Dahua 16/24-Port PoE Switch Web Config Manual

V1.0.5

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Important Safeguards and Warnings

Please read the following safeguards and warnings carefully before using the product in order to avoid damages and losses.

Attentions:

- Do not expose the device to lampblack, steam or dust. Otherwise it may cause fire or electric shock.
- Do not install the device at position exposed to sunlight or in high temperature. Temperature rise in device may cause fire.
- Do not expose the device to humid environment. Otherwise it may cause fire.
- The device must be installed on solid and flat surface in order to guarantee safety under load and earthquake. Otherwise, it may cause device to fall off or turnover.
- Do not place the device on carpet or quilt.
- Do not block air vent of the device or ventilation around the device. Otherwise, temperature in device will rise and may cause fire.
- Do not place any object on the device.
- Do not disassemble the device without professional instruction.
- To avoid personal injury or damage to the device, power off the device before removing the cable.
- Voltage stabilizer and lightning arrester are optional according to site power supply and surrounding environment.

Warning:

- Please use battery properly to avoid fire, explosion and other dangers.
- Please replace used battery with battery of the same type.
- Do not use power line other than the one specified. Please use it properly. Otherwise, it may cause fire or electric shock.
- Be sure to ground the device (cross section of copper wire: >2.5 mm^2, resistance to ground: ≤ 4 Ω).

Special Announcement:

- This manual is for reference only.
- All the designs and software here are subject to change without prior written notice.
- Always follow the instructions listed on the manual. We are not liable for any problems caused by unauthorized modifications or attempted repair.
- All trademarks and registered trademarks are the properties of their respective owners.
- If there is any uncertainty or controversy, please refer to the final explanation of us.
- Please visit our website for more information.

Table of Contents

1 Overview

1.1 Product Introduction

The product is a type of managed switch, it provides 16/24*10/100M PoE Ethernet port and 2 uplink Combo 1000M ports, supports layer 2 network management and PoE management functions based on Web, which helps to realize high speed data forwarding. It can be widely applied in places like security surveillance, network management and so on.

1.2 Product Features

- Provide web-based layer 2 network management.
- Support 250 meters long distance transmission.
- Support 2*1000M Combo ports.
- Support 16/24*10/100M self-adaptive RJ45 ports.
- Support one Console port.
- Conform to IEEE802.3, IEEE802.3u, IEEE802.3ab/z and IEEE802.3X standards.
- Standard 802.1Q VLAN(Access/Trunk/Hybrid)
- All ports auto adapt to MDI/MDIX mode.
- MAC auto learning and aging, MAC address list capacity is 4K.
- IEEE802.3X full duplex flow control and Backpressure half duplex flow control.
- Support AC 100~240V power supply.
- Conform to IEEE802.3af and IEEE802.3at standards, both port 1 and port 2 support Hi-PoE 60W.
- Support PoE power consumption management.
- Support SNMP V1/V2/V3 network management.
- Support iLinksView network management platform.
- Support STP/RSTP ring network protocol.
- Support manual aggregation and static LACP.
- Support many-to-one mirroring.
- Support port MAC binding.
- Excellent isolated circuit protection.
- Lightning protection up to level 4.

2 Device Structure

2.1 Structure of 24-Port PoE Switch

2.1.1 Front Panel

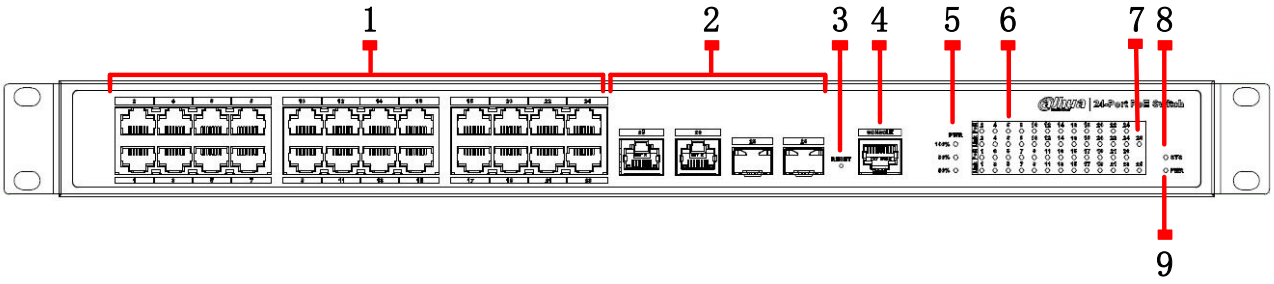


Figure 2-1

Refer to table 2-1 for the front panel description of 24-Port PoE Switch.

SN	Parameter	Note
1	RJ45 port	Ethernet port, support 10/100M self-adaptation
2	Combo port	Ethernet port, support 10/100/1000M self-adaptation, Fiber port supports 1000M.
3	Reset button	Long press the button to reset the device and recover default configuration.
4	Console serial port	Device debugging port
5	PoE power usage indicator	Current power consumption display
6	Downlink indicator light	Current port link status and PoE status.
7	Combo port indicator light	Combo port indicate link/act
8	System indicator light	System status. ● When device is booting up, the light is flashing quickly. ● When device is working properly, the light is flashing slowly.
9	Power indicator light	Device current power status.

Table 2-1

2.1.2 Rear Panel

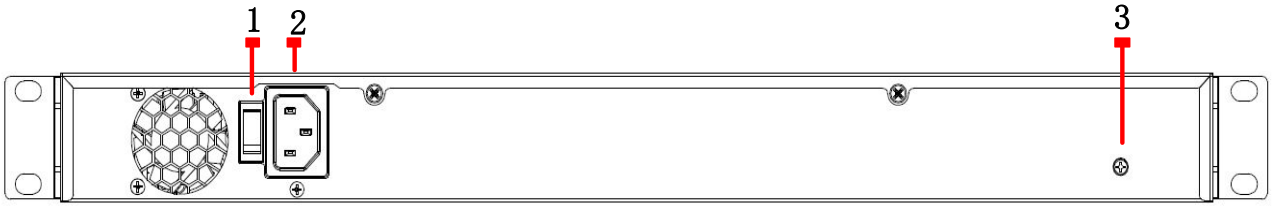


Figure 2-2

Refer to table 2-2 for the description of rear panel.

SN	Parameter	Note
1	Power switch	Control device power on and off
2	Power socket	Support AC 100～240 V
3	Ground terminal	Ground wire

Table 2-2

2.2 16-Port PoE Switch Front Panel

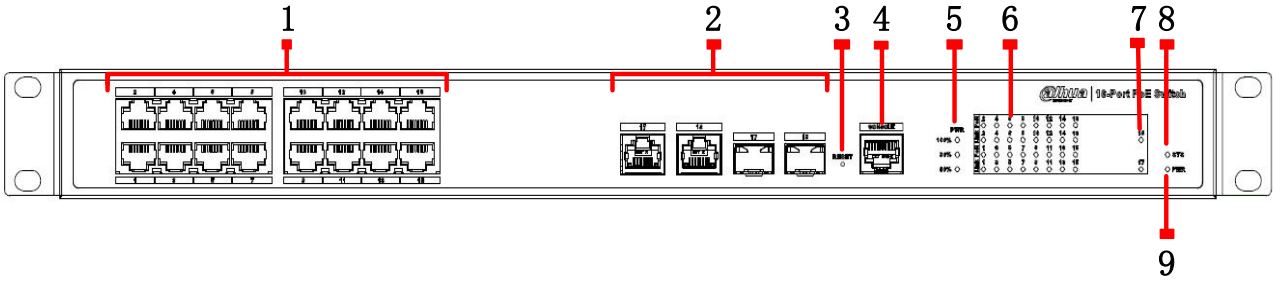


Figure 2-3

Refer to table 2-3 for more details.

SN	Parameter	Note
1	RJ45 port	Ethernet port, support 10/100M self-adaptation
2	Combo port	Ethernet port, support 10/100/1000M self-adaptation, Fiber port supports 1000M.
3	Reset button	Long press the button to reset the device.
4	Console serial port	Device debugging port
5	PoE power usage indicator	Current power consumption display
6	Downlink indicator light	Current port link status and PoE status.
7	Combo port indicator light	Combo port indicate link/act
8	System indicator light	System status. ● When device is booting up, the light is flashing quickly. ● When device is working properly, the light is flashing slowly.
9	Power indicator light	Device current power status.

Table 2-3

3 Log in Switch

3.1 Switch Login

It needs to log in switch first before configuring the switch, users can intuitively manage and maintain PFS42 series Ethernet switch via Web network management.

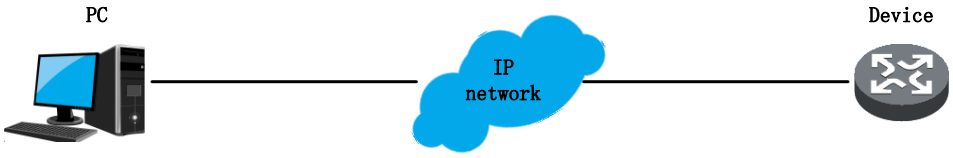


Figure 3-1

It can get access to switch via Web browser, please make sure your computer has connected to the network where the switch is located. It needs no extra config if it is the first time to use switch, now you can use Web to visit.

1. Modify the IP address and subnet mask of your computer network adapter into 192.168.1.50 and 255.255.255.0 respectively.
2. Open Web browser, input 192.168.1.110 in the address bar, and please note that 192.168.1.110 is the default management address of the switch.
3. Set the password of admin user, which shall not be less than 8 characters, and then click **Save**.

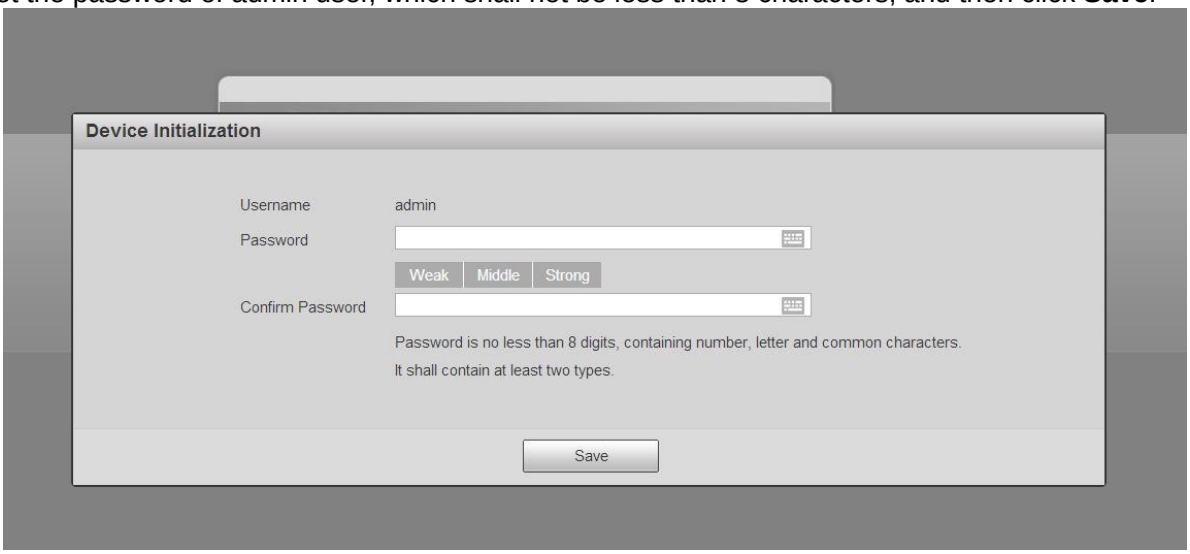


Figure 3-2

4. Enter user account and password, and then click **Login** to log in to the device.

Figure 3-3

5. The switch system information interface will be displayed if the username and password are correct.

- iLinksView is enabled by default, and the default username is admin, the default password is lt_91_il_02_nmp.
- When using the iLinksView to manage the device, note that the username and password must be the same as that you have set in the iLinksView, otherwise the iLinksView cannot discover the device.

3.2 WEB Interface Introduction

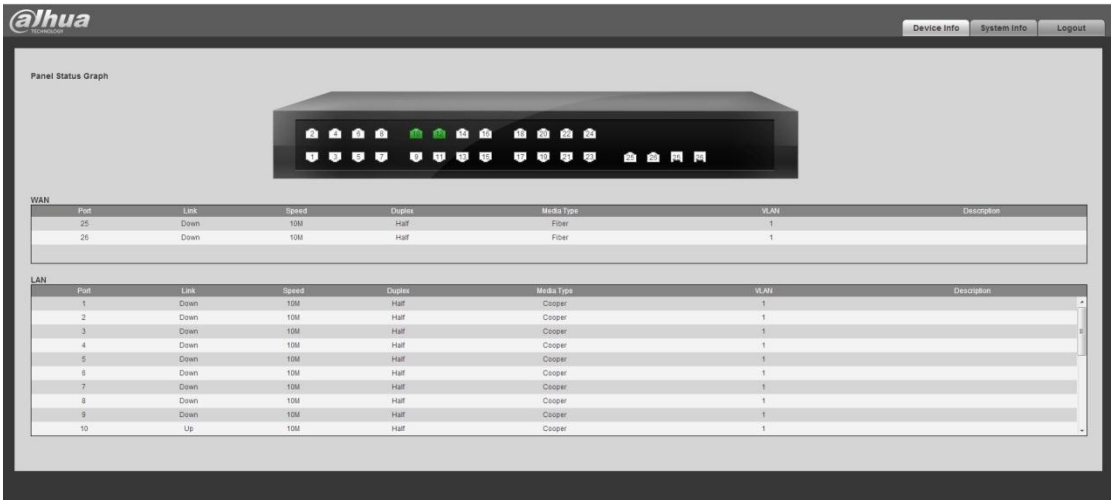
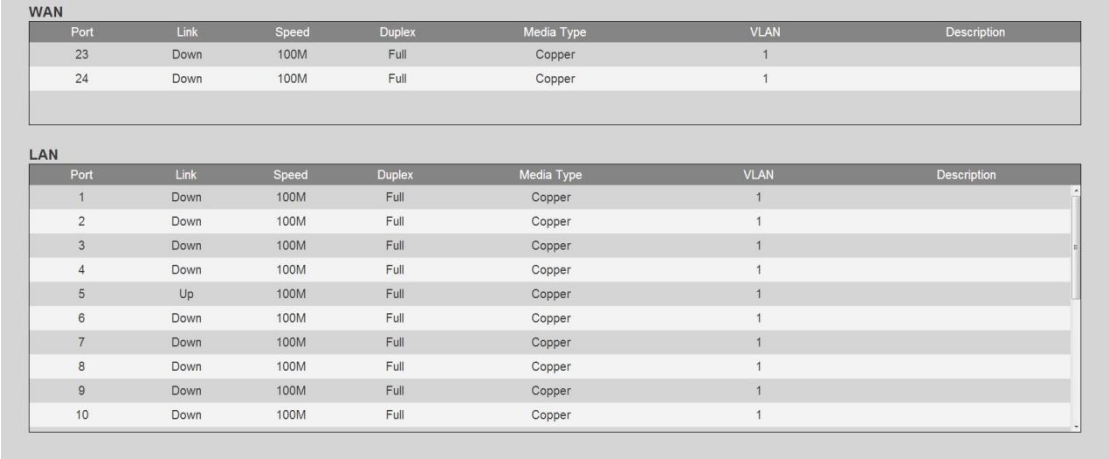


Figure 3-4

As it is shown in Figure 3-4, the whole WEB management interface is divided into several parts which includes device info display section, navigation bar, and config section etc.

3.2.1 Port Info Display Section

It is shown in Figure 3-5 that port info display is divided into WAN port state display and LAN port state display. It is able to display the current port Link state, port speed, duplex mode and so on.



WAN

Port	Link	Speed	Duplex	Media Type	VLAN	Description
23	Down	100M	Full	Copper	1	
24	Down	100M	Full	Copper	1	

LAN

Port	Link	Speed	Duplex	Media Type	VLAN	Description
1	Down	100M	Full	Copper	1	
2	Down	100M	Full	Copper	1	
3	Down	100M	Full	Copper	1	
4	Down	100M	Full	Copper	1	
5	Up	100M	Full	Copper	1	
6	Down	100M	Full	Copper	1	
7	Down	100M	Full	Copper	1	
8	Down	100M	Full	Copper	1	
9	Down	100M	Full	Copper	1	
10	Down	100M	Full	Copper	1	

Figure 3-5

3.2.2 Navigation Bar

The navigation bar control what is displayed in the config section. The contents in navigation bar is Displayed in the form of list, and it is divided by category. Please click the group name first if it needs to configure some item, click the sub items after the list is unfolded. For example, please click Port Management first if it needs to check the flow of the current port, and then click Port Statistics, refer to Figure 3-6 for more details.

Figure 3-6

3.2.3 Config Display Section

The config section will display the contents which are selected from the navigation bar, and it can be

checked and config can be modified in the config section.

Four config modules will be introduced via the following four chapters, which are system config, port management, device management and PoE.

4 System Config

4.1 System Config Overview

Click system info and you can see what is shown in Figure 4-1.

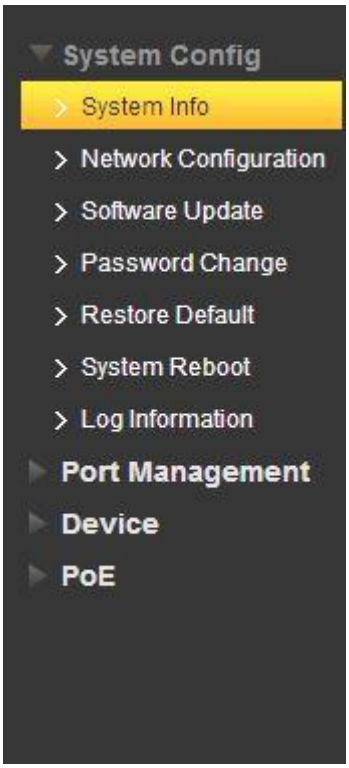


Figure 4-1

4.1.1 System Info

Refer to Figure 4-2 for the switch system info display interface, where you can search the device model, MAC address and software version.

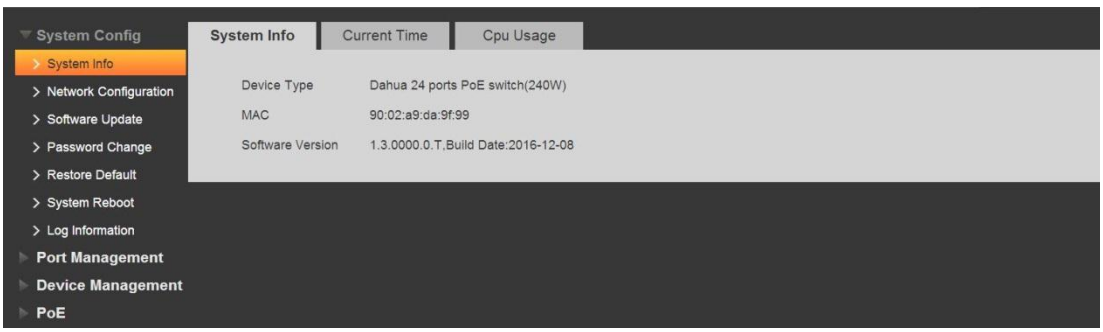


Figure 4-2

4.1.2 Current Time

Refer to Figure 4-3 for the display interface of switch system time, where you can set the device current time and time zone.

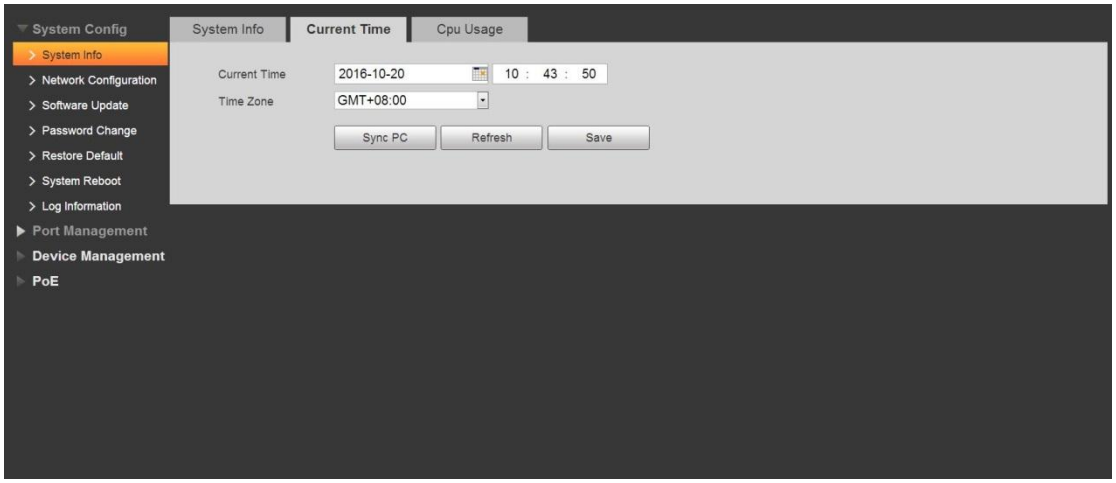


Figure 4-3

4.1.3 CPU Usage

Refer to Figure 4-4 for the display interface of switch CPU usage where you can search the CPU usage while the device is running.

