EN

User Manual

Gigabit Switch, Managed, 250W, 24x PoE, 4x SFP, 1000Mbps, Wall-/Rack mounting, Desktop

IAR-7SE2024MMA

About This Document

This document is **Web-based Configuration Guide,** including Web network management system (short for Web system) configuration instructions. It is intended for engineers or anyone who needs to configure the switch by Web system.

Announcement

The information in this document is subject to change without notice.

The document is only used as operation guide, except for other promises. No warranties of any kind, either express or implied are made in relation to the description, information or suggestion or any other contents of the manual.

The images shown here are indicative only. If there is inconsistency between the image and the actual product, the actual product shall govern.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
NOTE	Provides additional information to emphasize or supplement important points in the main text.

Content

1 Configuration Instruction

To facilitate configuration and the maintenance of the switch, the Web system is provided to users. You can log in the Web system to configure and maintain devices through the graphic user interface (GUI).

The Web-based configuration guide describes the configuration and maintenance of the switch through the Web system. It is intended for engineers or anyone who needs to configure the switch through the Web system.

Web System Overview

The Web system provides the functions as below.

- System Status
- Port Setting
- PoE (Only apply to PoE switches)
- VLAN
- QoS
- LACP
- Port Security
- Network Management
- Network Statistics
- System Management

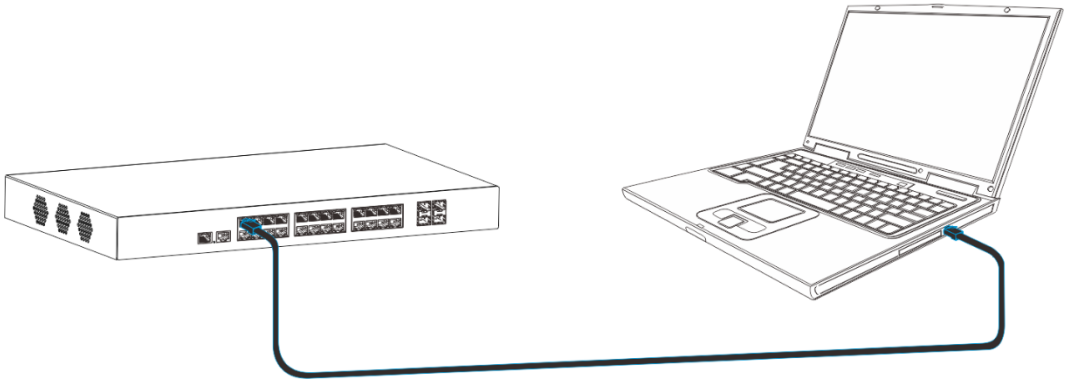
Please follow the instructions below to configure the Web system.

2 Environments Requirements

2.1 Hardware Requirements

The management PC recommended as below.

- Make sure the management PC has already been with Ethernet port.
- Use a network cable to connect the Ethernet port of PC and the Ethernet port of the switch.



2.2 Software Requirements

The browser version recommend as below.

- IE10 or higher
- Firefox browser
- Chrome

3 Set Up Network Connection

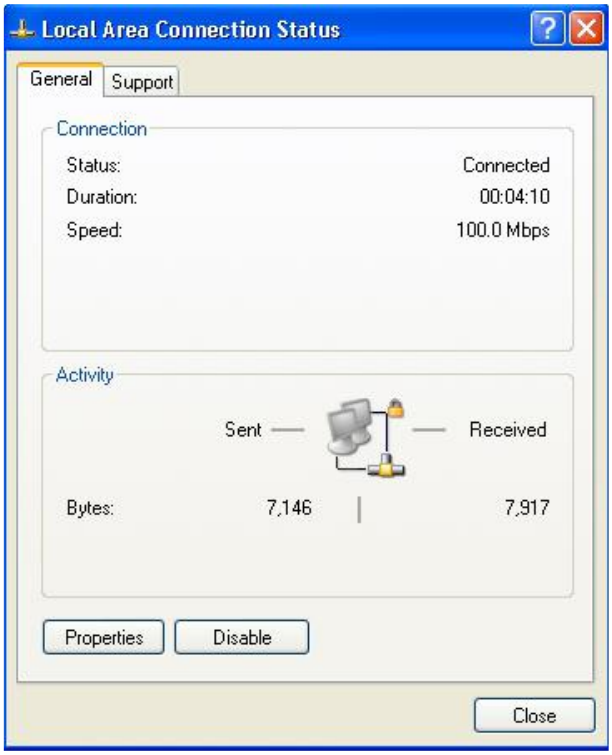
Before login the Web system to start configuration, users need to set up the network connection as follow steps.

- Set the IP of the PC and the switch in the same network segment. The default IP address of the switch is 192.168.1.200, network gate is 255.255.255.0.
- The port to connect management PC for Web setting must be management VLAN. By default, management VLAN is VLAN 1, and each port of the switch is VLAN1.
- If you need to connect the remote network, please make sure the management PC and the router can do the jobs above.
- This product can't assign the IP address for the management PC, please configure the management static IP manually before web configuration.

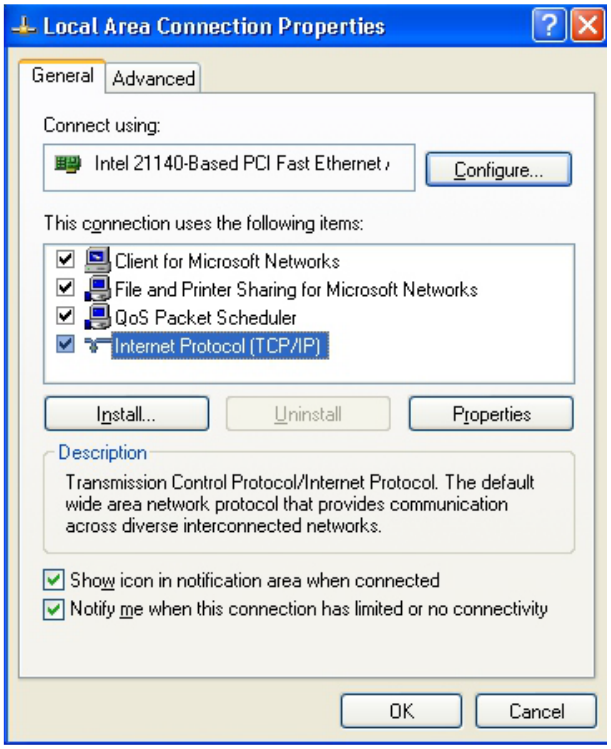
3.1 Set Static IP for the Management Computer

Operation steps (take Windows 7 as sample)：

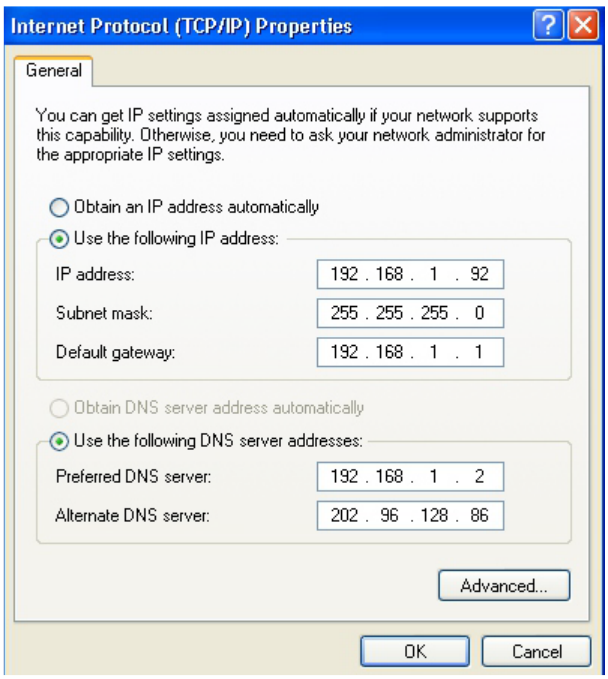
- Click <Start> to enter the <Start> menu, select <Control Panel> Double click <Network Connection> icon, then double click the <Local Connection> icon, <Local Area Connection Status> window pops out.



- Click <Property> button, enter <Local Area Connection Property> window.



