

PoE Switch (16/24-Port Managed Desktop Switch)

Web Operation Manual








Foreword

General

This manual introduces operations on web page of the 16&24-port managed desktop switch (hereinafter referred to as "the Switch"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.1	<ul style="list-style-type: none">• Updated general contents.• Added initializing steps.• Updated login steps.• Deleted DHCP.• Updated contents of configuring STP bridge.• Updated contents of configuring VLAN example.• Updated contents and configuration steps of link aggregation.• Updated contents and configuration steps of configuring HTTPS.• Deleted configuring QoS.• Deleted contents of port authorized status.• Updated configuration steps of configuring PoE settings.• Added configuring NAS and configuring Radius.• Added steps of configuring IGMP snooping.• Added steps of configuring legacy support and PD alive.	June 2022
V1.0.0	First release.	May 2021

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited to: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, comply with the guidelines when using it.

Operating Requirements



- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.
- Operating temperature range: $-10\text{ }^{\circ}\text{C}$ to $+55\text{ }^{\circ}\text{C}$ ($+14\text{ }^{\circ}\text{F}$ to $+131\text{ }^{\circ}\text{F}$).
- This is a class A product. In a domestic environment this might cause radio interference in which case the user may be required to take adequate measures.

Installation Requirements



- Connect the device to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the device.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.



- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Make sure the device is in horizontal installation, and install the device on solid and flat surface to avoid falling down.
- Use the power adapter or case power supply provided by the device manufacturer.
- Voltage stabilizer and lightning protection device are optional according to power supply and surrounding environment.
- Make sure to ground the device (cross section of copper wire: $> 2.5\text{ mm}^2$; resistance to ground: $\leq 4\ \Omega$).
- To ensure heat dissipation, the gap between the device and the surrounding area should not be less than 10 cm on the sides and 10 cm on top of the device.
- Connect class I electrical appliances to a power socket with protective earthing.

- Do not block the ventilator of the device with objects, such as newspapers, table clothes or curtains.
- Do not put open flames, such as a lit candle, on the device.
- When installing the device, make sure the power plug and appliance coupler are easy to reach to cut off the power.

Maintenance Requirements



When replacing the battery, make sure that the same type is used. Improper battery use might result in explosion.



- Power off the device before maintenance.
- Mark key components on the maintenance circuit diagram with warning signs.

Table of Contents

Foreword	I
Important Safeguards and Warnings.....	III
1 Login	1
2 Device Information.....	2
3 Configuring System.....	3
3.1 Configuring System Info	3
3.1.1 Viewing System Info.....	3
3.1.2 Configuring Current Time	4
3.1.3 Viewing CPU Usage.....	4
3.2 Configuring Network.....	4
3.3 Upgrading Software.....	5
3.4 Changing Password.....	6
3.5 Restoring to Default.....	6
3.6 Restarting the System	7
3.7 Log Information.....	7
3.8 Viewing Legal Information	8
4 Port Management	9
4.1 Configuring Port	9
4.2 Configuring Port Mirroring.....	10
4.3 Configuring Port Statistics.....	11
4.4 Configuring Port Speed Limit.....	12
4.5 Configuring Broadcast Storm Control	13
4.6 Long Distance Transmission	14
4.7 Port Isolation.....	15
5 Device Management.....	17
5.1 Ring Network.....	17
5.1.1 STP Definition.....	17
5.1.2 Configuring STP Bridge	17
5.1.3 Configuring STP Port	18
5.2 Configuring VLAN.....	19
5.2.1 VLAN Definition.....	19
5.2.2 VLAN Function.....	19
5.2.3 Port-based VLAN.....	20
5.2.4 Configuring VLAN List.....	21
5.2.5 Configuring Port VLAN	22

5.2.6 Example of Configuring VLAN.....	24
5.3 Link Aggregation	24
5.3.1 Static Aggregation Mode.....	25
5.3.2 LACP Mode	26
5.4 Security	27
5.4.1 MAC Address List	27
5.4.2 Binding Port MAC	28
5.4.3 Filtering Port MAC	29
5.5 Configuring SNMP	30
5.5.1 SNMP Protocol Version	30
5.5.2 Configuring SNMP	31
5.5.3 Example of SNMPv1/v2 Configuration	32
5.5.4 Example of SNMPv3 Configuration	32
5.6 802.1x	34
5.6.1 802.1x Networking Structure	34
5.6.2 802.1x Authentication Controlled/Uncontrolled Port	35
5.6.3 Trigger Mode of 802.1x Authentication	35
5.6.4 Configuring NAS.....	36
5.6.5 Configuring Radius	37
5.7 IGMP Snooping	38
5.7.1 IGMP Snooping Theory	38
5.7.2 Configuring IGMP Snooping	39
5.8 Configuring HTTPS.....	39
6 PoE	44
6.1 Configuring PoE Power.....	44
6.2 Viewing PoE Event Statistics.....	46
6.3 Configuring Green PoE	47
6.4 Configuring Legacy Support.....	48
6.5 Configuring PD Alive	48
Appendix Cybersecurity Recommendations.....	50

1 Login

Prerequisites

- The main program file running on the Switch must support web access.
- The IP address of the computer and the Switch must be on the same network segment.

Procedure

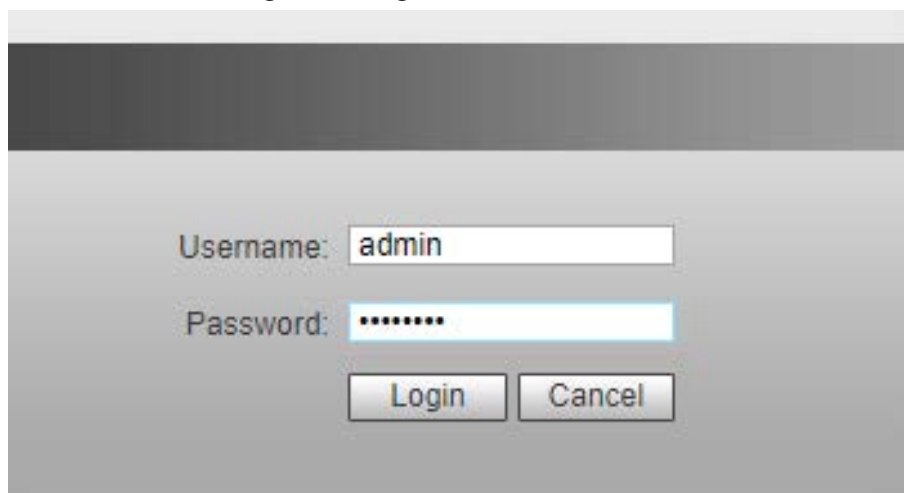
Step 1 Enter the IP address of the Switch (192.168.1.110 by default) in the address bar and press the Enter key.

Step 2 Enter the username and password, and then click **Login**.



- The username and the password are admin and admin123 by default.
- Change the password after the first login. The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
- For details on changing the password, see "3.4 Changing Password".

Figure 1-1 Log in to the web



The screenshot shows a web login interface with a dark header bar. Below the header, there are two input fields: "Username:" with the text "admin" and "Password:" with masked characters "*****". At the bottom of the form are two buttons: "Login" and "Cancel".

2 Device Information

You can view the information on the Switch.

Figure 2-1 Web management

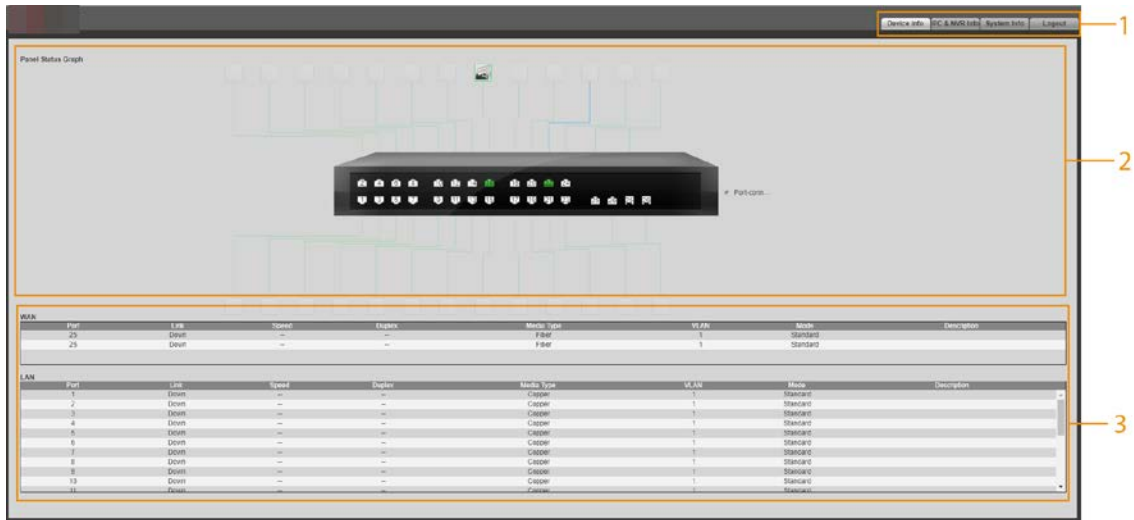


Table 1-1 Description of the web page

No	Function	Description
1	Navigation bar	<ul style="list-style-type: none"> ● Device Info: View information on the Switch. ● System Info: Configure the Switch by accessing System Config, Port Management, Device Management and PoE. ● Logout: Return to the login page.
2	Panel status graph	<ul style="list-style-type: none"> ● Switch port is green: Successfully connected to the port. ● Switch port is white: Failed to connect to the port.
3	Port info	Displays information on the port status of WAN and LAN, including the current port link status, port speed, duplex mode.

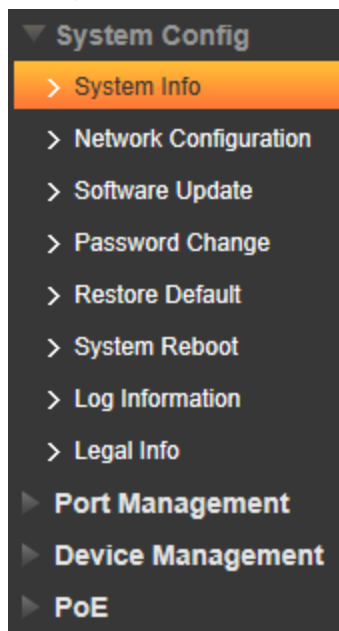
3 System Configuration

3.1 Configuring System Information

This section introduces operations of viewing system information, configuring system time, and viewing CPU usage.

Select **System Config** > **System Info**, and then you will see the options in the menu.

Figure 2-1 System configuration



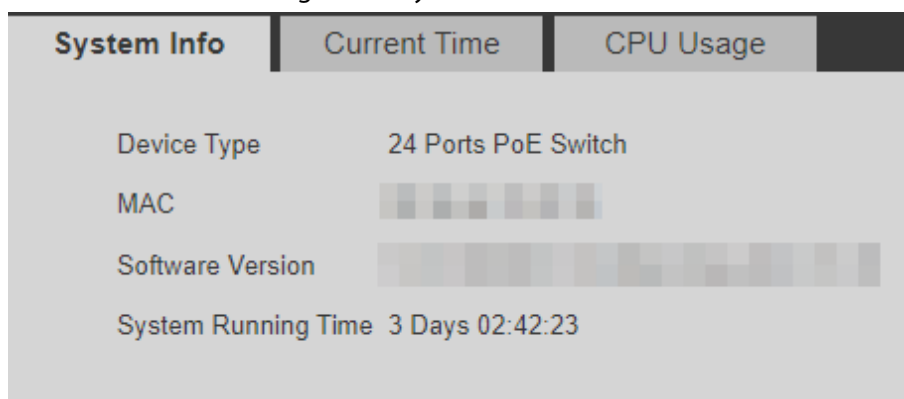
3.1.1 Viewing System Information

You can view information on the Switch model, MAC address and software version.

Step 1 Select **System Config** > **System Info** on the **System Info** page.

Step 2 View the system information of the Switch.

Figure 2-2 System info



3.1.2 Configuring Current Time

You can view and configure the current time and time zone of the Switch.

Step 1 Select **System Config > System Info > Current Time** on the **System Info** page.

Step 2 Configure the Switch time. There are two ways to configure the time.

- Manually configure the **Current Time** and **Time Zone**, and then click **Save**.
- Click **Sync PC** to sync the Switch time to the computer time.

Figure 2-3 Current time

System Info	Current Time	CPU Usage
Current Time	2000-05-06	05 : 01 : 34
Time Zone	GMT+08:00	
	Sync PC	Refresh Save

3.1.3 Viewing CPU Usage

Step 1 Select **System Config > System Info > CPU Usage** on the **System Info** page.