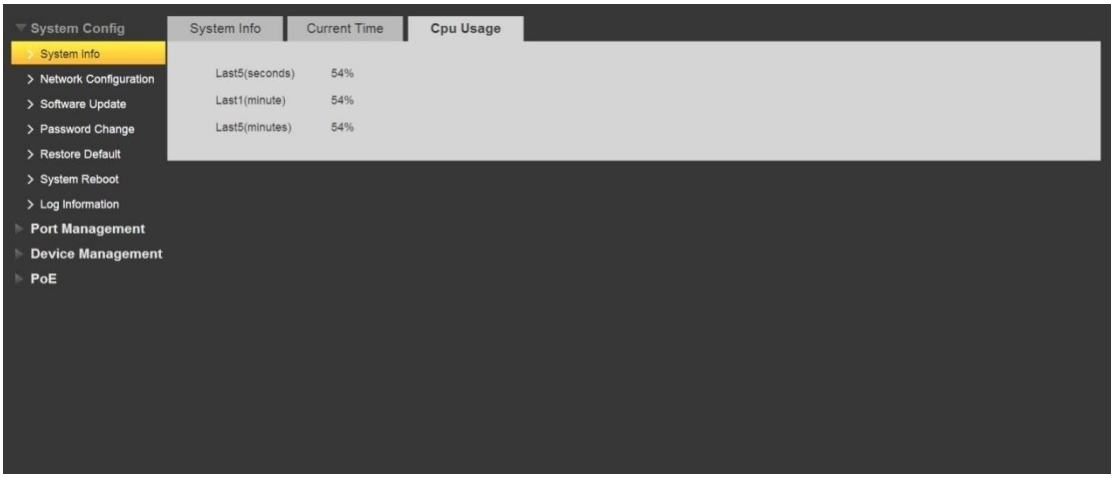


Figure 4-4

4.2 Network Config

Each host needs an IP address for network communication.

IP (Internet Protocol) address is a 32-bit address used on the Internet, it is a kind of uniform address format provided by IP protocol, which is generally displayed by 4 decimal numbers. IP address is a logic address distributed for each network and host on the Internet, which is used to identify each host and realize network intercommunication.

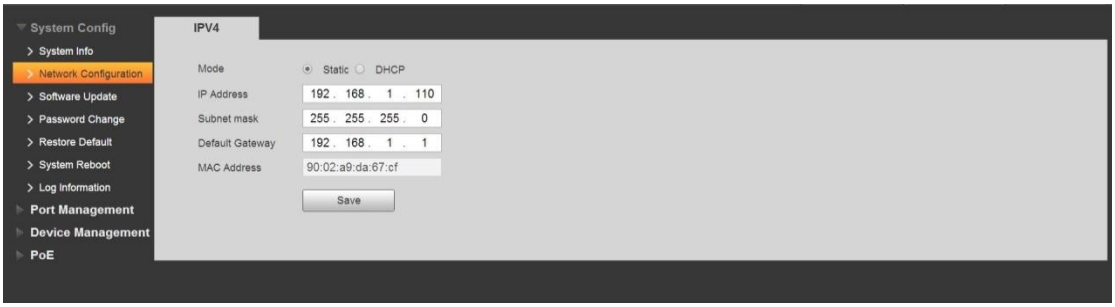


Figure 4-5

Refer to Figure 4-5 for the IP config interface, where you can check the device IP address, subnet mask, default gateway and MAC address. The default IP of switch is 192.168.1.110, which can be modified in this interface.

Refer to table 4-1 for the address config.

Parameter	Note
IP address	Switch management IP address, which can modify the management IP of the switch
Subnet mask	Switch subnet mask address, which can modify config.
Default gateway	Switch default route
MAC address	Physical address of the switch, which can't be modified.

Table 4-1

Note

Do not modify the subnet mask of switch randomly. It may fail to log in the switch if it is modified improperly.

4.3 DHCP

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

DHCP adopts client/server communication mode, the client makes config application to server, and the server returns to the IP address and other corresponding config information allocated by client, which is to realize dynamic config of IP address and so on.

In the typical application of DHCP, generally it includes one DHCP server and several clients (such as PC and laptop), which is shown in Figure 4-6.

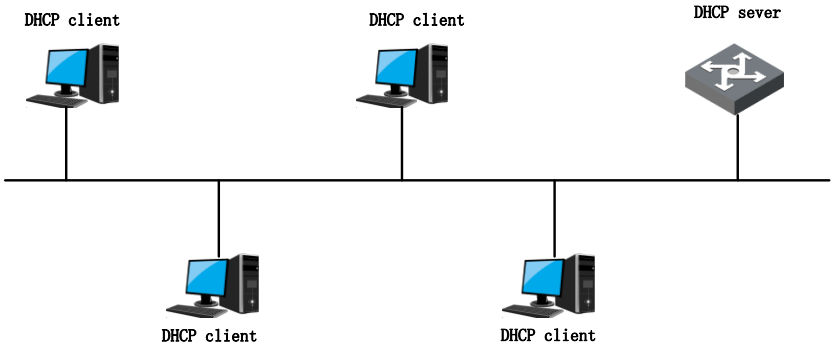


Figure 4-6

Config examples.

1. Networking requirement

   Configure switch as DHCP client, automatically acquire the switch management IP address.

2. Config steps

a. Check “DHCP”, which is shown in Figure 4-7.

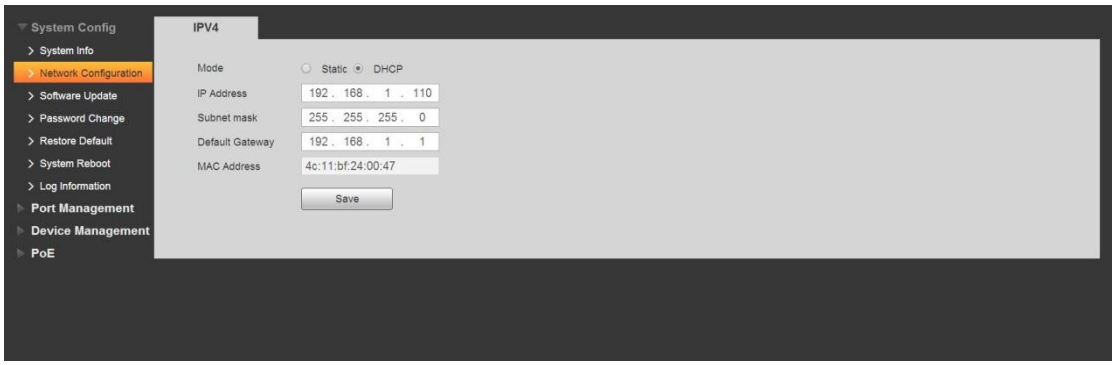


Figure 4-7

b. Click “Save”.

4.4 Software Upgrade

In the interface below, it provides the function of system file upgrade via WEB for the switch. You can download the latest version of system file on the Dahua website.

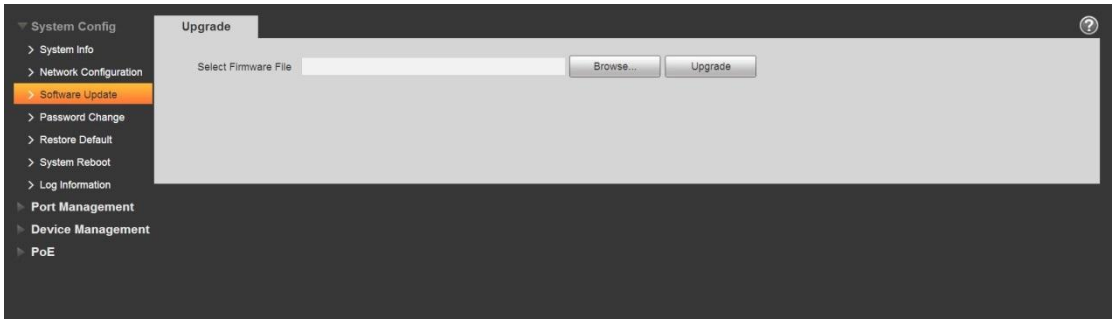


Figure 4-8

4.5 Password Change

You can modify the user login password in the following interface; the username is admin which can’t be

modified, and the factory default password is admin.

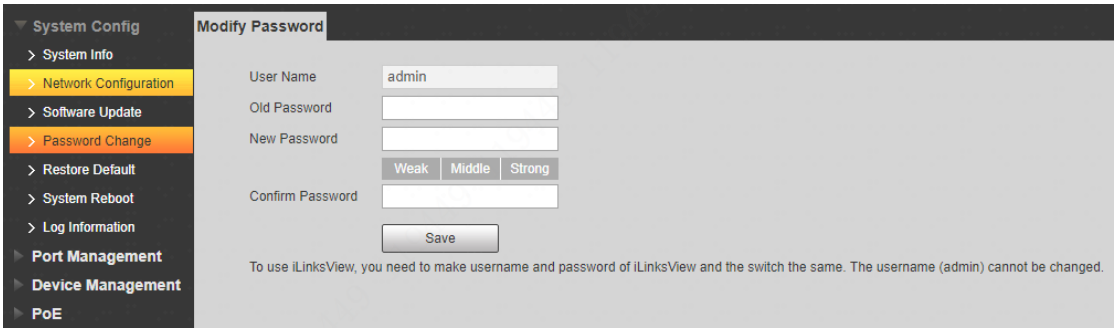


Figure 4-9

4.6 Restore Default

You can select default function when it needs to restore the switch config back to initial system default. Except management IP and login password, all other information will be restored to factory default setting.

Note

When the switch is reset by pressing the reset button on it, all configurations will be restored to factory default settings, the management address will be restored to 192.168.1.110, and the user needs to change the password for the first login.

Figure 4-10

4.7 System Reboot

It needs to save the config before rebooting the device. Otherwise, all the configurations will be lost after reboot. You need to log in the device WEB interface again after device reboot.

Figure 4-11

4.8 Log Information

Refer to Figure 4-12 for the system log display interface where you can check some system log information during the device operation, which is to make it convenient for maintenance personnel to analyze problems.

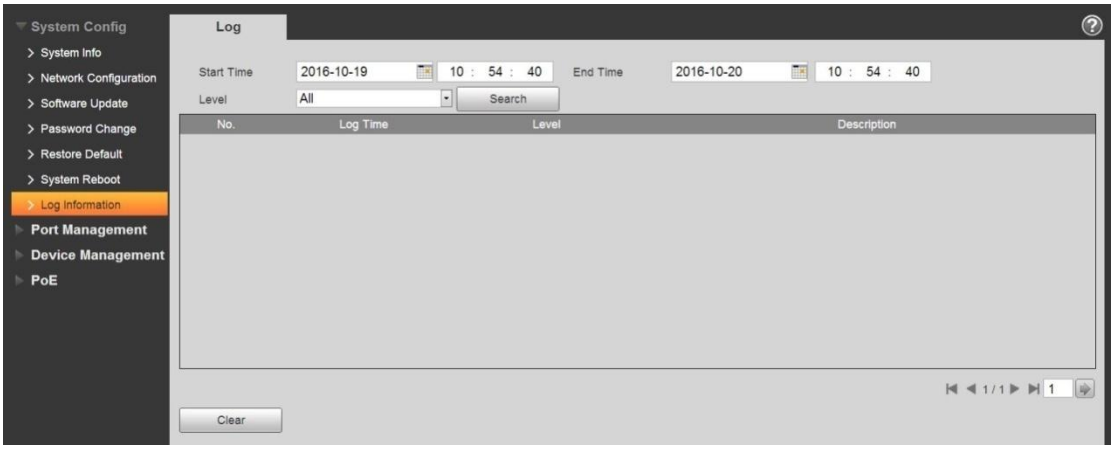


Figure 4-12

Config example.

1. Configure “Start Time” and “End Time”, set the period which needs to be searched.
2. Select event level, including Error, Warning and Info.
3. Click “Search”.

5 Port Management

5.1 Port Config

Port config can be used to configure each basic parameter which is related to switch port. The port basic parameter will directly affect the working mode of the port, please make config according to the practical requirements.

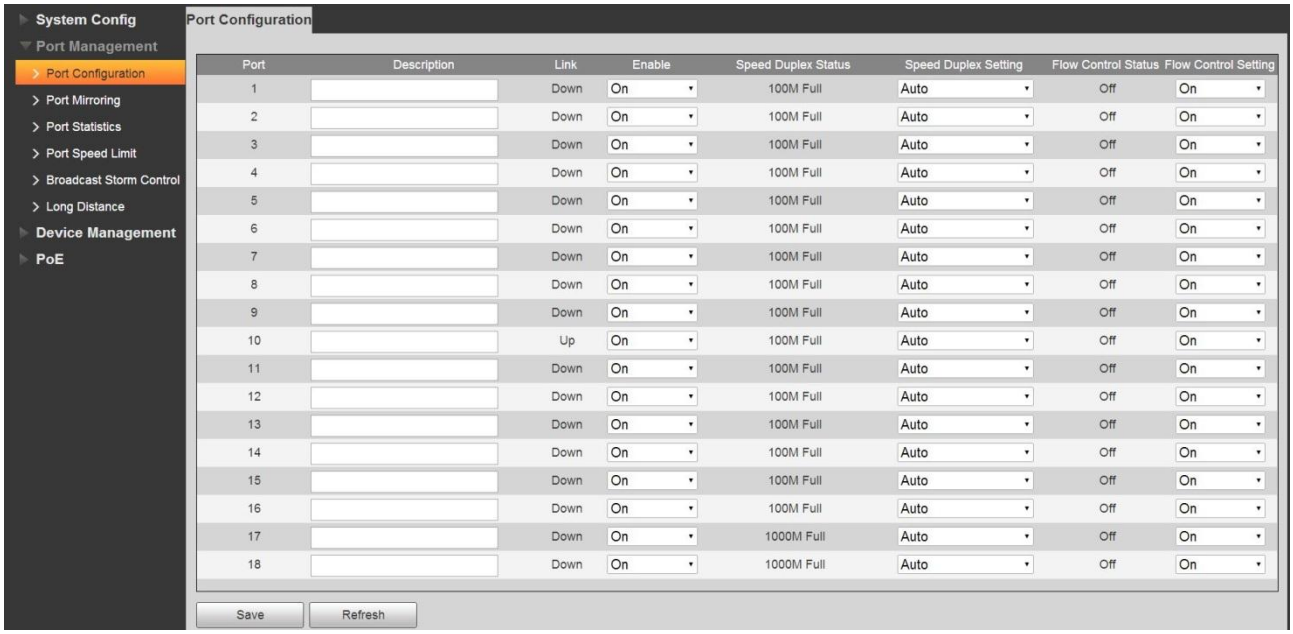


Figure 5-1

Refer to Figure 5-1 for the port config interface of the switch, in this interface you can check description, link state, speed duplex status, flow control status of each port, you can also add port description info, configure enable and disable state, speed, duplex mode and flow control function of each port.

- Port: It displays the switch port number;
- Port description: it adds description information for port;
- Enable: It is to configure port on/off.

Refer to table 5-1 for port status config.

Status	Note
On	Config link is in the status of enable.
Off	Config link is in the status of disable.

Table 5-1

- Link: It displays the port link status.

Refer to table 5-2 for port status display.

Status	Note
Up	It means the link is in the status of enable.
Down	It means the link is in the status of disable.

Table 5-2

- Speed—current: It displays the current speed status of the port.

Refer to table 5-3 for the port speed duplex display.

Port	Current speed	Speed duplex mode
Ethernet port	Auto(default)	Auto negotiation mode
	10M FULL	10M Full duplex
	10M HALF	10M Half duplex
	100M FULL	100M Full duplex
	100M HALF	100M Half duplex
	1000M FULL	1000M Full duplex
Fiber port	1000M-X	1000M Full duplex

Table 5-3

- Speed –config: It is to configure the port speed duplex mode.

Note
It will directly affect the port communication if you change port speed duplex mode; so please modify it carefully.

Refer to table 5-4 for port speed duplex config.

Port	Speed mode	Definition
Ethernet port	Auto（default）	Port speed duplex mode self-adaptation
	10M FULL	Port speed duplex mode 10M full duplex
	10M HALF	Port speed duplex mode 10M half duplex
	100M HALF	Port speed duplex mode 100M half duplex
	100M FULL	Port speed duplex mode 100M full duplex
	1000M FULL	Port speed duplex mode 1000M full duplex
Fiber port	1000-X	Fiber port is set as 1000M full duplex mode

Table 5-4

- Flow Control: It is to set switch flow control function.(The default setup is on).

On port flow control interface, **on** is to enable port flow control function and pause frames can be sent or received normally, **off** is to disable port flow control function.

Note
For Ethernet port, please enable port flow control function to synchronize the inbound speed and outbound speed in case there are packet losses resulting from the different speeds.

5.2 Port Mirroring

Port mirroring (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. See Figure 5-2.

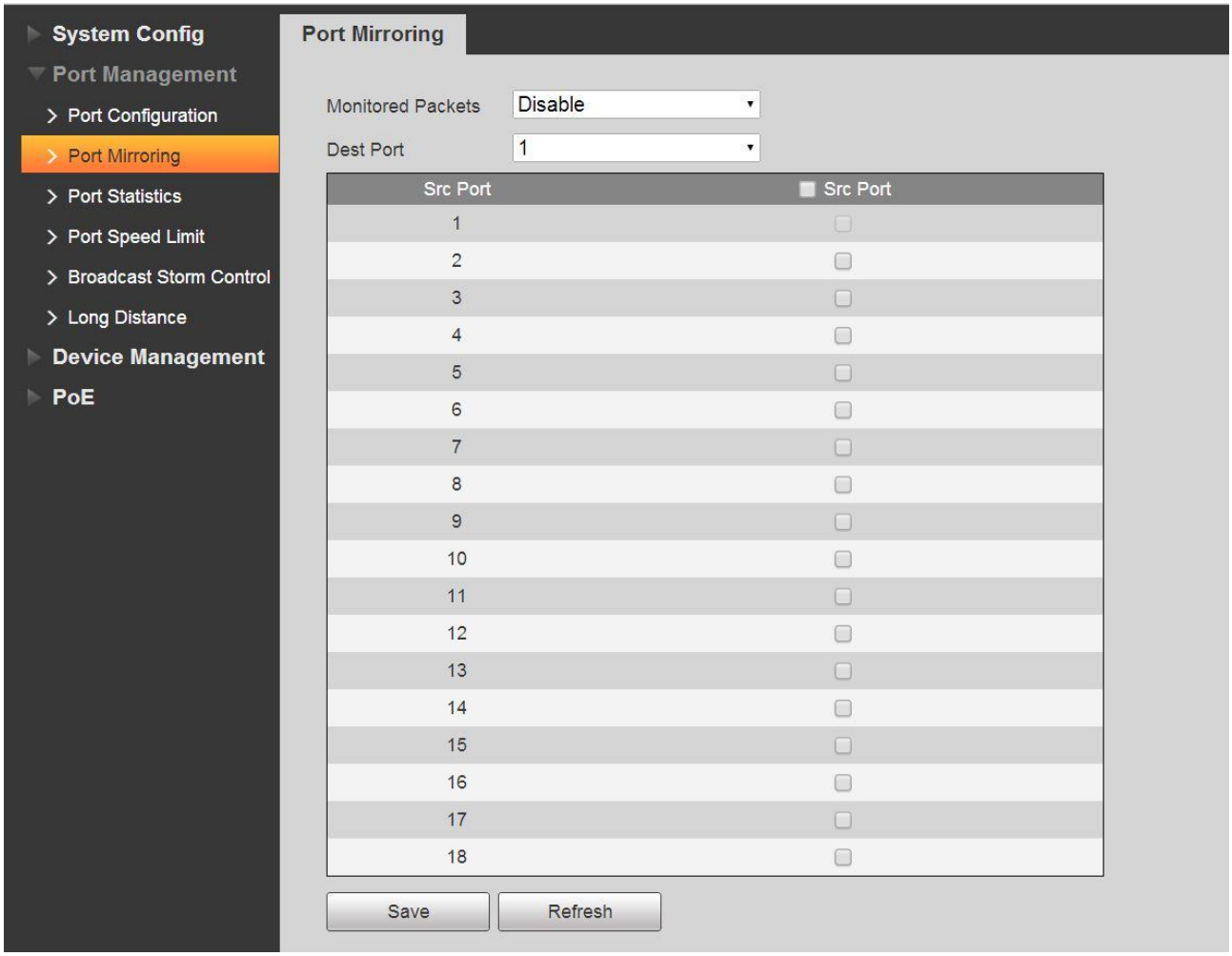


Figure 5-2

- Destination port: The monitor port. Please select only one item. The default setup is disabled.
- Source port: The port being monitored. Please select one or more item(s).
- Enable mirror: There are four modes: Disable, Tx only, Rx only, enable.

Refer to table 5-5 for port mirroring setup. .