- Select <Internet Protocol (TCP/IP)>, click <Property> button, enter <Internet Protocol (TCP/IP) Properties> window. Select the option <Use the following IP address>, input IP address (use arbitrary value between 192.168.1.1~ 192.168.1.254, except 192.168.1.200) and the subnet mask (255.255.255.0).
- Click "OK" to finish the configuration.



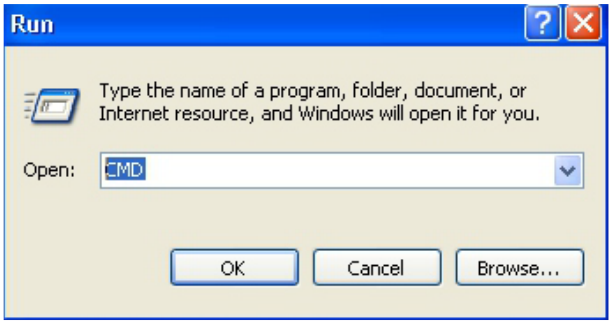
Note:

· DNS server address can be empty or be filled in with the real server address.

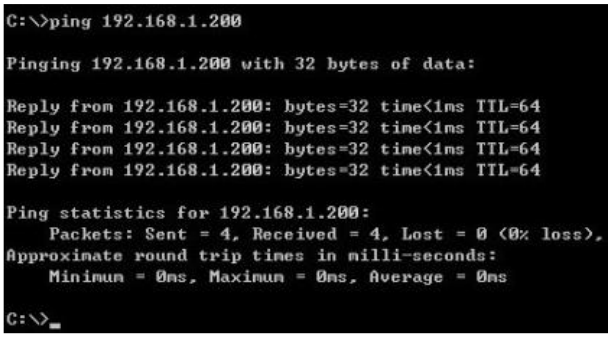
3.2 Confirm the Network Connection by Ping Command

Operation Steps as below:

- Click <Start> button to enter <Start> menu, select <Run>, popping out the dialog.



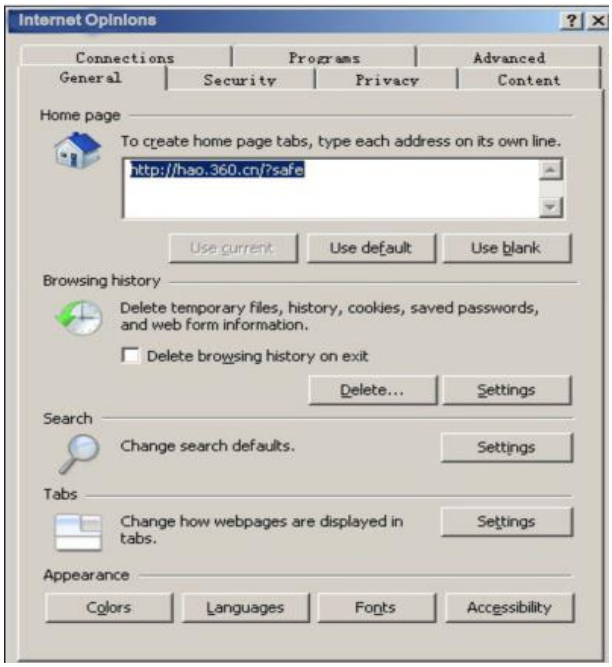
- Input "ping 192.168.1.200", and press enter. If there is equipment response displaying in the pop out dialog, that means network connection succeed, otherwise please check if the network connection is correct.



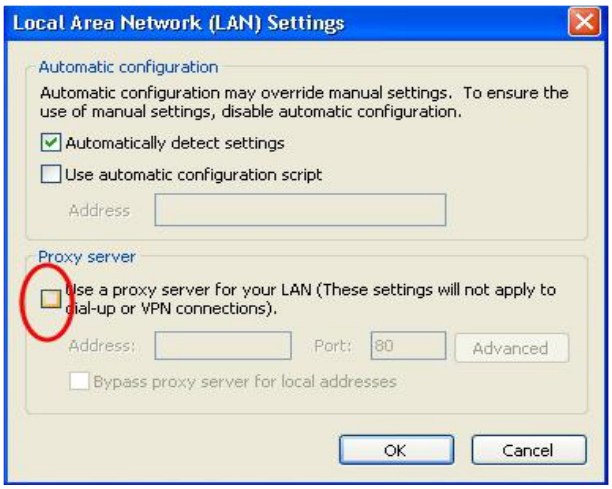
3.3 Cancel the Proxy Server

If this management PC uses proxy server to visit the internet, then the proxy service must be prohibited as follows:

- In browser, select <Tool/Internet Option> to enter <Internet Options> window.



- Select <Connections> tab in <Internet Options> window, and click <LAN Setting> button.



- Check if the <Use a proxy server for your LAN> option is selected. If selected, please deselect the option. Then click <OK> button.

Note:

- Please follow the steps to check if the switch is installed correctly:
- Whether the physical connection of the equipment is correct?
- Use network cable to connect the product's Ethernet port (except the console port) with managed computer network card, and ensure the link LED of the port is on.
- Whether the computer TCP/IP agreement setting is correct?
- Management PC's IP address must be 192.168.1.x (x range is 1~254 and x can't be 200, otherwise it will conflict with the product IP address 192.168.1.200), subnet mask: 255.255.255.0.
- Whether the computer's port VLAN ID is 1?
- By default, the management VLAN is VLAN 1, same as each port of switch.

Now the setting up tasks are finished.

Users can login the Web system and start configuration as following.

4 Login the Web System

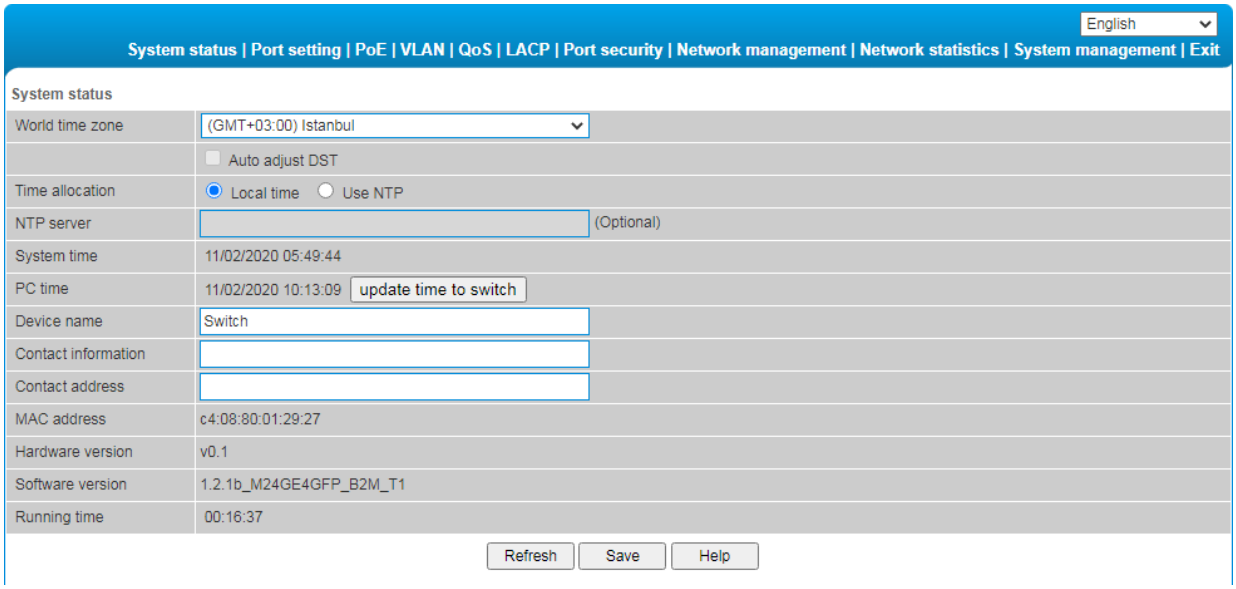
4.1 Login and Start

Open the browser, input the switch default address.

Press Enter, the user login page will show in front of you as follows.

