16/24-port ePoE Switch

Web Operation Manual

V1.0.0

Foreword

General

This manual introduces operations on web page of the 16/24-port ePoE 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, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	June 2022

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: 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, and comply with the guidelines when using it.

Transportation Requirements

Transport the device under allowed humidity and temperature conditions.

Storage Requirements

Store the device under allowed humidity and temperature conditions.

Installation Requirements

 WARNING

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electrical safety code and standards. Make sure that the ambient voltage is stable and meets the power supply requirements of the device.
- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.

- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- The device must be grounded by a copper wire with a cross-sectional area of 2.5 mm^2 and a ground resistance no more than 4 Ω.
- Voltage stabilizer and lightning surge protector are optional depending on the actual power supply on site and the ambient environment.
- 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.
- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.

Operation Requirements

 WARNING

- Do not disassemble the device without professional instruction.
- Operate the device within the rated range of power input and output.
- Make sure that the power supply is correct before use.
- Make sure the device is powered off before disassembling wires to avoid personal injury.
- Do not unplug the power cord on the side of the device while the adapter is powered on.

- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Operating temperature: –10 °C to +55 °C (+14 °F to +131 °F).
- This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- Do not block the ventilator of the device with objects, such as a newspaper, table cloth or curtain.
- Do not place an open flame on the device, such as a lit candle

Maintenance Requirements

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

Table of Contents

1 Login

Prerequisites

- The main program file running on the Switch must support web access.
- When logging in to the Switch, make sure that the IP address of the PC and the device must be on the same network.

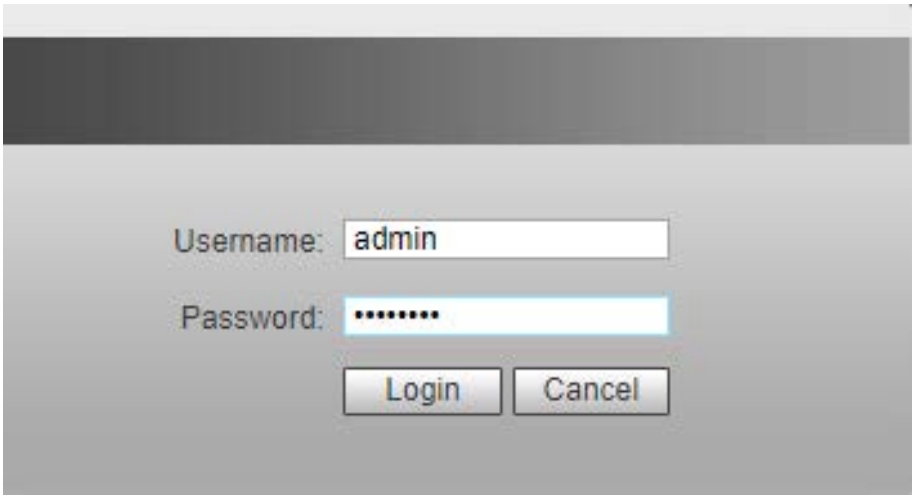
Procedure

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

Figure 1-1 Log in to the web



2 Device Information

You can view the information on the Switch.

Figure 2-1 Web display

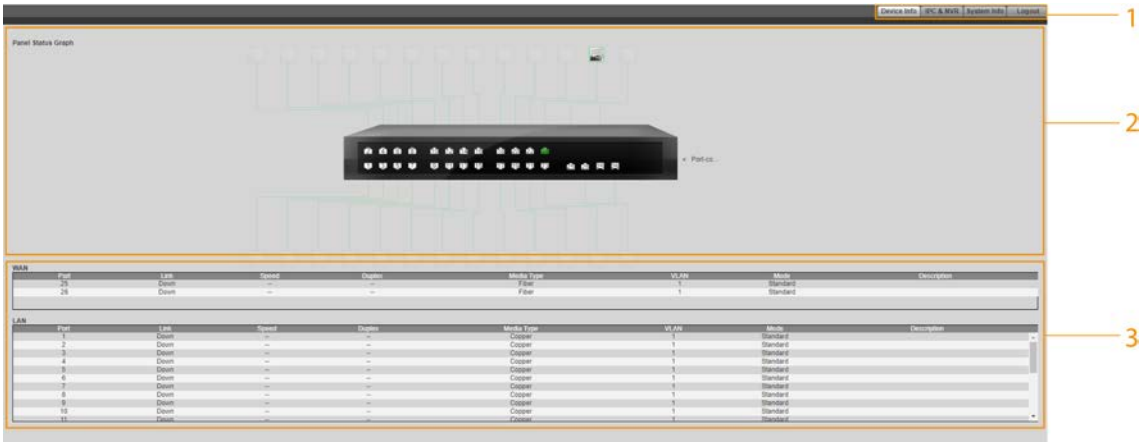


Table 2-1 Description of the web page

No.	Function	Description
1	Navigation bar	• **Device Info**: View the information on the Switch. • **IPC & NVR**: View the informtion on the IPC, NVR and other devices connected to the Switch. • **System Info**: Configure the Switch by accessing **System Config**, **Port Management**, **Device Management** and **PoE**. • **Logout**: Click to return to the login page.
2	Panel status graph	• Switch port is green: Successfully connected to the port. • Switch port is white: Failed to connect to the port. Select the checkbox next to the Switch, you can view the diagram of port connection.
3	Port information	Displays information on the port status of WAN and LAN, including the current port link status, port speed, duplex mode, media type, mode and description.

3 IPC and NVR

Click **IPC & NVR** to view the information on the IPC, NVR and other devices connected to the Switch.

4 System Information

4.1 Configuring System

4.1.1 Configuring System Information

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

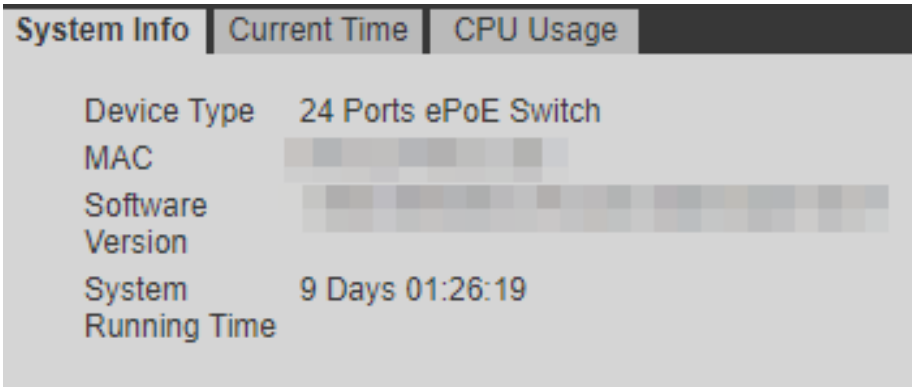
4.1.1.1 Viewing System Information

You can view information on the device type, MAC address and software version.

Step 1 Select **System Config** > **System Info**.

Step 2 View Switch system information.

Figure 4-1 System information



4.1.1.2 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**.

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.

4.1.1.3 Viewing CPU Usage

You can view the CPU usage.

Step 1 Select **System Config** > **System Info** > **CPU Usage**.

Step 2 View the CPU usage of the device.

4.1.2 Configuring Network

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**.

Step 2 Configure parameters.

Step 3 Click **Save**.

Table 4-1 Description of the network configuration

Parameter	Description
Mode	Select the mode for the device to obtain IP. • **Static**: Manually configure the IP address, subnet mask and default gateway. After clicking **Save**, you will be automatically redirected to the login page of the new IP address. • **DHCP**: When there is a DHCP server on the network, select **DHCP** and the device will automatically obtain a dynamic IP address.
IP address	When the mode is set to **Static**, enter the IP address, subnet mask and default gateway according to your network plan. • 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.
Subnet mask	
Default gateway	
MAC address	The physical address of the Switch, which cannot be modified.

4.1.3 Upgrading Software

Prerequisites

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

Procedure

Step 1 Select **System Config** > **Software Upgrade**.

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

Step 3 Click **Upgrade**.

4.1.4 Changing Password

You can modify the user login password. 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**.

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

Step 3 Click **Save**.

4.1.5 Restoring to Default

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

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

Step 1 Select **System Config** > **Restore Default**.

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

4.1.6 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**.

Step 2 Click **Manual**.

4.1.7 Viewing Log Information

The system log displays information on the Switch operations on the system log page.

Step 1 Select **System Config** > **Log Information**

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

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

Step 4 Click **Search**.

4.1.8 Viewing Legal Information

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

Step 1 Select **System Config** > **Legal Info**

Step 2 View related legal information.

4.2 Port Management

4.2.1 Configuring Port

Port configuration can be used to configure basic parameters related to the Switch port. The port

basic parameter will directly affect the working mode of the port. Please make configurations according to the practical requirements.

Step 1 Select **Port Management** > **Port Configuration**.

Step 2 Configure port parameters.

Step 3 Click **Save**.

Figure 4-2 Configure Port

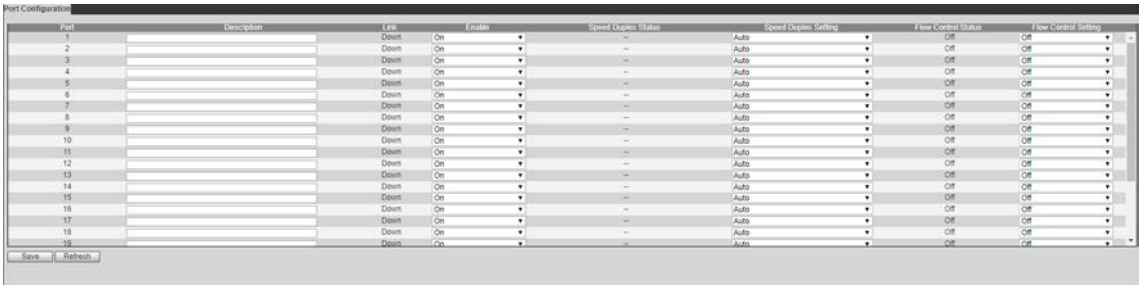


Table 4-2 Description of parameters

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. ● On: Enable the link. ● Off: Disable the link.
Speed Duplex Status	Displays the status of the port speed.
Speed Duplex Setting	Configured the method of port speed duplex. ● Ethernet port. ◇ Auto (default): Auto negotiation mode. ◇ 10M FULL: 10M 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. ● 1000M-X: 1000M Full duplex. The port communication can be directly affected if you change the port speed duplex mode. Please be advised.

Parameter	Description
Flow Control	Configure the Switch flow control. (The default setup is on). • On: Enable port flow control function. • Off: Disable port flow control function. For Ethernet port, you need to enable port flow control function to synchronize the inbound speed and outbound speed in case there are packet losses resulting from the different speeds.

4.2.2 Configuring Port Mirroring

Port mirroring (also called port monitor) is the process of copying the packet passing through a port or several ports (called a source port) to another port (called the destination port) connected with a monitoring device for packet analysis. It is to monitor the network and resolve the network malfunction.

Step 1 Select **Port Management** > **Port** > **Mirroring**.

Step 2 Configure parameters.

For example, enable port mirroring function so that the port 1 can monitor the packets of port 2 and port 3.

Step 3 Click **Save**.

Figure 4-3 Configure port mirroring

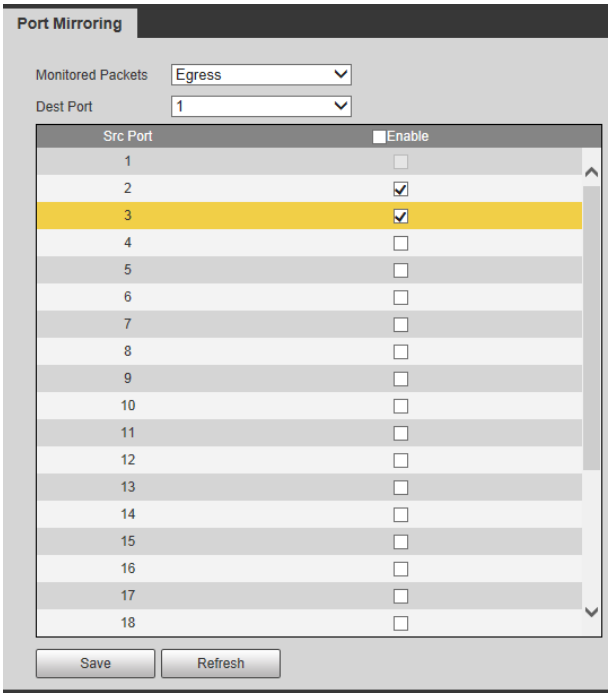


Table 4-3 Description of parameters

Parameter	Description
Monitored Packets	Select mirrored packets. • **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. Please select one or more port(s).
Enable	Enable the function on the selected ports.

4.2.3 Configuring Port Statistics

You can view port statistics including the inbound/outbound packet amount of each port, conflict statistics, packet loss amount, CRC error packet. The port working performance is low if the error packet amount is too huge, please check the port cable connection or confirm corresponding opposite port has problem or not.

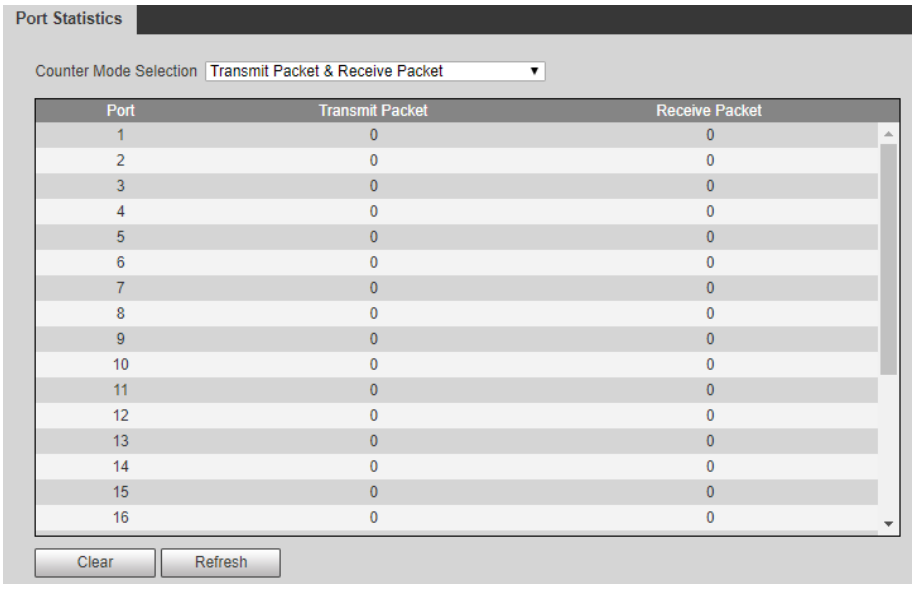
Procedure

Step 1 Select **Port Management** > **Port Statistics**.