Name	Note	
Mirrored Packets	Disable（default）	Disable the monitor function
	Tx only	Monitor output packets
	Rx only	Monitor input packets
	Enable	Monitor input/output packets
Destination port	Monitor port. Please select only one item. The default setup is disabled.	
Source port	The port being monitored. Please select one or more item(s).	

Table 5-5

Config example.

1. Network connection

Enable port mirroring function so that the port 1 can monitor the packets of port 2 and port 3.

2. Settings

（1） Enable port mirroring function and select the data streams to monitor.
（2） Select source port.
（3） Select destination port. Now the interface is shown as in Figure 5-3.

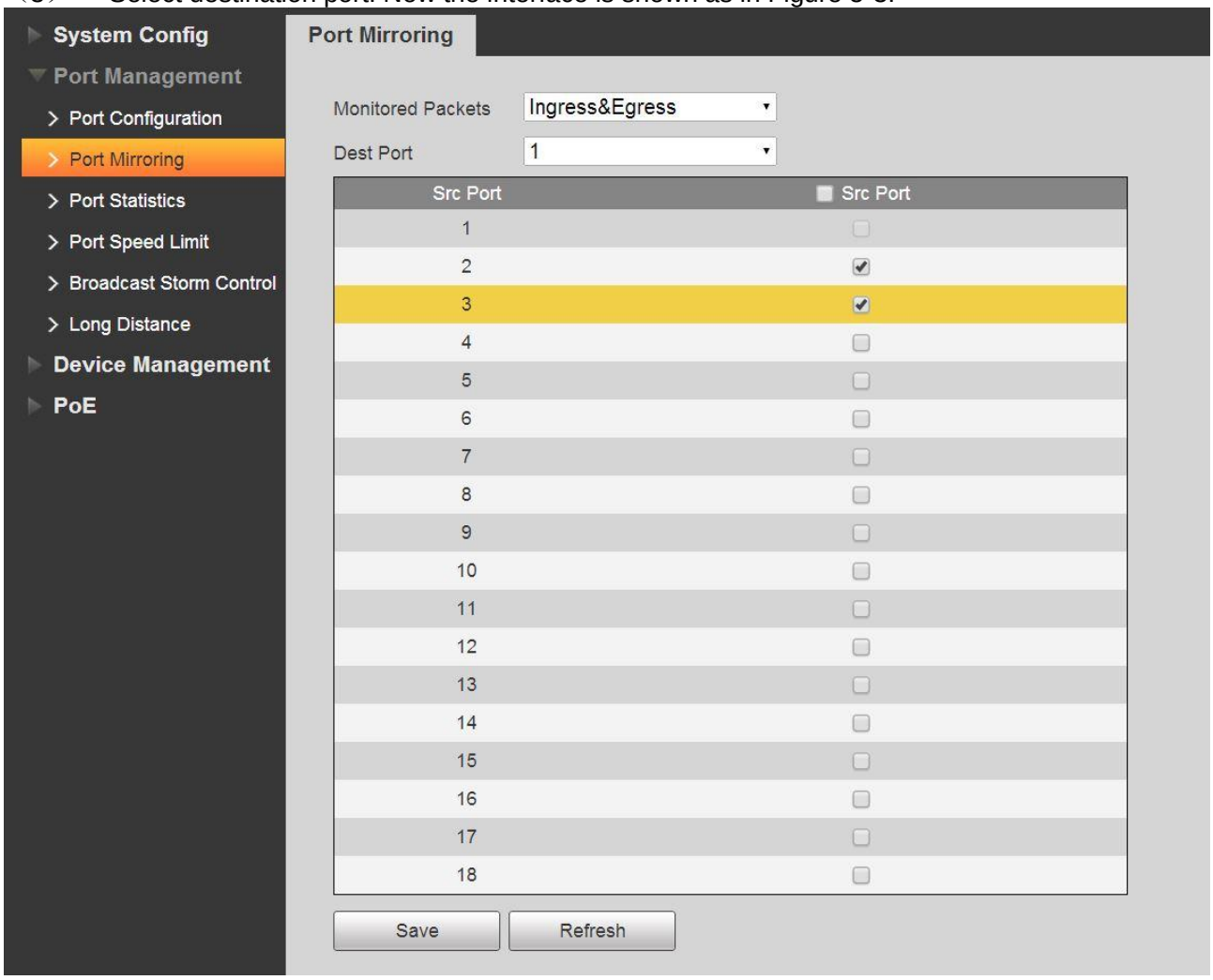


Figure 5-3

5.3 Port Statistics

Figure 5-4 is the switch port statistics interface. Here is to display the inbound/outbound packet amount of each port, conflict statistics, packet loss amount, CRC error packet and etc. 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.

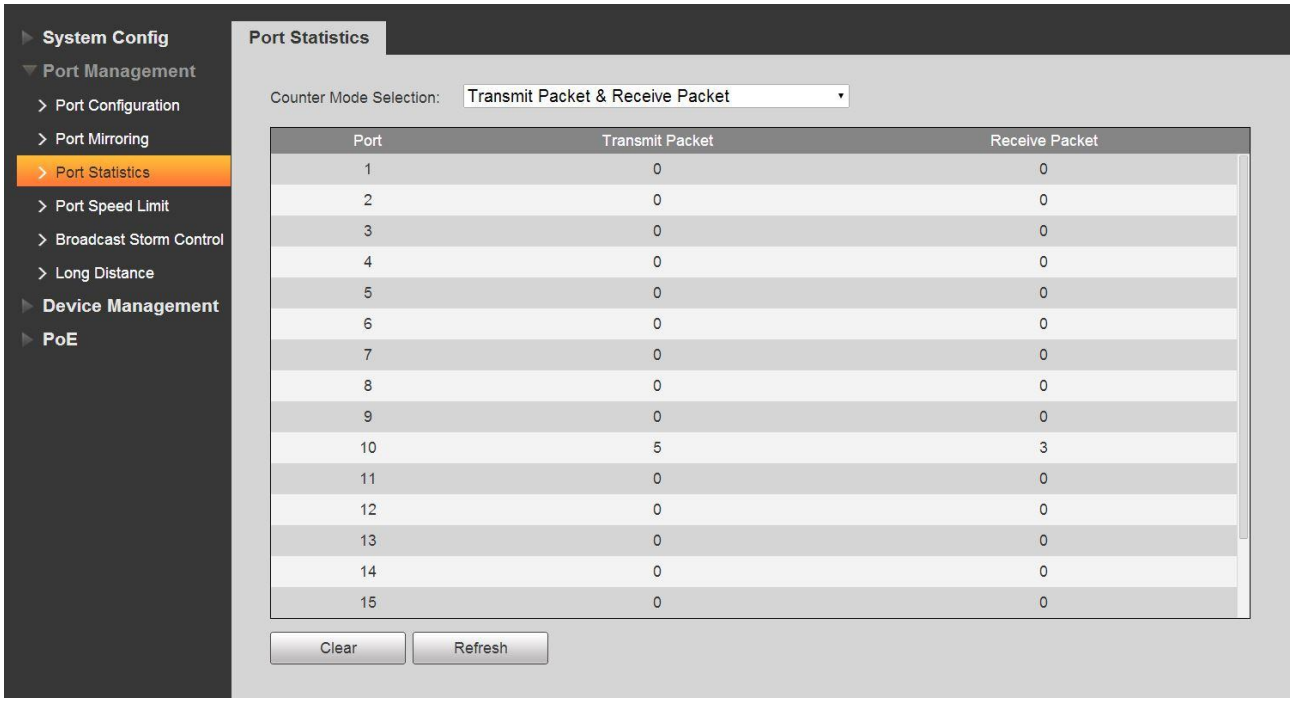


Figure 5-4

5.4 Port Speed Limit

Here is to set port speed limit parameters, restrict exchanging rate of inbound/outbound data packets. See Figure 5-5.

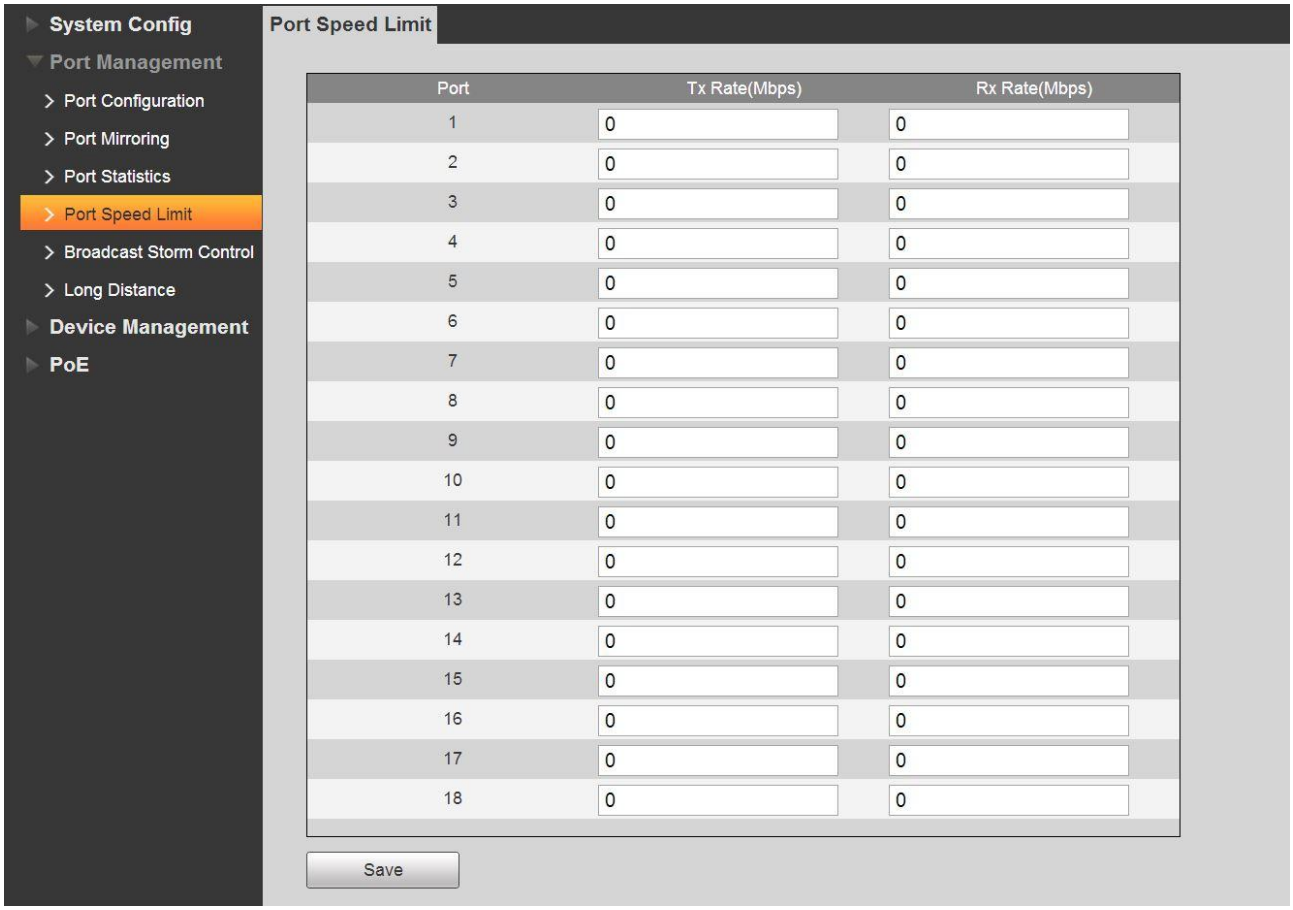


Figure 5-5

Refer to Figure 5-5 to set the speed limit policy of each port. Refer to Table 5-6 for port speed limit parameters.

Name	Note
Port	Display port list.
Tx speed	It is to set port outbound rate. The value ranges from 0 to 63Mbps. The default setup is 0, there is no speed limit.
Rx speed	It is to set port inbound rate. The value ranges from 0 to 63Mbps. The default setup is 0, there is no speed limit.

Table 5-6

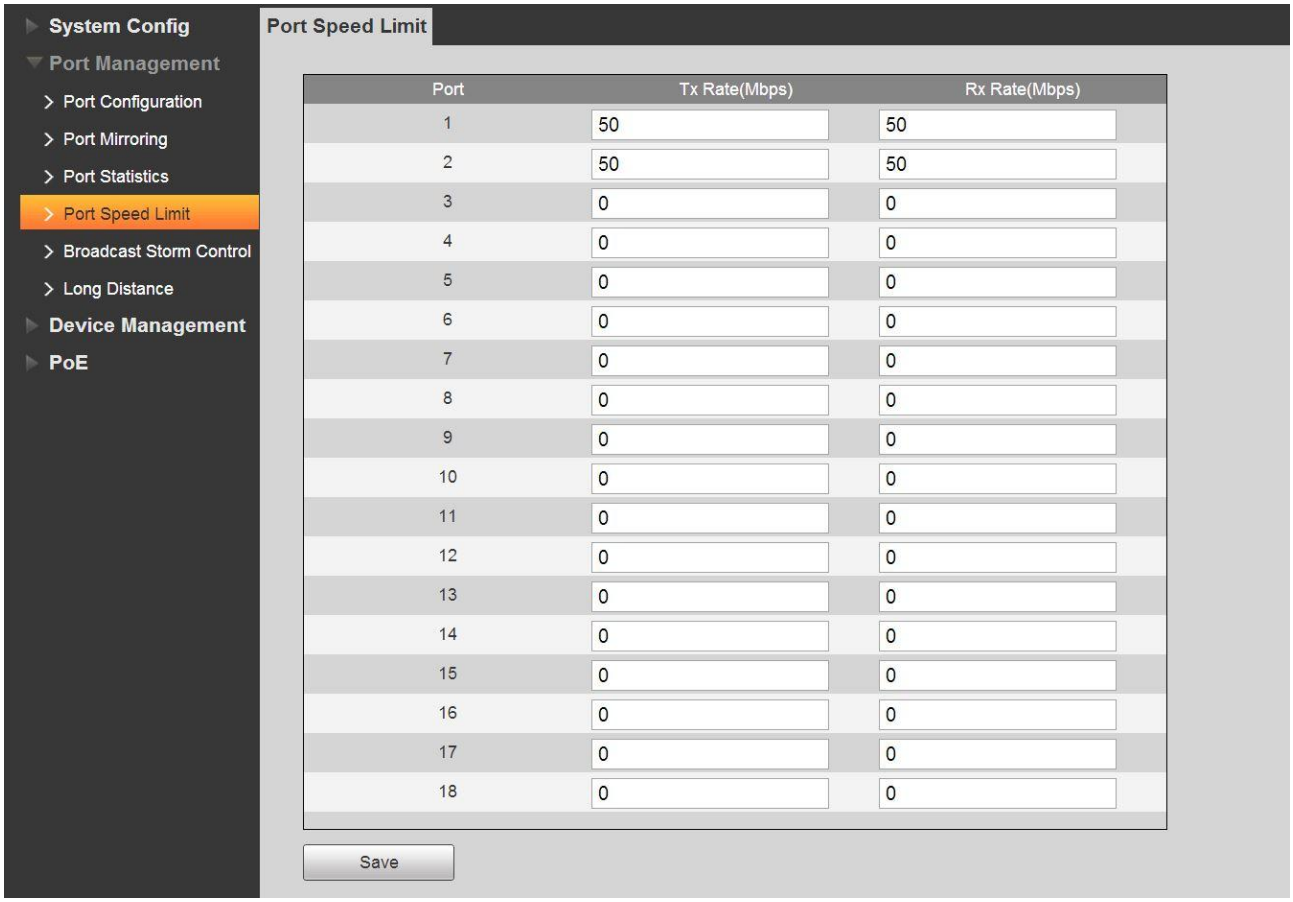
Config example.

1. Network connection

Set speed limit of port 1 and port 2. Each port speed is less than 50Mbps.

2. Settings

（1） Set the Tx/Rx speed of the port. See Figure 5-6.



.

Figure 5-6

（2） Click Save button.

5.5 Broadcast Storm Control

The broadcast storm refers to a phenomenon: the broadcast frames on the network are forwarded again and again, which affects the proper communications. It greatly reduces the network performance. The storm control can limit the broadcast flows of the port and it can discard the broadcast frames once the flow has exceeded the specified threshold. It is to reduce the risk of the broadcast storm and guarantee the network proper operation. See Figure 5-7.

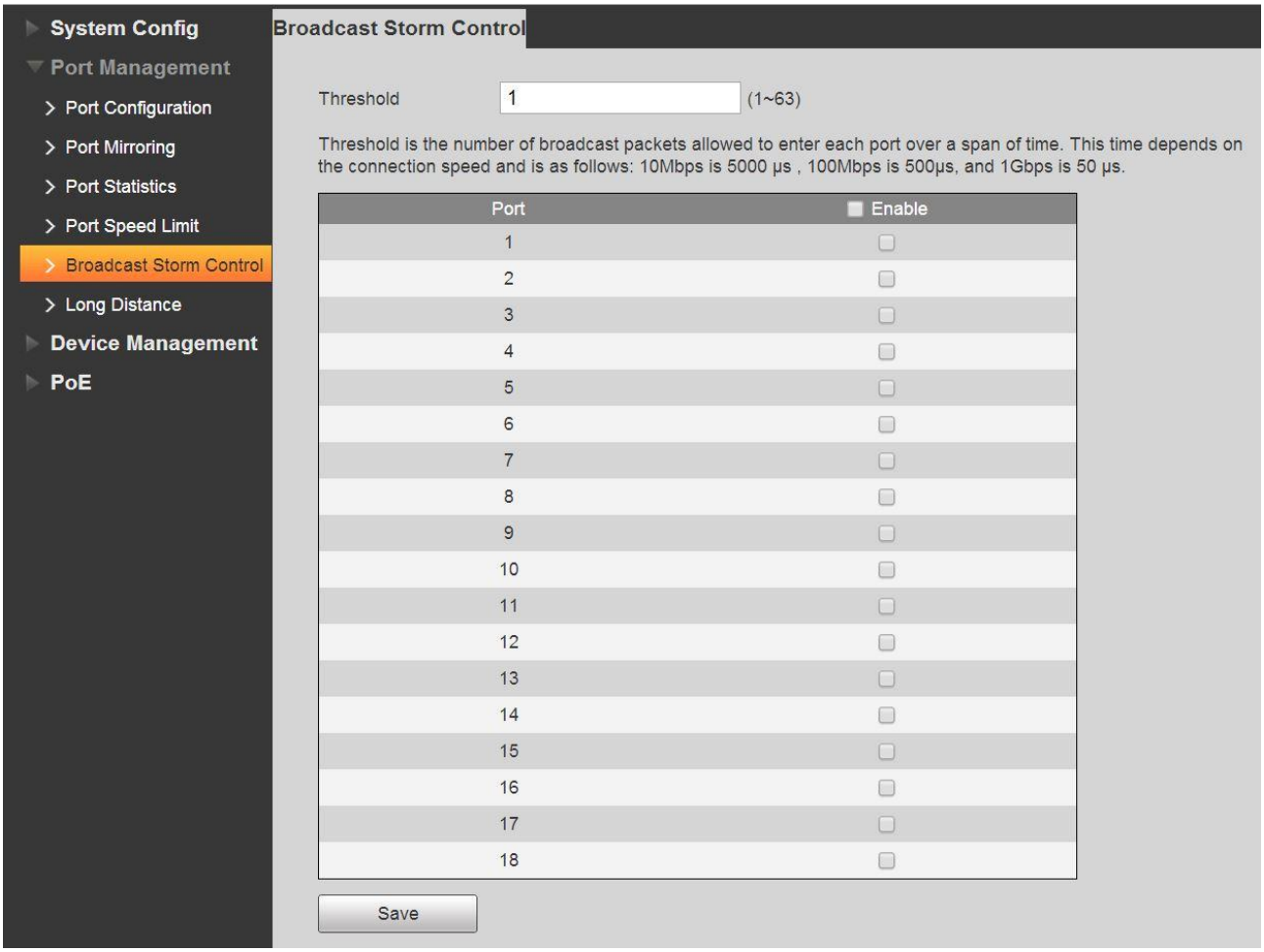


Figure 5-7

Refer to Table 5-7 for broadcast control parameters.

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

Table 5-7

Config example.

1. Network connection

Set all-port broadcast storm control function. In case there is malfunction port and device cannot properly transmit the data when there are so much broadcast packets.

2. Settings

（1） Set threshold value. It is the broadcast packets amount of one port.

（2） Select a port to configure.