Items	Default value
Switch default address	192.168.1.200
Subnet mask	255.255.255.0
Administrator's account	admin
Administrator's password	admin

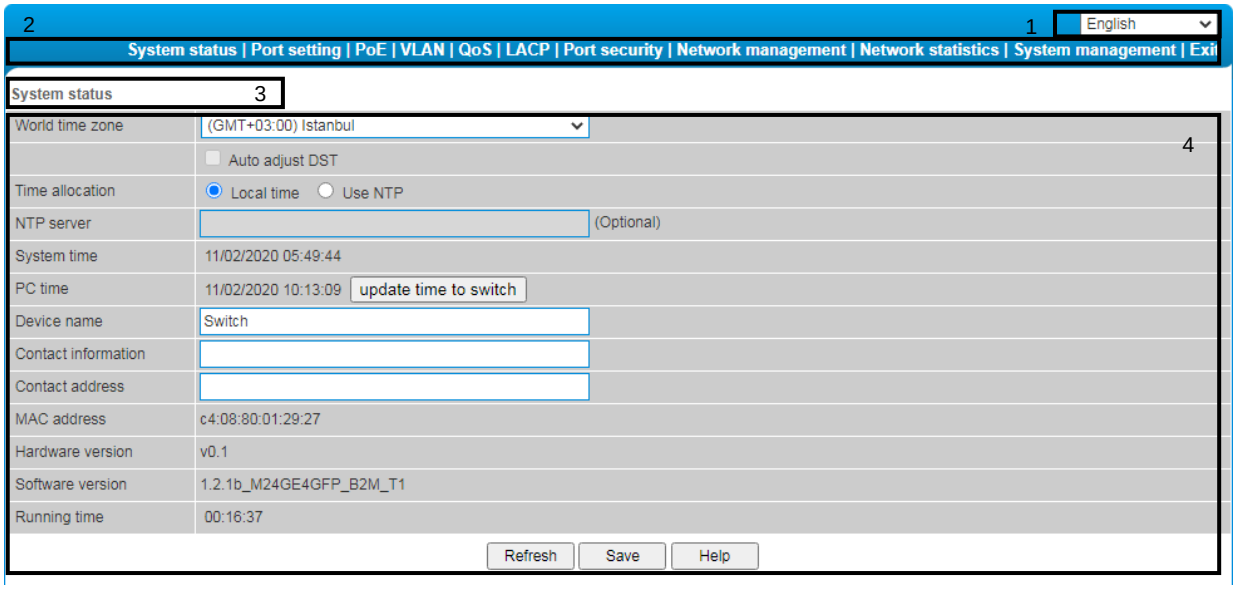
Input Administrator's account and password, press Enter, and click <Login in>, the Web system page will be shown as below:



4.2 Web System User Interface

Interface Layout

The layout and style of the Web system client GUI are described as follows.



Items	Descriptions
1	Language setting area
2	Navigation tree
3	Your Position
4	Configuration area

Operation Field and Buttons

The elements that users usually use on the Web system GUI are described as follows.

Items	Descriptions
	Input box. Please input the value as required.
Automatical	Drop down list box. Please choose the value as required.
Enable Disable	Enable/ disable option. Please choose as required.
Modify	Modify button. Click to change the configured parameter.
Add	Add button. Click to add the parameter into the system.
Delete	Delete button. Click to delete the parameter from the system.
Edit	Edit button. The same as <Modify>, click to change the configured parameter.
Save	Save button. Click to the save the configurations.

Refresh	Refresh button. Click to reload the page.

4.3 Saving Configuration

After performing configuration, users need to save the configuration data. If you do not save the configuration data, the configuration that you made will be lost after reboot.

To save configurations, please click the <Save> button at the bottom of the page to save the configuration data to memory.

4.4 Viewing Configuration

Finished configuration, click <Refresh> button on the page, users can view the saved configuration.

4.5 User Timeout

If users do not perform any operations on the Web system GUI for a long time, your account will be logged out and the login page is displayed.

The auto-log out interval time is 5 minutes by default.

If you need to continue operations, please log in again.

4.6 Logging-out Web System

To protect security of user accounts and switches, please log out of the Web system immediately after finishing the configurations.

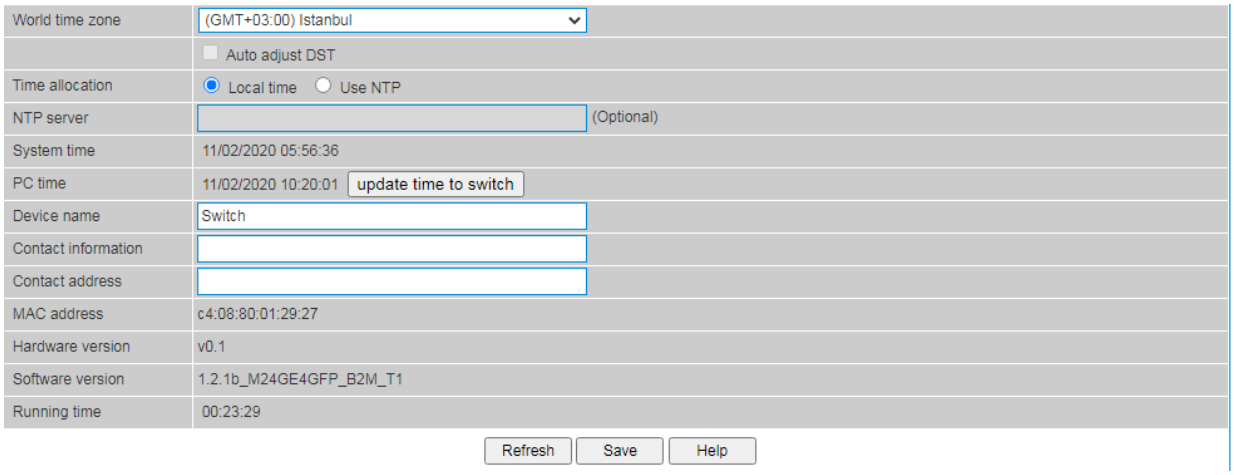
Users can log out of the Web system in either of the following ways:

- Click  on the top right corner of the page to close the browser.
- Click  on the top right corner of the page of Web system.

5 System Status

This chapter describes system status configuration. Users can configure system status and view the configuration information.

By default the switch supports local time setting.



Procedure

Choose <System Management> <Time> in the navigation tree to open the page.

- Local time.

  Set the parameters as required.

Items	Descriptions	Default value
World Time Zone	Display different time zones around the world. Select the time zone as required or “Auto Adjust DST”.	
Time Allocation	Choose local time.	
System Time	Display the current time of the system.	-
PC Time	Display the current time of management PC.	-
update time to switch	Click to update the <System Time> to synchronize with the <PC Time>.	-
Device Name	Name the switch by inputting the name.	-
Contact Information	Input the contact information.	-
Contact Address	Input the contact address.	-

  Click <Save>.

- Use NTP.

  Choose <Use NTP>. NTP is used when all the equipment clocks in the network have to be kept the same, meanwhile to ensure the accuracy of the clocks.

  Set the parameters as required.

Items	Descriptions	Default value
NTP Server	Enter the correct NTP server’s IP address to start setting.	Null