Step 2 Select **Counter Mode Selection**, including **Transmit Packet & Receive Packet**, **Collision Packet & Transmit Packet**, **Drop Packet & Receive Packet** and **CRC 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 whether there is a problem with the cable connected to the port or the device.

Figure 4-4 Configure port statistics



Related Operations

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

4.2.4 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**.

Step 2 Configure parameters.

Step 3 Click **Save**.

Figure 4-5 Port speed limit

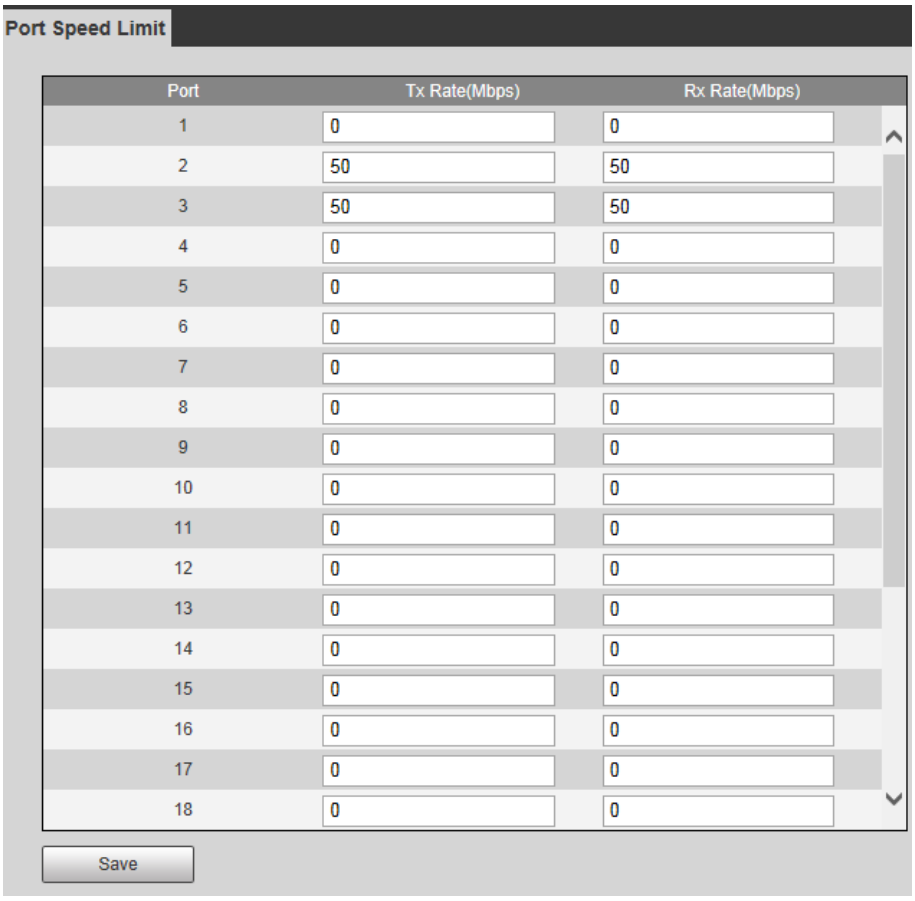


Table 4-4 Description of the port speed limit parameter

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

4.2.5 Configuring Broadcast Storm Control

Prerequisites

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 can 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.

Step 1 Select **Port Management** > **Broadcast Storm Control**.

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.

Step 4 Click **Save**.

Figure 4-6 Configure Broadcast Storm Control

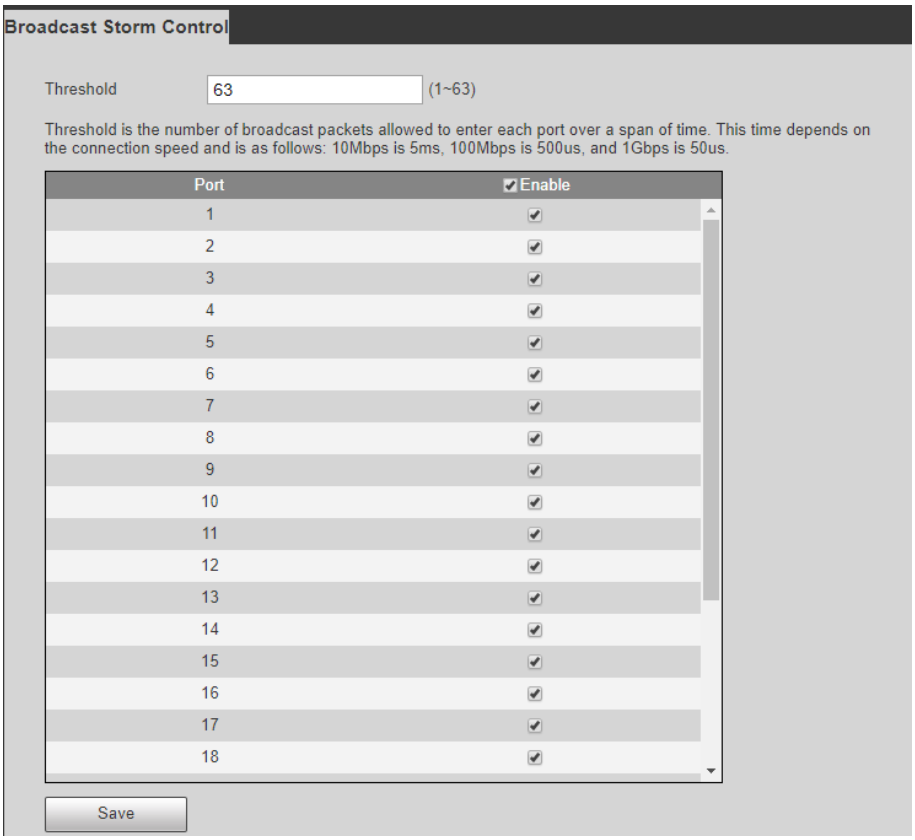


Table 4-5 Description of parameters

Name	Description
Threshold	The limit of the broadcast packets of one port during the specified period.
Port	Port name.

4.2.6 Configuring ePoE Functions

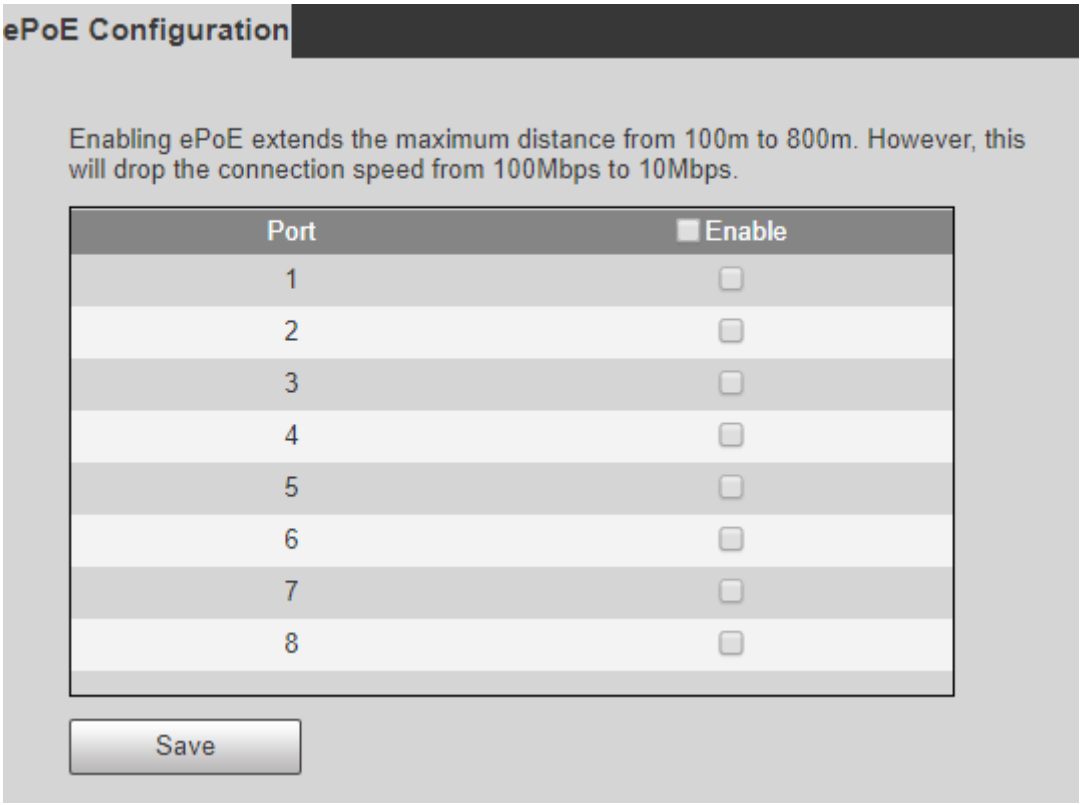
You can enable ePoE to extend the maximum distance. Enabling ePoE can extend the maximum distance from 100 m to 800 m while drop the connection speed from 100 Mbps to 10 Mbps.

Step 1 Select **Port Management** > **ePoE Configuration**.

Step 2 Select the checkbox next to **Enable** of the corresponding port.

Step 3 Click **Save**.

Figure 4-7 ePoE Configuration



4.2.7 Configuring Port Isolation

Port isolation is to achieve Layer 2 isolation between packets. 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**.

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

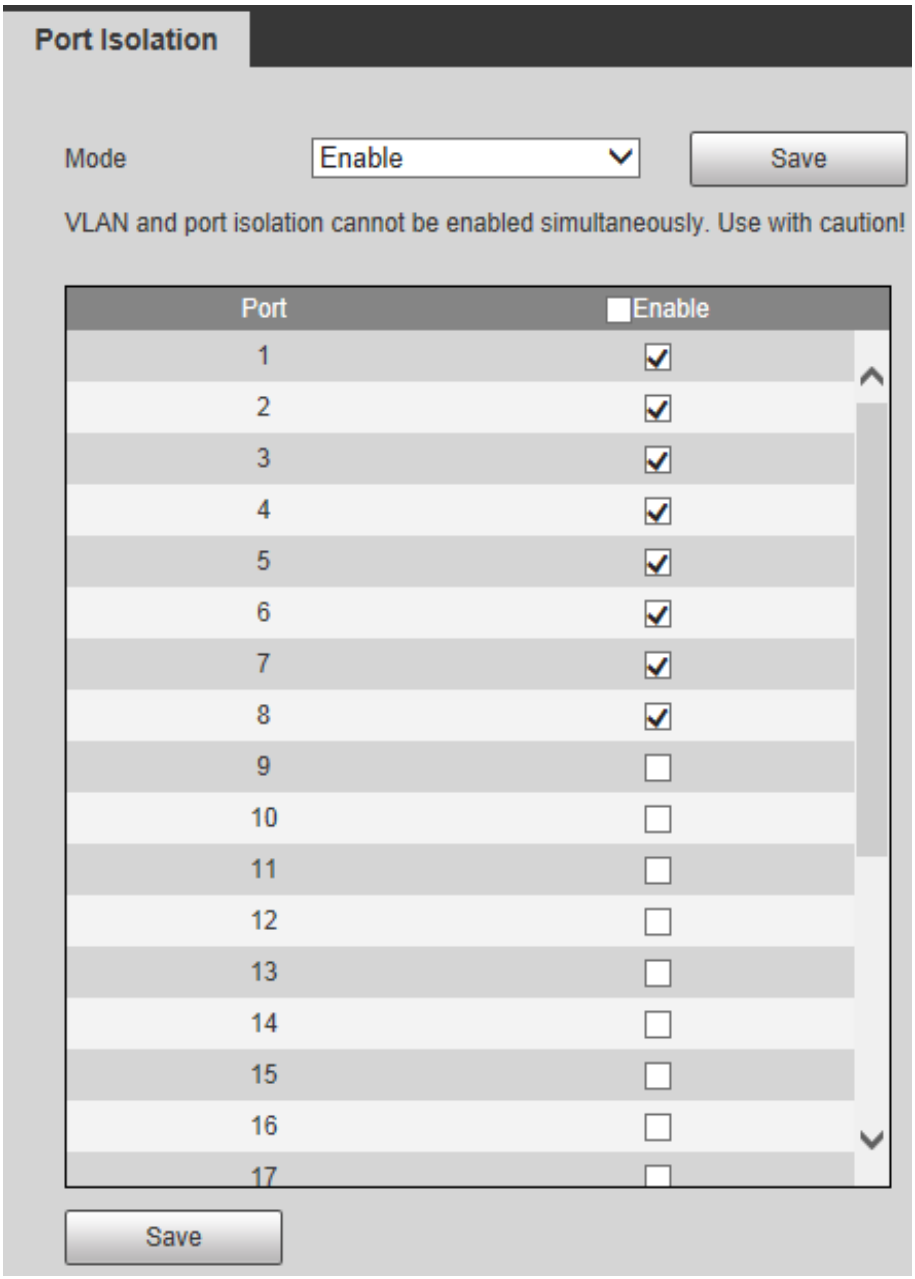
Step 3 Click **Save** on the right side of the mode.