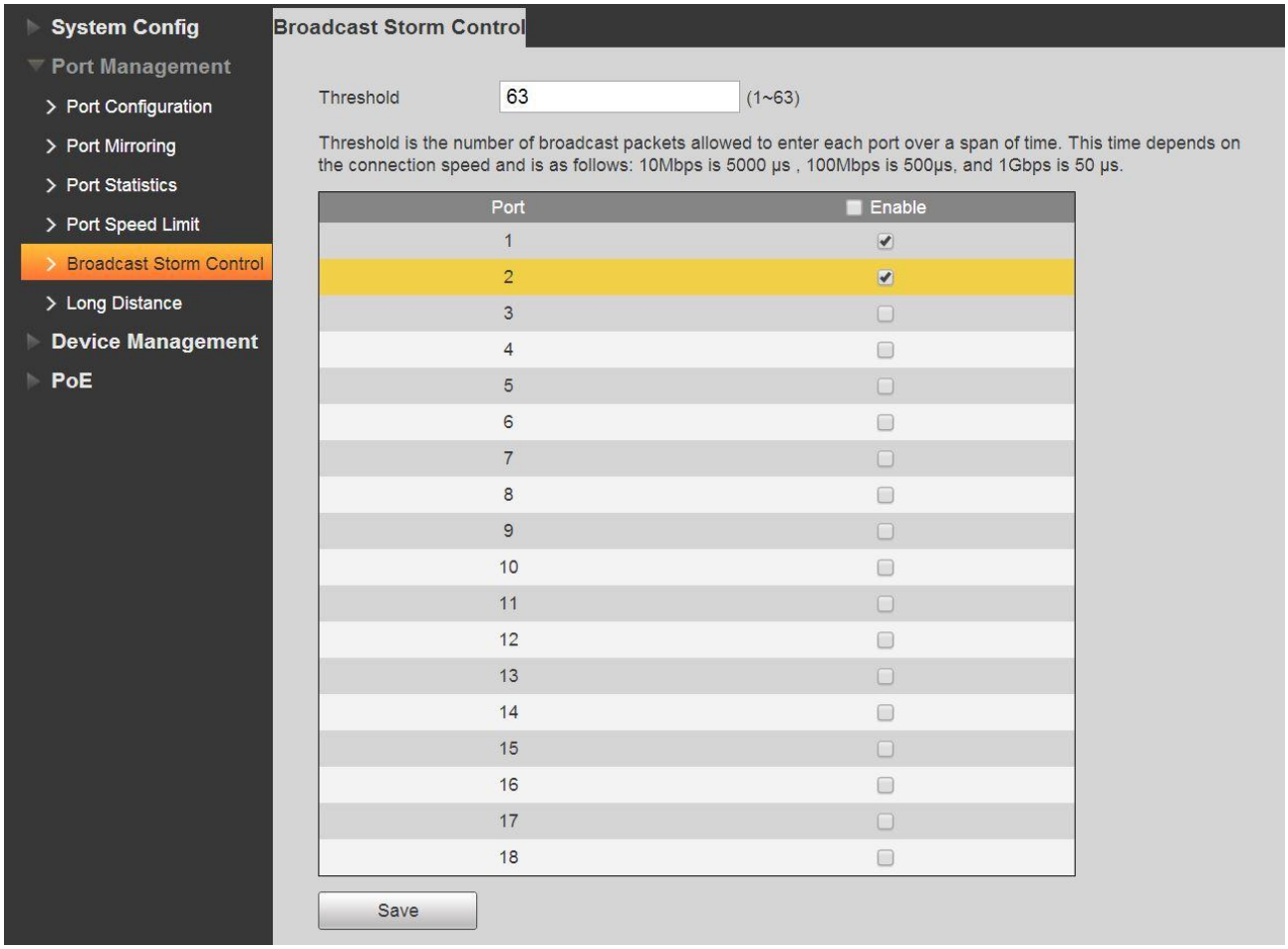


Figure 5-8

（3） Click Save button.

5.6 Long Distance Transmit

In this interface, it is to set port long distance transmission mode. For the standard Ethernet mode, the transmission speed can becomes 10Mbps/250meters instead of 100Mbps/100Meters. See Figure 5-9.

Figure 5-9

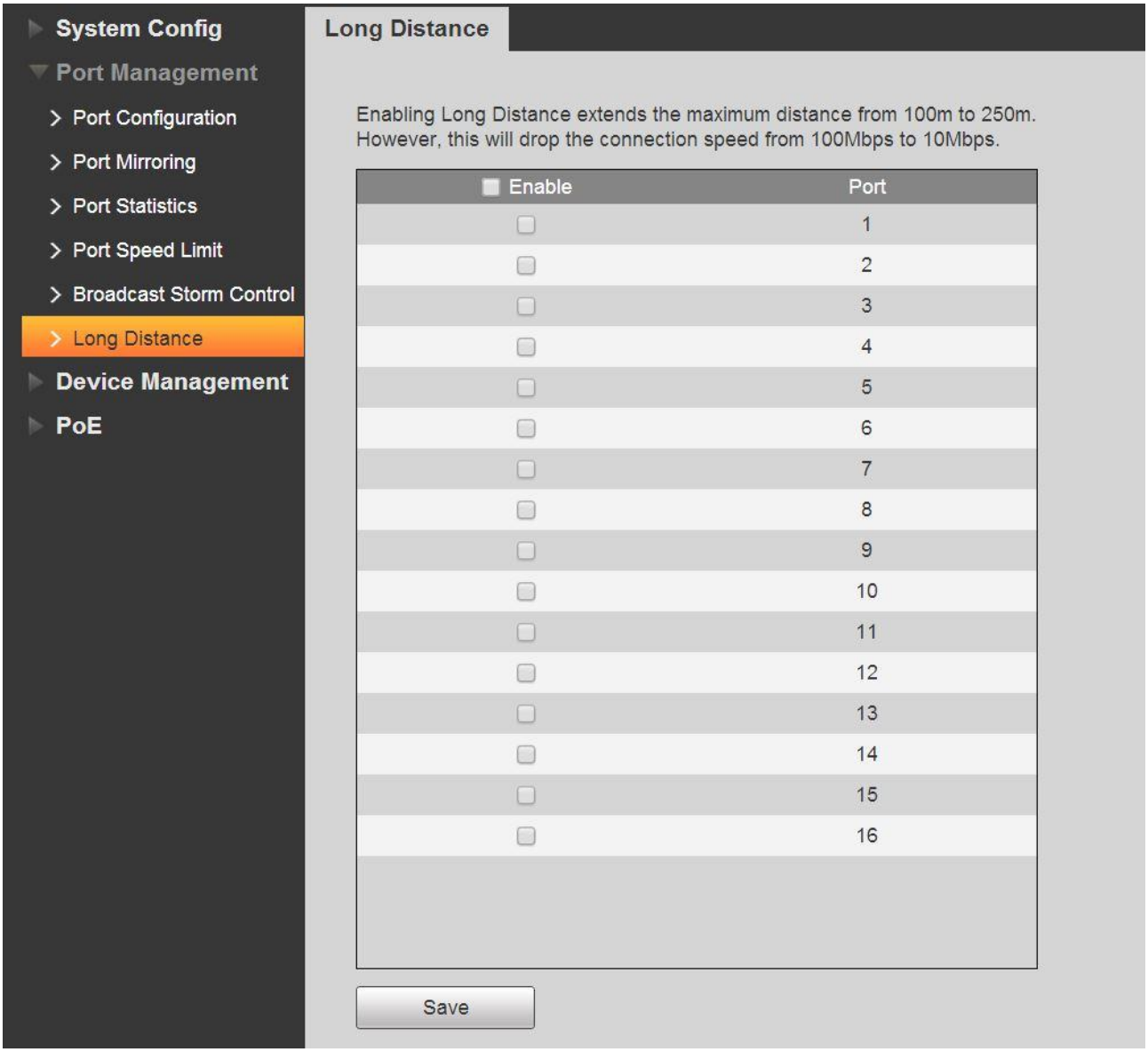


Figure 5-9

Config example.

1. Network connection

Set all-port long distance transmission function so that it can support 250 meters data proper transmission.

2. Settings

（1） Check a port to enable long distance transmission function.

（2） Click Save button. See Figure 5-10.

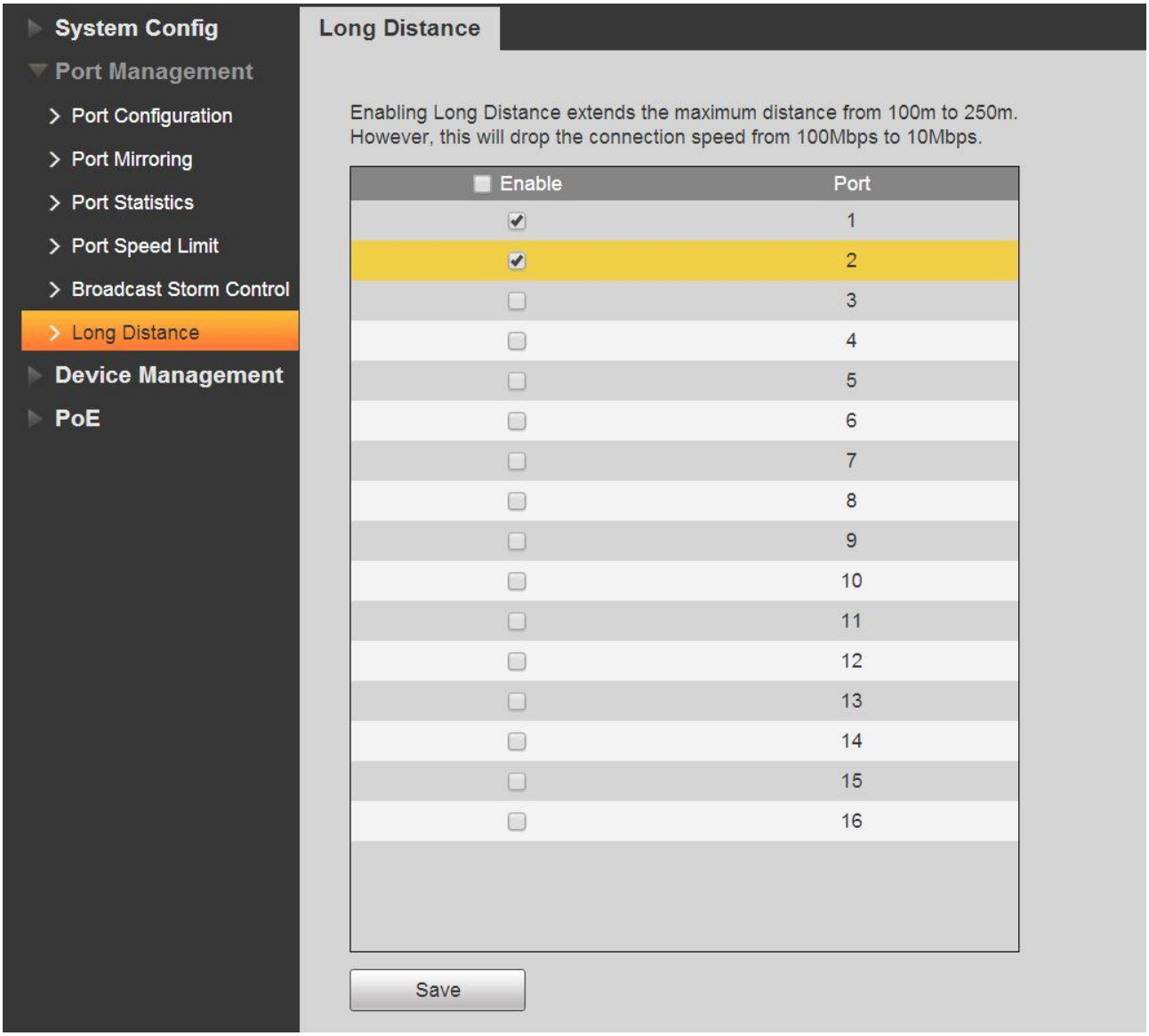


Figure 5-10

6 Device Management

6.1 Ring Network

6.1.1 STP Definition

The basic idea of STP protocol is very simple. We all know that the trees growing in the nature won't generate loop circuit, so it won't generate loop circuit if network grows like trees in the nature. Therefore, it defines Root Bridge, Root Port, Designated Port, Path Cost and other concepts in the STP protocol, which is to realize the purpose of clipping redundant loop circuit via structuring a tree, and meanwhile it can realize link backup and path optimization. The algorithm of structuring the tree is called Spanning Tree Algorithm.

The protocol packet adopted by STP is BPDU (Bridge Protocol Data Unit), which is called config info as well. BPDU contains enough information to ensure the calculation process of completing spanning tree. STP can confirm network topological structure via transmitting BPDU among devices.

BPDU format and field description can realize the functions of spanning tree, it is to realize information

interaction via transmitting BPDU packet among switches. All the switches which support STP protocol will receive and deal with the received packet. The packet carries all the useful information in the data area which can be used for spanning tree calculation. The BPDU frame format and field description of standard spanning tree is shown in Figure 6-1.

2	1	1	1	8	4
Protocol Identifier	Version	Message Type	Flag	Root ID	Root Path Cost
Bridge ID	Port ID	Message Age	Max Age	Hello Time	Forward Delay
8	2	2	2	2	2

Figure 6-1

- 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 bytes priority and 6 bytes MAC address.
- Root path cost: The cost of root path.
- Bridge ID: it means the ID of bridge which sends BPDU, which is made up of 2 bytes priority and 6 bytes MAC address.
- Port ID: It is to identify the port which sends BPDU.
- Message age: Life time of BPDU.
- Max age: Aging time of current BPDU, which is the longest time for port to save BPDU.
- Hello time: The period cycle of Bridge Root sending BPDU.
- Forward delay: It means the time of maintaining snoop and study status before sending data package after topology is changed.

6.1.2 Basic Concepts of STP

Bridge Identifier: it is the comprehensive numerical value of bridge priority and its MAC address, and the bridge priority is a parameter which can be set. The lower the Bridge ID, the higher the bridge priority becomes, which makes it increase the possibility of becoming Root Bridge.

Root Bridge: It is the switch with minimum bridge ID. Please select the best switch among the loop circuit and set it as the Root Bridge switch, which is to provide best network performance and reliability.

Designated Bridge: in each network segment, the bridge with lowest path cost to Root Bridge will become designated bridge, via which the data package will be forwarded to the network segment. The switch with the lowest Bridge ID will be selected as Designated Bridge when all the switches have the same Root Path Cost.

Root Path Cost: it is the total of all path costs on the path between two network bridges. The Root Path Cost of Root Bridge is zero.

Bridge Priority: it is a parameter which can be set by users, the range of numerical is from 0 to 61440. The smaller the value is set, the higher the priority becomes. The higher the bridge priority is, the more likely it becomes Root Bridge.

Root Port: the nearest port to root bridge on the non-root bridge switch, responsible for communication with Root Bridge, the path cost from this port to root bridge is the lowest. The port with highest port priority will become root port when several ports have the same path cost to Root Bridge.

Designated Port: it is the port on the designated bridge which implements data forward to the switch.

Port priority: range of numerical value is from 0 to 240, and it has to be the integral multiple of 16. The lower the port priority, the higher the priority means, and it is more likely to become root port.

Path Cost: STP protocol is used to select reference value of link. STP protocol can clip the network to a tree-shaped network structure without loop circuit via calculating path cost and blocking redundant links.

The networking diagram of spanning tree basic concept is shown in Figure 6-2. Switch A, B and C are connected sequentially, switch A is selected as Root Bridge after calculation by STP, the circuit between port 2 and port 6 is blocked.

Bridge: Switch A is the root bridge of the whole network; Switch B is the designated bridge of Switch C.
Port: port 3 and port 5 are the root ports of Switch B and Switch C respectively; port 1 and port 4 are the designated ports of Switch A and Switch B respectively; port 6 is the blocked port of Switch C.

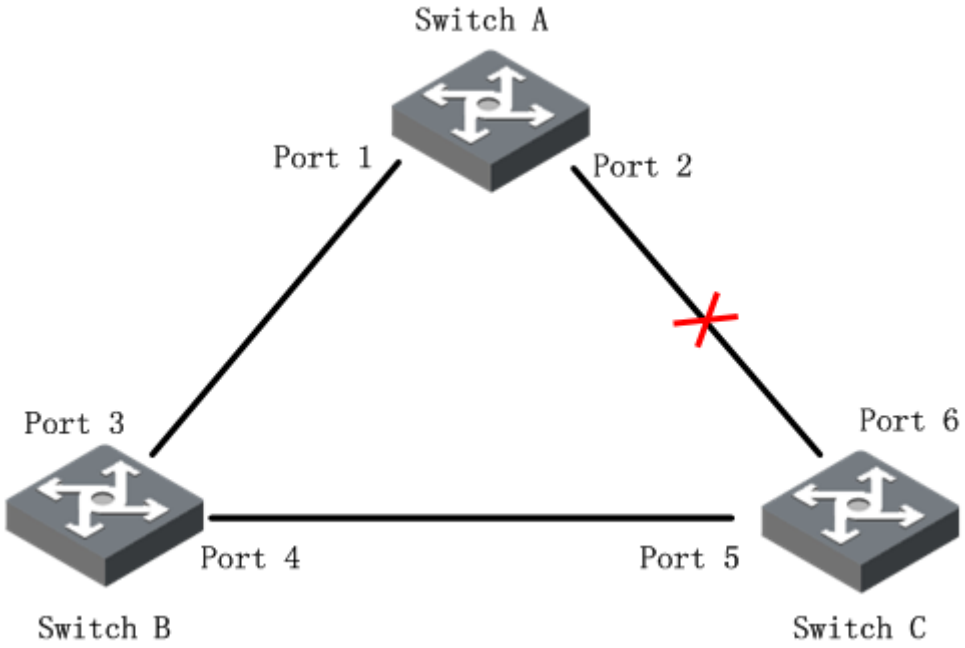


Figure 6-2

STP Timer
Hello Time
It ranges from 1s to 10s. It is the interval that the Root Bridge sends BPDU data package to all the switches, which is used to check if there is malfunction for the switch detection link.

Max.Age
It ranges from 6s to 40s. The switch will send BPDU data package to all the switches and calculate spanning tree again if it exceeds aging time and fails to receive BPDU data package sent by Root Bridge.

Forward Delay:
It ranges from 4s to 30s. It is the time which is spent in port state transition of switch.

The structure of spanning tree will generate corresponding change when the spanning tree is recalculated, which is caused by network malfunction. However, the new config message which has been recalculated can't be spread all over the network immediately, it will cause temporary loop circuit if the port state is immediately transferred. Therefore, the spanning tree protocol adopts a state transition mechanism. It will go through twice of transmission delay before data forwarding for both new root port and designated port, the delay guarantees that the new config message has spread all over the network.

Note:
In the condition of topological stable state, only root port and designated port realize data forwarding, the other ports are in the state of being blocked, they only receive BPDU packet but not forward data.

6.1.3 STP Bridge Settings

The STP bridge config interface is shown in Figure 6-3.

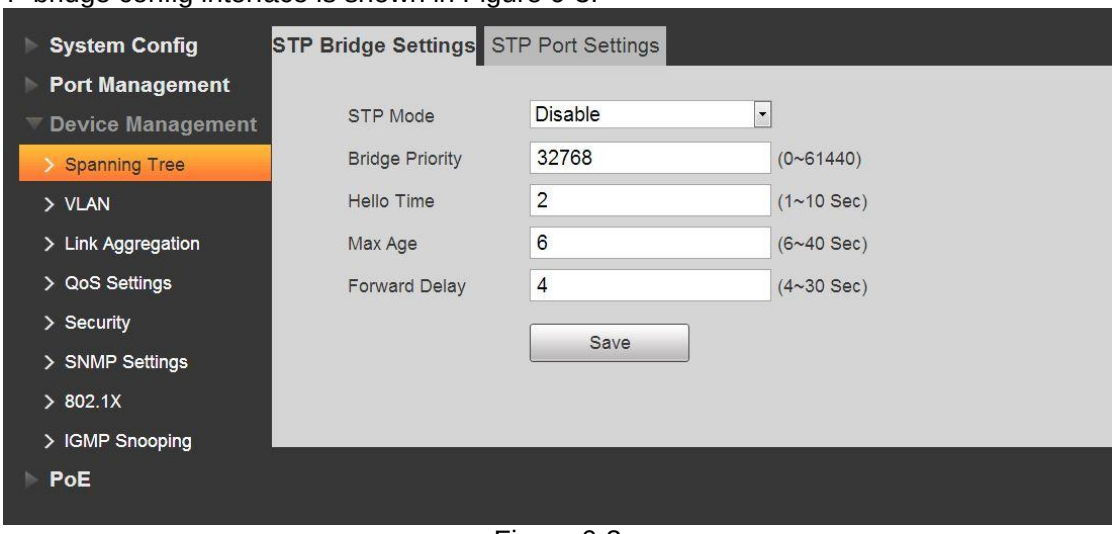


Figure 6-3

- STP Mode: Enable or disable ring network function.
- Bridge Priority: Set bridge priority, it ranges from 0 to 61440.
- Hello Time: Set the period of Root Bridge sending BPDU, it ranges from 1s to 10s.
- Max Age: Set the aging time of current BPDU, it ranges from 6s to 40s.
- Forward Delay: After setting topological change, the bridge maintains the time of snooping and study state, it ranges from 4s to 30s.

6.1.4 STP Port Settings

The STP port config interface is shown in Figure 6-4.