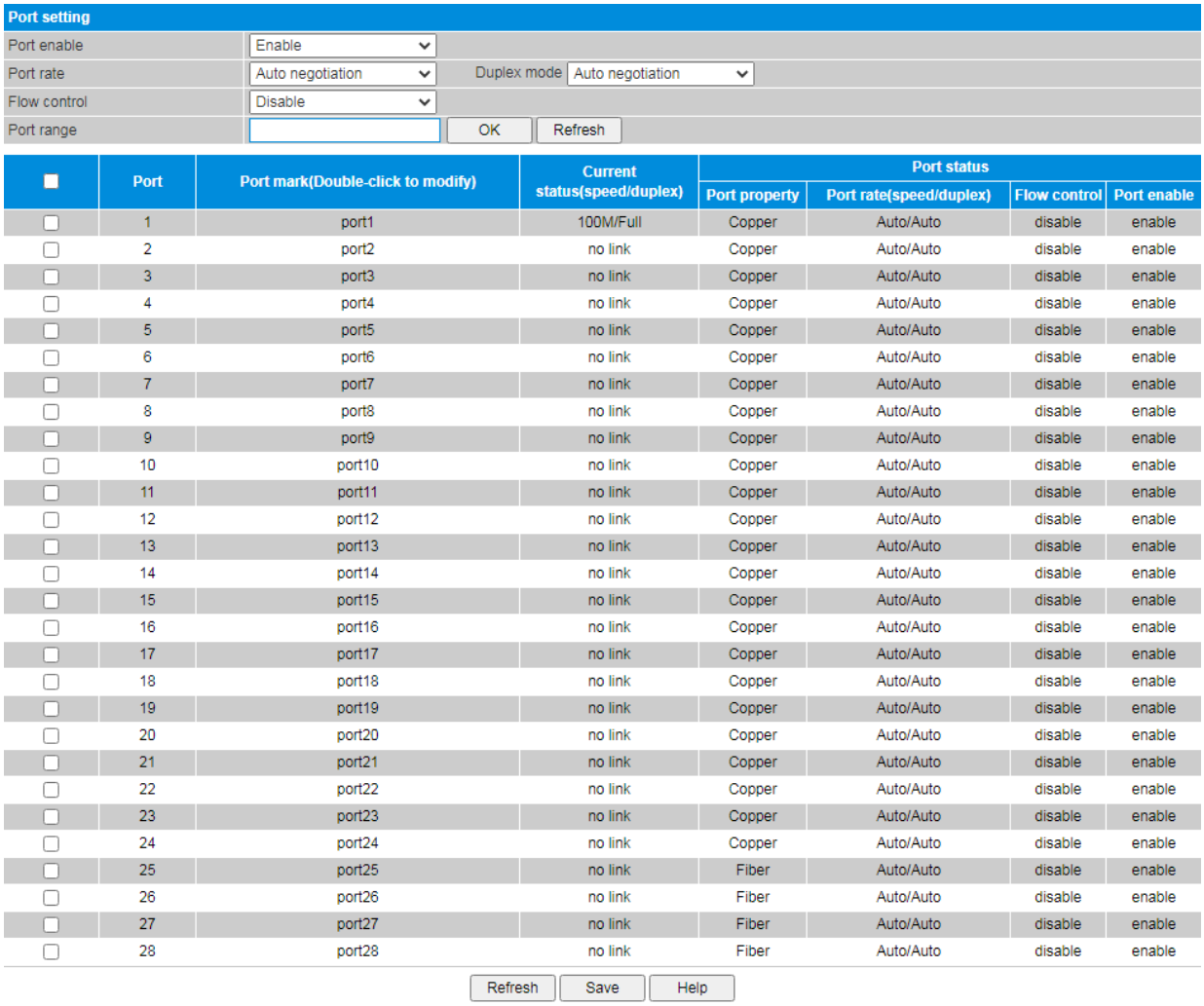
  Click <Save>.

6 Port Setting

This chapter describes Ethernet interface configurations. Users can configure the interfaces and view configuration information.

The switch provides Ethernet interfaces, Gigabit Ethernet interfaces. Configure these interfaces as required.

6.1 Port Setting



Port setting

Port enable	Enable		
Port rate	Auto negotiation	Duplex mode	Auto negotiation
Flow control	Disable		
Port range		OK	Refresh

	Port	Port mark(Double-click to modify)	Current status(speed/duplex)	Port status			
				Port property	Port rate(speed/duplex)	Flow control	Port enable
	1	port1	100M/Full	Copper	Auto/Auto	disable	enable
	2	port2	no link	Copper	Auto/Auto	disable	enable
	3	port3	no link	Copper	Auto/Auto	disable	enable
	4	port4	no link	Copper	Auto/Auto	disable	enable
	5	port5	no link	Copper	Auto/Auto	disable	enable
	6	port6	no link	Copper	Auto/Auto	disable	enable
	7	port7	no link	Copper	Auto/Auto	disable	enable
	8	port8	no link	Copper	Auto/Auto	disable	enable
	9	port9	no link	Copper	Auto/Auto	disable	enable
	10	port10	no link	Copper	Auto/Auto	disable	enable
	11	port11	no link	Copper	Auto/Auto	disable	enable
	12	port12	no link	Copper	Auto/Auto	disable	enable
	13	port13	no link	Copper	Auto/Auto	disable	enable
	14	port14	no link	Copper	Auto/Auto	disable	enable
	15	port15	no link	Copper	Auto/Auto	disable	enable
	16	port16	no link	Copper	Auto/Auto	disable	enable
	17	port17	no link	Copper	Auto/Auto	disable	enable
	18	port18	no link	Copper	Auto/Auto	disable	enable
	19	port19	no link	Copper	Auto/Auto	disable	enable
	20	port20	no link	Copper	Auto/Auto	disable	enable
	21	port21	no link	Copper	Auto/Auto	disable	enable
	22	port22	no link	Copper	Auto/Auto	disable	enable
	23	port23	no link	Copper	Auto/Auto	disable	enable
	24	port24	no link	Copper	Auto/Auto	disable	enable
	25	port25	no link	Fiber	Auto/Auto	disable	enable
	26	port26	no link	Fiber	Auto/Auto	disable	enable
	27	port27	no link	Fiber	Auto/Auto	disable	enable
	28	port28	no link	Fiber	Auto/Auto	disable	enable

Refresh Save Help

Procedure

Choose <Port Setting> <Port Setting> in the navigation tree to open the page.

- Enable the function.
- Configure the interfaces.

Items	Descriptions	Default value
Port Enable	Choose <Enable> to enable the function. If a port is disable, it can't forward data.	Enable
Port Rate	Indicates the interface speed, including: · Auto negotiation · 10 Mbits/s · 100 Mbits/s · 1000 Mbits/s	Auto Negotiation

	· 10 Gbits/s (please refer to the actual switch) When the port rate is auto negotiation, the port can automatically and directly connected the device on the other side to negotiate the port speed.	
Duplex Mode	Indicates the duplex mode of the interface, including · Auto negotiation · Full duplex · Half duplex To enable an interface to send and receive packets at the same time, enable the full duplex mode on the interface. To disable an interface from sending and receiving packets at the same time, enable the half duplex mode on the interface.	Auto Negotiation
Flow Control	Enable/disable the flow control function. If two switches have enabled the function, when one of them has be congested, it will send message to the other switch to notify it to temporarily stop sending messages or slow down the sending speed. Once receiving the message, the other one will stop sending or slow down the sending speed of messages so as to avoid packet loss and ensure normal operation of network services.	Disable
Port Range	Select the ports that need to be set. Multiple interfaces can be selected.	Null

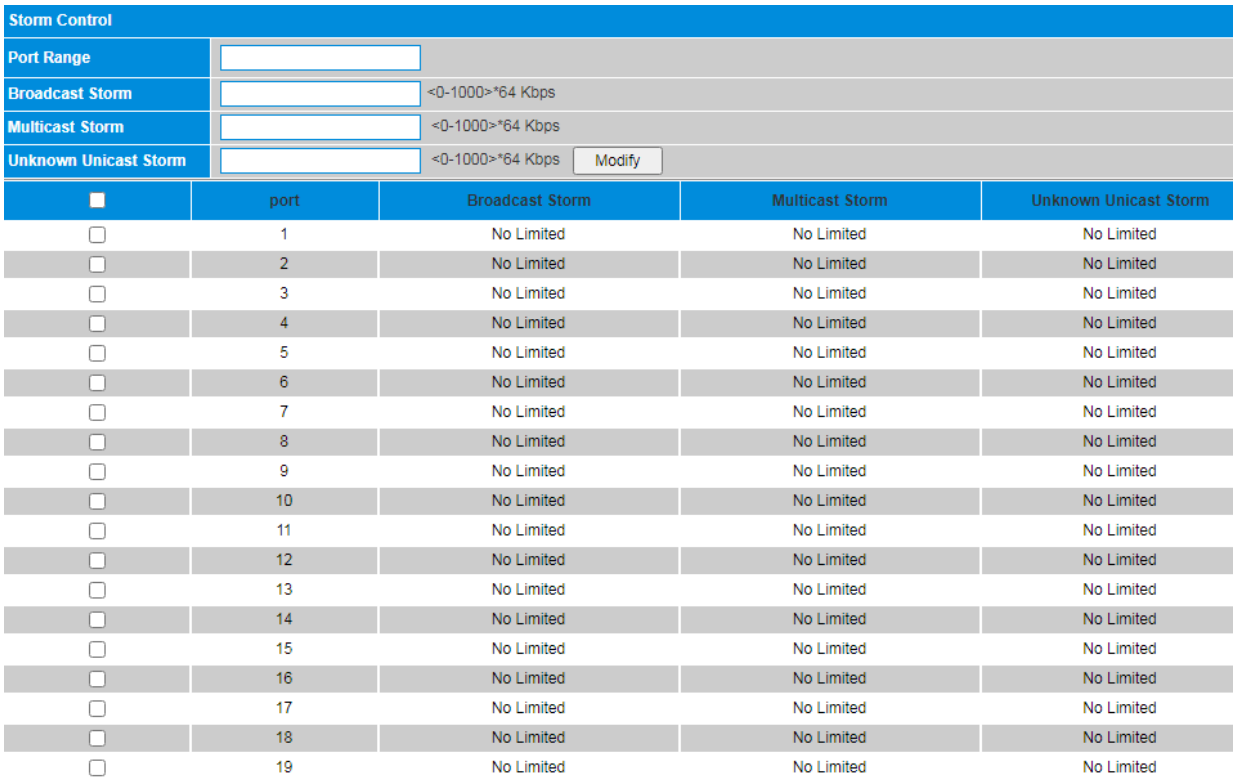
Click <OK> to change the configuration.