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

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

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

Figure 4-8 Configure port isolation



4.3 Device Management

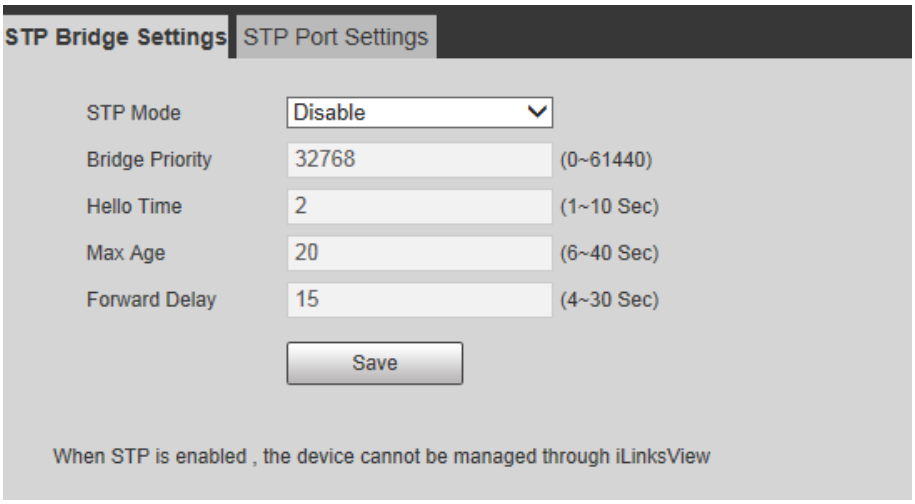
4.3.1 Configuring Spanning Tree

4.3.1.1 Configuring STP Bridge

Procedure

Step 1 Select **Device Management** > **Spanning Tree** > **STP Bridge Settings**.

Figure 4-9 STP bridge settings



Step 2 Configure parameters.

Step 3 Click **Save**.

Table 4-6 Description of the STP bridge settings

Parameter	Description
STP Mode	Enable or disable ring network function. • 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. It ranges from 0 to 61440.
Hello Time	Set the period of root bridge sending BPDU. It ranges from 1 s to 10 s.
Max Age	Set the aging time of current BPDU. It ranges from 6 s to 40 s.
Forward Delay	After setting topological change, the bridge maintains the time of snooping and study state. It ranges from 4 s to 30 s.

4.3.1.2 Configuring STP Port

Procedure

Step 1 Select **Device Management** > **Spanning Tree** > **STP Port Settings**.

Step 2 Configure parameters.

Step 3 Click **Save**.

Figure 4-10 Configure STP Port

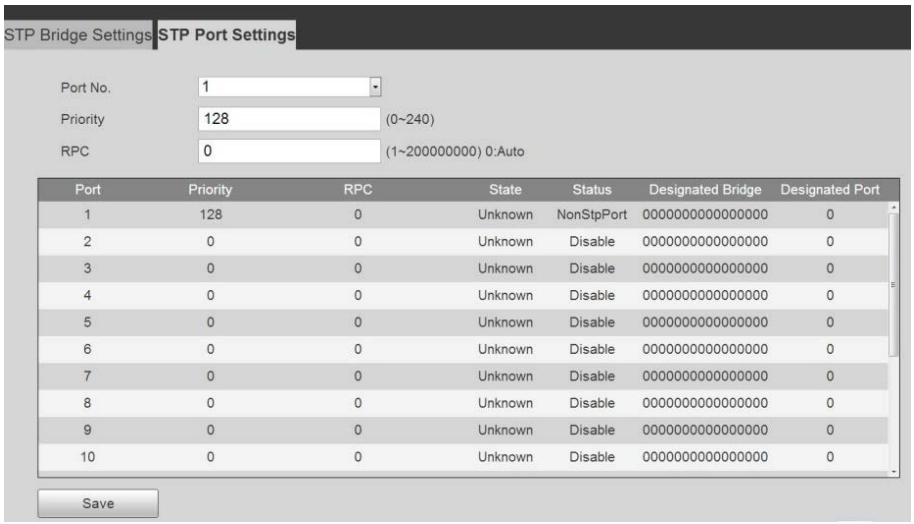


Table 4-7 Description of parameters

Parameter	Description
Port No.	Select the port you want to configure.
Priority	Configure 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 the RPC is set as 0.

4.3.2 Configuring VLAN

4.3.2.1 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.

4.3.2.2 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 devices 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.

4.3.2.3 Port-based VLAN

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 messages to, receive messages from and send messages to multiple VLANs, and is used to connect between the switches.
- Hybrid: The port allows multiple VLANs to pass messages to, receive messages from and send messages to 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 to multiple VLANs without a tag, while the trunk port only allows sending the default VLAN messages without a tag.

4.3.2.4 Configuring VLAN List

You can create and manage VLAN.

Procedure

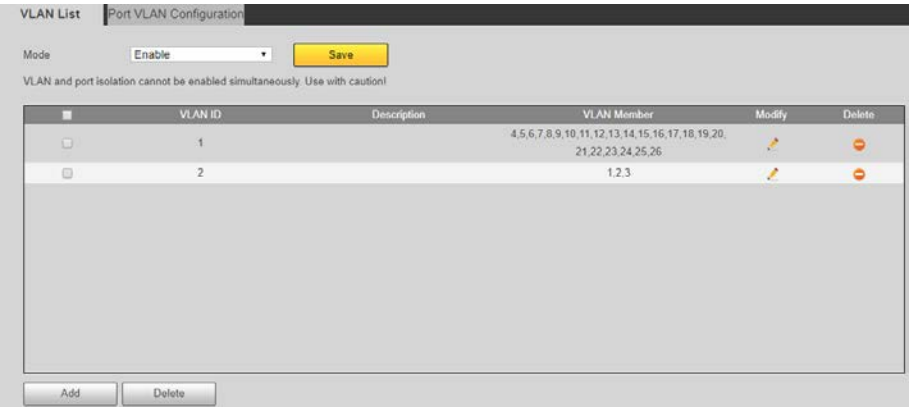
Step 1 Select **Device Management** > **VLAN** > **VLAN List**.

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

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

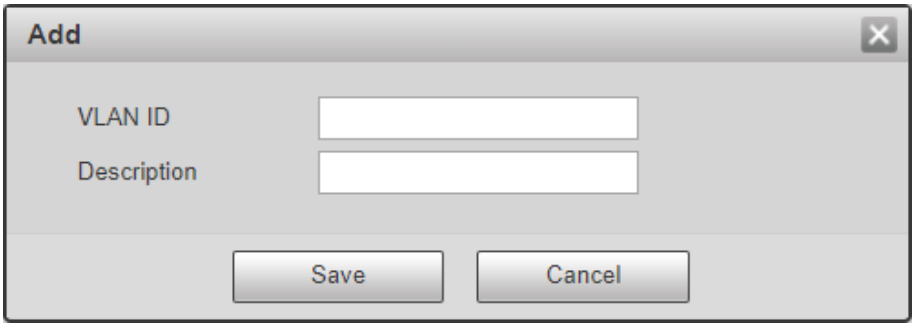
Port isolation and VLAN are mutually exclusive. When the port isolation is enabled, the VLAN will be automatically disabled.

Figure 4-11 Enable VLAN



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

Figure 4-12 Add VLAN



Step 5 Click **Save**.

Related Operations

- Modify VLAN: Select VLAN that has been added in the list, click to modify the VLAN ID and Description.
- Delete VLAN: Select VLAN that has been added in the list, click or click **Delete** to delete the VLAN.

4.3.2.5 Configuring Port VLAN

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

Step 1 Select **Device Management** > **VLAN** > **Port VLAN Configuration**.

Step 2 Configure parameters.

Step 3 Click **Save**.

Figure 4-13 Configure port VLAN

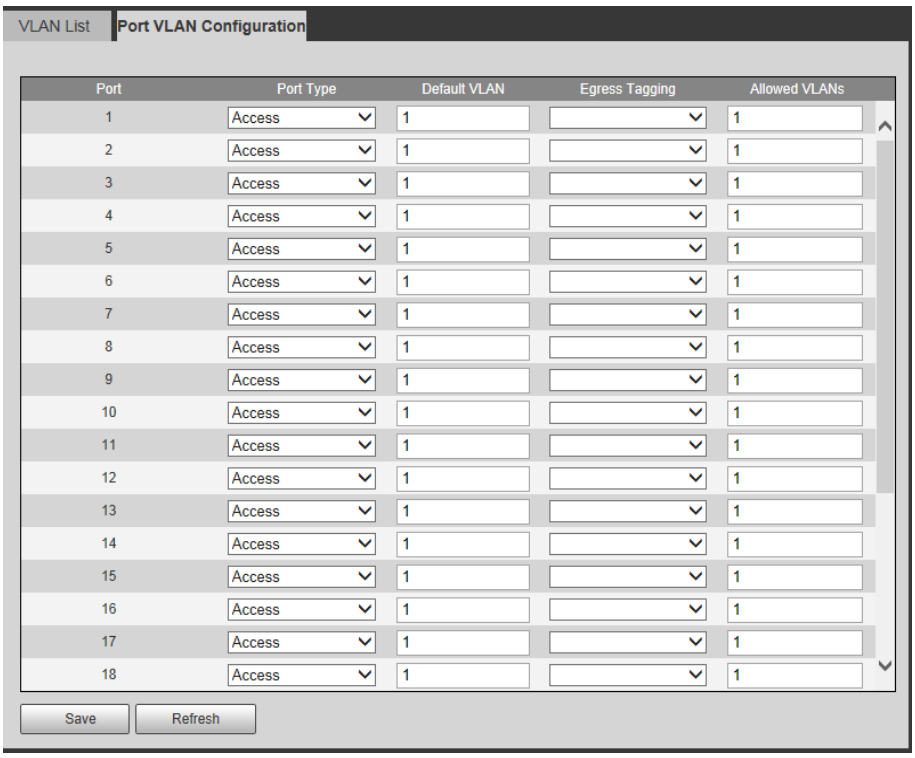


Table 4-8 Description of parameters

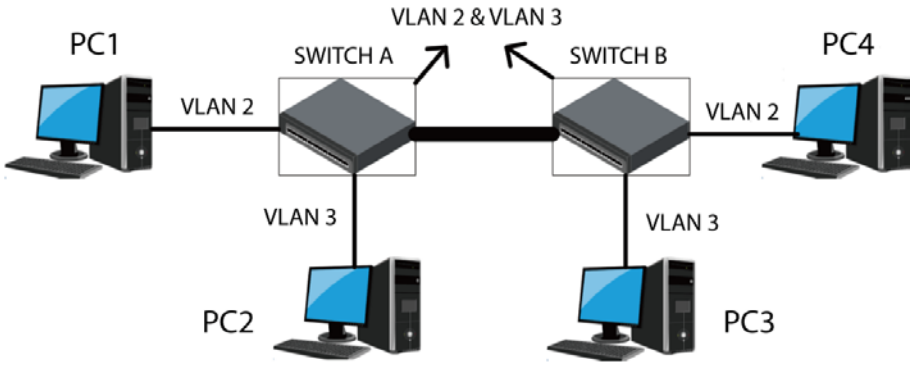
Parameters	Description
Port	Displays all ports of the Switch.
Port Type	Configure port type, including three types: **Access**, **Trunk** and **Hybrid**.
Default VLAN	Add port to VLAN, all ports belong to VLAN 1 by default. The range is from 1 to 4094.

Parameters	Description
Egress Tagging	Configure Egress tag type. • Access port: No need to configure. • Trunk port: ◇ 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: ◇ 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.

4.3.2.6 Example of Configuring VLAN

Configuration requirements: PC1 and PC2 belong to one department, and PC3 and PC4 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.

Figure 4-14 VLAN networking



Step 1 Select **Device Management** > **Spanning Tree** > **Port VLAN Configuration**.

Step 2 Configure parameters.

1) Configure port 1 as access port, and it belongs to VLAN2.
2) Configure port 2 as access port, and it belongs to VLAN3.
3) Configure port 3 as trunk port, and it belongs to VLAN2. Configure **Egress Tagging** of port 3 as **Untag Port VLAN**, and configure **Allowed VLANs** as 2 and 3.

Step 3 Click **Save**.

4.3.3 Link Aggregation

Link aggregation is to form several physical ports of the Switch into one logical port. Several links which 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 to increase bandwidth. Meanwhile, mutual dynamic backup can be realized among each member port in the same aggregation group 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 oppsite end devices of 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.

4.3.3.1 Static Aggregation Mode

Static aggregation mode allows manually adding member ports in the aggregation group. All the ports are in the forward status and share the overloaded flow. The creation of aggregation group and the adding of 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**.

Step 2 Configure **Link Aggregation Mode**.

Table 4-9 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**.

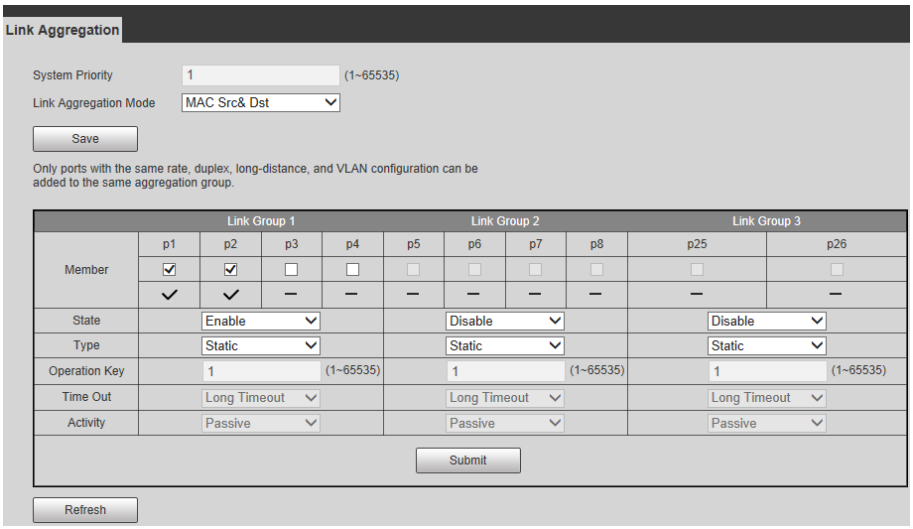
Link Group is an assembly of a group of Ethernet ports. The supported number of link groups is three by default, which can't be modified. The default status of all the aggregation groups is **Disable**, and member port is null by default.

Step 5 Select member port.

Step 6 Select **State** as **Enable**.

Step 7 Select **Type** as **Static**.

Figure 4-15 Link aggregation



Step 8 Click **Submit**.

4.3.3.2 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.