Step 2 View the CPU usage of the Switch.

Figure 2-4 CPU usage

System Info	Current Time	CPU Usage
Last5(seconds)	84%	
Last1(minute)	8%	
Last5(minutes)	8%	

3.2 Configuring Network

This section introduces the operations of viewing and configuring the IP address, subnet mask, default gateway and MAC address of the Switch.

Background Information

DHCP (Dynamic Host Configuration Protocol) is used to dynamically allocate IP address and other network configuration parameters for the network devices.


Procedure

Step 1 Select **System Config > Network Configuration** on the **System Info** page.

Figure 2-5 Network configuration

Step 2 Configure parameters.

Table 2-1 Description of the network configuration

Parameter	Description
Mode	<p>Select the mode for the Switch to obtain IP.</p> <ul style="list-style-type: none"> • Static: Manually configure the IP Address, Subnet mask and Default Gateway. After clicking Save, you will automatically be redirected to the login page of the new IP address. • DHCP: When there is a DHCP server on the network, select DHCP and the Switch will automatically obtain a dynamic IP address, saving you from configuring the IP address and other information.
IP address	<p>When the mode is set to Static, enter the IP address, subnet mask and default gateway according to your network plan.</p>
Subnet mask	
Default gateway	<p></p> <ul style="list-style-type: none"> • The IP address and the default gateway must be on the same network segment. • Do not modify the subnet mask at random. You might not be able to log in to the Switch in the future.
MAC address	The physical address of the Switch, which cannot be modified.

Step 3 Click **Save**.

3.3 Upgrading Software

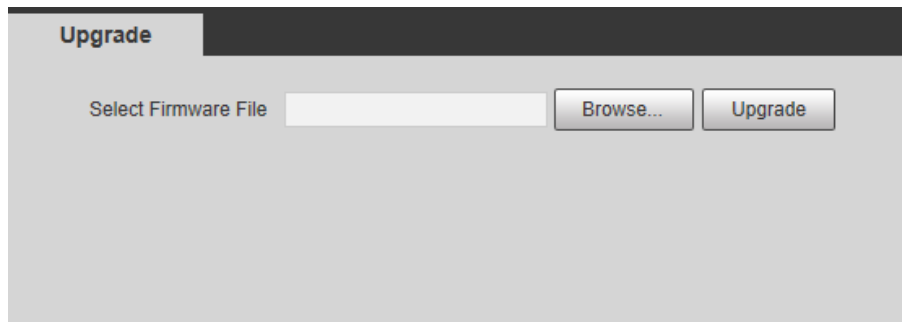
Prerequisites

Before upgrading, please contact technical support to obtain the latest system file.

Procedure

Step 1 Select **System Config > Software Upgrade** on the **System Info** page.

Figure 2-6 Upgrading software



Step 2 Click **Browse...** to choose the upgrade file.

Step 3 Click **Upgrade**.

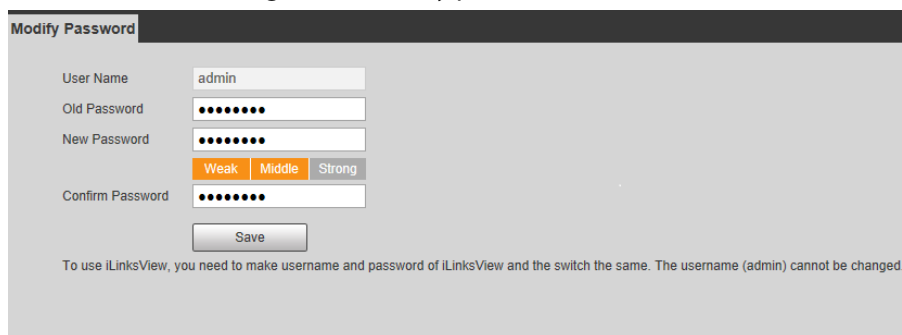
3.4 Changing Password

You can change the user login password in the **Password Change** tab. The username is admin by default, which cannot be changed. The default password is admin123, which can be changed.

Step 1 Select **System Config > Password Change** on the **System Info** page.

Step 2 Enter **Old Password**, **New Password** and **Confirm Password**.

Figure 2-7 Modify password



Step 3 Click **Save**.

3.5 Restoring to Default

You can restore the Switch to its default settings. There are two methods to restore the Switch to its default settings.



After the Switch is reset, all configurations will be restored to default settings, and the management address will be reset to 192.168.1.110. You need to change the password at your next login.

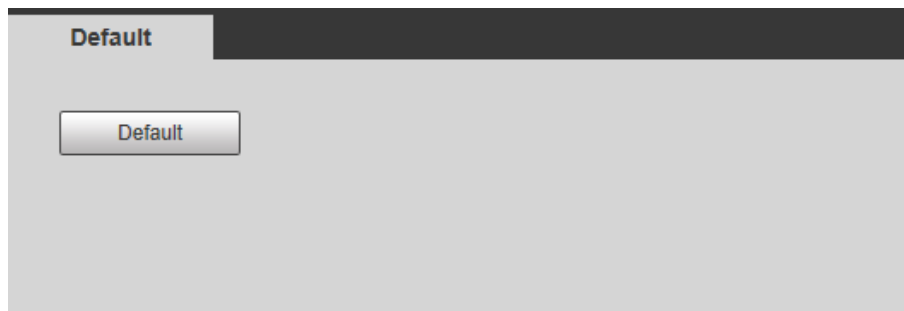
- Press and hold the Reset button of the Switch for 5 seconds.
- Restore the Switch to the default settings on the web page. This section uses this method as an example to introduce how to restore to the default settings.

Procedure

Step 1 Select **System Config > Restore Default** on the **System Info** page.

Step 2 Click **Default** to restore the Switch to its default settings.

Figure 2-8 Restore to default



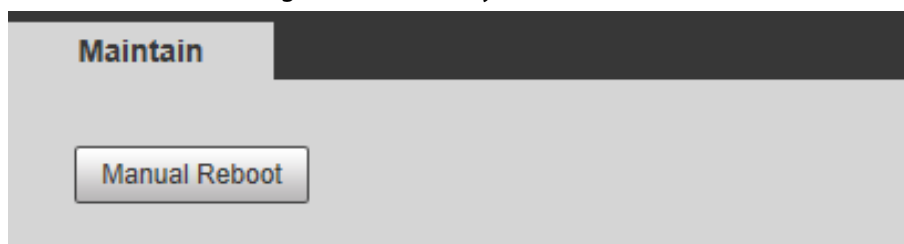
3.6 Restarting the System

The Switch can be restarted. Make sure to save the configurations before restarting the Switch, otherwise all the configurations will be lost. You need to log in to the web page again after the Switch restarts.

Step 1 Select **System Config** > **System Reboot** on the **System Info** page.

Step 2 Click **Manual Reboot**.

Figure 2-9 Restart system



3.7 Log Information

The system log displays information on the Switch operations.

Step 1 Select **System Config** > **Log Information** on the **System Info** page.

Step 2 Configure **Start Time** and **End Time**.

Step 3 Select **Log Type**, including **Error**, **Warning** and **Info**.

Step 4 Click **Search**.

Figure 2-10 Log information

The screenshot shows a web interface titled "Log". At the top, there are search filters: "Start Time" set to "2021-09-16 16 : 54 : 08", "End Time" set to "2021-09-17 16 : 54 : 08", and "Log Type" set to "All". A "Search" button is located to the right of the "Log Type" dropdown. Below the filters is a table with the following headers: "No.", "Log Time", "User", "Address", "Log Type", and "Description". The table body is currently empty. At the bottom left, there is a "Clear" button. At the bottom right, there are navigation controls including a "1 / 1" indicator and a "1" button.

3.8 Viewing Legal Information

You can view the software license agreement, privacy policy and open source software notice.

Step 1 Select **System Config** > **Legal Info** on the **System Info** page.

Step 2 View related legal information.

4 Port Management

4.1 Configuring Port

Port configuration can be used to configure basic parameters which are related to switch port. The port parameters will directly affect the working mode of the port. Make configurations according to the practical requirements.

Step 1 Select **Port Management > Port Configuration** on the **System Info** page.



Figure 3-1 Configure port

Port	Description	Link	Enable	Speed Duplex Status	Speed Duplex Setting	Flow Control Status	Flow Control Setting
1		Down	On	100M Full	Auto	Off	On
2		Down	On	100M Full	Auto	Off	On
3		Down	On	100M Full	Auto	Off	On
4		Down	On	100M Full	Auto	Off	On
5		Down	On	100M Full	Auto	Off	On
6		Down	On	100M Full	Auto	Off	On
7		Down	On	100M Full	Auto	Off	On
8		Down	On	100M Full	Auto	Off	On
9		Down	On	100M Full	Auto	Off	On
10		Up	On	100M Full	Auto	Off	On
11		Down	On	100M Full	Auto	Off	On
12		Down	On	100M Full	Auto	Off	On
13		Down	On	100M Full	Auto	Off	On
14		Down	On	100M Full	Auto	Off	On
15		Down	On	100M Full	Auto	Off	On
16		Down	On	100M Full	Auto	Off	On
17		Down	On	100M Full	Auto	Off	On
18		Down	On	100M Full	Auto	Off	On

Step 2 Configure port parameters.

Table 3-1 Description of parameters

Parameter	Description
Port	Displays the Switch port number.
Description	Add description information for port.
Link	Displays the port link status.
Enable	Configure port on and off. <ul style="list-style-type: none"> On: Enable the link. Off: Disable the link.
Speed Duplex Status	Displays the status of the port speed.

Parameter	Description
Speed Duplex Setting	<p>Configure the modes of the port speed duplex.</p> <ul style="list-style-type: none"> • Ethernet port. <ul style="list-style-type: none"> ◇ Auto (default): Auto negotiation mode. ◇ 10 M FULL: 10 M full duplex. ◇ 10 M HALF: 10 M half duplex. ◇ 100 M FULL: 100 M full duplex. ◇ 100 M HALF: 100 M half duplex. ◇ 1000 M FULL: 1000 M full duplex. • Fiber port. <ul style="list-style-type: none"> ◇ 1000 M FULL: 1000 M full duplex. <p> The port communication can be directly affected if you change the port speed duplex mode. Please be advised.</p>
Flow Control	<p>Configure the Switch flow control.</p> <ul style="list-style-type: none"> • On: Enable port flow control function. • Off: Disable port flow control function. <p> For Ethernet port, you need to enable port flow control function to synchronize the inbound speed and the outbound speed to avoid packet losses.</p>

Step 3 Click **Save**.

4.2 Configuring Port Mirroring

Port mirroring (also called port monitor) is the process of copying the packet of a port or several ports (called the source port) to another port (called the destination port), which is connected with a monitoring device for packet analysis. This enables monitoring the network and resolving the network malfunction.

Step 1 Select **Port Management > Port Mirroring** on the **System Info** page.

Step 2 Configure parameters.

Figure 3-2 Configure port mirroring

The screenshot shows a 'Port Mirroring' configuration window. At the top, there are two dropdown menus: 'Monitored Packets' set to 'Egress' and 'Dest Port' set to '1'. Below these is a table with 18 rows, each representing a source port. The table has two columns: 'Src Port' and 'Enable'. The 'Enable' column contains checkboxes. Ports 2 and 3 have their checkboxes checked and are highlighted in yellow. Ports 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, and 18 have their checkboxes unchecked. At the bottom of the window, there are two buttons: 'Save' and 'Refresh'.

Table 3-2 Description of parameters

Parameter	Description
Monitored Packets	<p>Select mirrored packets.</p> <ul style="list-style-type: none"> • Disable (default): Disable the monitor function. • Egress: Monitor output packets. • Ingress: Monitor input packets. • Ingress & Egress: Monitor input/output packets.
Dest Port	The Port that is used to monitor. You can select only one port. The default setup is disabled.
Src port	The port that is being monitored. Select one or more port(s).
Enable	Enable the function on the selected ports.

Step 3 Click **Save**.

4.3 Configuring Port Statistics

You can view port statistics including the transmit/receive packet amount of each port, collision statistics, drop packet and CRC error packet. The port working performance is low if the error packet amount is too huge. Check the port cable connection or confirm corresponding opposite port has problem or not.

Procedure

Step 1 Select **Port Management > Port Statistics** on the **System Info** page.

Figure 3-3 Configure port statistics

Port	Transmit Packet	Receive Packet
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	5	3
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0

Step 2 Select **Counter Mode Selection**, including **Transmit Packet & Receive Packet**, **Collision Packet & Transmit Packet**, **Drop Packet & Receive Packet** and **CRC (Cyclic Redundancy Check) Error Packet & Receive Packet**, and then view the results.