Click <Save>.

6.2 Storm

Storm control prevents broadcast storms and ensures device forwarding performance.

To limit the rate of incoming broadcast packets, multicast packets, and unknown unicast packets and prevent heavy traffic on a device, users can configure storm control on an interface.



	port	Broadcast Storm	Multicast Storm	Unknown Unicast Storm
☐	1	No Limited	No Limited	No Limited
☐	2	No Limited	No Limited	No Limited
☐	3	No Limited	No Limited	No Limited
☐	4	No Limited	No Limited	No Limited
☐	5	No Limited	No Limited	No Limited
☐	6	No Limited	No Limited	No Limited
☐	7	No Limited	No Limited	No Limited
☐	8	No Limited	No Limited	No Limited
☐	9	No Limited	No Limited	No Limited
☐	10	No Limited	No Limited	No Limited
☐	11	No Limited	No Limited	No Limited
☐	12	No Limited	No Limited	No Limited
☐	13	No Limited	No Limited	No Limited
☐	14	No Limited	No Limited	No Limited
☐	15	No Limited	No Limited	No Limited
☐	16	No Limited	No Limited	No Limited
☐	17	No Limited	No Limited	No Limited
☐	18	No Limited	No Limited	No Limited
☐	19	No Limited	No Limited	No Limited

Procedure

Choose <Port Setting> <Storm> in the navigation tree to open the page.

- Configure the interfaces.

  Set the parameters as required.

Items	Descriptions	Default value
Port Range	Select the ports that need to be set. Multiple interfaces can be selected.	Null
Broadcast Storm	Configure the broadcast storm control. The value ranges from 1 to 1000. When the value is null, there is no limit.	Null
Multicast Storm	Configure the multicast storm control. The value ranges from 1 to 1000. When the value is null, there is no limit.	Null
Unknown Unicast Storm	Configure the unicast storm control. The value ranges from 1 to 1000. When the value is null, there is no limit.	Null

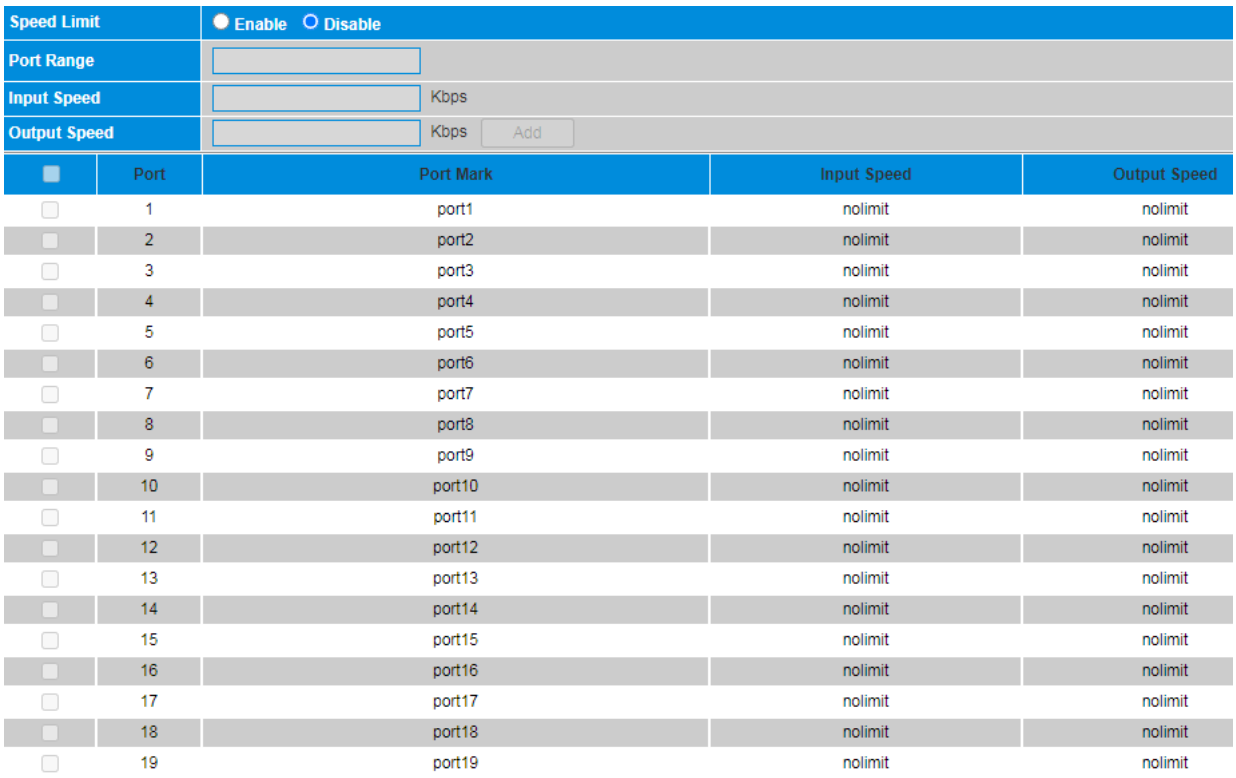
  Click <Edit> to change the configuration.

  Click <Save>.

6.3 Speed Limit

The switch provides port-based entry speed limit. Users can restrict every port traffic flows or cancel port flow restriction. Users can choose a fixed rate, the range is: downlink ports 1～1000Mbps, uplink port 1～1000Mbps, the accuracy is 1Mbps. Port restrictions including unicast packets, multicast packets and broadcast packets.

Users can view detailed information about interface-based rate limiting. Before sending traffic from an interface, users can configure rate limit on the interface in the outbound direction to control all outgoing packets, and configure rate limit on the interface inbound direction to control all incoming packets.



Port	Port Mark	Input Speed	Output Speed
1	port1	nolimit	nolimit
2	port2	nolimit	nolimit
3	port3	nolimit	nolimit
4	port4	nolimit	nolimit
5	port5	nolimit	nolimit
6	port6	nolimit	nolimit
7	port7	nolimit	nolimit
8	port8	nolimit	nolimit
9	port9	nolimit	nolimit
10	port10	nolimit	nolimit
11	port11	nolimit	nolimit
12	port12	nolimit	nolimit
13	port13	nolimit	nolimit
14	port14	nolimit	nolimit
15	port15	nolimit	nolimit
16	port16	nolimit	nolimit
17	port17	nolimit	nolimit
18	port18	nolimit	nolimit
19	port19	nolimit	nolimit

Procedure

Choose <Port Setting> <Speed Limit> in the navigation tree to open the page.

- Enable the function.
- Configure the interfaces.

Items	Descriptions	Default value
Port Range	Select the ports that need to be set. Multiple interfaces can be selected.	Null
Input Speed	The max input rate of port. The value ranges 64 kbps ~1000000 kbps. When the value is null, there is no rate limit for the interfaces.	Null
Output Speed	The max output rate of port. The value ranges 64 kbps ~1000000 kbps. When the value is null, there is no rate limit for the interfaces.	Null

Click <Edit> to change the configuration.

Click <Save>.