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

Table 4-10 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.
Operation Key	Configure operation Key. Members in the same aggregation group need to configure the same operation Key, ranging from 1 to 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	Activity is **Passive** by default and can be select as **Active**. ● When Activity is selected as **Active**, the device will actively initiate convergence negotiation. When Activity is selected as **Passive**, the device 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**.

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**.

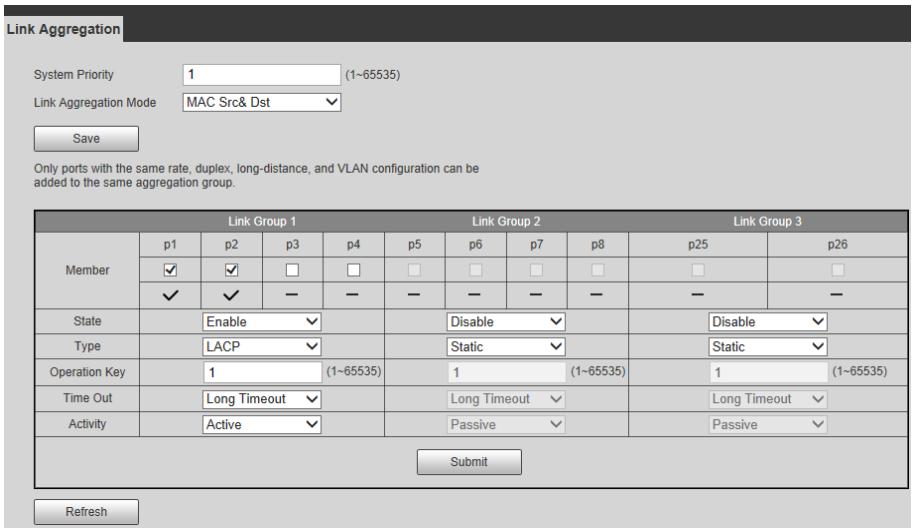
Step 5 Click **Submit**.

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 4-16 LACP Aggregation



4.3.4 QoS Settings

Quality of Service (QoS) reflects the ability of a network to meet customer needs. In the Internet, QoS evaluates the ability of the network to forward packets of different services.

4.3.4.1 Priority Mode

Step 1 Select **Device Management** > **QoS Settings** > **Priority Mode**.

Step 2 Configure **Priority Mode**.

Figure 4-17 Priority mode

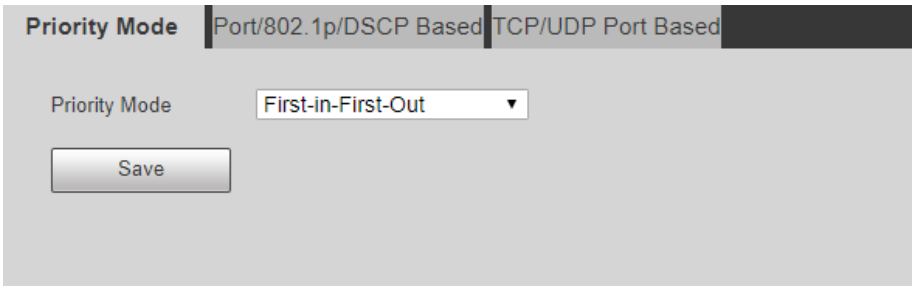


Table 4-11 Parameter description

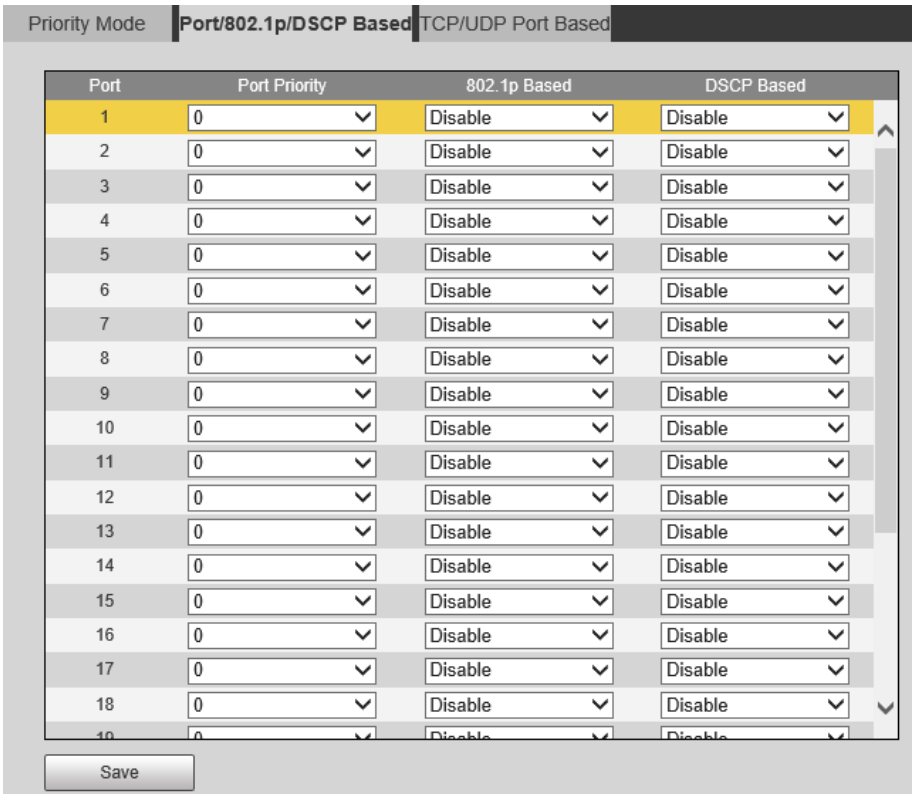
Name	Description
First-in-First-out	The first received packet will be forwarded first. When the QoS function is disabled, the Switch adopts FIFO mode to process the packets.
Weight-round-robin	The Switch forwards the packets according to the specified priority level.
All-high-before-low	Set the weight level to change the packet forwarding percentage in the high priority and low priority.

4.3.4.2 QoS Based on Port/802. 1p/DSCP

Step 1 Select **Device Management** > **QoS Settings** > **Priority Mode**.

Step 2 Configure **Port Priority**, **802. 1p Based**, and **DSCP Based**.

Figure 4-18 Port/802.1 p/DSCP



- **Based on port**
  When a port is set as the high priority, the received packets are placing in the high priority queue. Each port can be set as the high priority.
- **Based on 802.1p**
  802.1p priority is at the 2-layer packet head, and is for the scenes where there are no need to analyze the third head and can guarantee the QoS in the 2-layer.

Table 4-12 802.1p priority

Priority queue	802.1p priority (Decimal system)	802.1p priority (Binary system)	Key words
Low priority queue	0	000	best effort
	1	001	background
	2	010	spare

Priority queue	802.1p priority (Decimal system)	802.1p priority (Binary system)	Key words
	3	011	excellent effort
High priority queue	4	100	controlled load
	5	101	video
	6	110	voice
	7	111	network management

Table 4-13 IP priority

Priority queue	IP priority (Decimal system)	IP priority (Binary system)	Key words
High priority queue	46	101110	ef
	10	001010	af11
	18	010010	af21
	26	011010	af31
	34	100010	af41
	48	110000	cs6
Low priority queue	56	111000	cs7
	Others	—	—

4.3.4.3 TCP/UDP Port Based

TCP and UDP adopt 16bit port to recognize the applications. The server usually uses the port to recognize. For example, the TCP port of the FTP server is the 21, and TCP port of each Telnet server is 23, UDP port of each TFTP server is 69. All TCP/IP service is using the well-known 1–1023 port.
The Switch can process the received packets based on the TCP/UDP port such as FTP, SSH, TELNET, SMTP, and DNS. You can set packet high priority, low priority, or discard. The default setup is Q0.

Step 1 Select **Device Management** > **QoS Settings** > **TCP/UDP Port Based**.

Step 2 Select **Protocol**, and then configure the corresponding **Option** from **Q0**, **Q1**, **Disable** and **Discard**.

4.3.5 Security

4.3.5.1 MAC Address Table

Background Information

MAC (Media Access Control) records the relationship between the MAC address and the port, and information of VLAN to which the port belongs. When device forwards the message, it searches the MAC address list according to the message destination MAC address. If the MAC address list includes an item matching the packet destination MAC address, it uses the output port to forward the message. If the MAC address list has no item matching the packet destination MAC address, the

device adopts the broadcast mode to forward the packet through the corresponding VLAN (except the input port).

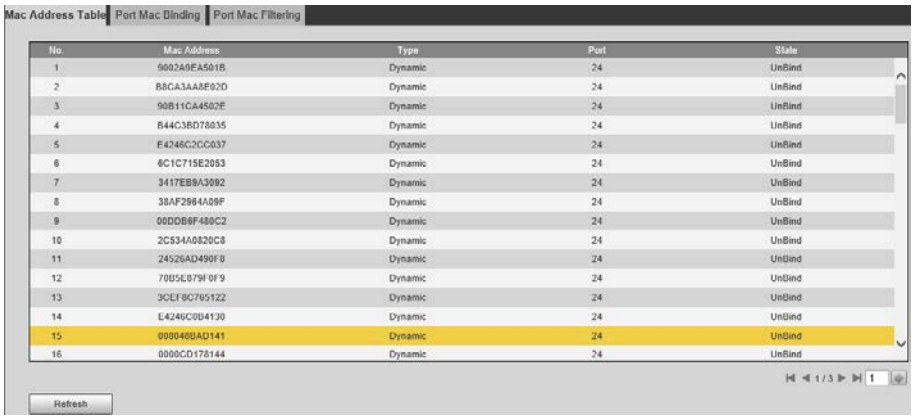
Procedure

Step 1 Select **Device Management** > **Security** > **MAC Address Table**.

Step 2 View MAC address list.

Step 3 Click **Refresh** to refresh the Mac address of each port.

Figure 4-19 MAC address list



4.3.5.2 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.

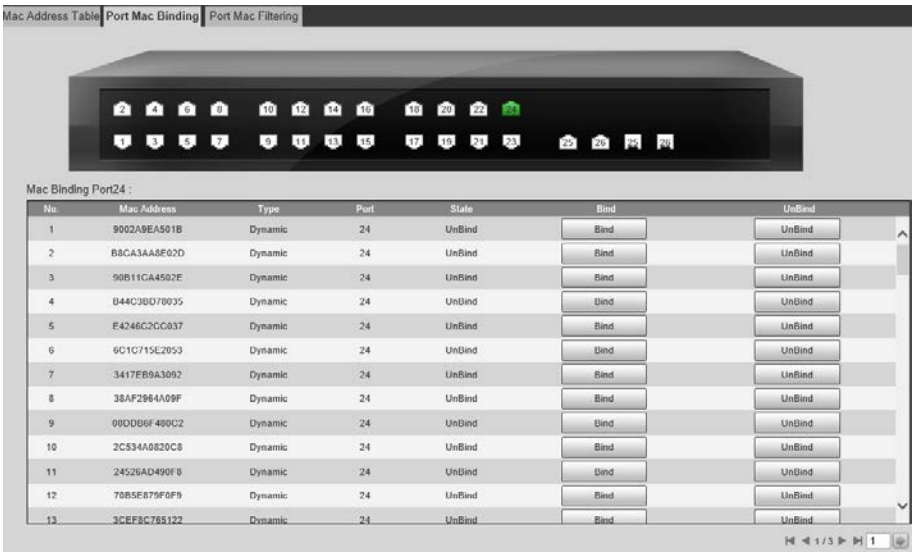
Procedure

Step 1 Select **Device Management** > **Security** > **Port MAC Binding**.

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

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

Figure 4-20 Bind port MAC



Related Operations

Unbind: In the list of bound devices, click **Unbind** to delete the bound device.

4.3.5.3 Filtering Port MAC

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

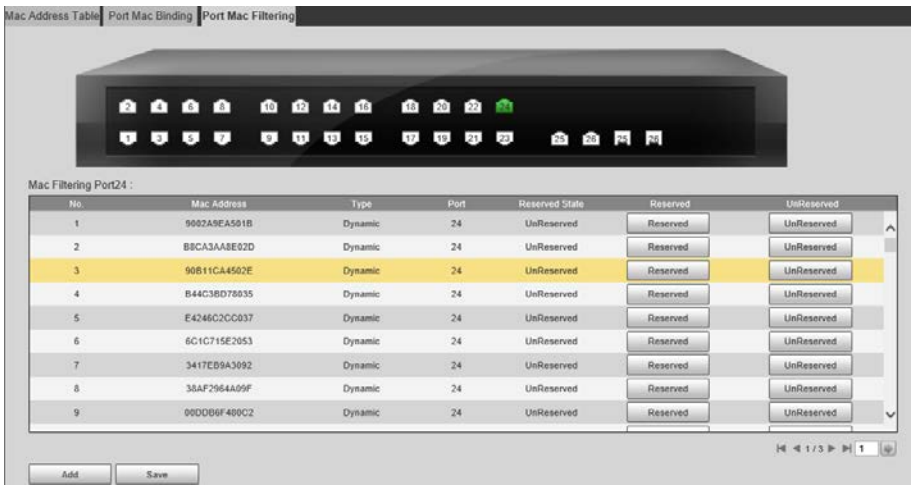
After the port is configured with the port MAC filtering function, when the port receives message, it will check if the source MAC address of message is the same as the allowed MAC address:

- 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.

Step 1 Select **Device Management** > **Security** > **Port MAC Filtering**.

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

Figure 4-21 Filter Port MAC



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

Step 4 Click **Save**.

4.3.6 Configuring SNMP

SNMP network includes two elements: NMS and Agent.

- NMS (Network Management System) is the SNMP network administrator. Provides user-friendly interactive interface and is suitable for the network administrator to complete the most management work.
- Agent is the object to be managed in the SNMP network. Receives, and 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.

4.3.6.1 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 device 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 has expanded the functions of the SNMPv1, which provides 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.

4.3.6.2 Configuring SNMP

Step 1 Select **Device Management** > **SNMP Settings**.

Step 2 Select SNMP version.

- Select **SNMP v1**, the device can only process information of SNMP v1.
- Select **SNMP v2**, the device can only process information of SNMP v2.
- Select **SNMP v3**, and then configure username, password and authentication type. When the server needs to access the device, 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.