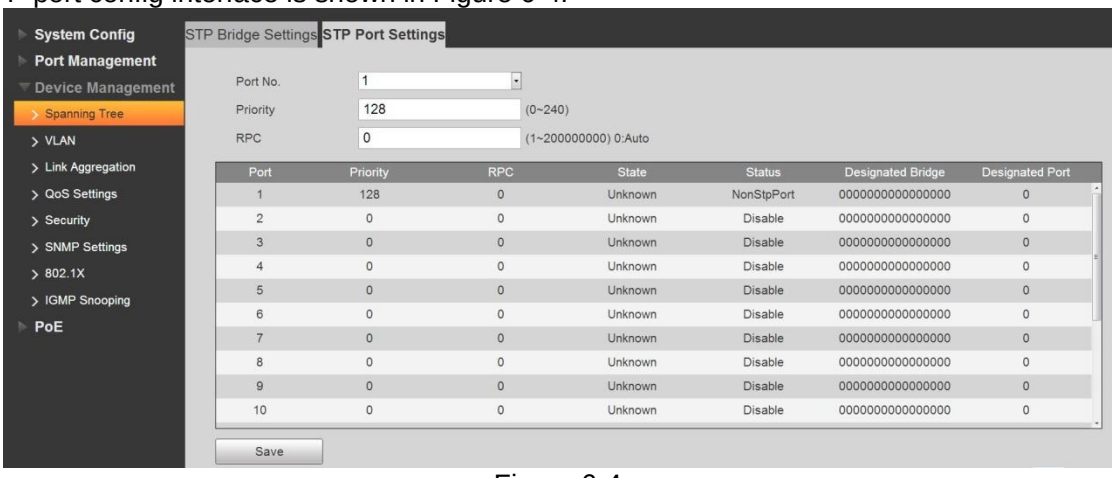


Figure 6-4

- Port No: Select the port you want to configure.
- Priority: Configure port priority, it ranges from 0-240, it has to be the integral multiple of 16.
- RPC: Configure the path cost from the current port to root bridge, it ranges from 1-200000000, it is the default path cost when it is set as 0.

6.2 VLAN Settings

6.2.1 VLAN Definition

Logically, it is to divide one LAN into many subsets. Each subset has its own broadcast area, so called virtual LAN (VLAN). A VLAN is logically divided on an organizational basis rather than on a physical basis.so that it realizes the isolated broadcast area in the VLAN.

6.2.2 VLAN Function

1) Enhance network performance. The broadcast packets are in the VLAN, it can effectively control the network broadcast storm, reduce network bandwidth and enhance network process capability.
2) Enhance 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 frame
3) Simplify the network management. The host of the same virtual working group is not limited in one physical area; it simplifies the network management and is easy to establish a working group for users in different areas.

6.2.3 VLAN Based on the port

The frames of the switch have tag frame and untag frame. Refer to the following figure for tag position.

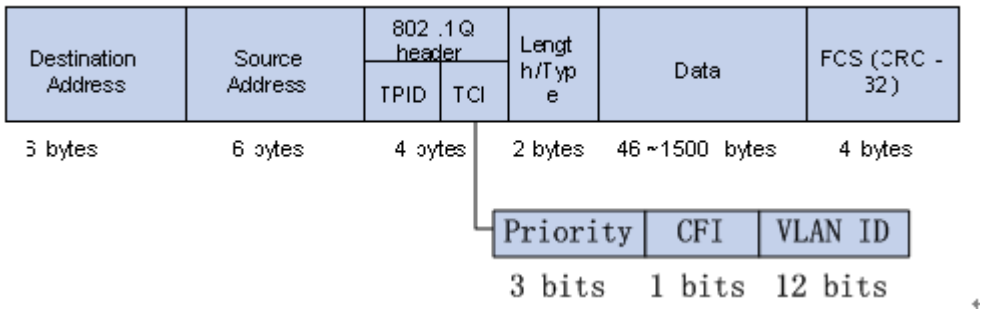


Figure 6-5

Untag is the general Ethernet frame. The network adapter of the general PC can recognize the frame and then communicate.

For tag frame, it adds the 4bytes vlan information after the source mac address and the destination address. It is the blue pane (the vlan tag head) in the above figure. Usually, the network adapter of the general PC cannot recognize this kind of frame, switch needs to use vlan tag to distinguish different VLANs, so that different VLANs cannot communicate with each other. Sometimes, it needs to communicate among different VLANs. So, there are different port types to allow the VLANs to communicate.

The port has three types:

- Access type port belongs to one VLAN. It is usually to connect to the computer port.
- Trunk type port allows several VLANs to pass and can receive or send out the frame of several

VLANs. Usually it is for the ports of the switch.

- Hybrid type can allow many VLANs to pass and can receive or send out the frame of several VLANs. It is to connect the switches and for the PCs of users.

When processing the data, the hybrid port and the trunk port are the same. The only difference is when they are sending data: Hybrid port can send out frame of several VLANs and without a tag, while the Trunk port can only send out the default VLAN frame without a tag.

Refer to table 6-1 for linkage type and frame processing methods for default VLAN.

Port Type	For frames without Tag	For frames with Tag	For the frames to be sent out
Access	Receive the frame and put the Tag of the default VLAN.	When VLAN ID is the same as the default VLAN ID, receive current frame. When the VLAN ID is different from the default VLAN ID, discard the frame.	Remove Tag and send out the frame.
Trunk	Put the default VLAN ID, when the default VLAN ID is in the accepted list, receive the frame and put the default VLAN Tag. Put the default VLAN ID, when the default VLAN ID is in the blocked list, discard the frame.	When the VLAN ID is in the accepted list, receive the frame. When the VLAN ID is in the blocked list, discard the frame.	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 frame.
Hybrid			When VLAN ID is on the accepted list, send out the frame. Use “port hybrid untagged/tagged vlan” to set with Tag or not when sending out.

Table 6-1

Config example.

1. Network connection

PC1 and IPC2 belong to one department, PC2 and IPC1 belong to one department, it can realize intercommunication within the department, but it fails to realize communication between departments.

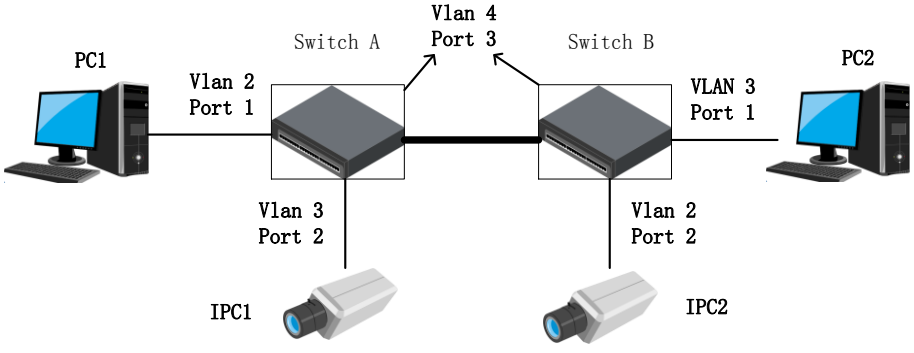


Figure 6-6

2. Hardware connection

(1) PC1 connects to port 1 of switch A, and it belong to vlan2，IPC1 connects to port 2 of switch A, and it belongs to vlan3；

(2) PC2 connects to port 1 of switch B, and it belong to vlan3, IPC2 connects to port 2 of switch B, and it belongs to vlan2；

(3) Port 3 of switch A connects to port 3 of switch B, and it belongs to vlan4.

3. Settings

switch A：Port 1 belongs to vlan2, configured as Access port, port 2 belongs to vlan3, configured as Access port, port 3 configured as trunk port, and it belongs to vlan4, and it allows vlan2, 3 and 4 to pass.

Switch B: Port 1 belongs to vlan2, configured as Access port, port 2 belongs to vlan3, configured as Access port, port 3 configured as trunk port, and it belongs to vlan4, and it allows vlan2, 3 and 4 to pass.

Please refer to Figure 6-7.

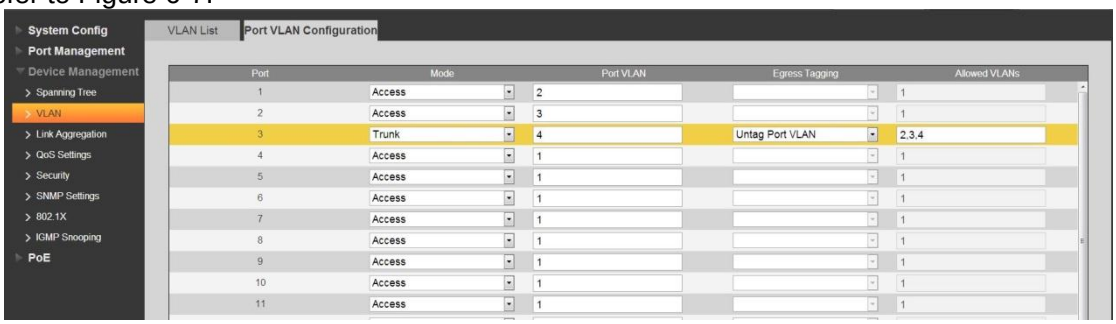


Figure 6-7

6.3 Link Aggregation

Link aggregation is to form several physical ports of 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, 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 has to be certain config 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 etc.

Note:

It is not recommended to implement config of port and advanced functions for the ports which are used for link aggregation.

Link aggregation can be divided into static aggregation and LACP, generally the opposite end devices of switch link aggregation are switch and network cards.

6.3.1 Static Aggregation Mode

Static aggregation mode allows it to manually add several member ports in the aggregation group, all the ports are in the forward status and share the overloaded flow. It needs to create aggregation group and add member ports via manual config without the participation of LACP (link Aggregation Control Protocol) protocol packet.

- Load Balancing Mode

There are three types of load balancing algorithm for port, which is shown in the following table.

Load Balancing Mode	Note
Source MAC	Load balance calculation based on the source MAC address of packet
Destination MAC	Load balance calculation based on the destination MAC address of packet.
MAC Src&Dst	Load balance calculation based on source & destination MAC address of packet.

Table 6-2

- Aggregation Group

It is an assembly of a group of Ethernet ports. The supported number of aggregation groups is three by default, which can't be modified. The default status of all the aggregation groups is disable, member port is null by default.

- Member Port

The switch created all the aggregation groups by default, the port members are null. It needs to enable aggregation group first if you want to configure member ports for aggregation group, and then click the aggregation group where the port is located to enable aggregation function.

Please refer to Figure 6-8 for the interface of static aggregation config, which includes load balance mode, aggregation group and port members.

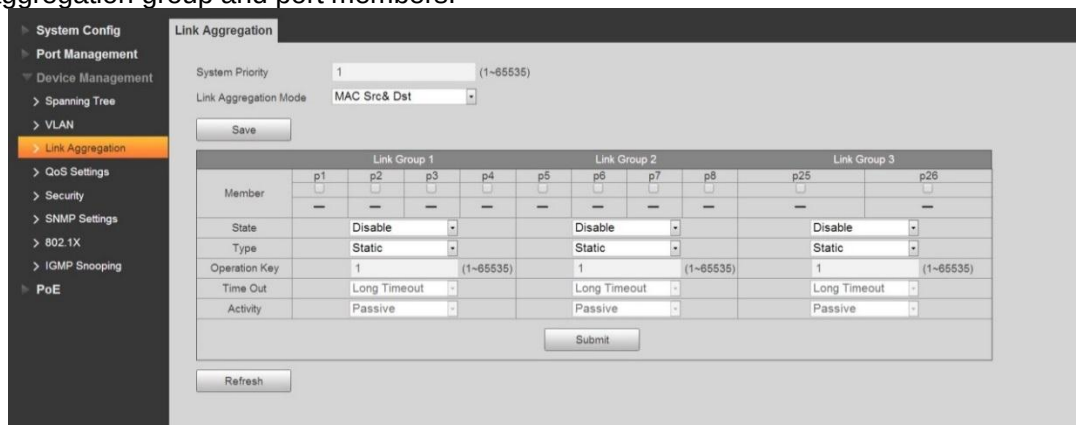


Figure 6-8

6.3.2 LACP Mode

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 and receive & send data via LACPDU packet interacting convergence information. The protocol can automatically add and delete ports in the convergence group, it 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 (it is decided by physical properties, upper layer protocol info and management Key of the port).

The end with high priority of the device will dominate convergence and convergence separation, the device priority is decided by system priority and system MAC, the device with smaller system priority value has higher priority, the device with smaller 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, the ports with same operation Key can be selected into the

same convergence group, the port with smaller port priority value will be selected by priority in the same convergence group, the port with smaller number will be selected when the port priority is the same. The selected ports will converge together to receive and send data after both parties interact convergence information.

The config parameter of LACP protocol mainly includes port LACP function enable, key value, activity (active/passive mode) and timeout config.

The ports which only enable LACP protocol can realize LACP negotiation, and then it may form convergence link. Secret key is the basis of negotiation, and ports with same secret key can negotiate to form a convergence link. Negotiation mode includes "active/passive". The device will actively launch convergence link when it selects "active"; the device will passively accept convergence negotiation launched by other devices when it selects "passive".

There is at least one or two ends which need to be set as "active" mode to realize successful negotiation when two devices are interconnected.

- Key value: members in the same convergence group, it needs to configure the same operation key, it ranges from 1 to 65535;
- Activity: it can select Active and passive by default, one end of the device which is involved in dynamic convergence has to select Active mode and the other end has to be configured with passive mode;
- Time out: It is Long Timeout by default, it can select Long Timeout and Short Timeout;

Config Example:

1. Network Requirement
   It needs to realize link backup and dual GB link uplink via link aggregation function because there is hidden trouble on the single GN link.
2. Config Steps
   (1) Select aggregation group 3, click port 25 and 26.
   (2) Select link aggregation mode as LACP, configure Activity as "Activity".
   (3) Click "Submit" to apply config.
   (4) Select link aggregation mode as "MAC Src&Dst" and the config result is shown in Figure 6-10, the corresponding ports which are successfully aggregated will display "√".

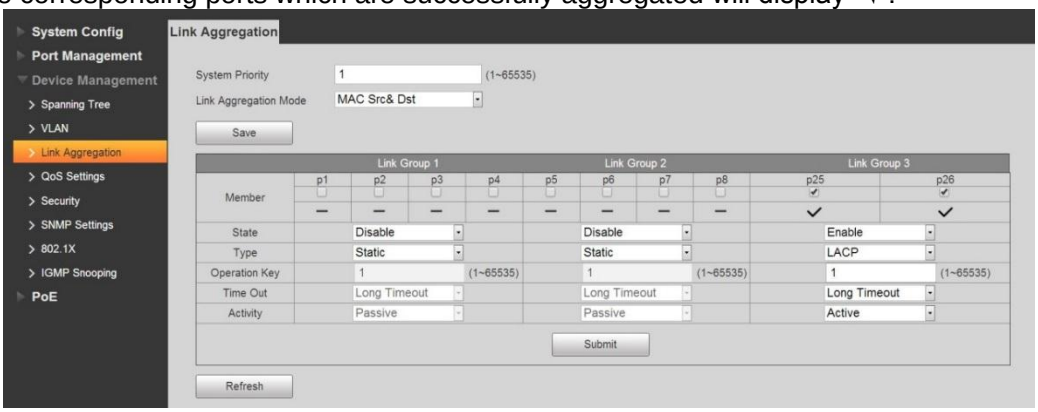


Figure 6-9

6.4 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.

The evaluation can be based on different criteria because the network may provide various services. Generally, QoS performance is measured with respect to bandwidth, delay, jitter, and packet loss ratio during packet forwarding process.

In traditional no QoS IP network, the device treats all packets as the same and the process policy is first

in first out (FIFO). It allocates the required resources according to the time the packet arrived. All packets share the network and device resources and for the resources a packet can get are depending on the time it arrives. This kind of service is called Best-Effort. It uses its max efforts to send out the packet to its destination, but there is no guarantee or assurance about the delay, jitter, and packet loss ration during the packet forwarding process.

The traditional Best-Effort service policy is for the WWW, E-mail service that is not sensitive to the bandwidth or the delay. But right now the new arising business are demanding high service level of the IP network. The user does not just want to merely send out the packet to the destination, he also wants to enjoy better service during the forwarding process such as there is special network bandwidth, reducing packet loss rate, manage or avoid the network congestion, adjusting network flows. All of these are requiring the network to have perfect service capability.

6.4.1 Network Congestion

In complicated Internet grouping and exchanging environments, congestion is everywhere. See Figure 6-10.

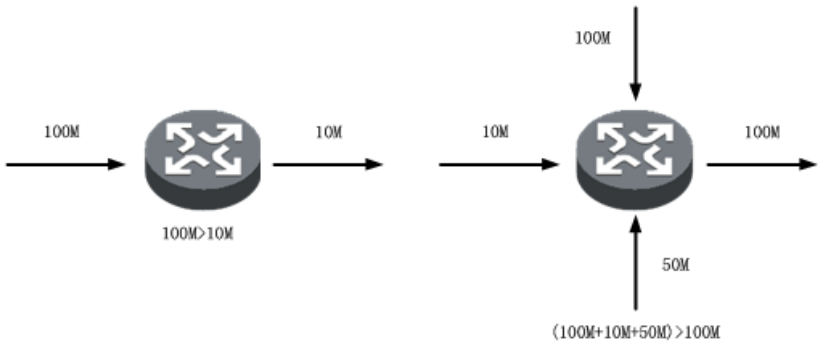


Figure 6-10

1) The group streams are from the high-speed linkage to the device and forward via the low speed linkage,
2) The group streams are connected to the network device via several ports and then forward via one port (the speeds of the multiple input ports are larger than the speed of the output port.)

If the flow speed is too huge, it may encounter resources threshold and result in flow congestion.

Not only the linkage bandwidth has the congestion, any insufficient resources of the forward place (such as the available process time, buffer, memory resources are not sufficient) may result in congestion. Besides, if the flow control is out of the range at some time and there are no sufficient network resources, it may trigger network congestion too.

The congestion has a series of negative effect:

- The congestion enhances the packet transmission delay and jitter, the high latency may result in sending the packet again.
- The congestion slows the network inbound and outbound flows and lower the usages rate of the network resources.
- The congestion consumes huge amount of network resources (especially storage resources), improper resources allocation may result in system down.

So, we can see the congestion prevents the flows getting the resources in time and it is the original

source to lower the service performance. In the complicated environments where there is group exchanging and multiple-user business, congestion is inevitable. So there shall be a proper way to deal with the congestion.

6.4.2 Congestion Settlement

The direct method to solve insufficient resources is to add network bandwidth. But the bandwidth has its limit, it cannot fix all the problems resulting from the network congestion.

The more effective way to solve network congestion is to add flow control and resources allocation function in the network. It can provide different services according to different business requirements, and allocate and use the resources more reasonably. During the resources allocation and flow control process, try to control the direction or indirect factors that may trigger network congestion, which is to reduce the occurrence rate of the congestion. When the network congestion occurs, it can allocate the resources according to the business type and requirements to reduce the effect of the congestion to the minimum level.

6.4.3 Queue Scheduling

Usually we adopt queue scheduling to settle the congestion management. Using the line algorithm to categorize the flows and use the priority algorithm to send out these kinds of flows first. Each queue algorithm is to fix the pending network flow problems; it has great effect on the bandwidth resources allocation, delay, jitter and etc.

This series product supports two priority queue: high priority queue and low priority queue. The priority of each packet is set according to the following four plans.

1. The physical port.
2. 802.1Q VLAN tag.
3. TOS/DS string of the IP packet.
4. TCP/UDP port.

When there are several QoS settings, once one priority setup item becomes the high priority, then the item will be put in the high priority line and then forward. When there are several high priorities, for the same level, it adopts First In First Out (FIFO).

6.4.4 Priority Mode

Each received packet maps to either high priority or low priority. The packet priority setup has three modes. See Figure 6-11.

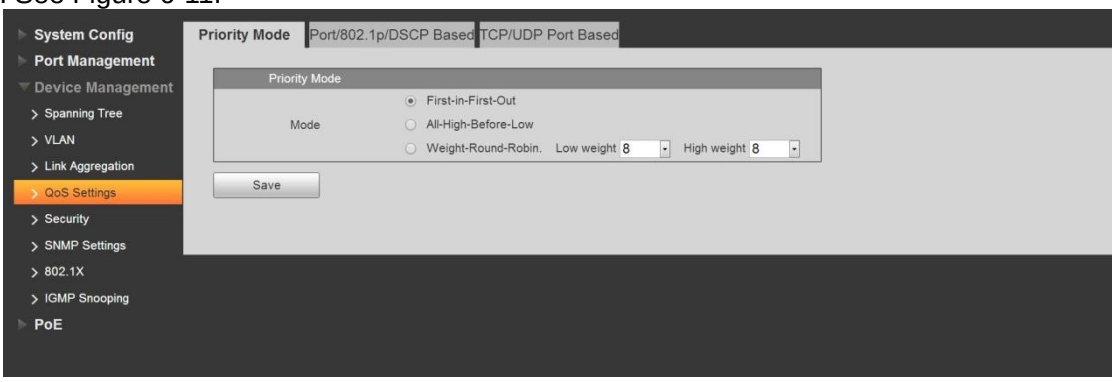


Figure 6-11

Refer to Table 6-3 for priority mode information.

Name	Note
First In First Out	The first received packet will be forwarded first. When QoS

(FIFO)	function is disabled, device adopts FIFO mode to process the packets.
All high before low	Device forwards the packets according to the specified priority level.
Weight round robin	Set the weight level to change the packet forwarding percentage in the high priority and low priority.