7 PoE

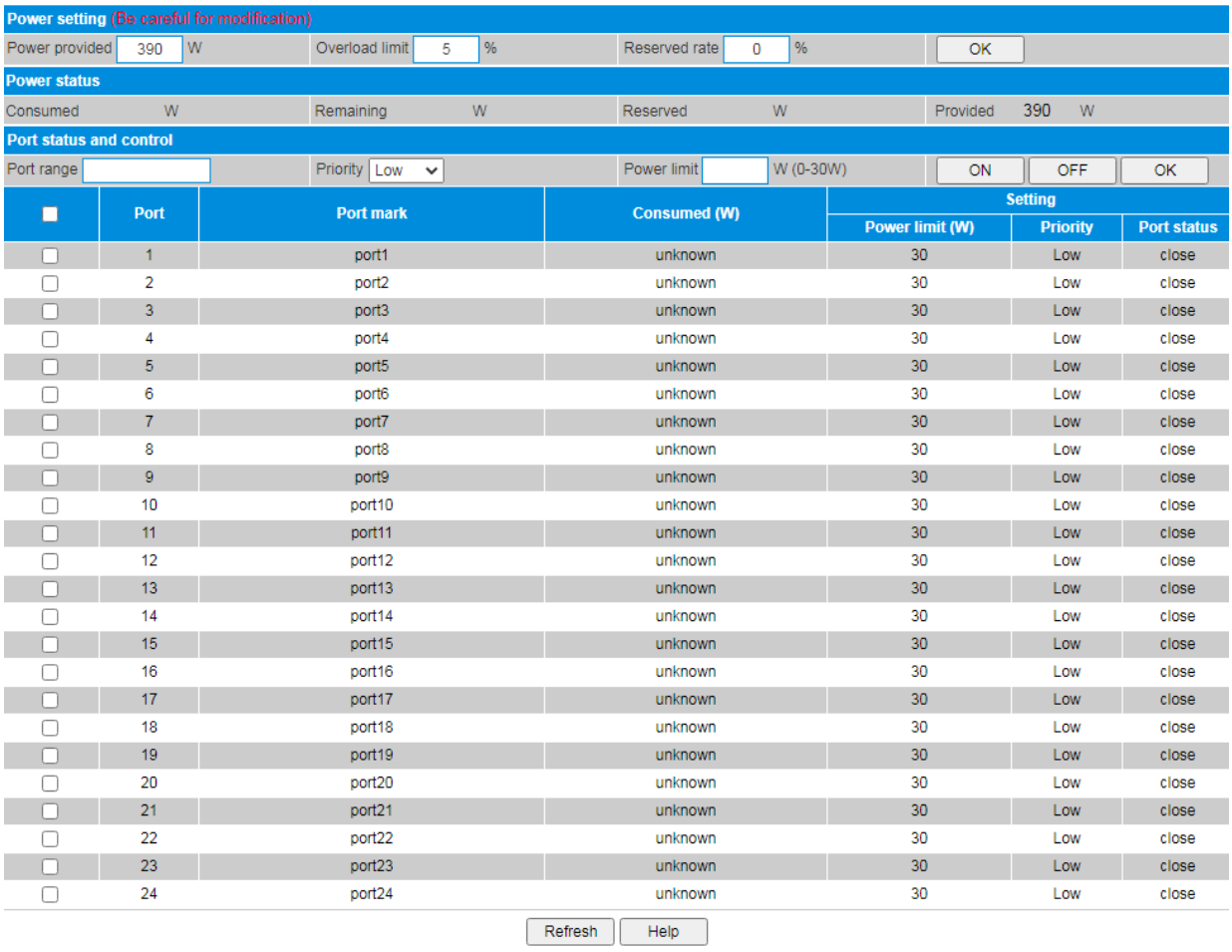
This chapter describes PoE (Power-over-Ethernet) configurations. Users can configure the output power of the switch and the interfaces.

This chapter only applies to the switches that support PoE function.

7.1 Power Control

Currently, the network devices are deployed flexibly; therefore, the cabling of power supply is complicated. To simplify cabling, users can configure the PoE function on the switch.

Users can set global PoE parameters and the PoE parameters on an interface, and view the PoE status of the switch and interfaces.



Procedure

Choose <PoE> <Power Control> in the navigation tree to open the page.

- Set global PoE parameters.

Set the parameters as required.

Items	Descriptions	Default value
PoE Provided	Input the maximum provided power of the switch. The value is less than the full load power consumption of the switch.	Based on the switch type.

Overload Limit	The limit percentage that allows over the preset <Power Provided> value. The value is less than 10%. This parameter is optional.	5%
Reserved Rate	Input the reserved rate from the preset <Power Provided> value. The value ranges from 0 to 100%. The switch supports reserved power function for reliability. The actual value of input power the switch divides to the interfaces (named as V) is equal to the value of <Power Provided> minus the value of <Power Provided> multiplies <Reserved Rate>. If the required input power of the switches over the value of real input power, the reserved power will be divided to each port as further demand. This parameter is optional.	0%

Click <OK> to save the configuration.

- The current power status will be displayed in the items of <Power status> as below.

Items	Descriptions
Consumed Power	The total actual output power of all the interfaces.
Remaining	The actual remained input power of the switch, not including the reserved power.
Reserved	The actual reserved power of the switch. The value is equal to the value of <Power Provided> minus <Remaining>.
Provided	The preset input power. The value is equal to <Power budget >.

- Set the PoE parameters on an interface as required.

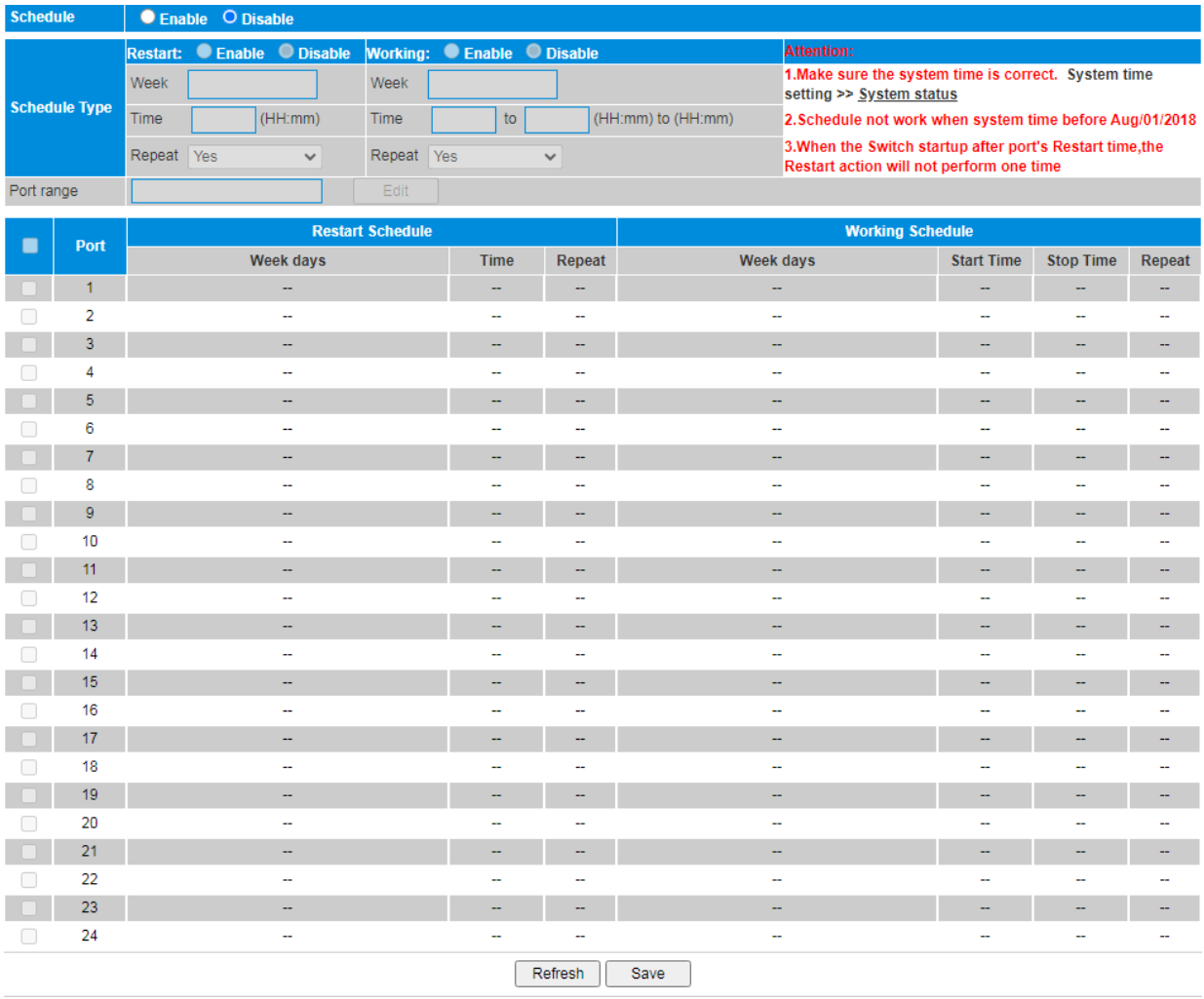
Items	Descriptions	Default value
Port Range	Select the ports that need to be set. Multiple interfaces can be selected.	Null
Priority	Indicates the power priority of an interface, including · Low · Middle · High In the same priority, the interfaces with larger port number will be shut off first when the power is not enough.	Low
Power Limit	Input the maximum output power of the interfaces. The value ranges from 0 to the max power of each interface. Please refer to the specifications of the switch.	Null
ON	Click the button, and click <Edit> to enable the PoE function of the selected interfaces.	Enable
OFF	Click to disable the PoE function of the selected interfaces.	_

Click <OK> to save the configuration.