If there are too many error packets from the port, the working status of the port is very poor. Make sure to check if there is a problem with the cable connected to the port or the Switch.

Related Operations

- Clear statistic results: Click **Clear**.
- Refresh statistic results: Click **Refresh**.

4.4 Configuring Port Speed Limit

You can set port speed limit parameters, and restrict exchanging rate of inbound/outbound data packets.

Step 1 Select **Port Management > Port Speed Limit** on the **System Info** page.

Step 2 Configure parameters.

Figure 3-4 Port speed limit

Port	Tx Rate(Mbps)	Rx Rate(Mbps)
1	0	0
2	50	50
3	50	50
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0

Save

Table 3-3 Description of the port speed limit parameter

Name	Note
Port	Displays port list.
Tx Rate	Set port outbound rate. The value ranges from 0 through 63 Mbps. The default setup is 0, which means there is no speed limit.
Rx Rate	Set port inbound rate. The value ranges from 0 through 63 Mbps. The default setup is 0, which means there is no speed limit.

Step 3 Click **Save**.

4.5 Configuring Broadcast Storm Control

Background Information

The broadcast frames on the network are forwarded continuously, which affects the proper communications, and greatly reduces the network performance. The storm control can limit the broadcast flows of the port and discard the broadcast frames once the flow exceeds the specified threshold, which can reduce the risk of the broadcast storm and ensure the network proper operation.

Procedure

- Step 1 Select **Port Management > Broadcast Storm Control** on the **System Info** page.
- Step 2 Configure **Threshold**.

Step 3 Select ports that need to be configured, and then select **Enable** to configure all-port broadcast storm control function.



You need to configure all the ports in case there might be malfunctions, and the Switch cannot properly transmit the data.

Figure 3-5 Configure broadcast storm control

Broadcast Storm Control

Threshold (1~63)

Threshold is the number of broadcast packets allowed to enter each port over a span of time. This time depends on the connection speed and is as follows: 10Mbps is 5ms, 100Mbps is 500us, and 1Gbps is 50us.

Port	<input checked="" type="checkbox"/> Enable
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>
7	<input checked="" type="checkbox"/>
8	<input checked="" type="checkbox"/>
9	<input checked="" type="checkbox"/>
10	<input checked="" type="checkbox"/>
11	<input checked="" type="checkbox"/>
12	<input checked="" type="checkbox"/>
13	<input checked="" type="checkbox"/>
14	<input checked="" type="checkbox"/>
15	<input checked="" type="checkbox"/>
16	<input checked="" type="checkbox"/>
17	<input checked="" type="checkbox"/>
18	<input checked="" type="checkbox"/>

Step 4 Click **Save**.

4.6 Long Distance Transmission

You can set port long distance transmission mode. For the standard Ethernet mode, the transmission speed can become 10 Mbps/250 meters instead of 100 Mbps/100 meters.

Step 1 Select **Port Management > Long Distance PoE** on the **System Info** page.

Step 2 Select the checkbox under **Enable** in the corresponding port.

Figure 3-6 Configure long distance

Long Distance

Enabling Long Distance extends the maximum distance from 100m to 250m. However, this will drop the connection speed from 100Mbps to 10Mbps.

<input type="checkbox"/> Enable	Port
<input checked="" type="checkbox"/>	1
<input checked="" 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"/>	11
<input type="checkbox"/>	12
<input type="checkbox"/>	13
<input type="checkbox"/>	14
<input type="checkbox"/>	15
<input type="checkbox"/>	16

Step 3 Click **Save**.

4.7 Port Isolation

Port isolation is to achieve layer 2 isolation between messages. You only need to add the port to the isolation group to isolate the layer 2 data between the ports in the isolation group. The port isolation function provides users a safer and more flexible networking solution.

Step 1 Select **Port Management > Port Isolation** on the **System Info** page.

Step 2 Select **Enable** in the **Mode** drop-down list.

Step 3 Click **Save** on the right side of the mode.



Port isolation and VLAN are mutually exclusive. When port isolation is enabled, the VLAN will be automatically disabled.

Figure 3-7 Configure port isolation

Port Isolation

Mode

VLAN and port isolation cannot be enabled simultaneously. Use with caution!

Port	<input type="checkbox"/> Enable
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>
7	<input checked="" type="checkbox"/>
8	<input checked="" type="checkbox"/>
9	<input type="checkbox"/>
10	<input type="checkbox"/>
11	<input type="checkbox"/>
12	<input type="checkbox"/>
13	<input type="checkbox"/>
14	<input type="checkbox"/>
15	<input type="checkbox"/>
16	<input type="checkbox"/>
17	<input type="checkbox"/>

Step 4 Select checkbox under **Enable** to select one or more ports to be isolated.

Step 5 Click **Save** below the port list.

5 Device Management

5.1 Ring Network

5.1.1 STP Definition

The protocol message adopted by STP is BPDU (Bridge Protocol Data Unit), which is also called configuration information. BPDU contains enough information to ensure the calculation process of spanning tree. STP can confirm network topological structure by transmitting BPDU among devices. BPDU format and field description can realize the functions of spanning tree. Information is interacted by transmitting BPDU message among switches. All the switches which support STP protocol will receive and deal with the received message. The message carries all the useful information in the data area which can be used for spanning tree calculation.

Figure 4-1 Frame format and field description of STP

Protocol Identifier	Version	Message Type	Flag	Root ID	Root Path Cost
Bridge ID	Port ID	Message Age	Max Age	Hello Time	Forward Delay

- Protocol Identifier: The identification of protocol.
- Version: The protocol version.
- Message Type: BPDU type.
- Flag: Flag bit.
- Root ID: Root bridge ID, which is made up of 2-byte priority and 6-byte MAC address.
- Root Path Cost: The cost of root path.
- Bridge ID: The ID of bridge that sends BPDU, which is made up of 2-byte priority and 6-byte MAC address.
- Port ID: Identifies the port that sends BPDU.
- Message Age: Life time of BPDU.
- Max Age: Aging time of current BPDU, also the longest time for port to save BPDU.
- Hello Time: The period cycle of Bridge Root sending BPDU.
- Forward Delay: The time of maintaining snoop and study status before sending data package, after topology is changed.

5.1.2 Configuring STP Bridge

Step 1 Select **Device Management > Spanning Tree > STP Bridge Settings** on the **System Info**

page.

Figure 4-2 STP bridge settings

STP Bridge Settings | STP Port Settings

STP Mode: (v)

Bridge Priority: (0~61440)

Hello Time: (1~10 Sec)

Max Age: (6~40 Sec)

Forward Delay: (4~30 Sec)

When STP is enabled, the device cannot be managed through iLinksView

Step 2 Configure parameters.

Table 4-1 Description of the STP bridge settings

Parameter	Description
STP Mode	Enable or disable ring network function. <ul style="list-style-type: none">• When STP is enabled, the Switch cannot be managed through iLinksView.• STP mode and link aggregation function are mutually exclusive. After configuring link aggregation, STP mode cannot be enabled.
Bridge Priority	Set bridge priority. The value ranges from 0 to 61440.
Hello Time	Set the period of root bridge sending BPDU. The time ranges from 1 s to 10 s.
Max Age	Set the aging time of current BPDU. The time ranges from 6 s to 40 s.
Forward Delay	After setting topological change, the bridge maintains the time of snooping and study state. The time ranges from 4 s to 30 s.

Step 3 Click **Save**.

5.1.3 Configuring STP Port

Step 1 Select **Device Management > Spanning Tree > STP Port Settings** on the **System Info** page.

Figure 4-3 Configure STP port

Step 2 Configure parameters.

Table 4-2 Description of parameters

Parameter	Description
Port No.	Select the port you want to configure.
Priority	Configure the port priority. The value ranges from 0 to 240, and must be the integral multiple of 16.
RPC	Configure the path cost from the current port to root bridge. The value ranges from 1 to 200000000. The path cost is default when RPC is set as 0.

Step 3 Click **Save**.

5.2 Configuring VLAN

5.2.1 VLAN Definition

Logically, one LAN (Local Area Network) can be divided into many subsets. Each subset has its own broadcast area: virtual LAN (VLAN). A VLAN is divided from a LAN on a logical basis rather than on a physical basis, to realize the isolated broadcast area in the VLAN.

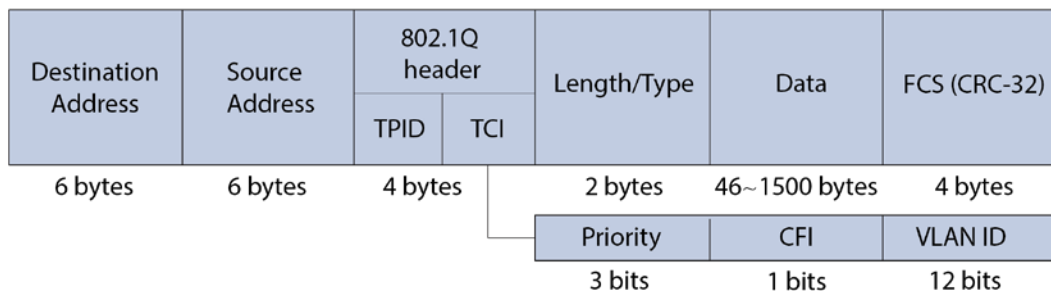
5.2.2 VLAN Function

- Enhance the network performance. The broadcast packets are in the VLAN, which can effectively control the network broadcast storm, reduce network bandwidth and enhance network processing ability.
- Enhance the network security. The switches in different VLANs cannot access each other, and the hosts in different VLAN cannot communicate with each other. They need a router or the three-layer switch to forward the message.
- Simplify the network management. The host of the same virtual working group is not limited in one physical area, which can simplify the network management and facilitate to establish working groups for users in different areas.

5.2.3 Port-based VLAN

The messages of the switch include tag and untag messages.

Figure 4-4 Tag position



Untag is the general Ethernet message. The network adapter of the general PC can recognize the message to communicate.

The VLAN tag head refers to the 4bytes VLAN information after the source MAC address and the destination address. In the above figure, the blue pane is the VLAN tag head. Generally, the network adapter of the general PC cannot recognize this kind of message. Therefore, the Switch needs to use VLAN tag head to distinguish different VLANs, and different VLANs cannot communicate with each other. Sometimes, you do not need to communicate among between different VLANs. Therefore, different port types enable different VLANs to communicate.

Port Types

The port types include Access, Trunk and Hybrid.

- Access: The port belongs to one VLAN, and is used to connect to the computer port.
- Trunk: The port allows multiple VLANs to pass, to receive and send messages of multiple VLANs, and is used to connect between the switches.
- Hybrid: The port allows multiple VLANs to pass, to receive and send messages of multiple VLANs, and is used to connect between the switches, and connect the user's computer.



When processing the data, the Hybrid port and the Trunk port are the same. The only difference is when they are sending data, the Hybrid port allows sending messages of multiple VLANs without a tag, while the Trunk port only allows sending the default VLAN messages without a tag.

Table 4-3 Linkage type and frame processing methods for default VLAN

Port Type	For messages without Tag	For messages with Tag	For message to be sent
Access	Receive the message and put the Tag of the default VLAN.	<ul style="list-style-type: none"> • When VLAN ID is the same as the default VLAN ID, receive the message. • When the VLAN ID is different from the default VLAN ID, discard the message. 	Discard Tag and send out the message.

Port Type	For messages without Tag	For messages with Tag	For message to be sent
Trunk	<ul style="list-style-type: none"> Put the default VLAN ID, when the default VLAN ID is in the accepted list, receive the message and put the default VLAN Tag. Put the default VLAN ID, when the default VLAN ID is in the blocked list, discard the message. 	<ul style="list-style-type: none"> When the VLAN ID is in the accepted list, receive the message. When the VLAN ID is in the blocked list, discard the message. 	<ul style="list-style-type: none"> When VLAN ID is the same as the default VLAN ID, and it is on the accepted list, remove the tag and send out the message. When the VLAN ID is different from the default VLAN ID, and it is on the accepted list, keep the tag and send out the message.
Hybrid			When VLAN ID is on the accepted list, send the message. Use port hybrid untagged /tagged VLAN to set with Tag or not when sending messages.

5.2.4 Configuring VLAN List

You can create and manage VLAN.

Procedure

Step 1 Select **Device Management > VLAN > VLAN List** on the **System Info** page.