Figure 4-22 SNMP v1 and SNMP v2

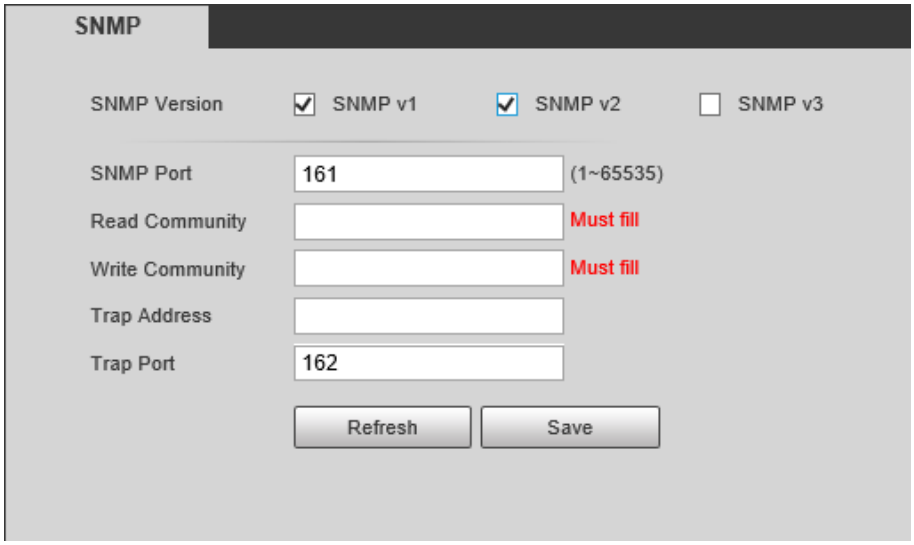
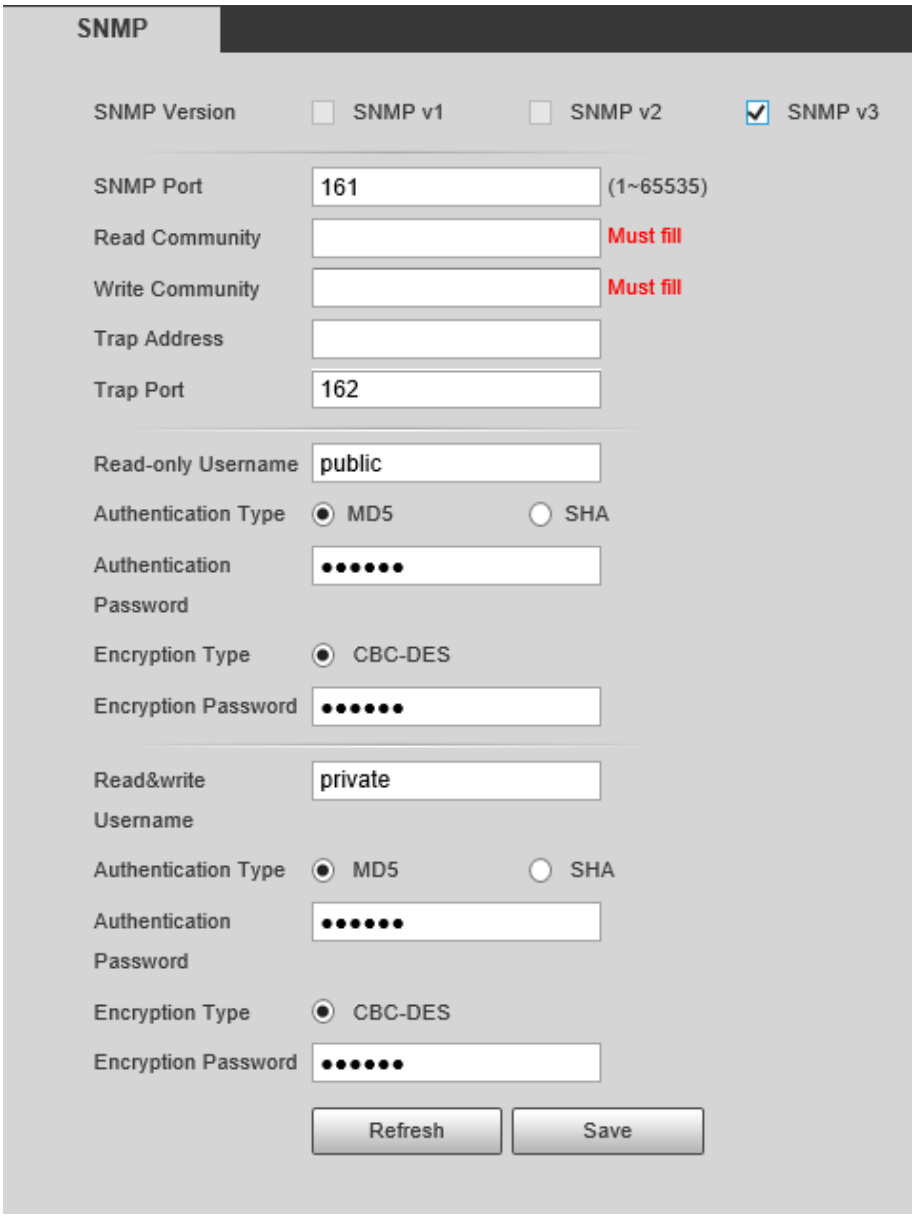


Figure 4-23 SNMP v3



Step 3 Configure parameters.

Table 4-14 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	Set trap destination port.
Read-only username	Set the read-only username. It is for V3 only.
Authentication type	Set authentication mode when the security level is **Authentication no encryption** or **Authentication and encryption**. The authentication mode includes MDS and SHA.

Name	Description
Authentication password	Set 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	Set read and write user.

4.3.6.3 Example of SNMPv1/v2 Configuration

NMS is connected with the Switch, and the following requirements needs 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 a fault occurs.

Figure 4-24 Example of SNMP v1/v2 configuration

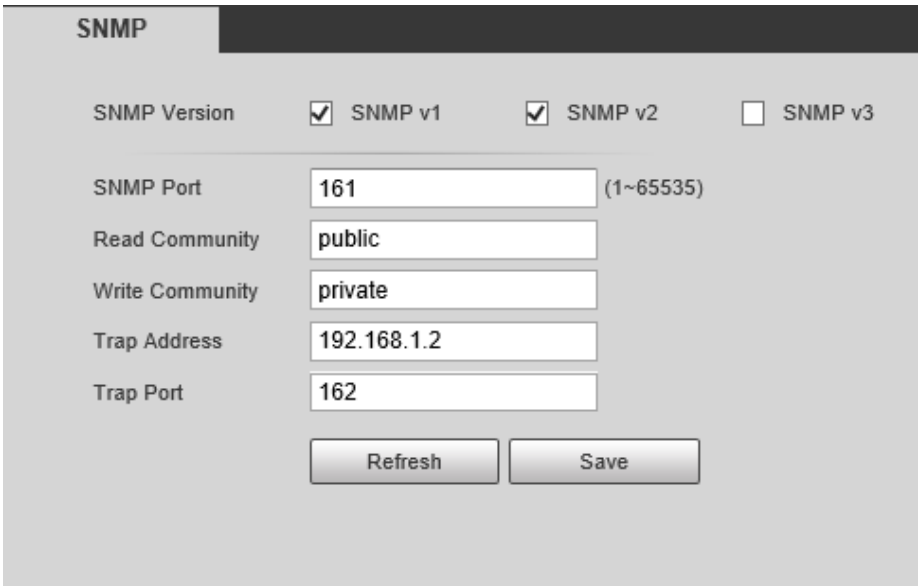
Step 1 Select **Device Management** > **SNMP Settings** on the **System Info** page.

Step 2 Select **SNMP Version** to **SNMP v2**.

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.

Figure 4-25 SNMPv2 configuration



Step 4 Click **Save**.

4.3.6.4 Example of SNMPv3 Configuration

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, 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 4-26 Example of SNMPv3 configuration

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.

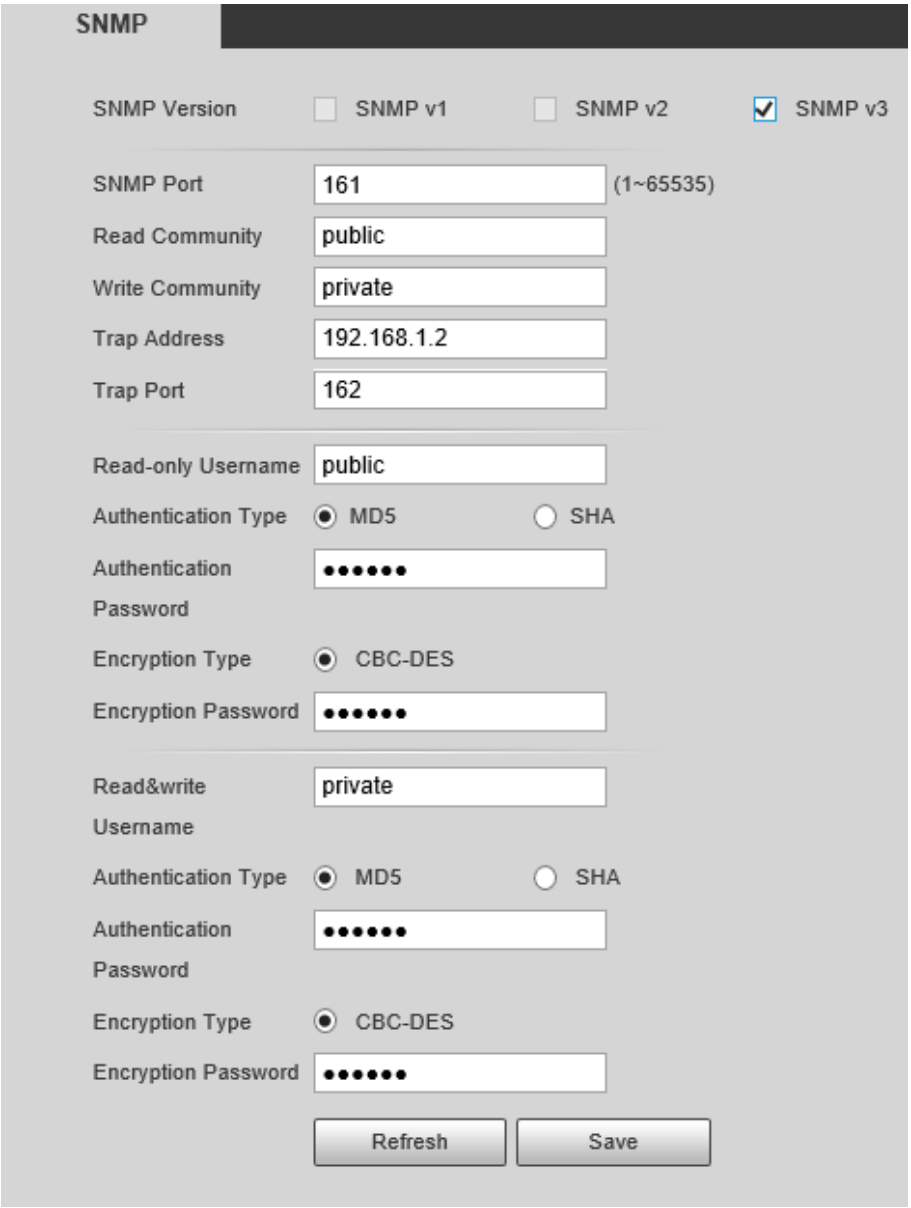
Step 4 Enter user as **Read-only Username**.

- 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 4-27 SNMP v3 configuration



Step 6 Click **Save**.

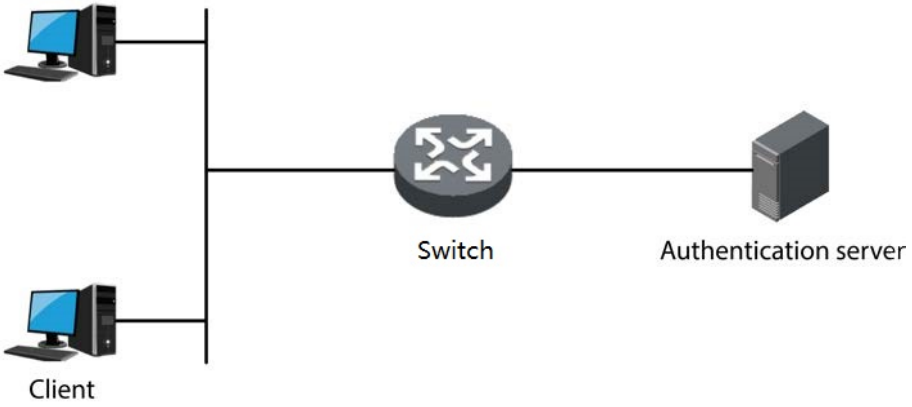
4.3.7 802.1x

IEEE 802.1x is the authentication standard designated by IEEE about user accessing network. It 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.

4.3.7.1 802.1x Networking Structure

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

Figure 4-28 802.1x 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.
- Device 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 RADIUS (Remote Authentication Dial-In User Service) server. Authentication server can verify the legality of 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 Switch. The role of Authentication server can be replaced by the Switch in some small-scale network environment, which means that the Switch realizes local authentication, authorization and billing upon the client.

4.3.7.2 802.1x 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 under authorization 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 authorized status.

4.3.7.3 Trigger Mode of 802.1x Authentication

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

- Client Active Trigger Mode
  - Multicast trigger: the Client actively sends authentication request message to the Device 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 Device to

trigger authentication, and the destination address of the message is the broadcast MAC address. The mode can solve the problem that the Device fails to receive authentication request from the Client because some devices in the network fail to support the multicast message above.

- Device Active Trigger Mode
  The device active trigger mode is used to support the Client that cannot actively send authentication request message, and there are two types of device active trigger authentication:
  - ◇ Multicast trigger: The Device 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 Device 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 Device fails to receive the Client response within the set duration.