7.2 Schedule

The PoE function of each interface can be set to restart and work regularly.

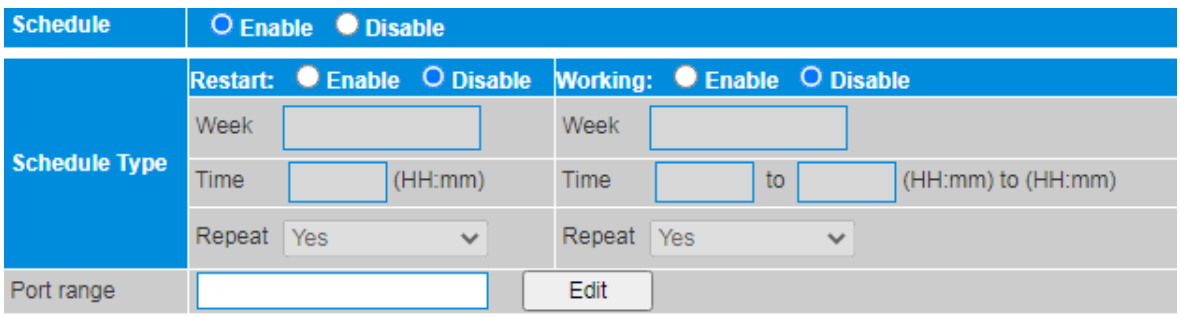
The function is disable by default.



Procedure

Choose <PoE> <Schedule> in the navigation tree to open the page.

- Enable the function.



Configure the restarting and working schedule type of the switch and Set the parameters as required.

Items	Descriptions	Default value
Restart		

Enable/disable	Choose enable to enable the function.	Disable
Week	Select on which day of the week the PoE function of selected interfaces restart. Multiple days can be selected.	Null
Time	Set the restart time, the format is as 13:00, the function will restart at 13:00:59.	Null
Repeat	Choose yes, the PoE of the selected interfaces will restart at setting time weekly. Choose no, it will only restart one time at this week.	Yes
Port range	Select the ports that need to be set. Multiple ports can be selected.	Null
Working		
Enable/disable	Choose enable to enable the function.	Disable
Week	Select on which day of the week the PoE function of selected interfaces work. Multiple days can be selected.	Null
Time…to…	Set the working duration, the function will start and stop as setting. The time format is as 13:00, the function will start or stop at 13:00:59. Outside this time period, the PoE function of selected interfaces will be disable.	Null
Repeat	Choose yes, the PoE function of the selected interfaces will start and stop at setting time weekly. Choose no, it will only work at setting this week.	Yes
Port range	Select the ports that need to be set. Multiple ports can be selected.	Null

Click <Edit> to change the configuration.

Click <Save>.

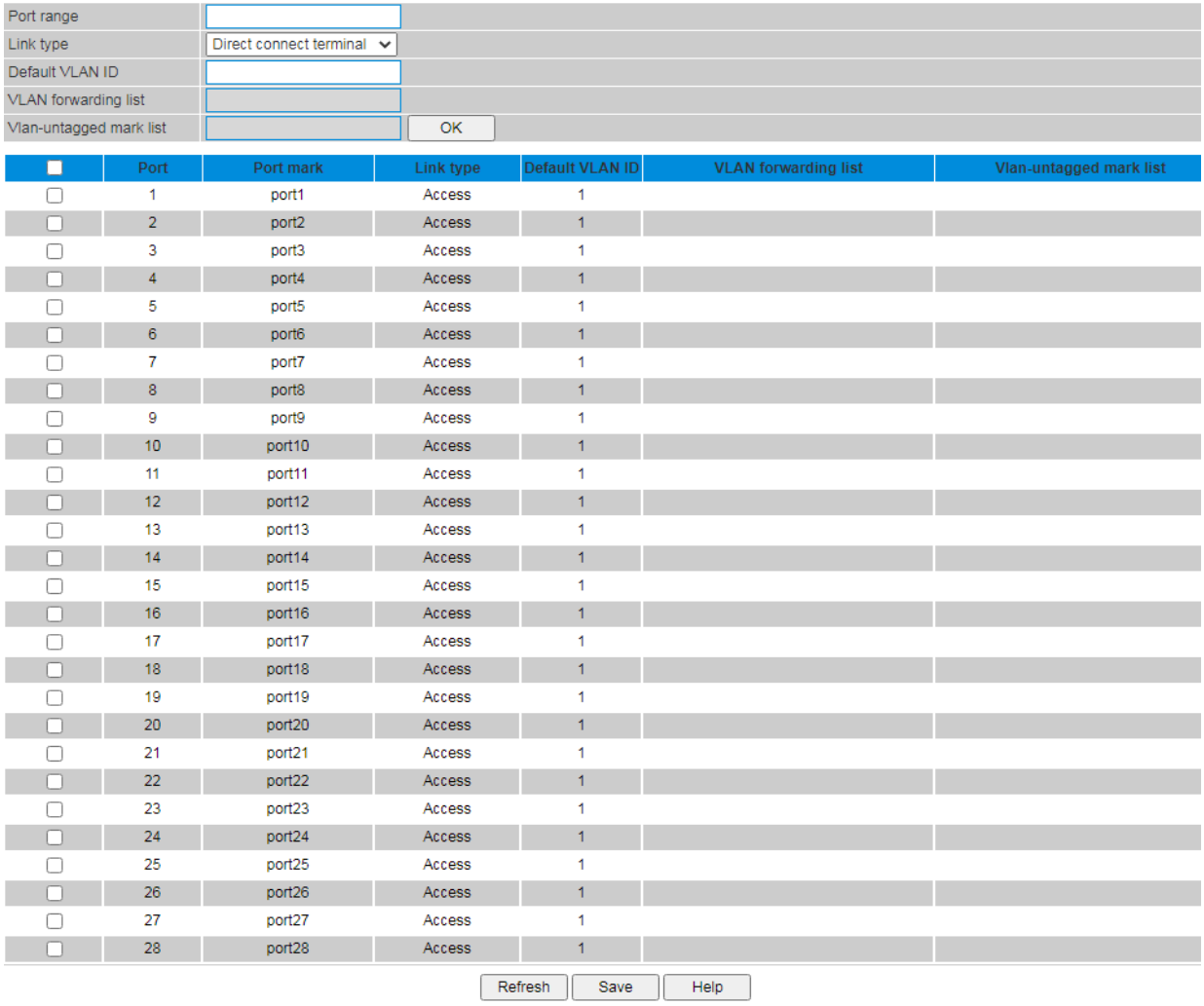
8 VLAN

This chapter describes how to configure and query VLANs.

A local area network (LAN) can be divided into several logical LANs. Each logical LAN is a broadcast domain, which is called a virtual LAN (VLAN). To put it simply, devices on a LAN are logically grouped into different LAN segments, regardless of their physical locations. VLANs isolate broadcast domains on a LAN.

8.1 Port VLAN

The switch supports to define VLAN members according to switch port. After specify the port to a VLAN, specified VLAN packets can be forwarded by the port.



Procedure

Choose <VLAN> <Port VLAN> in the navigation tree to open the page.

- Configure VLAN.