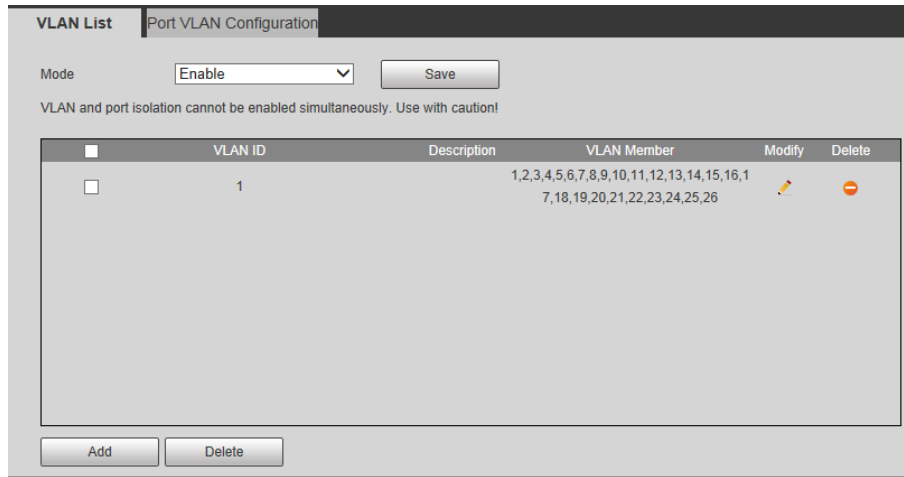
Step 2 Select **Enable** in the **Mode** drop-down list.

Step 3 Click **Save** on the right side of the mode.



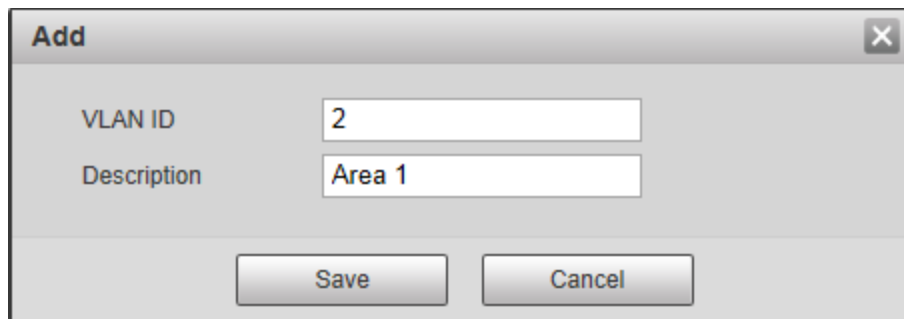
Port Isolation and VLAN are mutually exclusive. When the Port Isolation is enabled, the VLAN will be automatically disabled.

Figure 4-5 Enable VLAN





Step 4 Click **Add**, and then configure **VLAN ID** and **Description** in the **Add** window.

Figure 4-6 Add VLAN



Step 5 Click **Save**.

Related Operations

- Add VLAN member: On the **Port VLAN Configuration** page, after configuring VLAN related to port, the added VLAN member can be displayed.
- Modify VLAN: Select VLAN that has been added in the list, and then click  to modify VLAN ID and Description.
- Delete VLAN: Select VLAN that has been added in the list, and then click  to delete VLAN.

5.2.5 Configuring Port VLAN

You can add port to VLAN, and configure parameters of VLAN.

Step 1 Select **Device Management > VLAN > Port VLAN Configuration** on the **System Info** page.

Figure 4-8 Configure port VLAN

Port	Port Type	Default VLAN	Egress Tagging	Allowed VLANs
1	Access	1		1
2	Access	1		1
3	Access	1		1
4	Access	1		1
5	Access	1		1
6	Access	1		1
7	Access	1		1
8	Access	1		1
9	Access	1		1
10	Access	1		1
11	Access	1		1
12	Access	1		1
13	Access	1		1
14	Access	1		1
15	Access	1		1
16	Access	1		1
17	Access	1		1
18	Access	1		1

Save Refresh

Step 2 Configure parameters.

Table 4-4 Description of parameters

Parameters	Description
Port	Displays all ports of the Switch.
Port Type	Configure the port type, including three types: Access, Trunk and Hybrid.
Default VLAN	Add port to VLAN, all ports belong to VLAN 1 by default. The range is from 1 through 4094.
Egress Tagging	<p>Configure the Egress tag type.</p> <ul style="list-style-type: none"> ● Access port: No need to configure. ● Trunk port: <ul style="list-style-type: none"> ◇ Untag Port VLAN: Indicates that if the data steam tag is the same as the PVID (Port-based VLAN ID), the tag will be stripped. ◇ Tag All: Indicates that all data is tagged. ● Hybrid port: <ul style="list-style-type: none"> ◇ Tagged Only: Indicates that only tagged data can transmit to this port. ◇ Untagged Only: Indicates that only untagged data can transmit to this port.
Allowed VLAN	Configure the allowed VLAN.

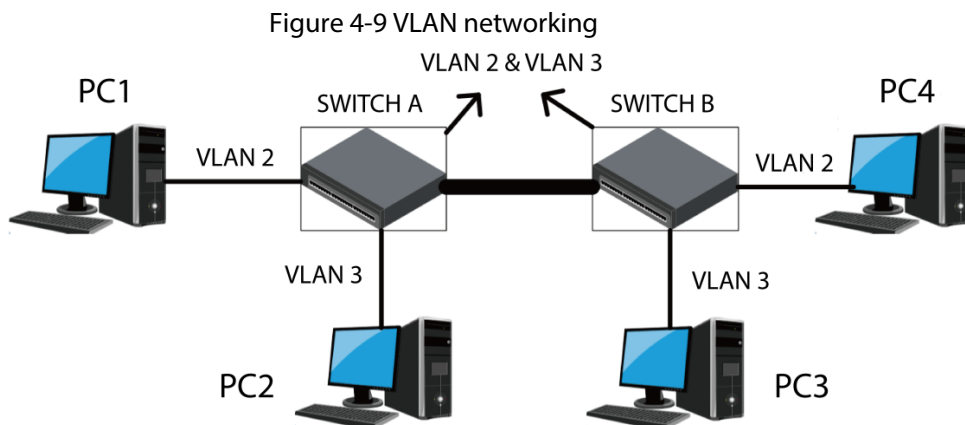
Step 3 Click **Save**.

5.2.6 Example of Configuring VLAN

Background Information

Configuration requirements: PC1 and PC4 belong to one department, and PC2 and PC3 belong to one department. Only PCs in the same department can communicate.

Hardware connection: PC1 connects to port 1 of switch A, and it belongs to VLAN2. PC2 connects to port 2 of switch A, and it belongs to VLAN3. PC3 connects to port 2 of switch B, and it belongs to VLAN3. PC4 connects to port 1 of switch B, and it belongs to VLAN2.



Procedure

- Step 1** Select **Device Management > VLAN > Port VLAN Configuration** on the **System Info** page.
- Step 2** Configure parameters.
- 1) Configure port 1 to access port, and it belongs to VLAN2.
 - 2) Configure port 2 to access port, and it belongs to VLAN3.
 - 3) Configure port 3 to trunk port, and it belongs to VLAN2. Configure **Egress Tagging** of port 3 to **Untag Port VLAN**, and configure **Allowed VLANs** to 2 and 3.

Figure 4-10 Configure port VLAN

Port	Mode	Port VLAN	Egress Tagging	Allowed VLANs
1	Access	2		1
2	Access	3		1
3	Trunk	4	Untag Port VLAN	2,3
4	Access	1		1
5	Access	1		1
6	Access	1		1
7	Access	1		1
8	Access	1		1
9	Access	1		1
10	Access	1		1
11	Access	1		1

- Step 3** Click **Save**.

5.3 Link Aggregation

Link aggregation is to form several physical ports of the Switch into one logical port. Several links

that belong to the same aggregation group can be considered as a logical link with bigger bandwidth.

Link aggregation can realize sharing responsibility of communication flow among each member port in the aggregation group, which is to increase bandwidth. Meanwhile, mutual dynamic backup can be realized among each member port in the same aggregation group, which is to improve the link reliability.

There must be certain configurations for member ports which belong to the same aggregation group. These configurations include STP, QoS, VLAN, port properties, MAC address study, mirroring, 802.1x and MAC filtering.



- The link aggregation is mutually exclusive with STP mode. When STP mode is enabled, link aggregation cannot be configured. You must disable STP mode before configuring link aggregation.
- We do not recommend implementing configuration and advanced functions for the ports which are used for link aggregation.
- Link aggregation can be divided into static aggregation and LACP. Generally, the peer devices with the switch link aggregation are switch and network adapter.
- Only the ports with the same speed rate, duplex, long distance and VLAN configuration can be in the one aggregation group.

5.3.1 Static Aggregation Mode

Static aggregation mode allows manually adding several member ports in the aggregation group. All the ports are in the forward status and share the overloaded flow. Creating aggregation group and adding member ports need to be manually configured without the participation of LACP (link Aggregation Control Protocol) protocol message.

Step 1 Select **Device Management > Link Aggregation** on the **System Info** page.

Step 2 Configure **Link Aggregation Mode**.

Table 4-5 Description of link aggregation mode.

Parameters	Description
Source MAC	Link aggregation calculation based on the source MAC address of packet.
Destination MAC	Link aggregation calculation based on the destination MAC address of packet.
MAC Src&Dst	Link aggregation calculation based on source and destination MAC address of packet.

Step 3 Click **Save**.

Step 4 Select **Link Group**.

For example, select **Link Group 1**.



Link Group is an assembly of a group of Ethernet ports. The supported number of link group is three by default, which can't be changed. The default status of all the link groups is **Disable**, and member port is null by default.

Step 5 Select member port.

For example, select port P1 and P2.

Step 6 Select **State** as **Enable**, and then select **Type** as **Static**.

Figure 4-11 Link aggregation

Step 7 Click **Submit**.

5.3.2 LACP Mode

Background Information

LACP (Link Aggregation Control Protocol) is used to realize link dynamic convergence and convergence separation which is based on IEEE 802.3ad standard. The both parties of convergence devices converge the matched links together, receive and send data through LACPDU message interacting convergence information. The protocol can automatically add and delete ports in the convergence group, which is equipped with high flexibility and provides the capability of load balance.

After enabling the LACP function of the port, the port will inform the opposite end of the system priority, system MAC, port priority, port number and operation Key (decided by physical properties, upper layer protocol information and management Key of the port).

The end with higher priority of the Switch will dominate convergence and convergence separation, and the Switch priority is decided by system priority and system MAC. The Switch with lower system priority value has higher priority. And the Switch with lower system MAC has higher priority when the system priority value is the same. The end with higher device priority will select convergence port according to port priority, port number and operation Key. Only the ports with same operation Key can be selected into one convergence group, and the port with lower port priority value will be selected by priority in the same convergence group. When the port priority is the same, the port with the smaller number will be selected. The selected ports will converge together to receive and send data after both parties interact convergence information.

The configuration parameter of LACP protocol mainly includes State, Operation key, Timeout and Activity.

Table 4-6 Description of LACP configuration parameters

Parameters	Description
State	Including Enable and Disable, the ports which enable only LACP protocol can realize LACP negotiation, and then it might form convergence link.

Parameters	Description
Operation Key	Configure operation Key. Members in the same aggregation group need to configure the same operation Key, ranging from 1 through 65535. Operation Key is the basis of negotiation, and only ports with the same operation key can negotiate to form a convergence link.
Time Out	Long Timeout is selected by default, and can be selected as Short Timeout.
Activity	<p>Activity is Passive by default and can be select as Active.</p> <ul style="list-style-type: none"> When Activity is selected as Active, the Switch will actively initiate convergence negotiation. When Activity is selected as Passive, the Switch will passively accept convergence negotiation initiated by other devices. When two devices are interconnected, at least one or both ends need to be set as Active, the mode can be successfully negotiated.

Procedure

- Step 1** Select **Device Management > Link Aggregation** on the **System Info** page.
- Step 2** Select **Link Group**.
- Step 3** Select member port.
- Step 4** Select **State** as **Enable**, select **Type** as **LACP**, and then select **Activity** as **Active**.
- Step 5** Click **Submit**.
- Step 6** Select **Link Aggregation Mode** as **MAC Src&Dst**.
- Step 7** Click **Save**.

After the aggregation is successful, ✓ will be displayed under the corresponding port.

Figure 4-12 LACP aggregation

Link Aggregation

System Priority: 1 (1~65535)

Link Aggregation Mode: MAC Src&Dst

Save

Only ports with the same rate, duplex, long-distance, and VLAN configuration can be added to the same aggregation group.