4.3.7.4 Configuring NAS

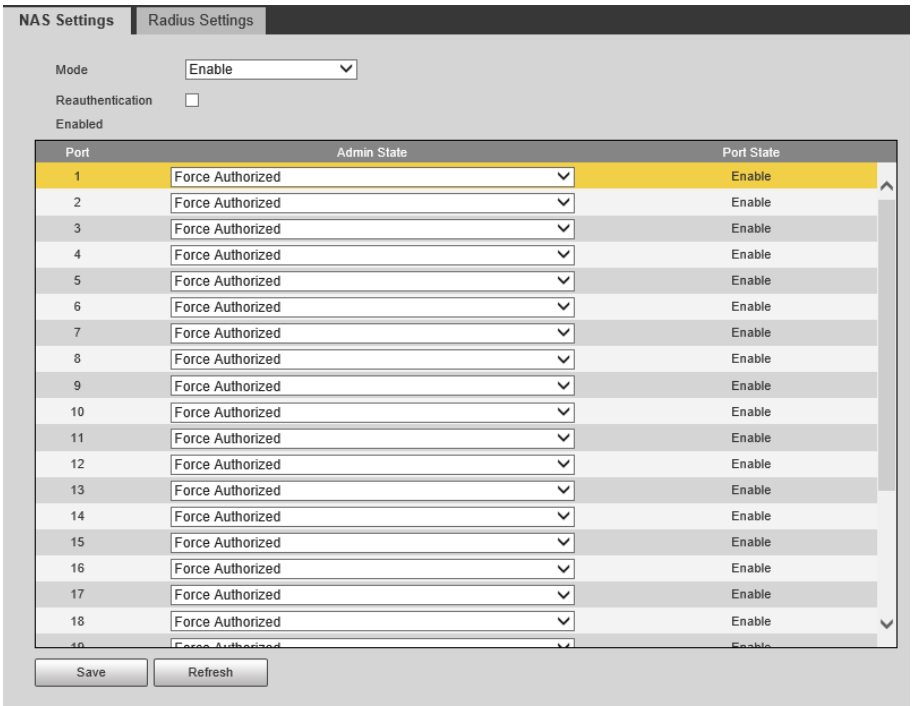
By configuring the authorization status of the port, you can control whether users connected to the port need to be authenticated to access network resources.

Step 1 Select **Device Management** > **802.1X** > **NAS Settings**.

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

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

Figure 4-29 Configure NAS



Step 4 Click **Save**.

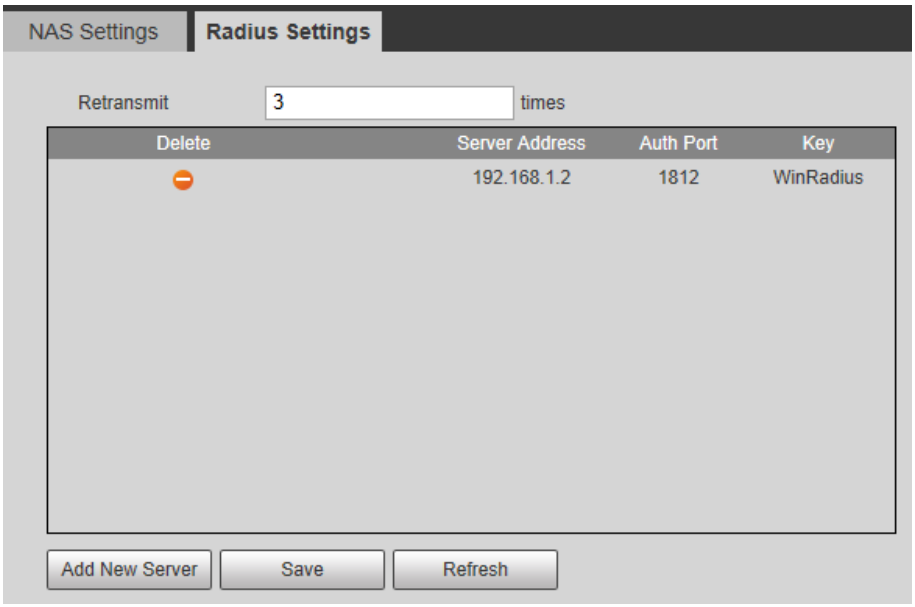
4.3.7.5 Configuring Radius

Configure the authentication server address.

Step 1 Select **Device Management** > **802.1X** > **Radius Settings**.

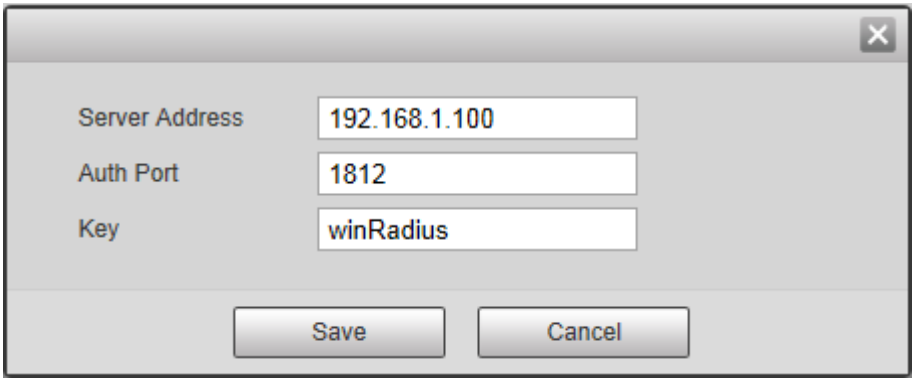
Step 2 Enter **Retransmit** times.

Figure 4-30 Configure Radius



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

Figure 4-31 Add new server



Step 4 Click **Save**.

4.3.8 IGMP Snooping

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

4.3.8.1 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 it is to forward multicast data according to the mapping relation.

The multicast data will be broadcasted in the layer two network when the layer two device doesn't 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 multi-casted to designated receivers.

IGMP Snooping can only forward the information to the needed receivers through layer two multicast, which can bring 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.

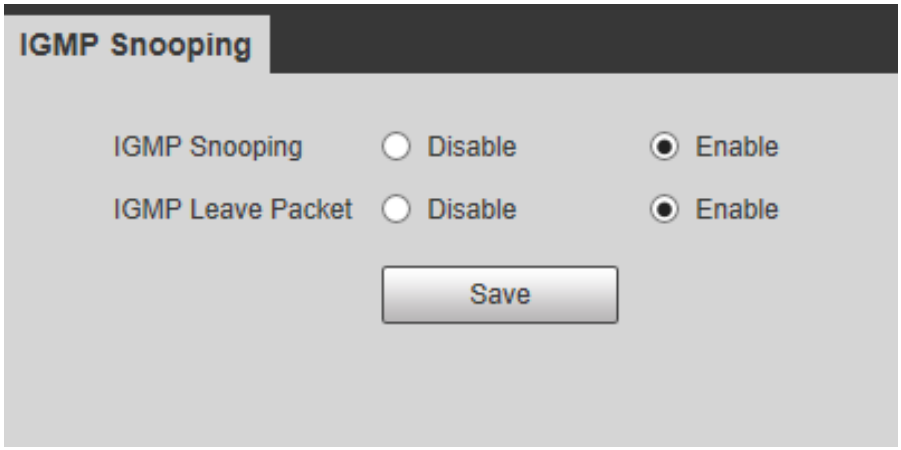
4.3.8.2 Configuring IGMP Snooping

Step 1 Select **Device Management** > **IGMP Snooping**.

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 4-32 Configure IGMP Snooping



Step 3 Click **Save**.

4.3.9 Configuring HTTPS

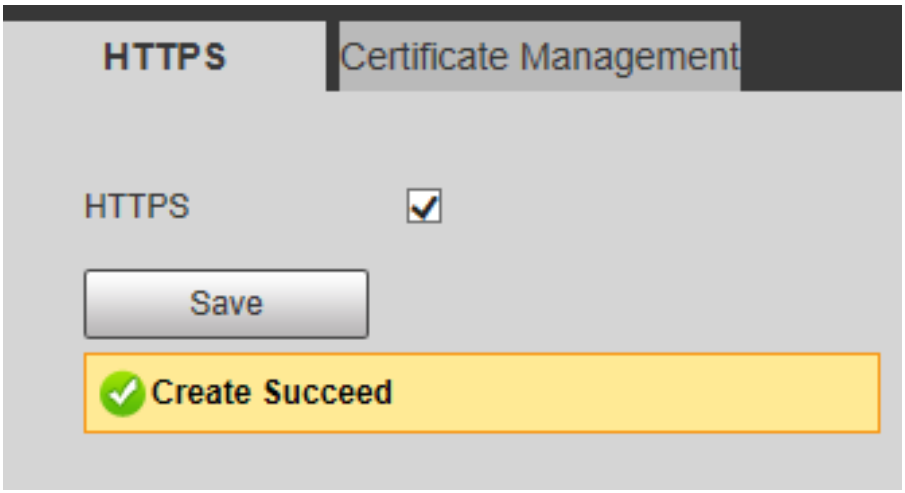
HTTP (HyperText Transfer Protocol) defines how the browser (the World Wide Web client process) requests a World Wide Web document from the World Wide Web server, and how the server transmits the document to the browser. From a hierarchical point of view, HTTP is a transaction-oriented application layer 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. 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 device 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**.

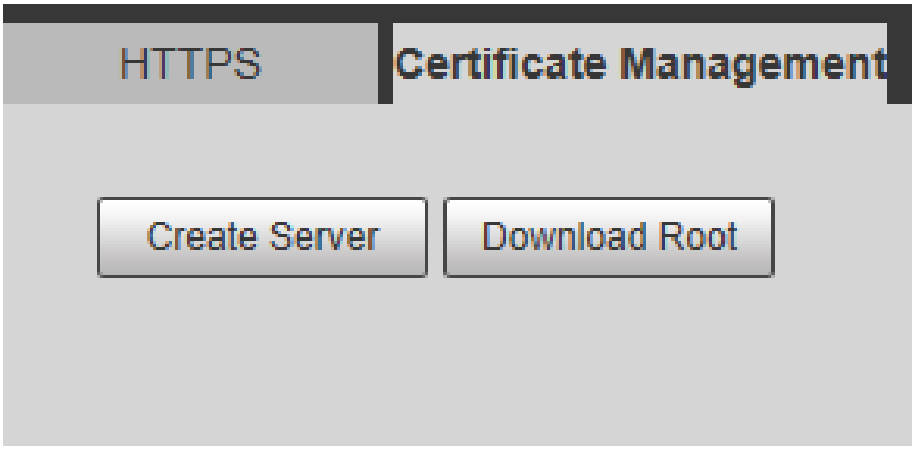
Step 2 Select **HTTPS**, click **Save**.

Figure 4-33 HTTPS



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

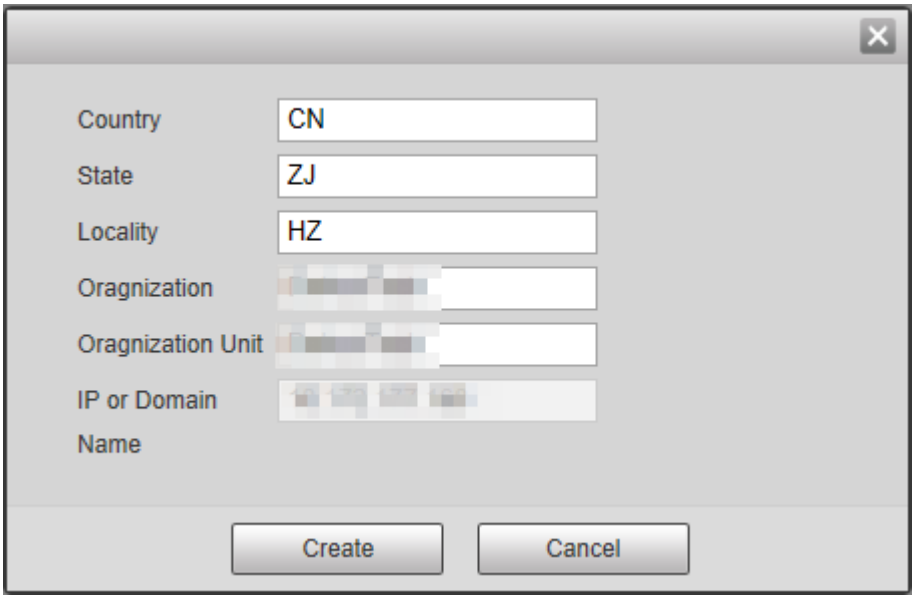
Figure 4-34 Certificate management



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.

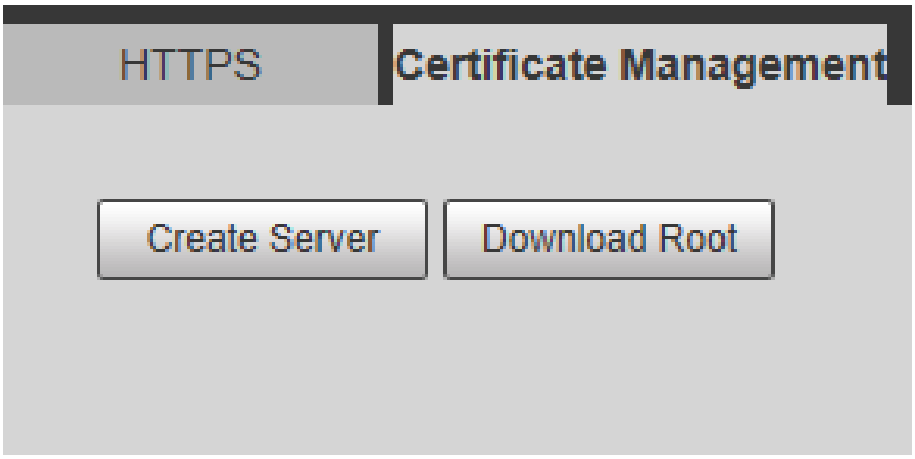
Figure 4-35 Create Server (1)



Step 5 Click **Create**.