Table 6-3

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

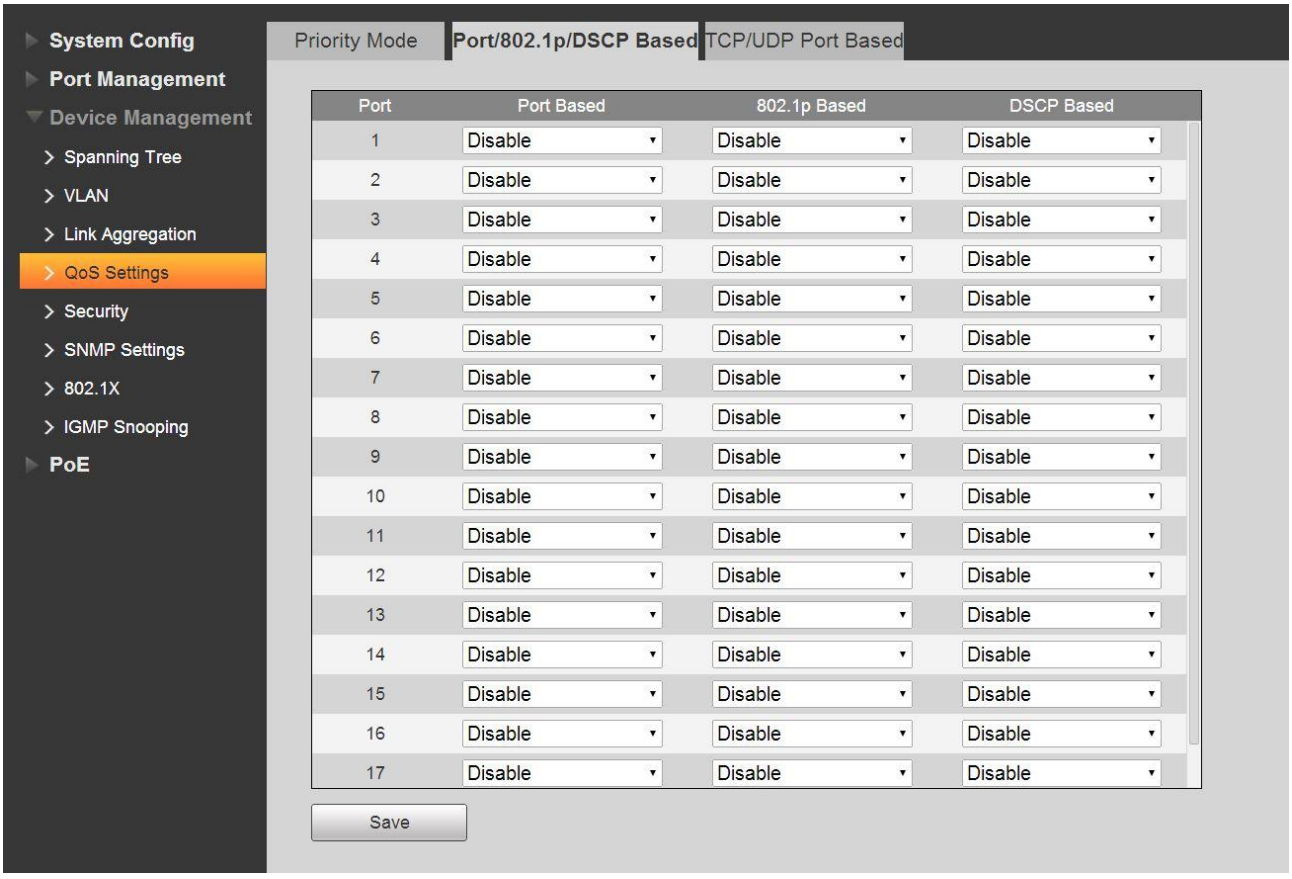


Figure 6-12

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 set as the high priority.

Based on 802.1p

802.1p priority is at the 2-layer packet head. It is for the environment where there is no need to analyze the 3rd head and shall guarantee the QoS in the 2-layer.

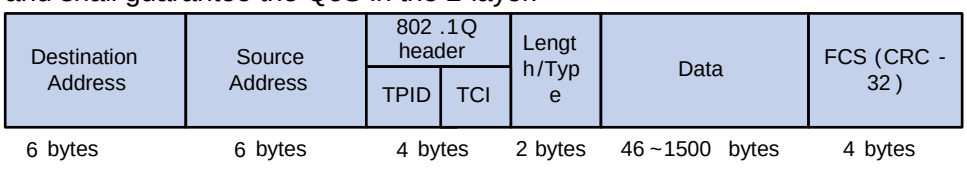


Figure 6-13

In Figure 6-14, the four-byte 802.1Q tag head includes 2-byte TPID（Tag Protocol Identifier）and 2-byte

TCI（Tag Control Information）. The TPID value is 0x8100. In Figure 6-9, it displays the detailed contents of the tag head of the 802.1Q, Priority string is the 802.1p priority. The priority is called 802.1p since the priority is defined in 802.1p specifications.

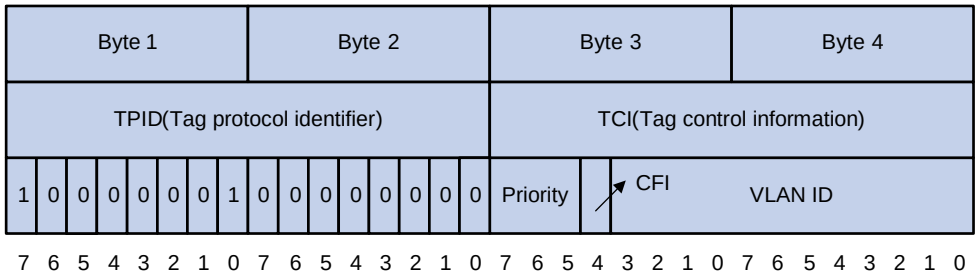


Figure 6-14

Refer to Table 6-4 for 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
	3	011	excellent-effort
High priority queue	4	100	controlled-load
	5	101	video
	6	110	voice
	7	111	network-management

Table 6-4

Based on the TOS/DS string of the IP packet

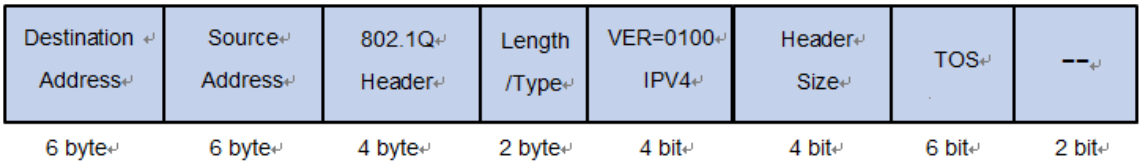


Figure 6-15

In Figure 6-10, the ToS string of the IP packet head has 8 bits, RFC2474 redefines the ToS domain of the IP packet head, and it is called (Differentiated Services). DSCP priority uses the first 6-bit (0-5). The value ranges from 0 to 63, and the last 2-bit (6, 7) are the reserved bit.

Refer to Table 6-5 for IP priority information.

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

queue			

Table 6-5

6.4.6 TCP/UDP Port

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, 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.

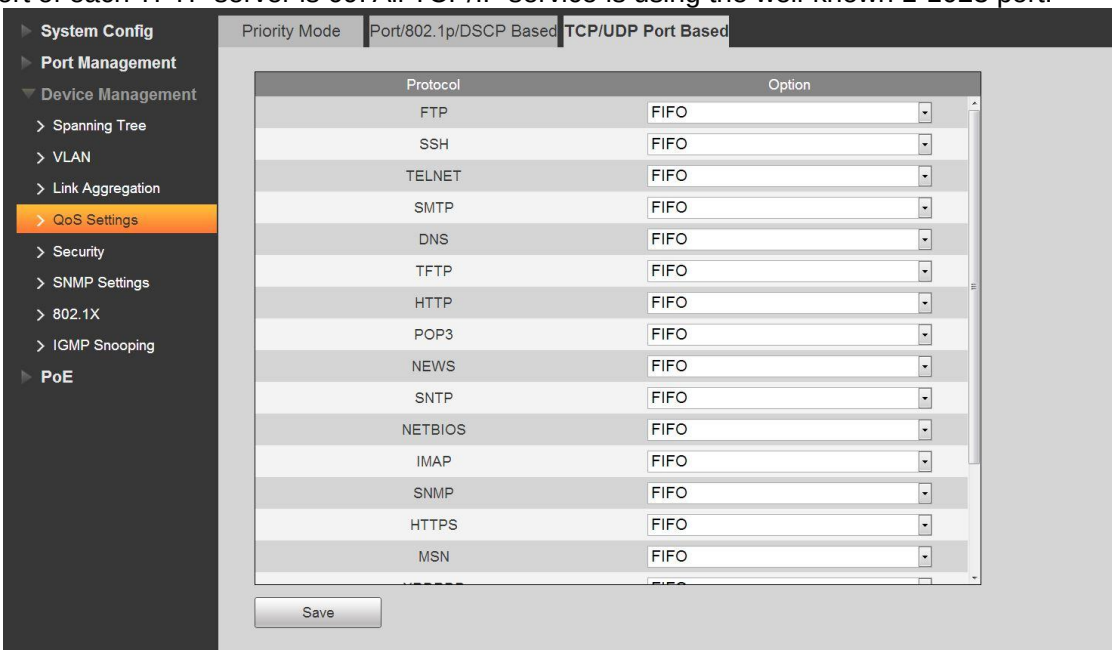


Figure 6-16

In Figure 6-11, this series product can process the received packets based on the TCP/UDP port such as FTP, SSH, TELNET, SMTP, and DNS. Here is to set packet high priority, low priority, or discard. The default setup is FIFO.

Config example.

1. Network connection

- In Figure 6-12, connect the device with the FTP server, and use the port 1 and port 2 to connect the device.
- Properly set QoS function, the port 2 has high priority than port 1 and is blocked to access FTP server.

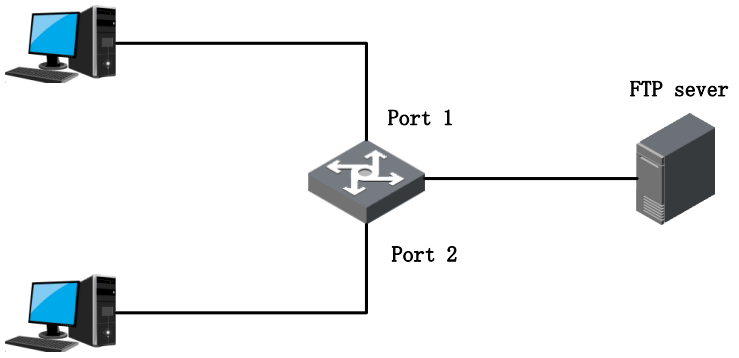


Figure 6-17

2. Settings

（1） Set the device mode is all-high-before-low mode

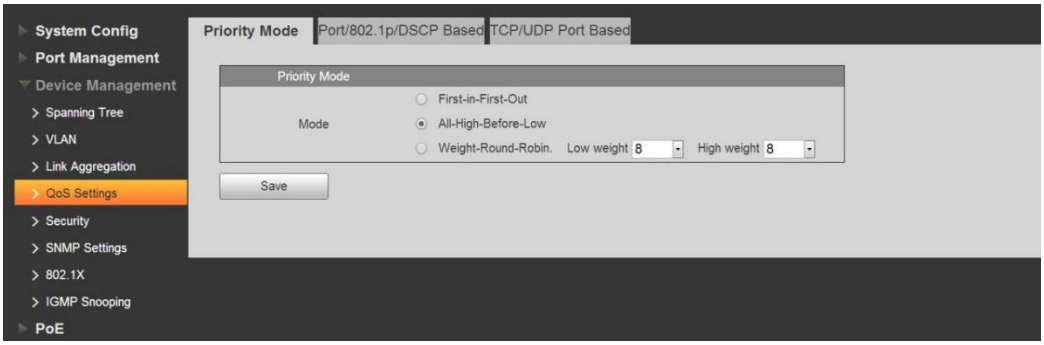


Figure 6-18

（2） Set port 2 as high priority.

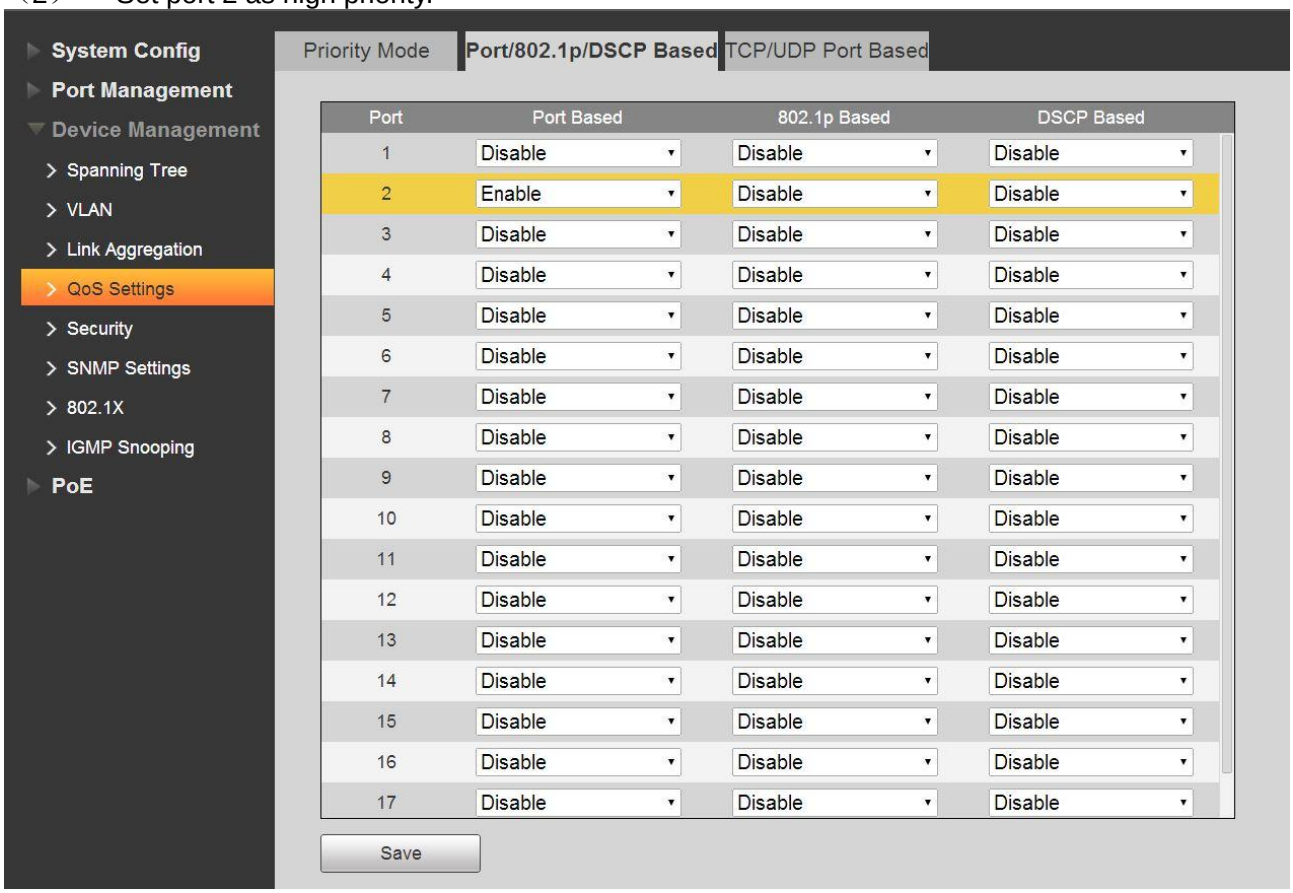


Figure 6-19

（3） Set device to discard FTP data packet, block user to access FTP server.

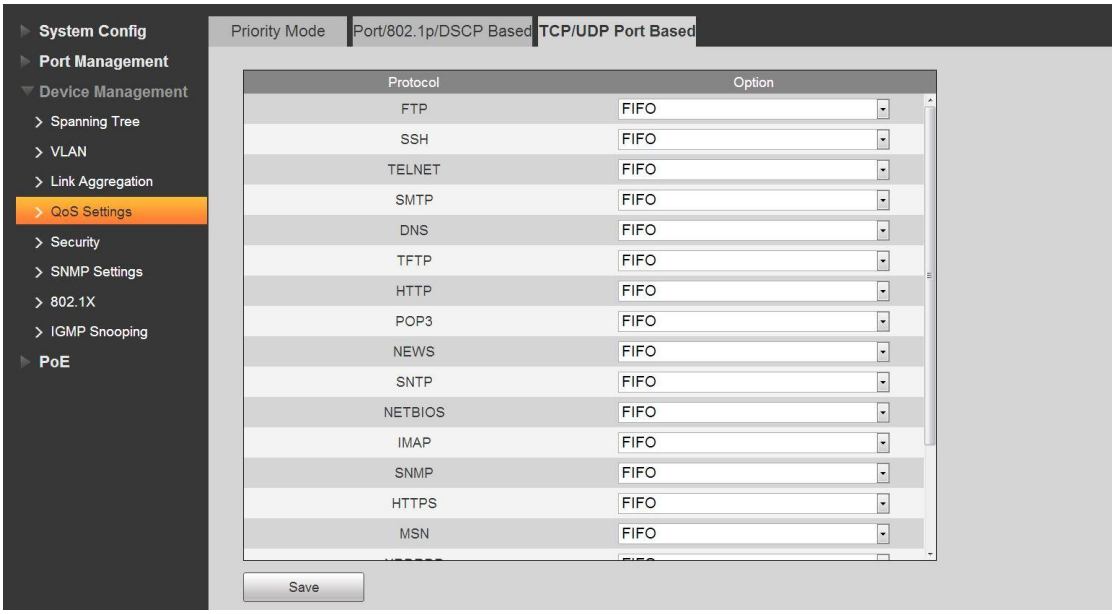


Figure 6-20

6.5 Security

MAC (Media Access Control) records the relationship between the MAC address and the port, and port belonging VLAN information and etc.

6.5.1 MAC Address List

When device forwards the packet, it searches the MAC address sheet according to the packet 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 packet. If the MAC address has no item matching the packet destination MAC address, device adopts the broadcast mode to forward the packet via the corresponding VLAN (except the input port).

Refer to the following figure for MAC address information.

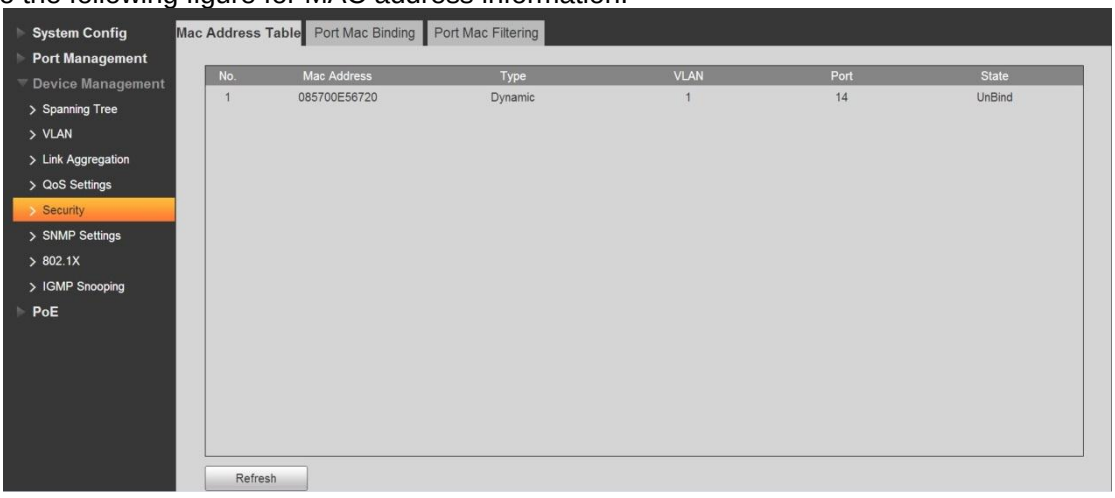


Figure 6-21

6.5.2 Port MAC Binding

In Figure 6-22, click current connected port, set port MAC binding function so that current port only

forward the binding MAC address.

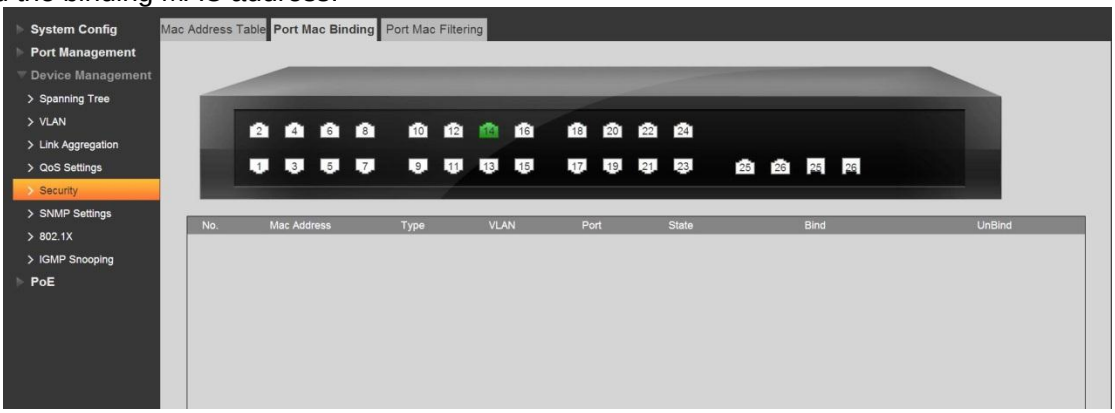


Figure 6-22

Config example.