Member	Link Group 1				Link Group 2				Link Group 3	
	p1	p2	p3	p4	p5	p6	p7	p8	p25	p26
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State	Enable				Disable				Disable	
Type	LACP				Static				Static	
Operation Key	1 (1~65535)				1 (1~65535)				1 (1~65535)	
Time Out	Long Timeout				Long Timeout				Long Timeout	
Activity	Active				Passive				Passive	

Submit

Refresh

5.4 Security

5.4.1 MAC Address List

When the Switch forwards the message, it searches for the MAC address list according to the message destination MAC address. If the MAC address list includes an item matching the message destination MAC address, it uses the output port to forward the message. If the MAC address list has

no item matching the message destination MAC address, the Switch adopts the broadcast mode to forward the message through the corresponding VLAN (except the input port).

Step 1 Select **Device Management > Security > MAC Address Table** on the **System Info** page.

Step 2 View MAC address list.

Figure 4-13 MAC address list

No.	Mac Address	Type	Port	State
1		Dynamic	20	UnBind
2		Dynamic	20	UnBind
3		Dynamic	20	UnBind
4		Dynamic	20	UnBind
5		Dynamic	20	UnBind
6		Dynamic	20	UnBind
7		Dynamic	20	UnBind
8		Dynamic	20	UnBind
9		Dynamic	20	UnBind
10		Dynamic	20	UnBind
11		Dynamic	20	UnBind
12		Dynamic	20	UnBind
13		Dynamic	20	UnBind
14		Dynamic	20	UnBind
15		Dynamic	20	UnBind
16		Dynamic	20	UnBind

5.4.2 Binding Port MAC

Click the current connected port and configure the port MAC binding function to enable the current port to only forward the binding MAC address.

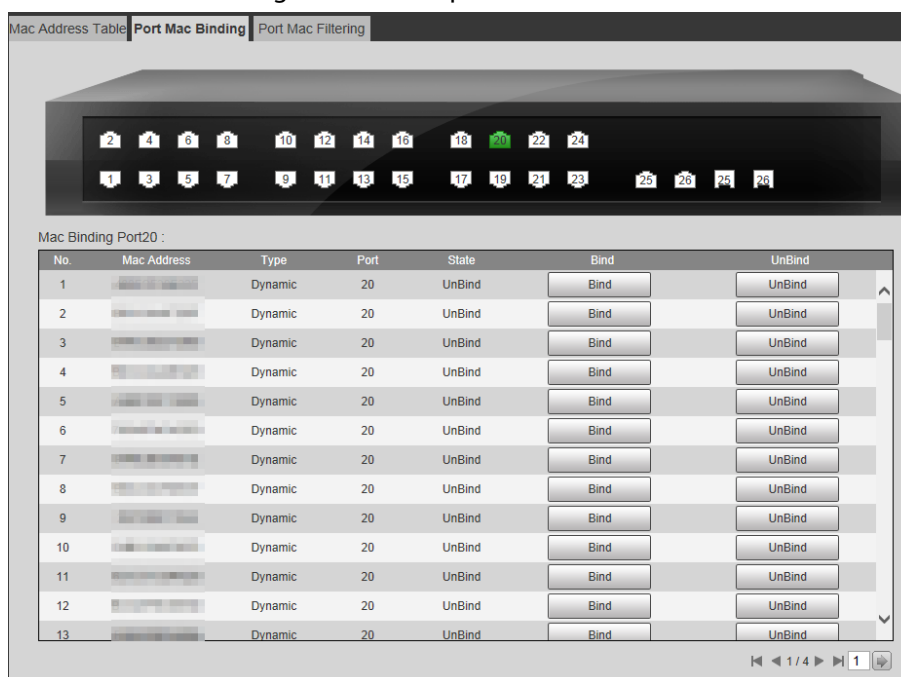
Procedure

Step 1 Select **Device Management > Security > Port MAC Binding** on the **System Info** page.

Step 2 Click the port that is displayed in green, and the port is currently connected.

Step 3 In the list of switches that have been bound to the current port, click **Bind**.

Figure 4-14 Bind port MAC



Related Operations

Unbind: In the list of bound switches, click **Unbind** to delete the bound switch.

5.4.3 Filtering Port MAC

The function is used to restrict the allowed MAC message under port, which can prevent counterfeit attack.

Background Information

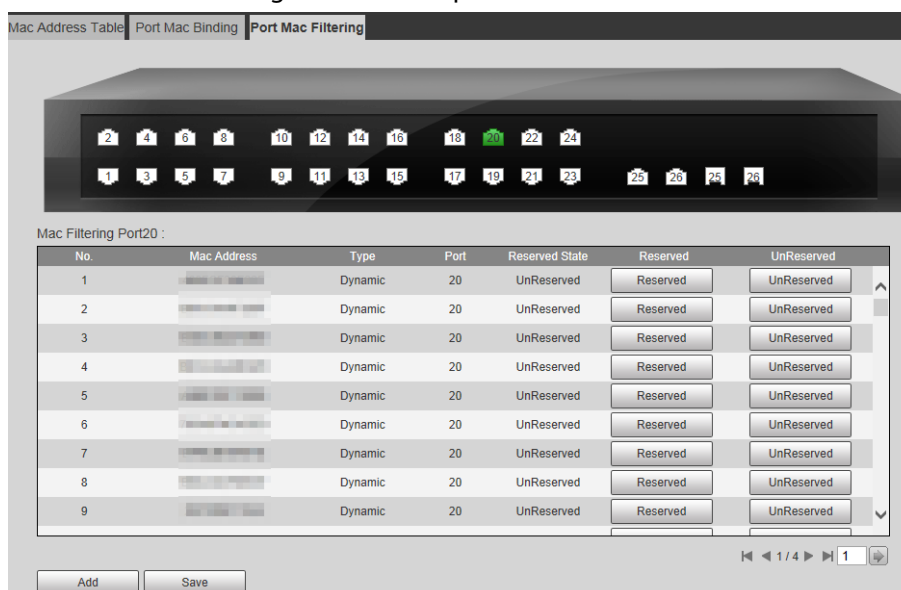
After the port is configured with the port MAC filtering function, when the port receives message, it will check if the source MAC address of message is the same as the allowed MAC address:

- If it is same, then the message is considered as legal, and it will continue to implement follow-up processing.
- If it is not, then the message is considered as illegal, and it will be discarded.

Procedure

- Step 1 Select **Device Management > Security > Port MAC Filtering** on the **System Info** page.
- Step 2 Click the port that is displayed in green, and the port is currently connected.

Figure 4-15 Filter port MAC



Step 3 Click **Add**, and then enter the MAC address that needs to be filtered in **Add MAC Allowlist** window.

Step 4 Click **Save**.

5.5 Configuring SNMP

SNMP network includes two elements: NMS and Agent.

- NMS (Network Management System) is the SNMP network administrator and provides user-friendly interactive interface, which is suitable for the network administrator to complete the most management work.
- Agent is the object to be managed in the SNMP network, and receives, processes the NMS query message. In some urgent situation such as when the port status has changed, Agent can automatically send out the alarm information to the NMS.

5.5.1 SNMP Protocol Version

The Agent supports SNMPv1, SNMPv2 and SNMPv3.

- SNMPv1 adopts community name to certify. The community name is like a password to restrict the communication between the NMS and Agent. If the NMS community name and the managed Switch community name are not the same, then the NMS and the Agent cannot establish the SNMP connection, which means that the NMS cannot access the Agent and the NMS will discard the warning information from the Agent.
- SNMPv2 adopts the community name to certify. SNMPv2c expands the functions of the SNMPv1, provided more operation types, supports more data types and provides more error codes. Therefore, the errors can be accurately distinguished.
- SNMPv3 adopts User-Based Security Model (USM) to certify. The network administrator can set the authentication and encryption function. The authentication is to check the validity of the message sender and to avoid the illegal access. The encryption is to encrypt the communication messages between the NMS and the Agent in case there is eavesdrop. The authentication and

the encryption function can enhance the security level between the NMS and the Agent.



Make sure that the NMS and the Agent are using the same SNMP version, otherwise the NMS and Agent connection might fail.

5.5.2 Configuring SNMP

Step 1 Select **Device Management > SNMP Settings** on the **System Info** page.

Step 2 Select SNMP version.

- Select **SNMP v1**, and the Switch can only deal with information of SNMP v1.
- Select **SNMP v2**, and the Switch can only deal with information of SNMP v2.
- Select **SNMP v3**, and then configure username, password and authentication type. When the server needs to access the Switch, it needs to set the corresponding username, password and authentication type to complete the security verification, and the v1 and v2 versions are not selectable.



We recommend you select the SNMP v3. Selecting SNMP v1 or SNMP v2 might be risky.

Step 3 Configure parameters.

Table 4-7 Description of parameters

Name	Description
SNMP Port	The listening port of the agent on the Switch.
Read Community	The community name to access the network administrator. The permission is read. The default setup is public.
Write Community	The community name to access the network administrator. The permission is write. The default setup is private.
Trap Address	Specifies the server IP address.
Trap Port	Sets trap destination port.
Read-only Username	Sets the read-only username. It is for V3 only.
Authentication Type	Sets authentication mode when the security level is Authentication no encryption or Authentication and encryption . The authentication mode includes MDS and SHA.
Authentication Password	Sets authentication password.
Encryption Type	When the authentication mode is authentication and encryption , it is to set encryption mode. This series product supports 3DES only.
Encryption Password	When the authentication mode is authentication and encryption , it is to set the encryption password.
Read&write Username	Sets read and write user.

5.5.3 Example of SNMPv1/v2 Configuration

Background Information

NMS is connected with the Switch, and the following requirements need to be completed.

- NMS monitors and manages the Switch through SNMP v1 or SNMP v2.
- The Switch can actively send Trap messages to the NMS when an error occurs.

Figure 4-18 Example of SNMP v1/v2 configuration



Procedure

- Step 1 Select **Device Management > SNMP Settings** on the **System Info** page.
- Step 2 Select **SNMP Version** to **SNMP v2**, and then set the SNMP port number to 161.
- Step 3 Configure **Read Community**, **Write Community**, **Trap Address** and **Trap Port** to public, private, 192.168.1.2 and 162 separately.

Figure 4-19 SNMPv2 configuration

The screenshot shows the 'SNMP' configuration page. At the top, there are three radio buttons for 'SNMP Version': 'SNMP v1' (unchecked), 'SNMP v2' (checked), and 'SNMP v3' (unchecked). Below this, there are several input fields: 'SNMP Port' is set to '161' (with a range of 1~65535 in parentheses), 'Read Community' is set to 'public', 'Write Community' is set to 'private', 'Trap Address' is set to '192.168.1.2', and 'Trap Port' is set to '162'. At the bottom, there are two buttons: 'Refresh' and 'Save'.

- Step 4 Click **Save**.

5.5.4 Example of SNMPv3 Configuration

Background Information

NMS is connected with the Switch, and the following requirements need to be met.

- NMS monitors and manages the Switch through SNMPv3.
- The Switch can automatically send out Trap message to the NMS when there is any malfunction.
- When NMS connects Agent to SNMP, it requires authentication. The authentication mode is MD5,

and the authentication password is admin123.

- The SNMP message among the NMS and the Agent must be encrypted, the encryption mode is DES56, and the encryption password is admin123.

Figure 4-20 Example of SNMPv3 configuration



Procedure

- Step 1** Select **Device Management > SNMP Settings** on the **System Info** page.
- Step 2** Select **SNMP Version** as **SNMP v3**.
SNMP port number is 161.
- Step 3** Configure **Read Community**, **Write Community**, **Trap Address** and **Trap Port** to public, private, 192.168.1.2 and 162 separately.
- Step 4** Enter user as **Read-only Username**.
- Select MDS as **Authentication Type**.
 - Enter admin123 as **Authentication Password**.
 - Enter admin123 as **Encryption Password**.
- Step 5** Enter user1 as **Read-only Username**.
- Select MDS as **Authentication Type**.
 - Enter admin123 as **Authentication Password**.
 - Enter admin123 as **Encryption Password**.

Figure 4-21 SNMP v3 configuration

SNMP

SNMP Version SNMP v1 SNMP v2 SNMP v3

SNMP Port (1~65535)

Read Community

Write Community

Trap Address

Trap Port

Read-only Username

Authentication Type MD5 SHA

Authentication

Password

Encryption Type CBC-DES

Encryption Password

Read&write Username

Authentication Type MD5 SHA

Authentication

Password

Encryption Type CBC-DES

Encryption Password

Step 6 Click **Save**.