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

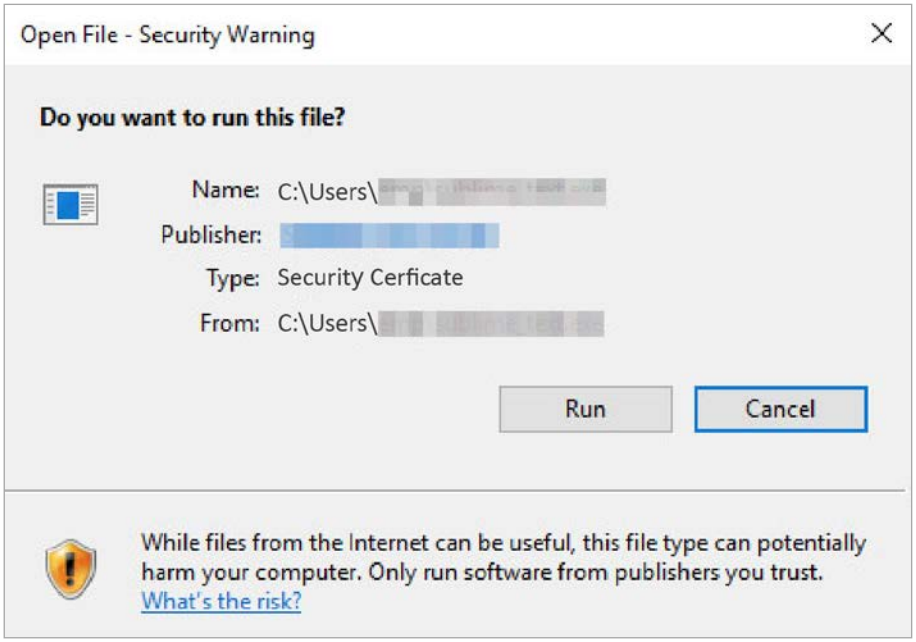
Figure 4-36 Create Server (2)



Step 6 Click **Download Root**.

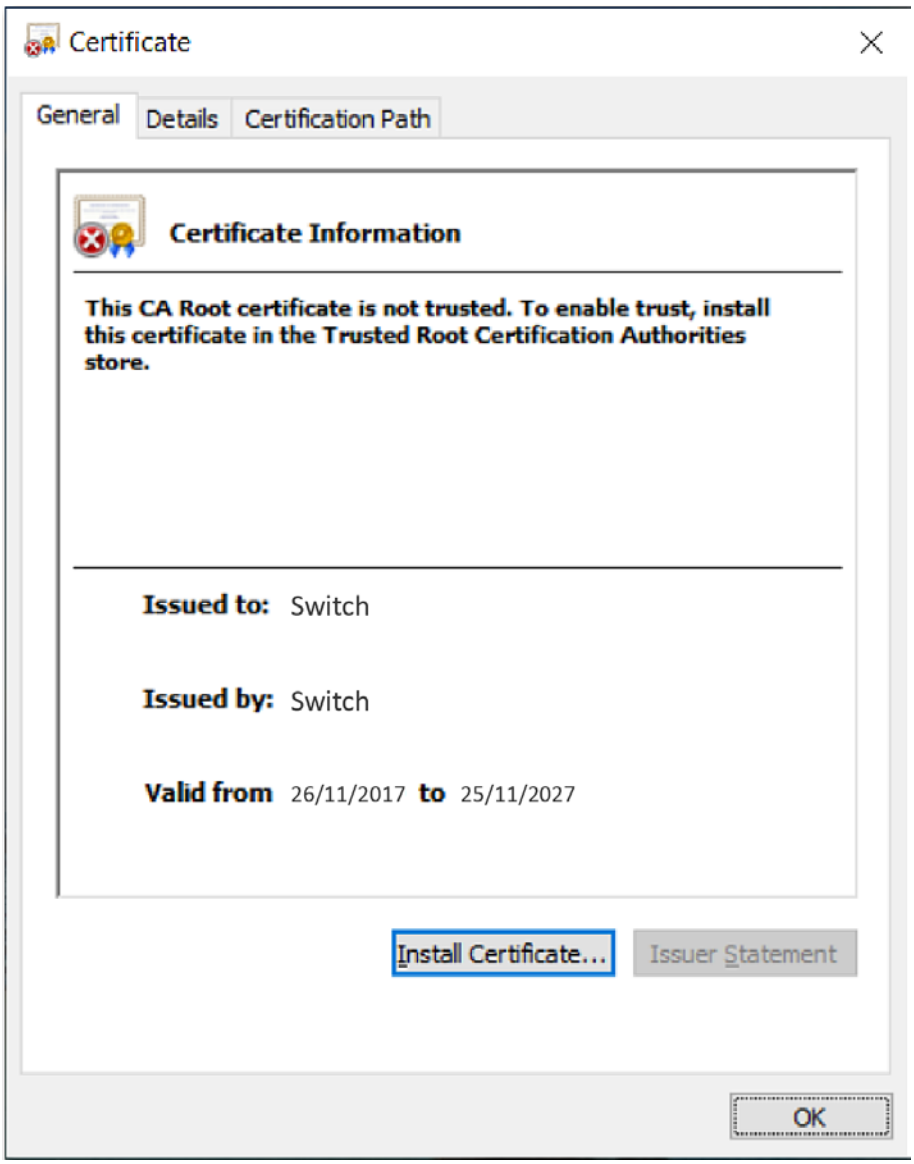
Step 7 Open the downloaded root certificate file, and then click **Run** on the **Security Warning** dialog box that pops up.

Figure 4-37 Download files



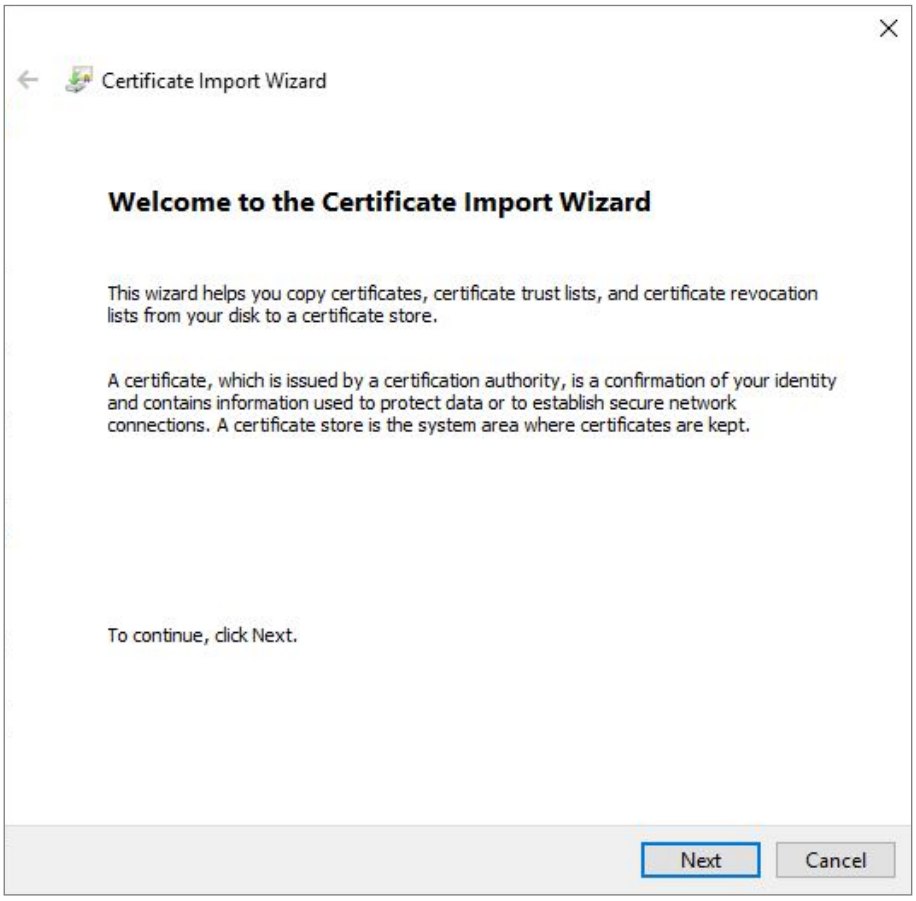
Step 8 Click **Install Certificate** in the **Certificate** dialog box that pops up.

Figure 4-38 Certificate



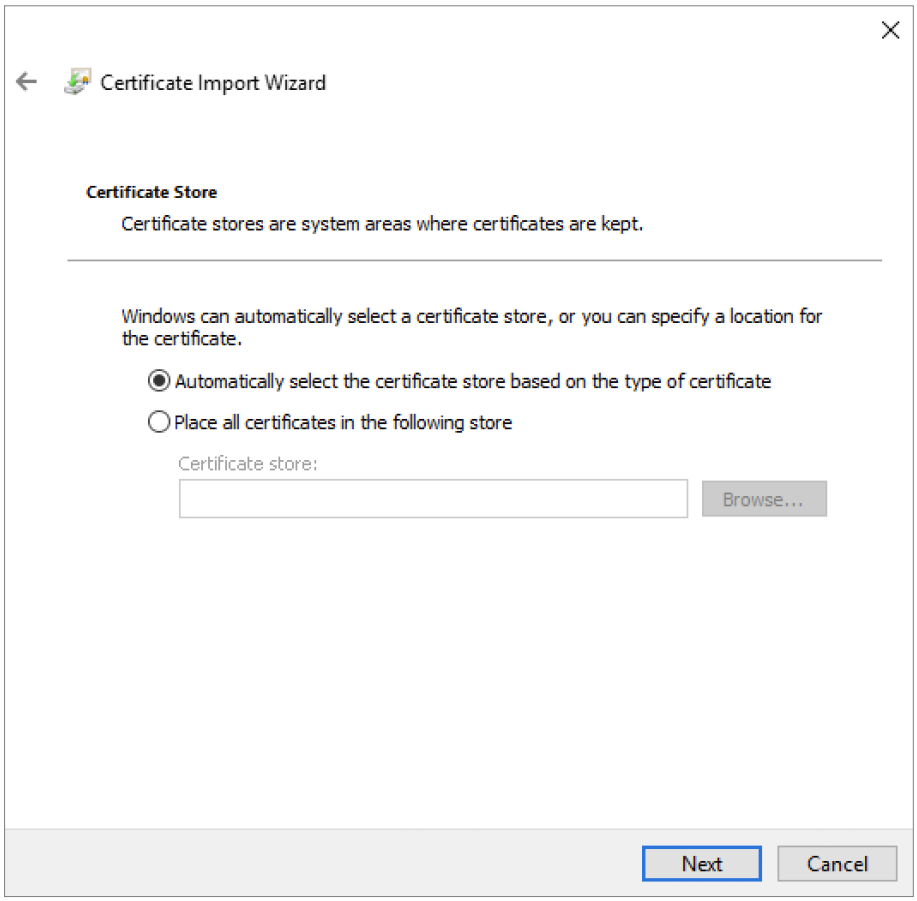
Step 9 Click **Next** in the displayed **Certificate Import Wizard** dialog box.

Figure 4-39 Certificate import wizard



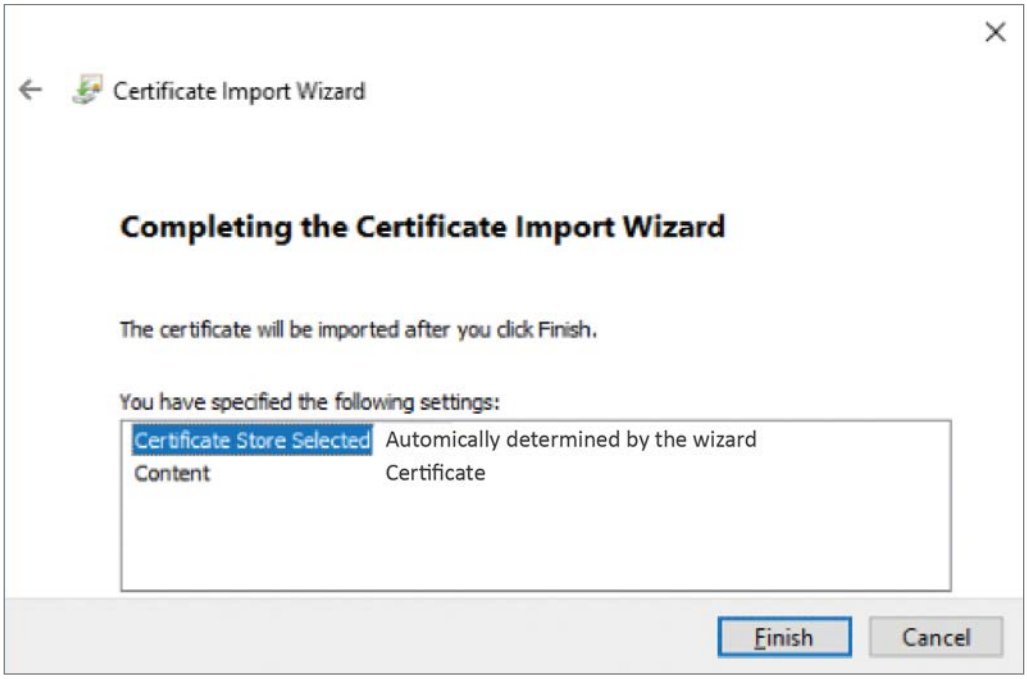
Step 10 Select **Automatically select the certificate store base on the type of certificate**, and then click **Next**.

Figure 4-40 Store certificate



Step 11 Click **Finish**.

Figure 4-41 Complete the certificate import wizard



4.4 PoE

4.4.1 Configuring PoE Power

Power over Ethernet (PoE) means the device uses the Ethernet port to power the device through the twisted pair cable remotely. 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 complies with the IEEE 802.3af and IEEE 802.3at 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.

Procedure

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

Step 2 Configure parameters.