1. Network connection

User uses WEB to set port MAC binding so that the port can only be used by current device.

2. Settings

（1） From **Device Management**>**Security**, go to **MAC Address Table** interface.

（2） Select **Port MAC Binding** interface.

（3） Select the port whose connection status is green, and then click Bind button. See Figure 6-23.

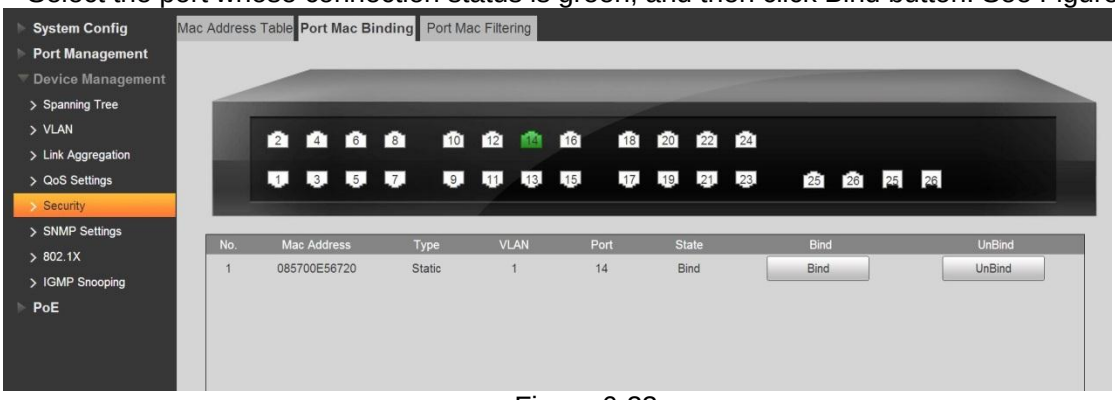


Figure 6-23

6.5.3 Port Mac Filtering

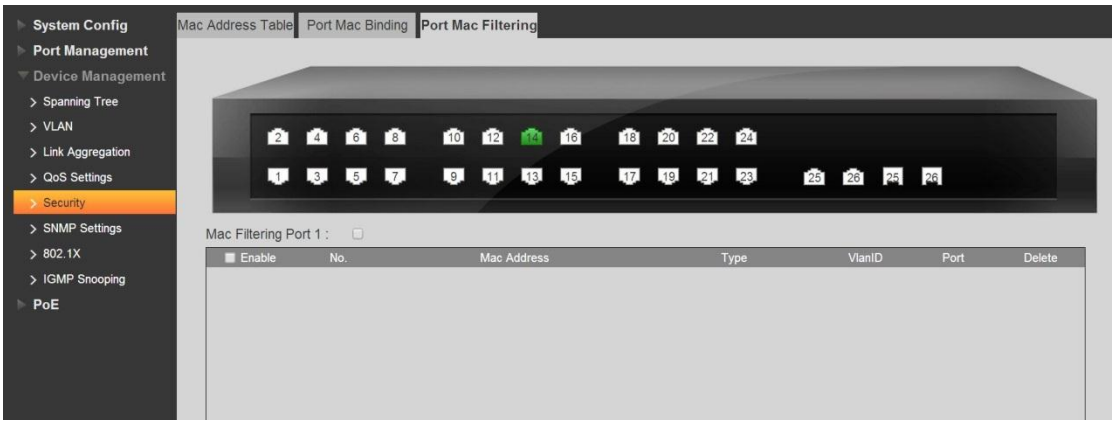


Figure 6-24

As it is shown in Figure 6-24 that the function is used to restrict allowed MAC packet under port, which can prevent counterfeit attack. After the port is configured with the function, when the port receives packet, it will check if the source MAC address of packet is the same as the allowed MAC address:

- If it is same, then the packet is considered as legal, and it will continue to implement follow-up processing;
- If it is different, then the packet is considered as illegal, and it will be discarded.

6.6 SNMP Settings

SNMP network includes two elements: NMS and Agent.

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

When NMS manages the device, it pays great attention on some parameters such as port status, CPU usage rate and etc. All these parameters together are called the Management Information Base (MIB). These parameter are called the nodes in the MIB. MIB defines the layers of these nodes and the properties of these objects such as object name, access rights, data type and etc. Each Agent has its own MIB. All managed devices have their own MIB file, and compiling these MIB files on the NMS can generate the MIB of each device. The NMS reads and writes the nodes of the MIB according to the access rights setup so that it can manage the Agent. Refer to the following figure for the relationship among NMS, Agent and MIB.

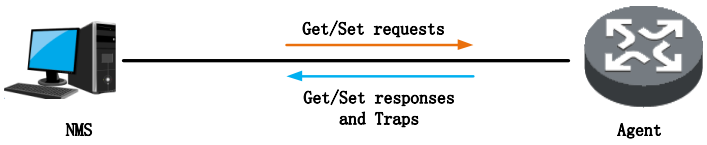


Figure 6-25

MIB adopts the tree organization, it consists of many nodes. Each node represents one managed object. The managed object can use an unique number representing the path beginning from the root. This number is called Object Identifier (OID). Refer to the following figure for detailed information. The managed object B can use a series number {1.2.1.1} to identify. This is the OID of the managed object.

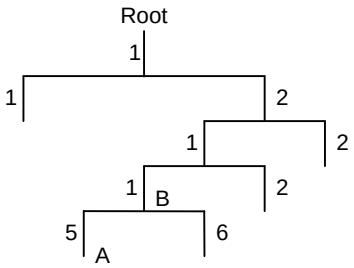


Figure 6-26

SNMP provides three basic operations to realize the interactive between the NMS and the Agent:

- Get: NMS uses it to search the value of one or more nodes of the Agent MIB.
- Set: NMS uses it to set the value of one or more nodes of the Agent MIB.
- Trap: NMS uses it to send Trap information to the NMS. The Agent does not require the NMS to send the responding message and NMS does not respond the Trap information. SNMPv1,SNMPv2 and SNMPv3 all support Trap operation.

SNMP protocol version

Right now, the Agent supports SNMPv1, SNMPv2 and SNMPv3.

- SNMPv1 adopts community name to certify. The community name is just like a password, it Is to restrict the communication between the NMS and Agent. If the NMS community name and the managed device community name are not the same, the NMS and the Agent cannot establish the SNMP connection, which means the NMS cannot access the Agent and the NMS discards the

warning information from the Agent.

- SNMPv2 adopts the community name to certify. SNMPv2c has expand the functions of the SNMPv1. It provides more operation types and supports more data types, provides abundant error codes and can accurately distinguish the errors.
- 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 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.

Note: Please make sure the NMS and the Agent are using the same SNMP version, otherwise the NMS and Agent connection may fail.

6.6.1 SNMP

This interface is to set the SNMP. The V1 and V2 include the following setups.

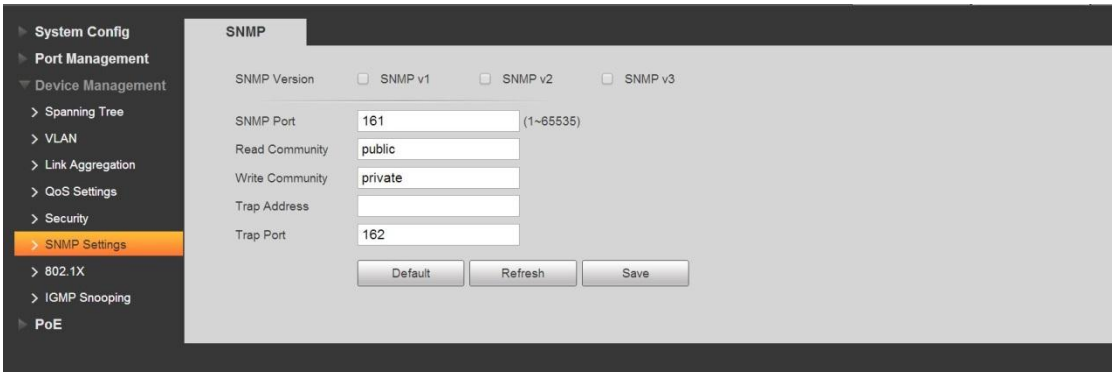


Figure 6-27

In Figure 6-21, SNMP V1 and V2 setup interface includes SNMP port, version, read community, write community, Trap address, and Trap port.

Figure 6-28 is the SNMP V3 setup interface.

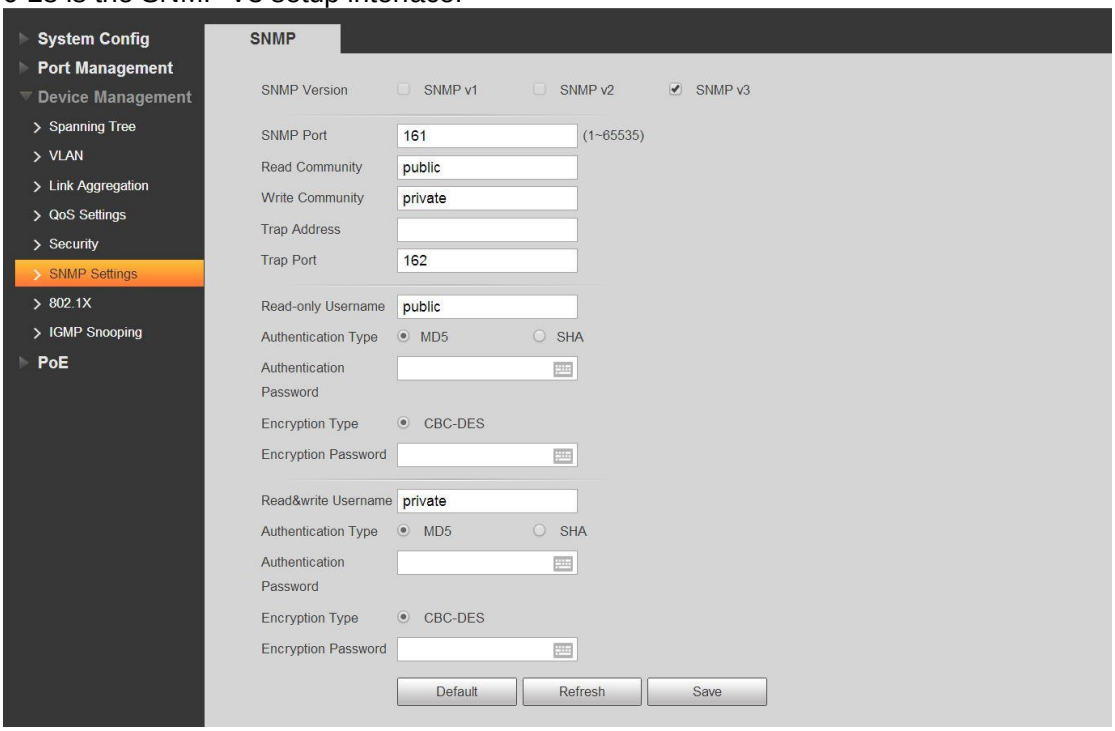


Figure 6-28

Refer to Table 6-6 for detailed information.

Name	Note
Read community	The community name to access the network administrator. The right is read. The default setup is public.
Write community	The community name to access the network administrator. The right is write. The default setup is private.
Trap address	It is to specify the server IP address.
Trap port	It is to set trap destination port.
Read-only user name	Set the read-only user name. It is for V3 only.
Authentication mode	It is to set authentication mode when the security level is “Authentication no encryption” or “Authentication and encryption”. The authentication mode includes MDS and SHA.
Authentication password	It is to set authentication password.
Encryption mode	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 password	It is to set read/write user.

Table 6-6

Config example.

SNMPv1/v2

1. Network connection

Refer to Figure 6-23, the NMS connects with the Switch and it shall realize the following requirements.
NMS monitors and manages the Switch via SNMPv1 and SNMPv2c.
Switch can auto send out Trap message to the NMS when there is a malfunction.

Figure 6-23

2. Settings

1) In the navigation bar, from **Device**> **SNMP Settings**, system goes to SNMPv1 interface by default.
2) Select SNMP version as v1 or v2.
3) SNMP port number is 161, set “Read Community”, “Write Community”, “Trap address” and “Trap Port”. See Figure 6-29.

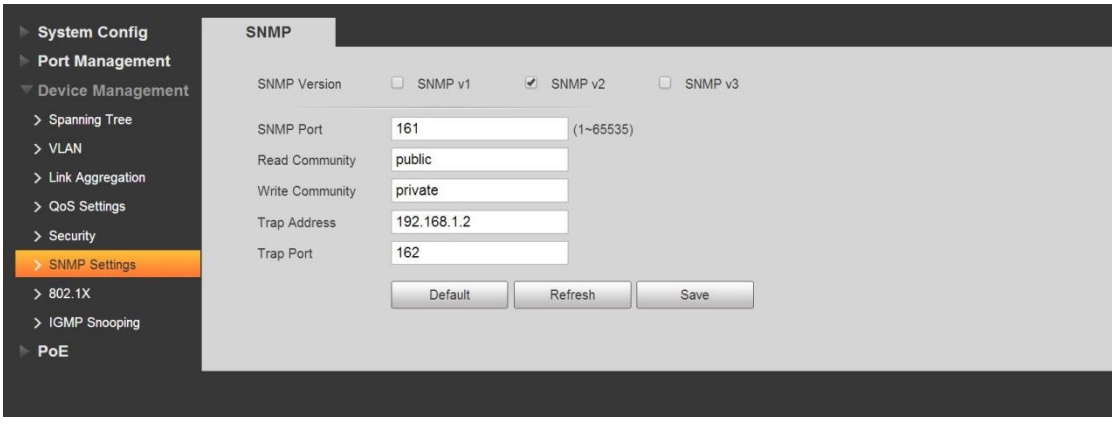


Figure 6-29

SNMPv3

1. Network connection

Refer to Figure 6-31, the NMS connects with the Switch and it shall realize the following requirements.

- NMS monitors and manages the Switch via SNMPv3.
- Switch can auto send out Trap message to the NMS when there is a malfunction.
- When NMS connects Agent via SNMP, it requires authentication. The authentication mode is MD5, the authentication password is admin123.
- The SNMP message among the NMS and the Agent shall be encrypted, the encryption mode is DES56, and the encryption password is admin123.

Figure 6-31

2. Settings

（1） In the navigation bar, from **Device**>**SNMP Settings**, system goes to SNMPv1 interface by default.
（2） Select SNMP version as v3.
（3） SNMP port number is 161, set “Read Community”, “Write Community”, “Trap address” and “Trap Port”. Trap port is 162.
（4） Input read-only user name as “user”.
（5） Authentication mode is MD5.
（6） Authentication password is “admin123”.
（7） Encryption mode is “CBC-DES”
（8） The encryption password and confirm password is “admin123”.
（9） Input read/write user name as “user1”.
（10） Authentication mode is “MD5”.
（11） Encryption password is “admin123”.
（12） Encryption mode is “CBC-DES”
（13） Encryption password is “admin123”.
（14） Click Save button. See Figure 6-32.

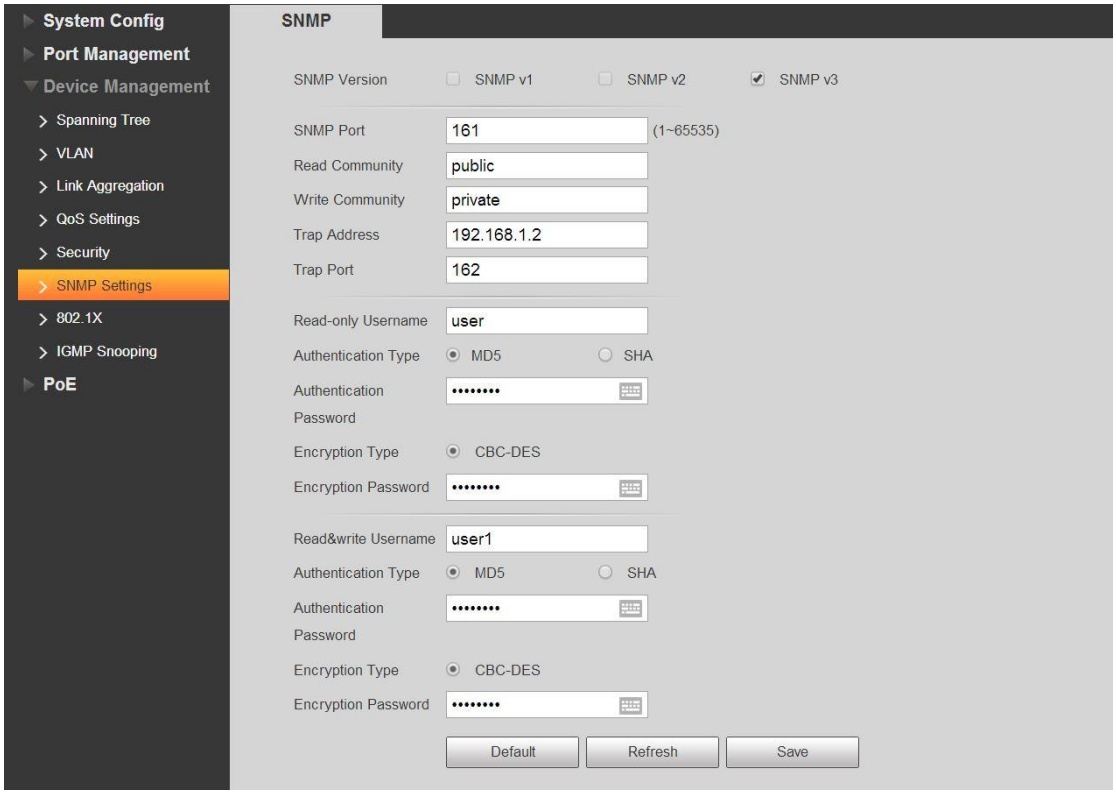


Figure 6-32

6.7 802.1x

IEEE 802.1x is the authentication standard about user network access which is designated by IEEE, it is a type of network access control protocol based on port, therefore, the exact 802.1x authentication function has to be configured on the device port. As for the user device which is accessed to port has to control access upon network source via authentication.

6.7.1 802.1x Networking Structure

802.1x system includes three parts which are Client, Device and Authentication Server, which is shown in Figure 6-33.

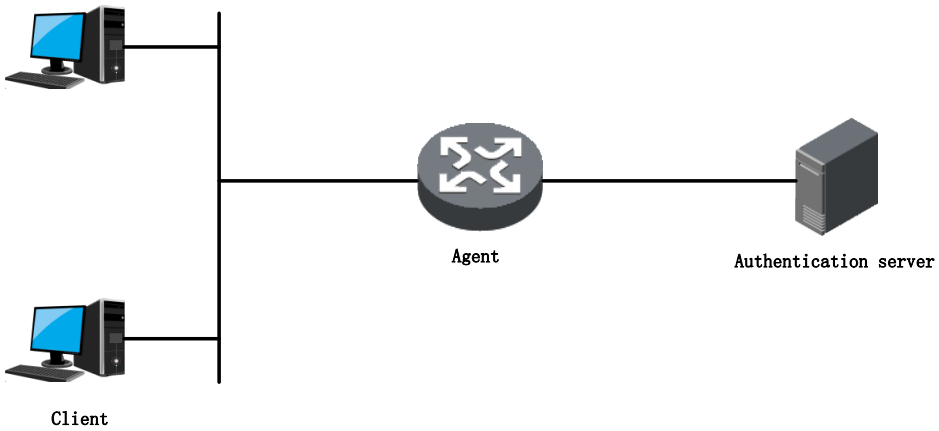


Figure 6-33

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

device end in the LAN. The client has to install client software which supports 802.1x authentication.

- Device end is the network device which controls client access in the LAN, it is located between client and authentication server, which provides LAN access port for customers (physical port or logical port), and it implements authentication upon the connected client via interaction with server.
- Authentication server is used to implement authentication, authorization and billing, generally it 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 device end, and inform the device of verification results, it is decided by device end whether it allows client access or not. 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.

6.7.2 802.1x 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 which arrived the port can be displayed on both controlled port and uncontrolled port.

- The uncontrolled port is always in the status of bidirectional connection, which is mainly used to transmit authentication packet and make sure that the client can always send or receive authentication packet.
- The controlled port is always in the status of bidirectional connection under authorization status, which is used to transmit business packet; it is forbidden to receive any packet from client when it is in the unauthorized status.

6.7.3 Trigger Mode of 802.1x Authentication

The authentication process of 802.1x is actively launched by client, it can be launched by device as well.