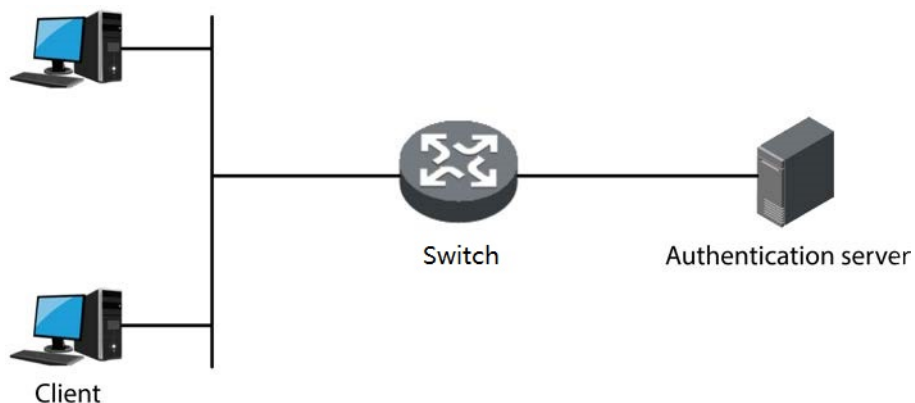
5.6 802.1x

IEEE 802.1x is the authentication standard designated by IEEE about user accessing network, and is a type of network access control protocol based on port. Therefore, the exact 802.1x authentication function must be configured on the device port, and for the user device which is accessed through the port can have control on the access on network source through authentication.

5.6.1 802.1x Networking Structure

802.1x system includes three parts: Client, Device and Authentication server.

Figure 4-22 802.1x networking structure



- Client is the user terminal device that requests for LAN access, which is authenticated by the

device in the LAN. The Client must be installed with client software which supports 802.1x authentication.

- Switch is the network device that controls client access in the LAN, which is located between the Client and Authentication server. The Switch provides LAN access port for customers (physical port or logical port), and implements authentication upon the connected Client through interaction with the server.
- Authentication server is used to implement authentication, authorization and billing, and generally is a RADIUS (Remote Authentication Dial-In User Service) server. Authentication server can verify the legality of the Client according to the Client authentication information sent by the Switch, and inform the device of verification results. Whether it allows client access is decided by the Device. The role of Authentication server can be replaced by Device in some small-scale network environment, which means that the Device realizes local authentication, authorization and billing upon the client.

5.6.2 802.1x Authentication Controlled/Uncontrolled Port

The LAN access ports provided by device for client can be divided into two logical ports which are controlled port and uncontrolled port. Any frame is sent to the port can be visible on both controlled port and uncontrolled port.

- The uncontrolled port is always in the status of bidirectional connection. The port is mainly used to transmit authentication messages and make sure that the Client can always send or receive authentication messages.
- The controlled port is always in the status of bidirectional connection in the authorized status. The port is mainly used to transmit business message; and is forbidden to receive any messages from the Client when it is in the unauthorized status.

5.6.3 Trigger Mode of 802.1x Authentication

The 802.1X authentication process can be initiated by the Client or the Switch.

- Client Active Trigger Mode
 - ◇ Multicast trigger: the Client actively sends authentication request message to the Switch to trigger authentication, and the destination address of the message is the multicast MAC address 01-80-C2-00-00-03.
 - ◇ Broadcast trigger: the Client actively sends authentication request message to the Switch to trigger authentication, and the destination address of the message is the broadcast MAC address. The mode can solve the problem that the Switch fails to receive authentication request from the Client because some devices in the network fail to support the multicast message above.
- Switch Active Trigger Mode

The mode is used to support the Client that cannot actively send authentication request message, and there are two types of trigger authentication:

 - ◇ Multicast trigger: The Switch actively sends request message of identity type to trigger authentication to the Client at regular interval (it is 30 s by default).
 - ◇ Unicast trigger: When the Switch receives unknown message from source MAC address, it will actively send Identity-typed request message in unicast to the MAC address to trigger

authentication. It will send the message again if the Switch fails to receive the Client response within the set duration.

5.6.4 Configuring NAS

By configuring the authorization status of the port, you can control whether users connected to the port need to be authenticated to access network resources.

Step 1 Select **Device Management > 802.1X > NAS Settings** on the **System Info** page.

Step 2 Select **Enable** to enable **NAS** (Network Attached Storage).

Step 3 Select ports and configure the **Admin State**.

Figure 4-23 Configure NAS

The screenshot shows the 'NAS Settings' page with the 'Radius Settings' tab selected. The 'Mode' is set to 'Enable' and 'Reauthentication' is disabled. Below is a table with columns for 'Port', 'Admin State', and 'Port State'. All 18 ports are configured with 'Port based 802.1X' and 'Globally Enabled'. 'Save' and 'Refresh' buttons are at the bottom.

Port	Admin State	Port State
1	Port based 802.1X	Globally Enabled
2	Port based 802.1X	Globally Enabled
3	Port based 802.1X	Globally Enabled
4	Port based 802.1X	Globally Enabled
5	Port based 802.1X	Globally Enabled
6	Port based 802.1X	Globally Enabled
7	Port based 802.1X	Globally Enabled
8	Port based 802.1X	Globally Enabled
9	Port based 802.1X	Globally Enabled
10	Port based 802.1X	Globally Enabled
11	Port based 802.1X	Globally Enabled
12	Port based 802.1X	Globally Enabled
13	Port based 802.1X	Globally Enabled
14	Port based 802.1X	Globally Enabled
15	Port based 802.1X	Globally Enabled
16	Port based 802.1X	Globally Enabled
17	Port based 802.1X	Globally Enabled
18	Port based 802.1X	Globally Enabled
19	Port based 802.1X	Globally Enabled

Table 4-8 Description of admin state

State	Description
Force Authorized	The port is always in the authorized status, and users are allowed to access network resources without authentication.
Force Unauthorized	The port is always in an unauthorized status, and users are not allowed to authenticate. The Switch does not provide authentication services for clients that access through this port.
Port based 802.1X	Indicates that the initial state of the port is an unauthorized state, and users are not allowed to access network resources. If the user is authenticated, the port is turned to an authorized state, which allows users to access network resources.

Step 4 Click **Save**.

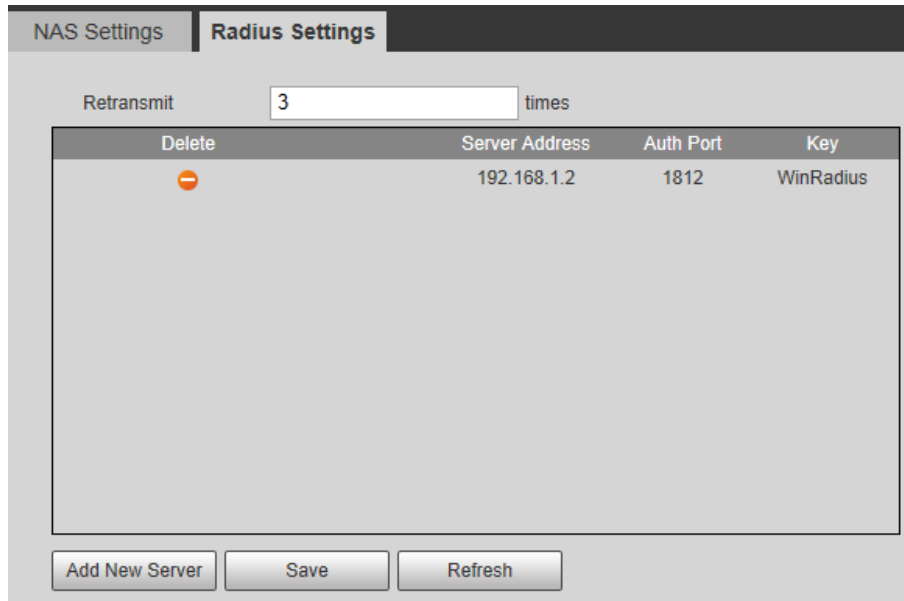
5.6.5 Configuring Radius

Configure the authentication server address.

Step 1 Select **Device Management > 802.1X > Radius Settings** on the **System Info** page.

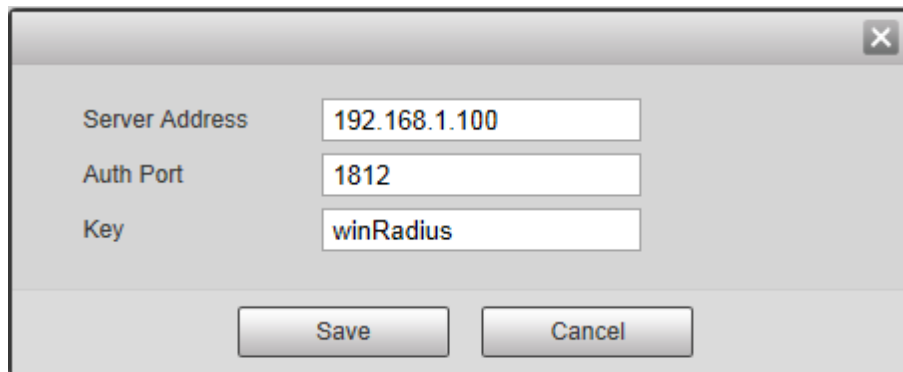
Step 2 Enter **Retransmit** times.

Figure 4-24 Radius configuration



Step 3 Click **Add New Server**, enter server address, authorized port and key in the pop-up window.

Figure 4-25 Add new server



Step 4 Click **Save**.

5.7 IGMP Snooping

IGMP Snooping (Internet Group Management Protocol Snooping) is operated on the layer two device. It can generate layer two multicast forwarding table by snooping the IGMP message between layer three device and host, which is to manage and control the forwarding of multicast data message and realize required distribution on layer two of multicast data packet.

5.7.1 IGMP Snooping Theory

Operating layer two device of IGMP Snooping can establish mapping relation for port and MAC multicast address through analysis on received IGMP message, and forward multicast data according to the mapping relation.

The multicast data will be broadcasted in the layer two network when the layer two device does not operate IGMP Snooping. After layer two device operates IGMP Snooping, the known multicast data of multicast group will not be broadcasted in the layer two network but multicasted to designated

receivers.

IGMP Snooping can only forward the information to the needed receivers through layer two multicast with the following advantages:

- Reduce broadcast message in the layer two network, and save network bandwidth;
- Enhance security of multicast information;
- Bring convenience for realizing individual billing for each host.

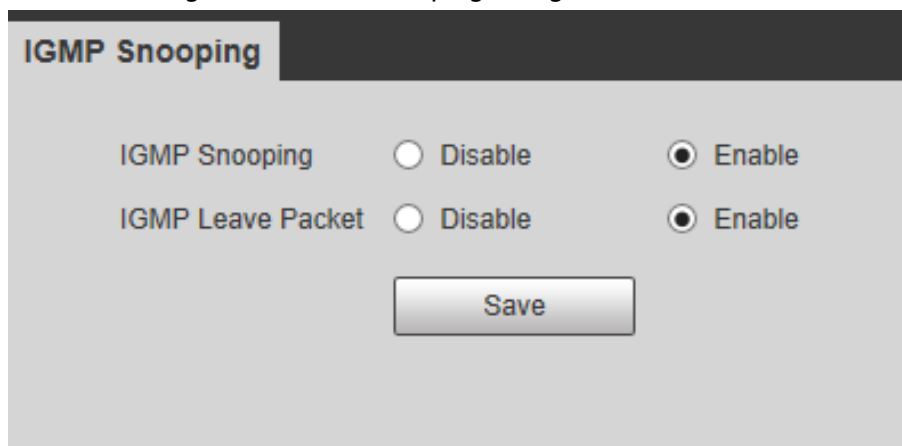
5.7.2 Configuring IGMP Snooping

Step 1 Select **Device Management > IGMP Snooping** on the **System Info** page.

Step 2 Configure IGMP Snooping.

- **IGMP Snooping:** Enable or disable IGMP Snooping function.
- **IGMP Leave Packet:** Enable or disable the function of quick leave.

Figure 4-26 IGMP Snooping configuration



The screenshot shows a configuration window titled "IGMP Snooping". It contains two rows of radio button options. The first row is for "IGMP Snooping" with "Disable" and "Enable" options, where "Enable" is selected. The second row is for "IGMP Leave Packet" with "Disable" and "Enable" options, where "Enable" is selected. A "Save" button is located at the bottom center of the window.

Step 3 Click **Save**.

5.8 Configuring HTTPS

HTTP (Hyper Text Transfer Protocol) defines how the browser (the World Wide Web client process) requests a World Wide Web document from the World Wide Web server, and how the server transmits the document to the browser. From a hierarchical point of view, HTTP is a transaction-oriented application layer protocol, which is an important basis for reliable exchange of files (including text, audio, image and other multimedia files) on the World Wide Web.

