the left is a sidebar menu with the following items: Administration, Port Management, Link Aggregation, Network Extension, PoE Management, VLAN Management, Device Management, and Configuration Management (which is highlighted with a red bar). The main content area has a dark header with the HIKVISION logo and a 'Help' button. Below the header, the page title is 'Configuration Management'. The first section is 'Backup Settings', which includes the instruction 'Click the "Backup..." button to save all current settings to your PC.' and a red 'Backup...' button. The second section is 'Restore Previous Settings', which includes the instruction 'You should select "All files" from the "Files of type" drop-down list, otherwise you may not find the file.' and a red 'Restore...' button. Below this instruction is a file selection area with a 'Choose file' button and the text 'No file chosen'.

## 9.1 Backup Settings

If you have made a lot of configuration on the switch such that it may have a better status or can preferably fulfill the requirements of corresponding scenes, it is recommended to back up the existing configuration, in order to facilitate the troubleshooting and save the time for next configuration.

**Backup Settings:** Click **Backup...** and perform operations as per the prompts given in the Web network management page.

## 9.2 Restore Previous Settings

If you have to make the same configuration on several switches, or performance degradation of switch occurs due to some inadvertent operations performed by you, you can use the restoration configuration function to restore the original switch configuration of the switch.

**Restore Previous Settings:** Click the **Choose file** in the pop window, find and double click the formerly backed-up configuration file. Click **Restore...**, the switch imports the configuration file, and the configuration gets valid once rebooting is finished.