1. Client Active Trigger Mode

- Multicast trigger: the client actively send authentication request packet to device in order to trigger authentication, the destination address of the packet is the multicast MAC address 01-80-C2-00-00-03.
- Broadcast trigger: the client actively send authentication request packet to device in order to trigger authentication, the destination address of the packet is the broadcast MAC address. The mode is able to solve the problem that the device fails to receive authentication request from client because some devices fail to support the multicast packet above in the network.

2. Device Active Trigger Mode

The device active trigger mode is used to support the client which is unable to actively send authentication request packet, there are two types of device active trigger authentication:

- Multicast trigger: The device actively sends request packet of identity type to trigger authentication to client at regular interval (it is 30s by default).
- Unicast trigger: when the device receives unknown packet from source MAC address, it will actively send Identity-typed request packet to the MAC address unicast in order to trigger authentication. It will send the packet again if the device fails to receive client response within the setting duration.

6.7.4 Port Authorized Status

It can control if the port accessed users need to visit network source via authentication by configuring authorized status for the port. The port supports three following authorized states:

- Authorized-force: It means that the port is always in the authorized status, which allows users to visit network source without authentication.
- Unauthorized-force: it means that the port is always in the unauthorized status, which doesn't allow authentication for users. The device won't provide authentication service for the client which is accessed to the port.
- Port based 802.1x: it means that the port initial status is unauthorized status, which doesn't allow users to visit network source; The port will be switched to authorized status if the users pass

authentication, and it will users to visit network source.

Config Example:

1. Network Requirement
   The client IP is 192.168.1.1/24 segment, authentication server IP is 192.168.1.100, and it is required to be authenticated by authentication server when all the ports of device are accessed.
2. Config Steps

(1) Enable authentication function, all ports are enabled based on 802.1x authentication, which is shown in Figure 6-34.

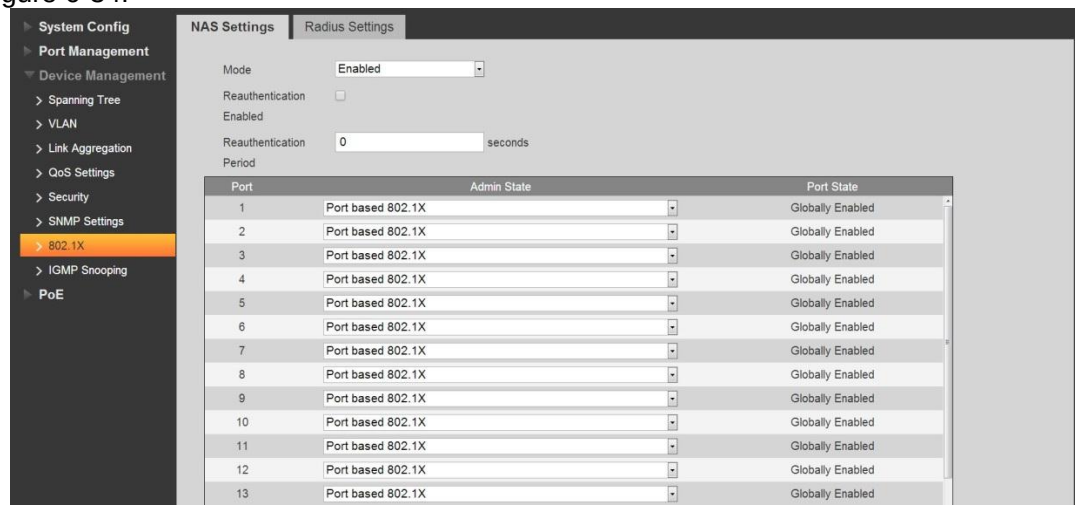


Figure 6-34

(2) Configure the address of authentication server, which is shown in Figure 6-35.

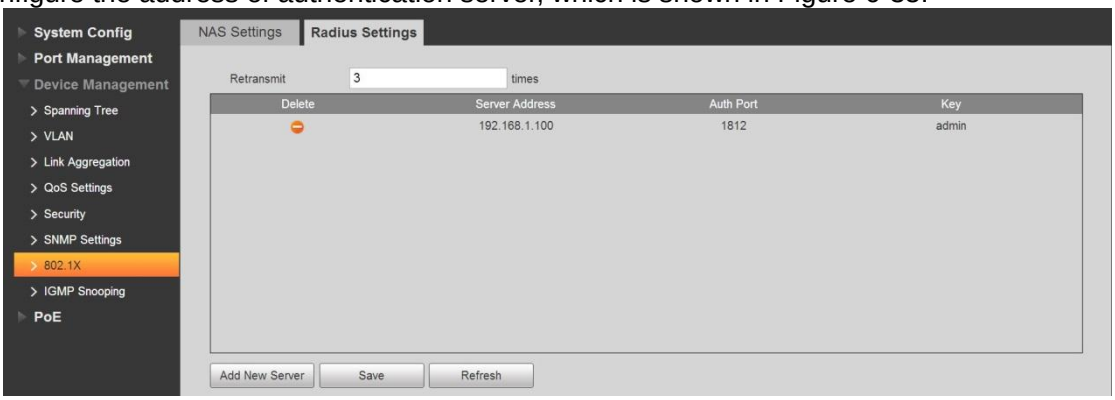


Figure 6-35

6.8 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 layer two required distribution of multicast data packet.

6.8.1 IGMP Snooping Theory

Operating layer two device of IGMP Snooping can establish mapping relation for port and MAC multicast address via analysis upon received IGMP packet, 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 multicasted to designated receivers.

IGMP Snooping can only forward the information to the needed receivers via layer two multicast, which can bring following advantages:

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

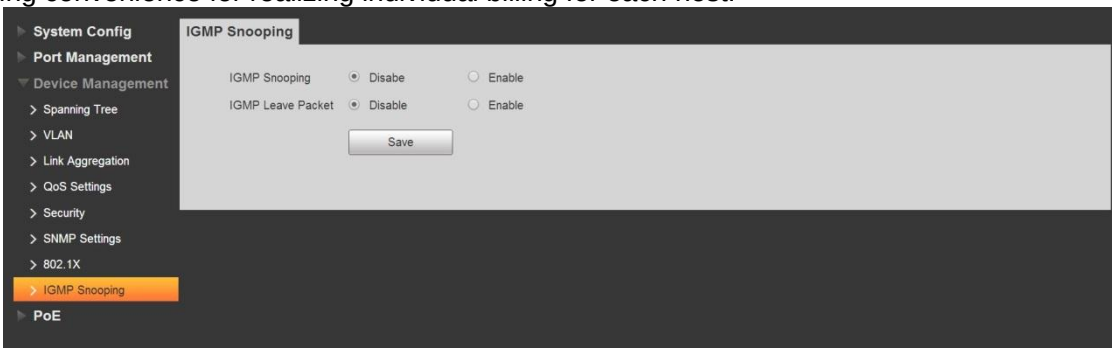


Figure 6-36

The IGMP Snooping config interface is shown in Figure 6-36.

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

7 PoE

7.1 PoE Settings

Power over Ethernet (PoE) means the device uses the Ethernet port to provide power to the device via the twisted pair cable remotely. The PoE function realizes the centralized power supplying and easy to backup. The network terminal just uses one simple network cable without external power source. It complies the IEEE 802.3af and IEEE 802.3at and adopts the universal recognized power port. It is for the IP camera, IP phone, wireless access point (wireless AP), portable device recharger, POS, data acquisition and etc.

Refer to Figure 7-1 for PoE system. It includes PoE power, Power Sourcing Equipment (PSE), power interface (PI) and powered device (PD).

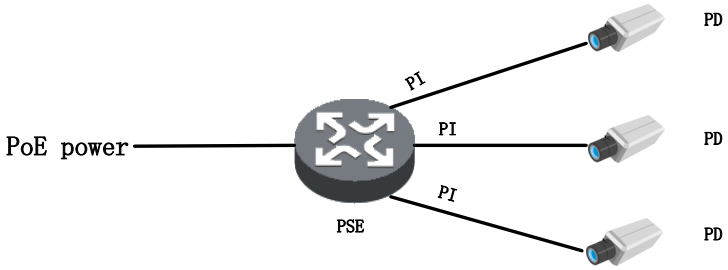


Figure 7-1

1. PoE power

PoE is to provide power to the whole system.

2. PSE

PSE is to provide power to the PD directly. The PSE supports the functions such as search, detect PD, categorize PD, and provide power to it, realize power consumption management, check the PD connection and etc.

3. PI

PI refers to the Ethernet interface that has the PoE function. It is called PoE port. It includes FE and GE.

The PoE remote power supplying has two modes:

- Over signal wires—The PSE uses the pairs (1, 2, 3, 6) for transmitting data in a category 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) not transmitting data in a category 3/5 twisted pair cable to supply DC power to PDs.

Note: The power supplying mode is depending on the PD specifications. The selected mode shall supports PSE and PD at the same time. If the PSE and the PD power supplying mode are not the same (such as the PSE does not support the spare wire power supplying, or the PD supports spare wire supplying only), please use converter to provide power to the PD.

4. PD

PD refers to the device receiving power from the PSE. It includes IP phone, wireless AP, portable recharger, POS, network camera and etc.

When the PD enjoys the power from the PoE device, it can connect to other device to backup the power.

Refer to Table 7-1 for port detailed setup information.

Name	Note
Port	In the panel figure to select the PoE port. The select port(s) will be displayed in the Selected Ports list at the bottom of the interface.
Power Status	Enable or disable PoE on the selected ports. ● The system does not supply power to or reserve power for the PD connected to a PoE port if the PoE port is not enabled with the PoE function. ● You are allowed to enable PoE for a PoE port if 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. **Important** 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.
Total power consumption reserved value	It is to set PoE port total power consumption reserved value. The PoE total power consumption value refers to the total power consumption for the PD from the all PoE port When the connected PD power consumption is higher than the PoE total power consumption, it stops providing power to the PD.

Table 7-1

Refer to Figure 7-2 for setup interface.

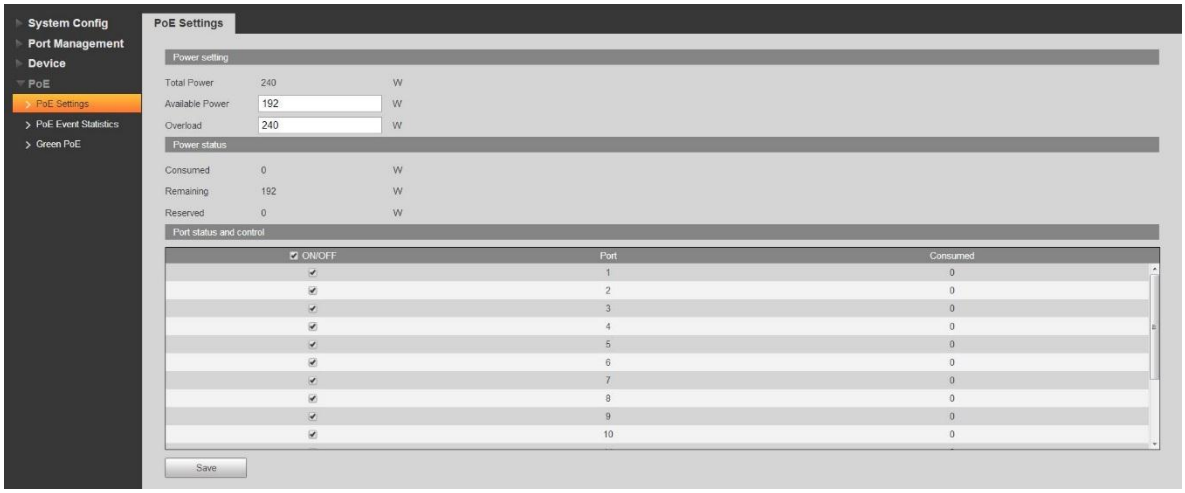


Figure 7-2

7.2 PoE Events

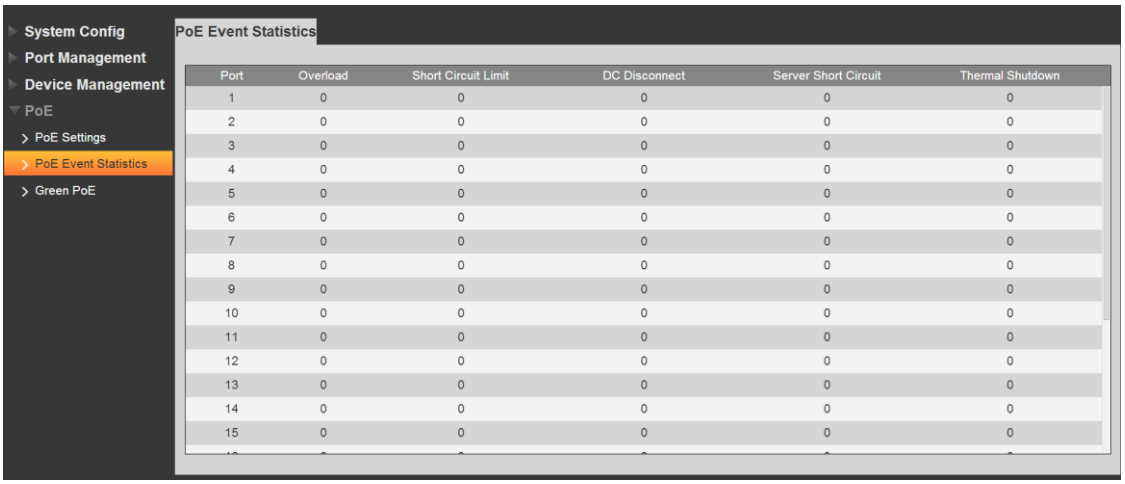


Figure 7-3

In Figure 7-3, it is to display the PoE event statistics of each port. It includes Overload, Short Circuit Limit, DC Disconnect, Server Short Circuit, and Thermal Shutdown.

Refer to Table 7-2 for PoE event parameters.

Name	Note
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
Server 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.

Table 7-2

7.3 Green PoE

In Figure 7-4, it is to set PoE energy-saving parameters. The PoE function is off in the specified period to save power. When the period is over, the port auto resumes providing power.

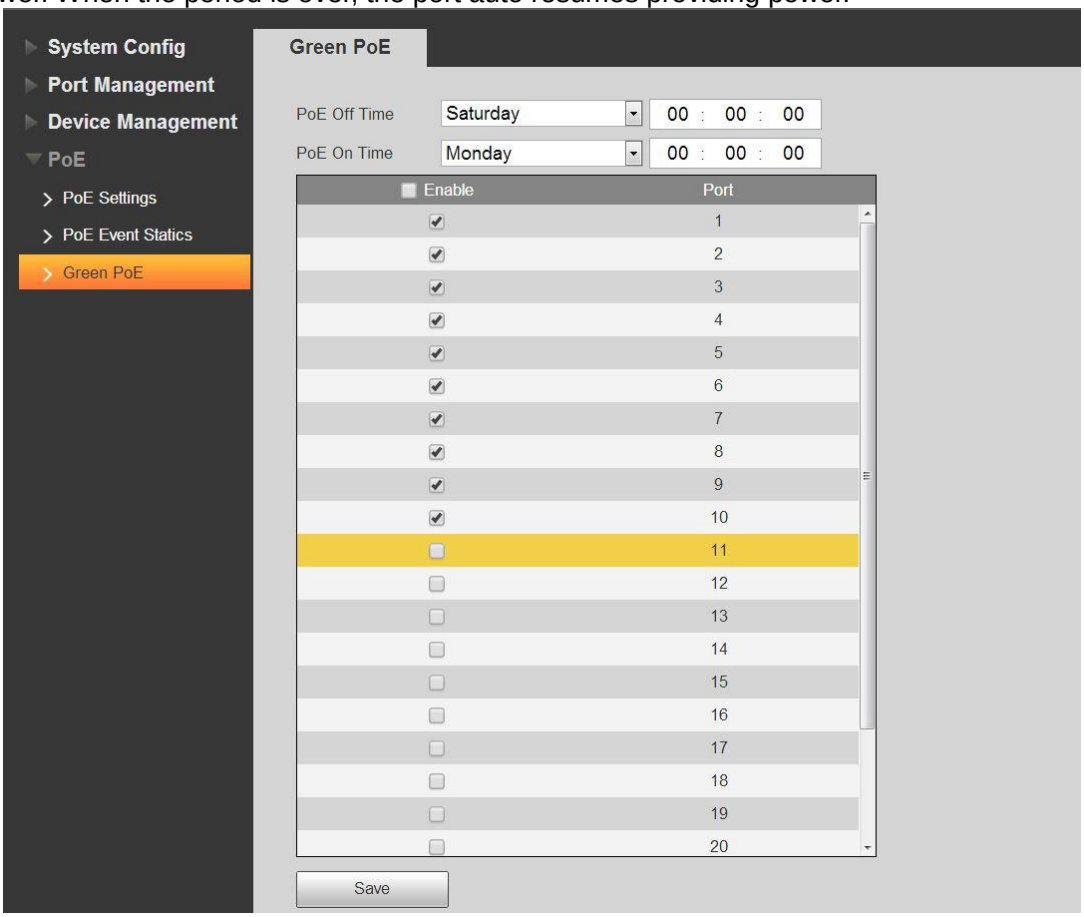


Figure 7-4

Refer to Table 7-3 for detailed Green PoE setup information.

Name	Note
PoE off time	The single port input current has exceeded its output port current threshold.
PoE on time	The sending port is short-circuit when the chip is proving power to the port.
Port	The ports to be selected.

Table 7-3

Config example.

1. Network connection

The port 1 to 10 is to shut down on each Saturday and each Sunday, and auto resumes on each Monday.

2. Settings

（1） Set the port off period is from Saturday to Sunday, and auto resume power on Monday.

（2） Set ports.

（3） Click Save. Refer to Figure 7-5 for detailed information.

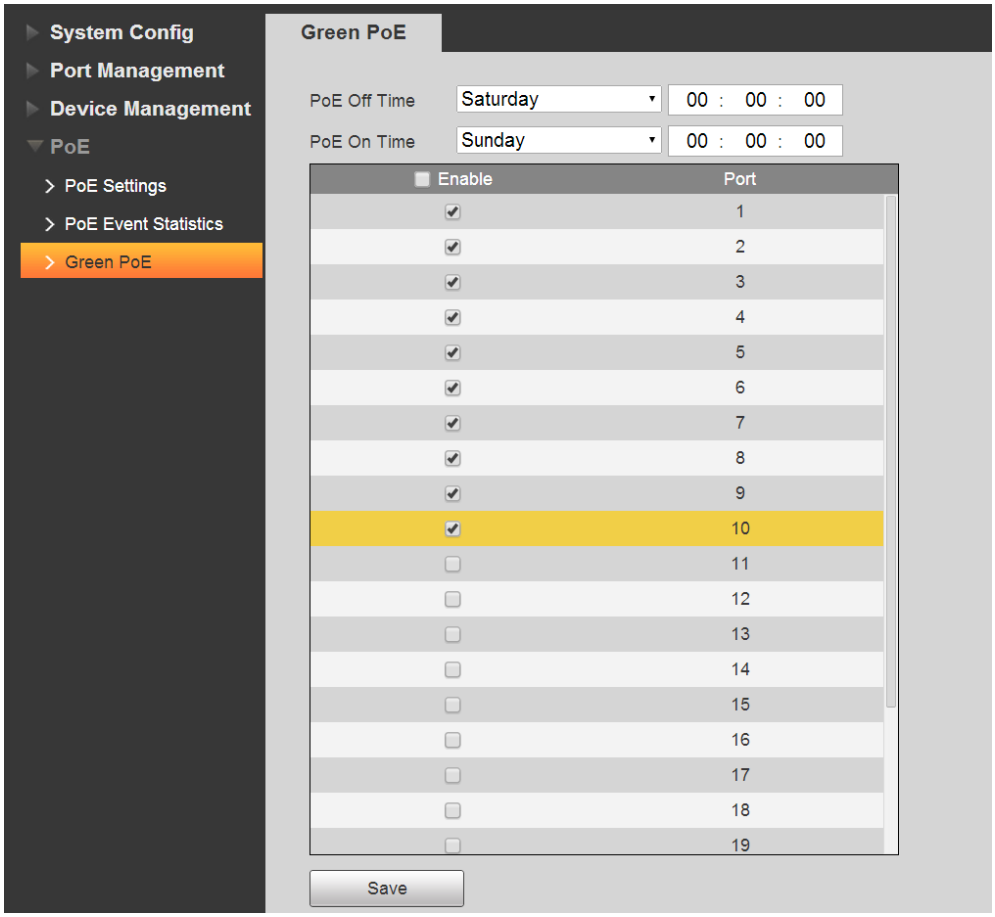

System Config
Port Management
Device Management
PoE
PoE Settings
PoE Event Statistics
Green PoE
Green PoE
PoE Off Time
Saturday
00 : 00 : 00
PoE On Time
Sunday
00 : 00 : 00
Enable
Port
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
Save

Figure 7-5

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199, Bin'an Road, Binjiang District, Hangzhou, P.R. China
Postcode: 310053
Tel: +86-571-87688883
Fax: +86-571-87688815
Email: overseas@dahuatech.com
Website: www.dahuasecurity.com