HTTPS is an HTTP channel with security as the goal. The SSL layer/TLS layer is added to HTTP. The security foundation to be the HTTPS is SSL/TLS, so SSL/TLS is required for the details of encryption. It is a URI scheme (abstract identifier system), the syntax is similar to the http: system. It is used to ensure the secure transmission of HTTP data. The system is built into the browser Netscape Navigator and provides authentication and encrypted communication methods. It is now widely used in security-sensitive communications on the World Wide Web, such as protecting account security and protecting user information.



- If you configure HTTPS for the first time or change the Switch IP, you need to create server

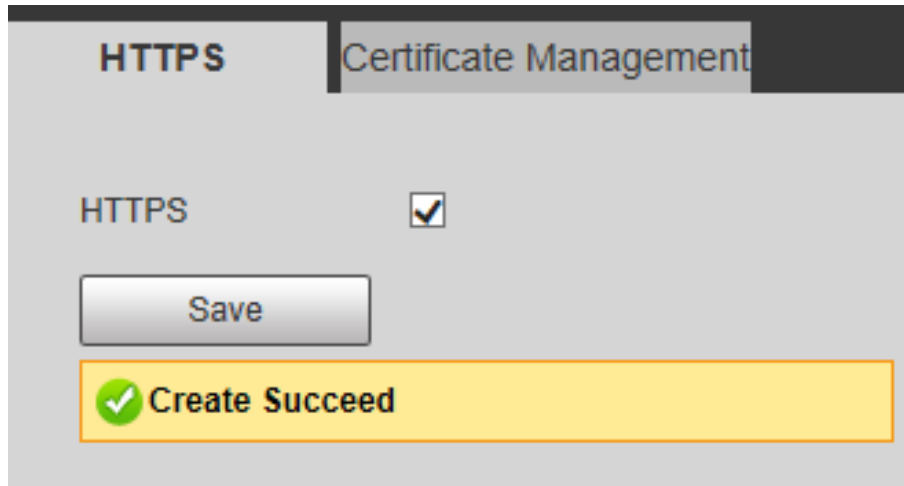
certificate again.

- If you use HTTPS for the first time after replacing your computer, you need to download root certificate again.

Step 1 Select the checkbox next to the **HTTPS**, from **Device Management > HTTPS** on the **System Info** page.

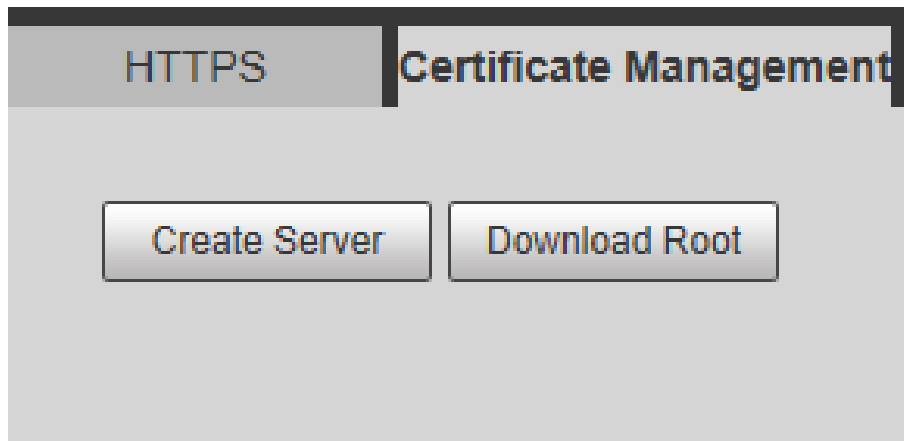
Step 2 Select **HTTPS**, and then click **Save**.

Figure 4-27 HTTPS



Step 3 Select **Certificate Management**, and then click **Create Server**.

Figure 4-28 Certificate management

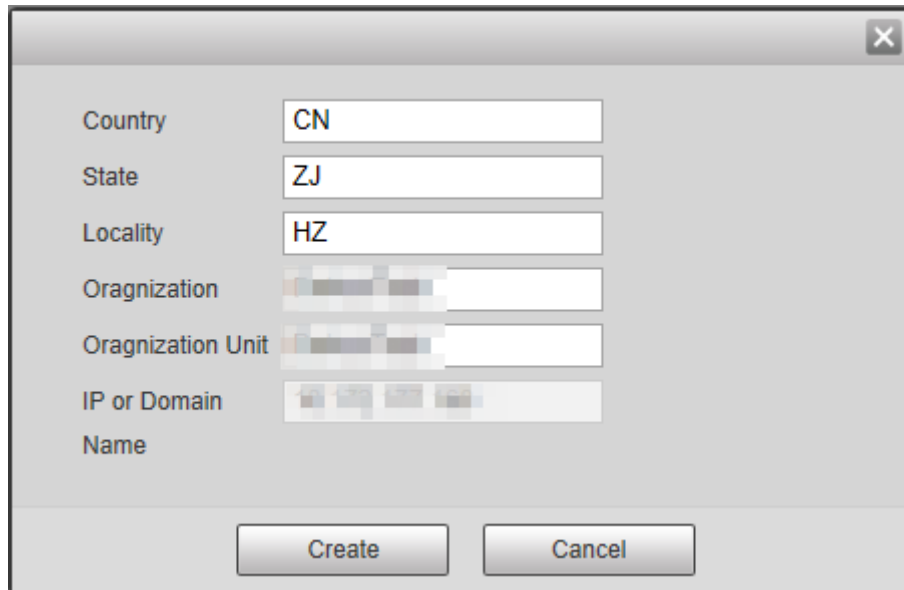


Step 4 Enter information of **Country, State, Locality** and other parameters.



The value of the **IP or Domain** must be consistent with the device IP or domain name.

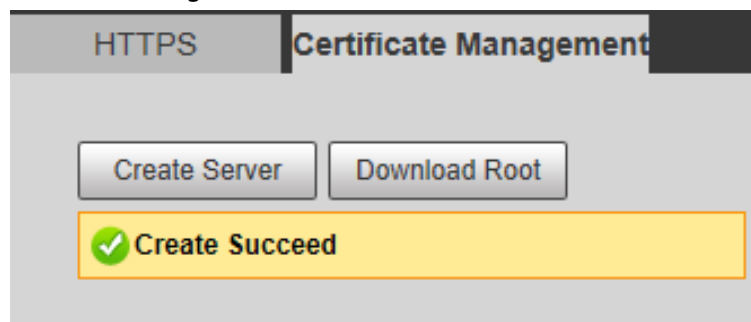
Figure 4-29 Create Server (1)



Step 5 Click **Create**.

After the creation is successful, the prompt **Create Succeed** displays.

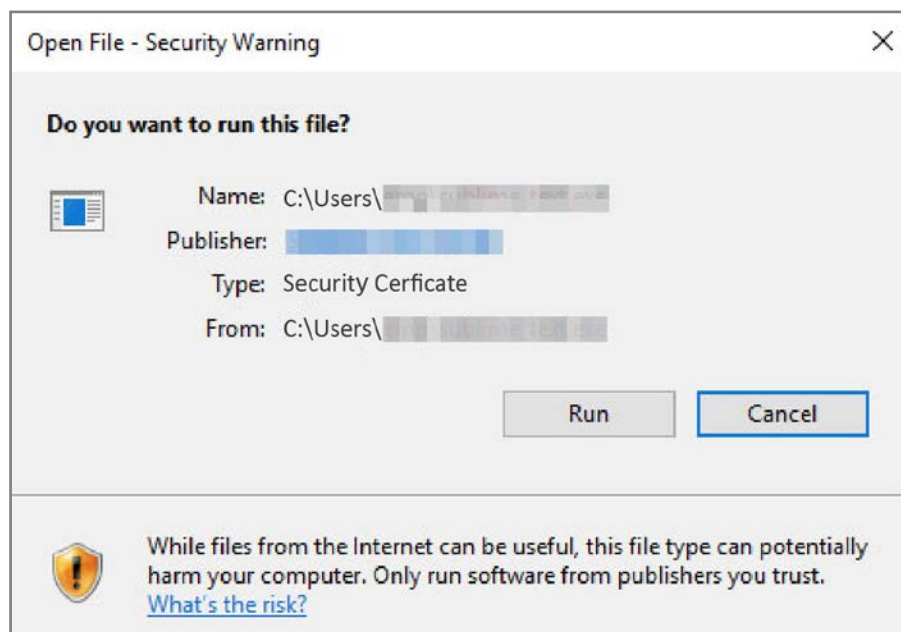
Figure 4-30 Create Server (2)



Step 7 Click **Download Root**.

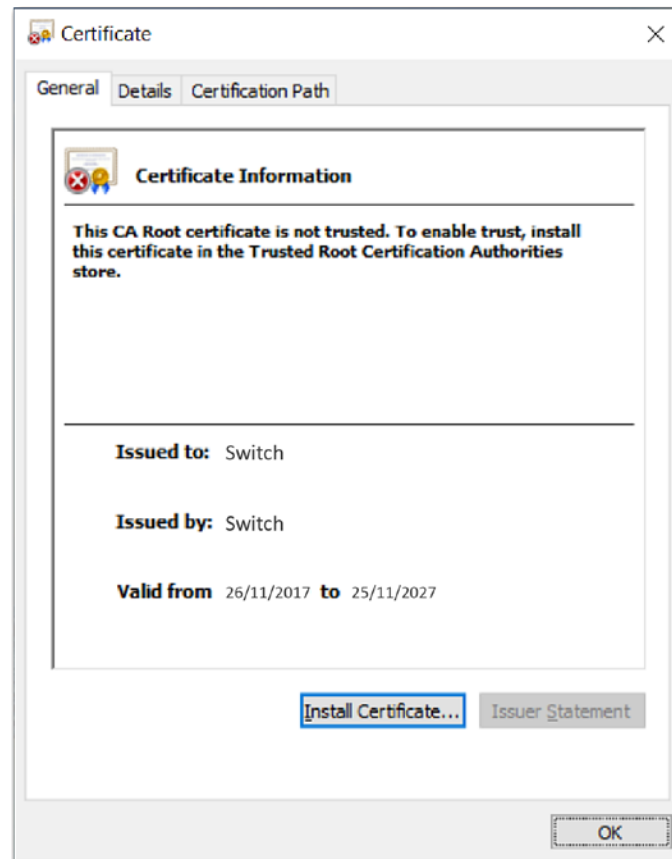
Step 8 Open the downloaded root certificate file, and then click **Run** on the **Security Warning** dialog box that pops up.

Figure 4-31 Download files



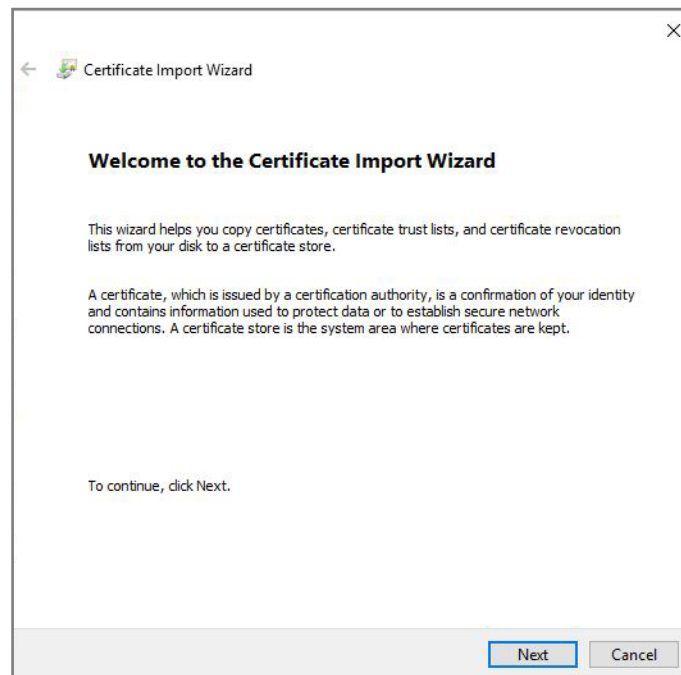
Step 9 Click **Install Certificate**.