Figure 4-42 Configure PoE

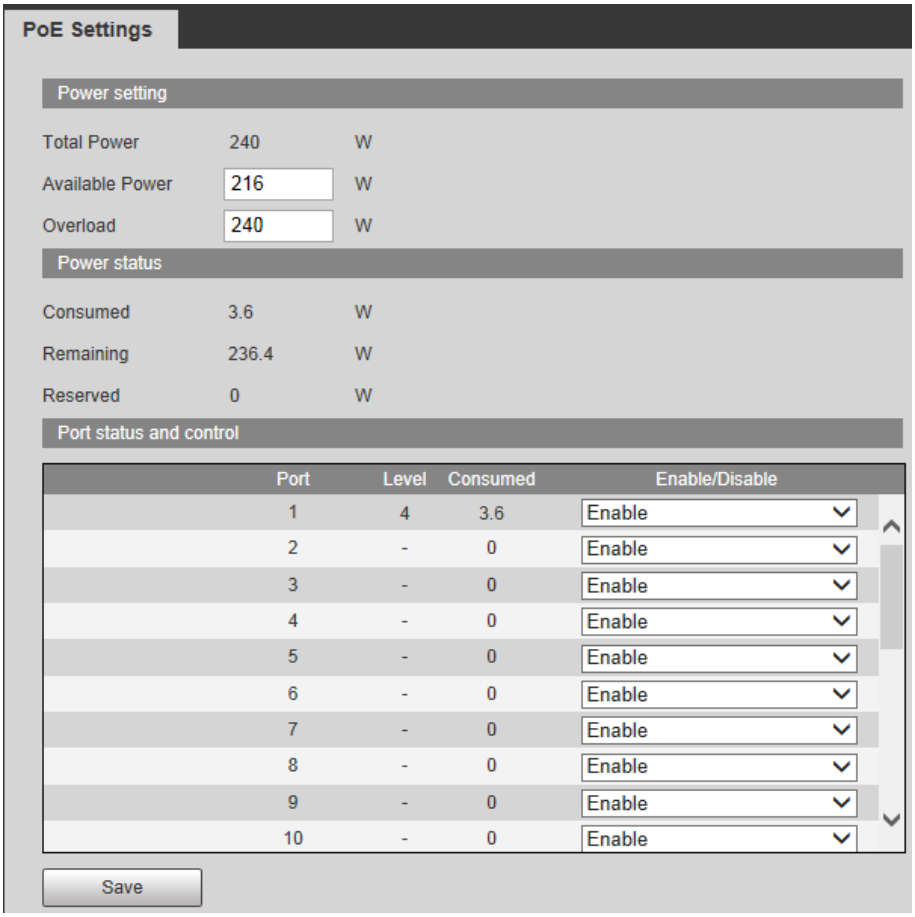


Table 4-16 Description of parameters

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.

Parameters		Description
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.
Port status and control	Level Power	Displays the power supply level to the terminal devices. The power supply level ranges from 0 to 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	Enables or disables PoE on the selected ports. ● 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.  ● 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**.

4.4.2 Viewing PoE Event Statistics

Display the PoE event statistics of each port. It includes **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 4-43 PoE events statistics

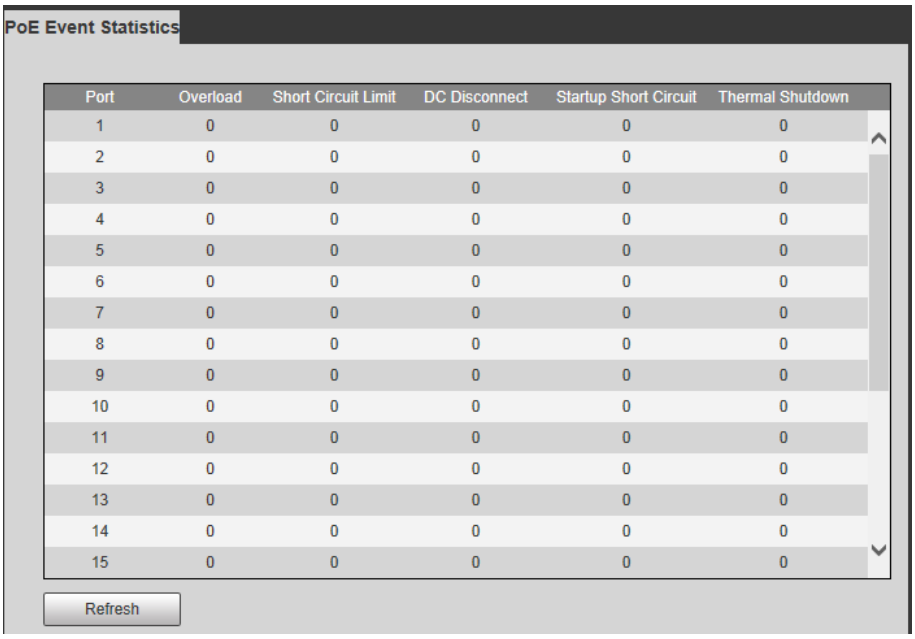


Table 4-17 Description of parameters

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 reason.

4.4.3 Configuring Green PoE

Background Information

The PoE function is off during the specified period to save power by configuring parameters on the Green PoE interface. When the period is over, the port automatically resumes supplying power.

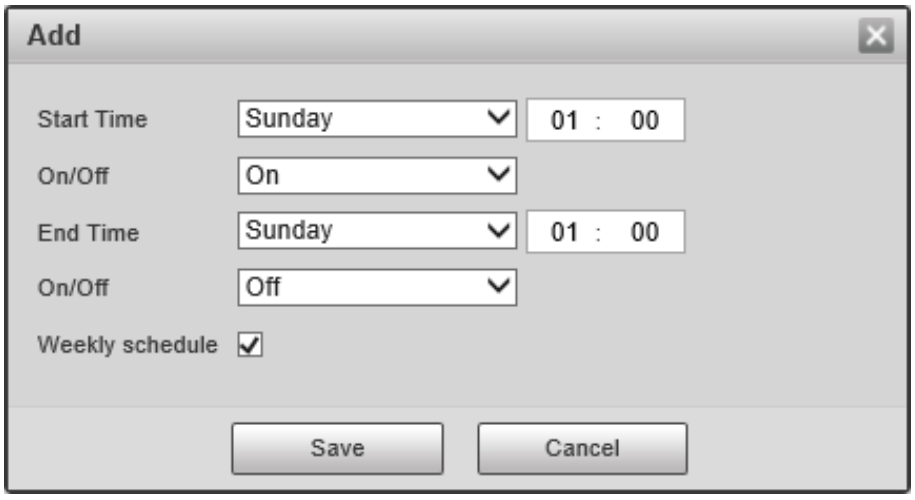
Procedure

Step 1 Select **PoE** > **Green PoE**.

Step 2 Click **Add energy saving**, configure **Start Time**, **On/Off**, **End Time**, and **On/Off**, and then click **Save**.

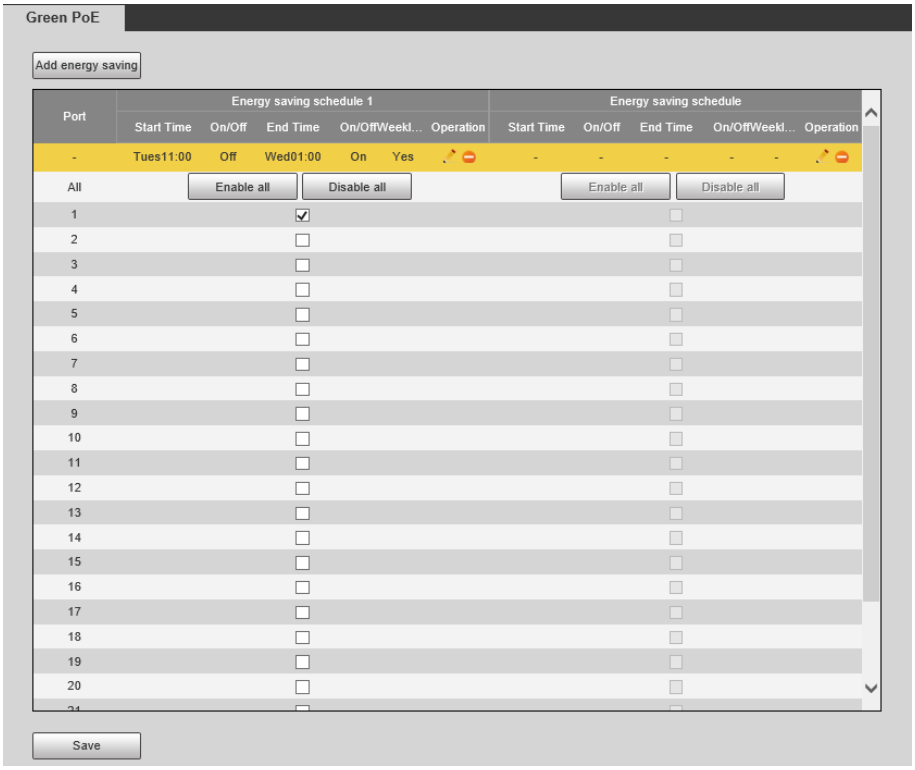
Click the **Weekly schedule** checkbox to enable the function.

Figure 4-44 Configure green PoE



Step 3 Select the port that needs to enable the power saving function.

Figure 4-45 Green PoE



Step 4 Click **Save**.

Related Operations

- Edit the energy saving schedule: Click .
- Clear the energy saving schedule: Click .

4.4.4 Configuring Legacy Support

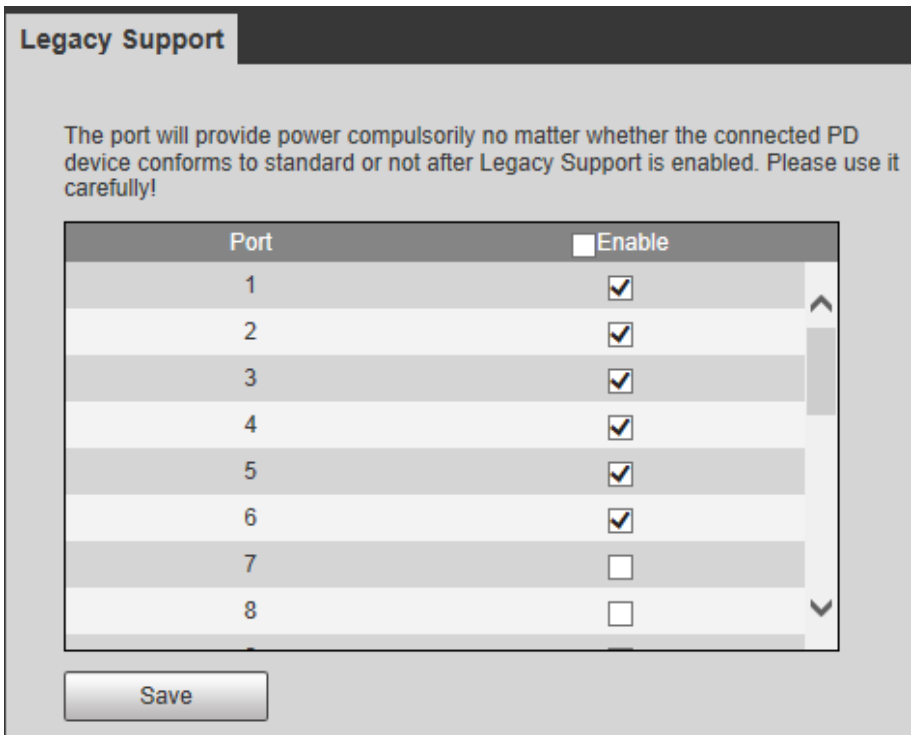
If the legacy support of a port is enabled, the port will provide power compulsorily no matter whether the connected PD device conforms to standard or not. Be cautious.

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

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

Step 3 Click **Save**.

Figure 4-46 Configure Legacy Support



4.4.5 Configuring PD Alive

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

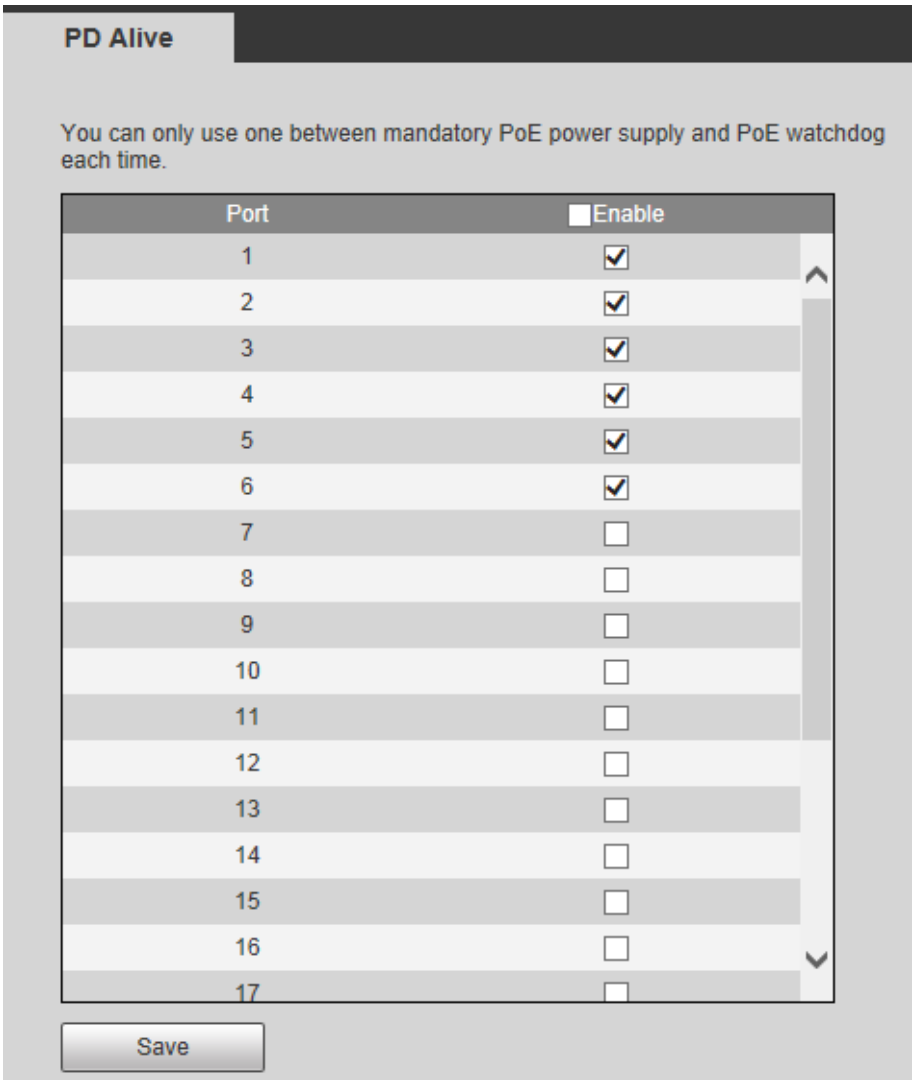
You can only use one between **Legacy Support** and **PD Alive** each time.

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

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

Step 3 Click **Save**.

Figure 4-47 Configure PD alive



Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic equipment 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.