Figure 4-32 Certificate



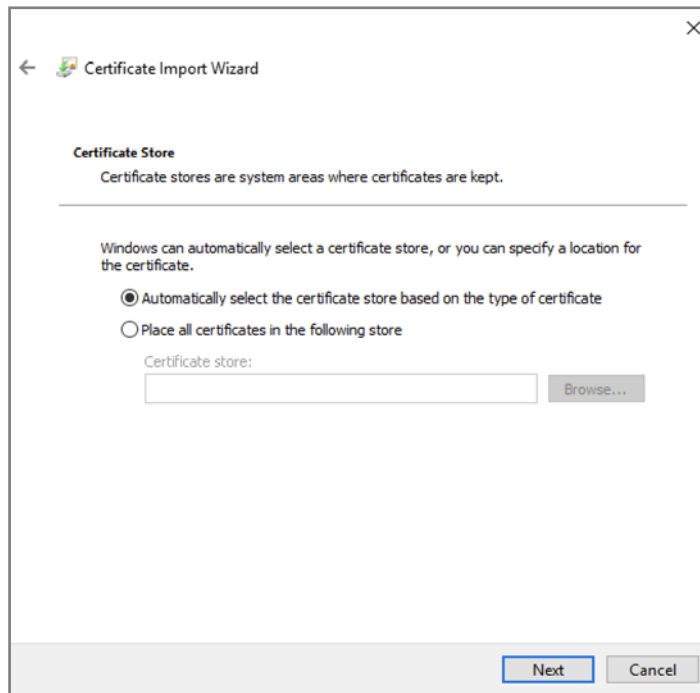
Step 10 Click **Next**.

Figure 4-33 Certificate import wizard



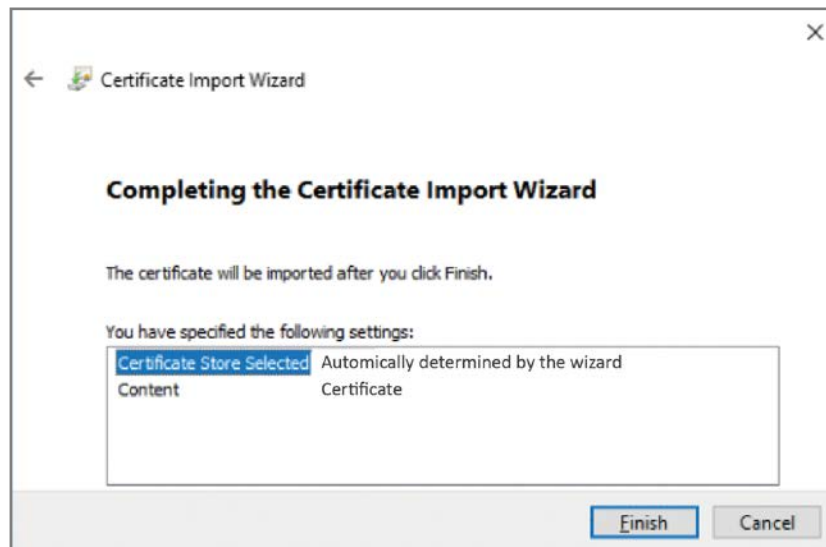
Step 11 Select **Automatically select the certificate store base on the type of certificate**, and then click **Next**.

Figure 4-34 Store certificate



Step 12 Click **Finish**.

Figure 4-35 Complete the certificate import wizard



6 PoE

6.1 Configuring PoE Power

Background Information

Power over Ethernet (PoE) means the device is remotely powered up through the Ethernet port and connected to the PD (Powered Device) with the twisted pair cable. The PoE function realizes the centralized power supply and easy backup. The network terminal just uses one simple network cable without external power source. It meets the IEEE 802.3af and IEEE 802.3at standard and adopts the universal recognized power port. It is applicable for the IP camera, IP phone, wireless access point (wireless AP), portable device recharger, POS, data acquisition and more.

Figure 5-1 PoE system

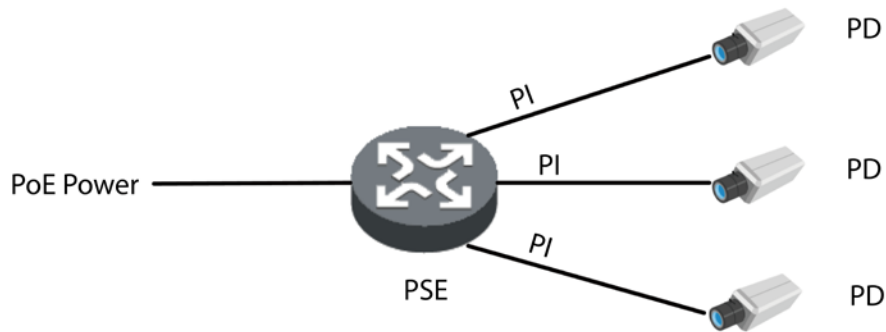



Table 5-1 Description of PoE system

Part	Description
PoE Power	Supplies power to the whole system.
PSE	Directly supplies power to the PD. Supports searching, detecting PD, categorizing PD, realizing power consumption management and checking the PD connection.
PI	<p>The Ethernet port that has the PoE function. It includes FE and GE. The PoE remote power supply has two modes:</p> <ul style="list-style-type: none"> Over signal wires: The PSE uses the pairs (1, 2, 3, 6) that transmit data in 3/5 twisted pair cable to supply DC power while transmitting data to PDs. Over spare wires: The PSE uses the pairs (4, 5, 7, 8) that do not transmit data in 3/5 twisted pair cable to supply DC power to PDs. <p> The power supply mode is different depending on the PD specifications. The selected mode must support PSE and PD at the same time. If the PSE and the PD power supply mode are not the same (the PSE does not support the spare wire power supply, or the PD supports spare wire power supply only), use converter to provide power to the PD.</p>

Part	Description
PD	The device that receives power from the PSE. It includes IP phone, wireless AP, portable recharger, POS, network camera and other devices. When the PD receives power from the PoE device, it can connect to other power supply to back up the power.

Procedure


Step 1 Select **PoE > PoE Settings**.

Step 2 Configure parameters.

Figure 5-2 Configure PoE

Table 5-2 Description of parameters

Parameters		Description
Power Setting	Total Power	Displays the total PoE power.
	Available Power	Configures the available PoE power.
	Overload Power	Configures the overload PoE power.
Power Status	Consumed Power	Displays the current PoE power consumed by all ports.
	Remaining Power	Displays the current remaining PoE power.
	Reserved Power	Unusable PoE power. Reserved power= total power-overload power.

Parameters		Description
Port status and control	Level Power	Displays the power supply level to the terminal devices. The power supply level ranges from 0 through 8, and the Hi-PoE power supply standard level is displayed as 5+.
	Consumed Power	Displays the current PoE power consumed by the corresponding single port.
	Enable/Disable	<p>Enables or disables PoE on the selected ports.</p> <ul style="list-style-type: none"> When selecting the Disable, the system does not supply power to the PD or reserve power for the PD. When selecting the Enable, the PoE port will not result in PoE power overload. Otherwise, you are not allowed to enable PoE for the PoE port. <p></p> <ul style="list-style-type: none"> By default, PoE is disabled on a PoE port. PSE power overload: When the total amount of the power consumption of all ports exceeds the maximum power of PSE, the system considers the PSE is overloaded.

Step 3 Click **Save**.

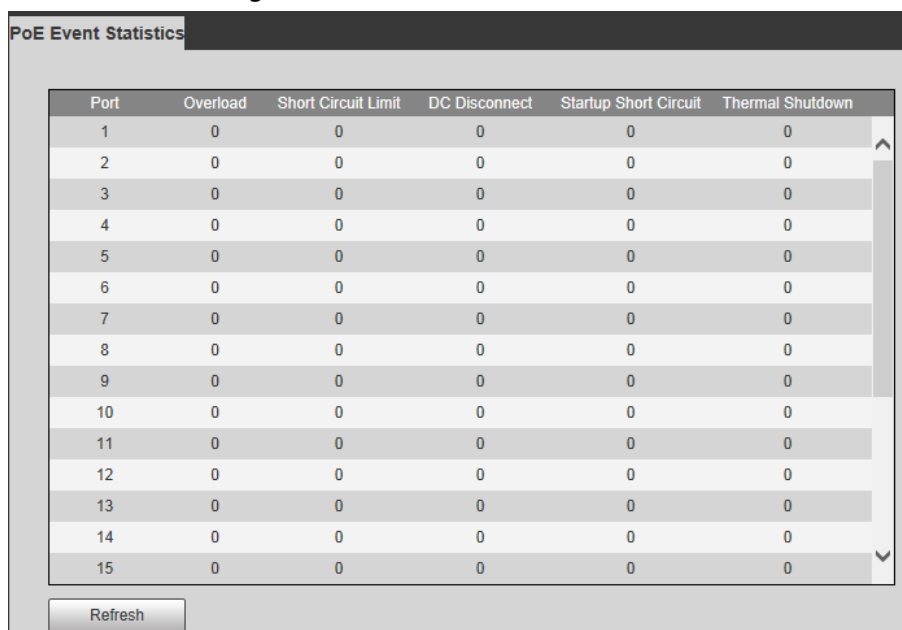
6.2 Viewing PoE Event Statistics

The page displays the PoE event statistics of each port, including **Overload**, **Short Circuit Limit**, **DC Disconnect**, **Server Short Circuit**, and **Thermal Shutdown**.

Step 1 Select **PoE > PoE Event Statistics** on the **System Info** page.

Step 2 View PoE event statistics.

Figure 5-3 PoE events statistics



Port	Overload	Short Circuit Limit	DC Disconnect	Startup Short Circuit	Thermal Shutdown
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0
8	0	0	0	0	0
9	0	0	0	0	0
10	0	0	0	0	0
11	0	0	0	0	0
12	0	0	0	0	0
13	0	0	0	0	0
14	0	0	0	0	0
15	0	0	0	0	0

Refresh

Table 5-3 Description of parameters

Name	Description
Overload	Single port boot up power current has exceeded the current threshold.
Short Circuit Limit	When powering chip sends power to the port, it becomes short-circuit.
DC Disconnect	Single port power is off.
Startup Short Circuit	The power is short-circuit when the powering chip sends out power.
Thermal Shutdown	The powering chip temperature is too high resulting from short-circuit or other reasons.

6.3 Configuring Green PoE

You can set **PoE Off Time** to a specified period to save power. When the period is over, the port automatically resumes supplying power.

- Step 1 Select **PoE > Green PoE** on the **System Info** page.
- Step 2 Configure **PoE Off Time** and **PoE On Time**.
- Step 3 Select the port that needs to enable the power saving function.

Figure 5-4 Configure green PoE

Green PoE

PoE Off Time: Saturday 00 : 00 : 00

PoE On Time: Monday 00 : 00 : 00

Port	Enable
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>
7	<input checked="" type="checkbox"/>
8	<input checked="" type="checkbox"/>
9	<input checked="" type="checkbox"/>
10	<input checked="" type="checkbox"/>
11	<input type="checkbox"/>
12	<input type="checkbox"/>
13	<input type="checkbox"/>
14	<input type="checkbox"/>
15	<input type="checkbox"/>
16	<input type="checkbox"/>
17	<input type="checkbox"/>
18	<input type="checkbox"/>
19	<input type="checkbox"/>

Save

Step 4 Click **Save**.

6.4 Configuring Legacy Support



If the legacy support of a port is enabled, the port will provide power compulsorily no matter whether the connected PD device conforms to the standard or not. Be cautious with the function.

Step 1 Select **PoE > Legacy Support** on the **System Info** page.

Step 2 Select port that needs to enable the **Legacy Support** function.

Figure 5-5 Configure Legacy Support

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

Save

Step 3 Click **Save**.

6.5 Configuring PD Alive

When the Switch detects that the camera has no data output, it will judge that the camera is crashed and will restart the camera through the PoE to solve the problem.



You can only use one between **Legacy Support** and **PD Alive** each time.

Step 1 Select **PoE > PD Alive** on the **System Info** page.

Step 2 Select port that needs to enable **PD Alive** function.

Figure 5-6 Configure PD alive

PD Alive

You can only use one between mandatory PoE power supply and PoE watchdog each time.

Port	<input type="checkbox"/> Enable
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>
9	<input type="checkbox"/>
10	<input type="checkbox"/>
11	<input type="checkbox"/>
12	<input type="checkbox"/>
13	<input type="checkbox"/>
14	<input type="checkbox"/>
15	<input type="checkbox"/>
16	<input type="checkbox"/>
17	<input type="checkbox"/>

Step 3 Click **Save**.

Appendix Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters.
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
- Do not contain the account name or the account name in reverse order.
- Do not use continuous characters, such as 123, abc, etc.
- Do not use overlapped characters, such as 111, aaa, etc.

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the “auto-check for updates” function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. Physical Protection

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The device supports password reset function. Please set up related information for password reset in time, including the end user’s mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus

reducing the risk of ARP spoofing.

8. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. Audio and Video Encrypted Transmission

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. Network Log

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. Construct a Safe Network Environment

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.