Items	Descriptions	Default value
Port Range	Select the ports that need to be set. Multiple interfaces can be selected.	Null
Link Type	Link type of the interfaces, including · Access: ports normally used for connecting devices, only belongs to one VLAN. By default, all ports are Access ports.	Access

	· Trunk: ports belonging to multiple VLAN, can receive and send multiple VLAN packets.	
Default VLAN ID	Input the default VLAN ID of the interface. The value ranges from 1 to 4094. Note: If the VLAN ID of the port changes, the VLAN ID of the switch connecting with this port must be changed to the same.	Null
VLAN Forwarding List	Input ID of VLAN that allowed to access in Trunk. VLAN packets can be transferred, other will be discarded. The value ranges from 1 to 4094.	Null
VLAN Untagged Mark List	Input ID of untagged VLAN in Trunk. The value ranges from 1 to 4094.	Null

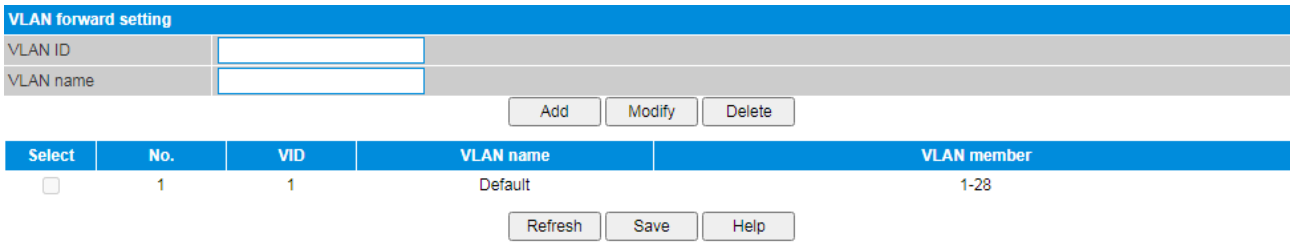
Click <OK>.

Click <Save>.

8.2 VLAN Forward

The switch supports to add, modify and delete the VLAN.

VLAN 1 is the default VLAN and cannot be deleted.



Procedure

Choose <VLAN> <VLAN Forward> in the navigation tree to open the page.

- Create a VLAN.

Items	Descriptions	Default value
VLAN ID	Input the VLAN ID. The value ranges from 1 to 4094.	Null
VLAN Name	Input the description of the VLAN	Null

Click <Add>.

Click <Save>.

- Modify a VLAN.

Select the VLANID.

Set the parameters as required.

Click <Modify>.

Click <Save>.

- Delete a VLAN.

Select the VLAN that need to be deleted.

Click <Delete>.

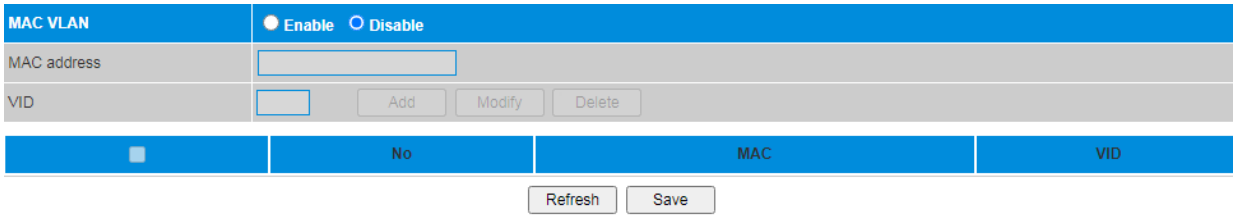
Click <Save>.

8.3 MAC-based VLAN

The switch supports to divide VLAN based on MAC address of the devices.

Dividing VLAN based on MAC address. In this way, the security of users can be further improved (the VLAN configuration will not be easily changed illegally).

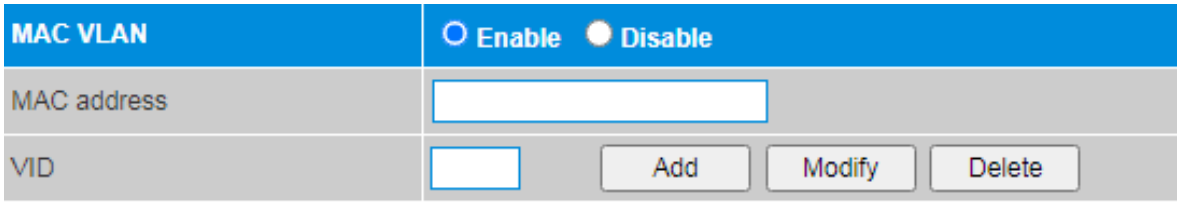
The function is disable by default.



Procedure

Choose <VLAN> <MAC-based VLAN> in the navigation tree to open the page.

- Enable the MAC-based VLAN function.



- Add a VLAN.

Items	Descriptions	Default value
MAC Address	Input the MAC address that need to be set.	Null
VID	Input the VLAN ID. The value ranges from 1 to 4094.	Null

Click <Add>.

Click <Save>.

- Modify a VLAN.

Select the VLAN that need to be modified.

Set the parameters as required.

Click <Modify>.

Click <Save>.

- Delete a VLAN.

Select the VLAN that need to be deleted.

Click <Delete>.

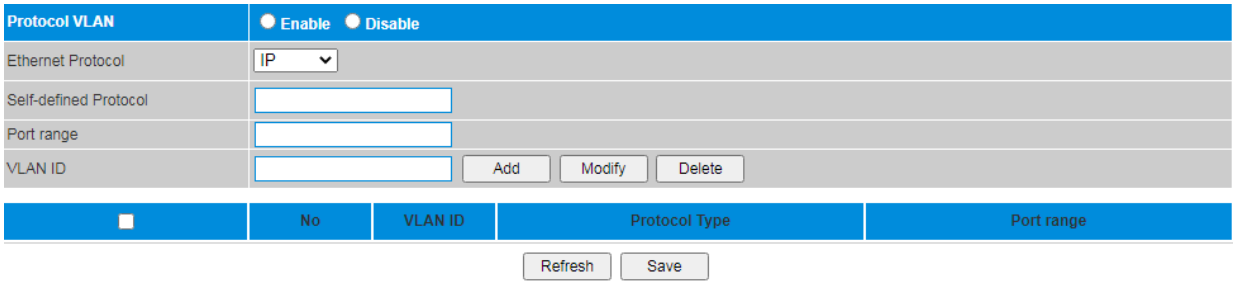
Click <Save>.

8.4 Protocol-based VLAN

The switch supports to divide VLAN based on the protocols, including Ethernet protocol and private protocol.

The supporting Ethernet protocols are as follows.

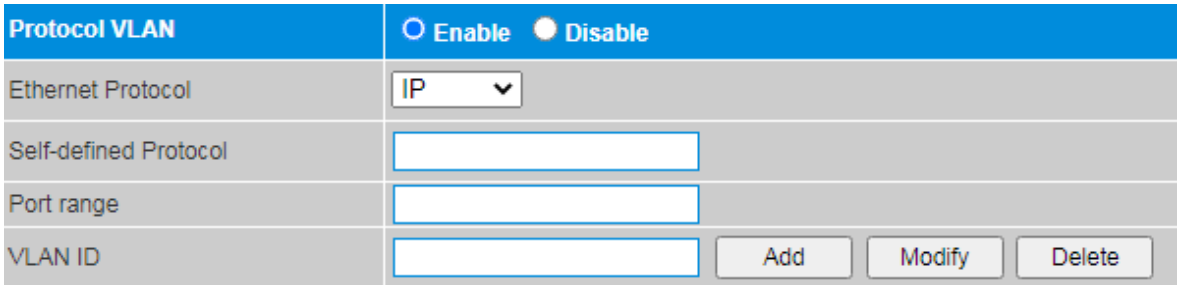
- IP
- ARP
- RARP
- IPv6
- PPPoE
- MPLS
- IS-IS
- LACP
- 802.1x



Procedure

Choose <VLAN> <Protocol-based VLAN> in the navigation tree to open the page.

- Enable the function.



- Create a VLAN.

Items	Descriptions	Default value
Ethernet Protocol	Choose the protocol.	Null
Self-defined Protocol	Input the private protocol.	Access
Port Range	Select the ports that need to be set.	Null
VLAN ID	Input the VLAN ID of the interface. The value ranges from 1 to 4094.	Null

Click <Add>.

Click <Save>.

- Modify a VLAN.

Select the VLAN that need to be modified.

Set the parameters as required.

Click <Modify>.

Click <Save>.

- Delete a VLAN.

  Select the VLAN that need to be deleted.

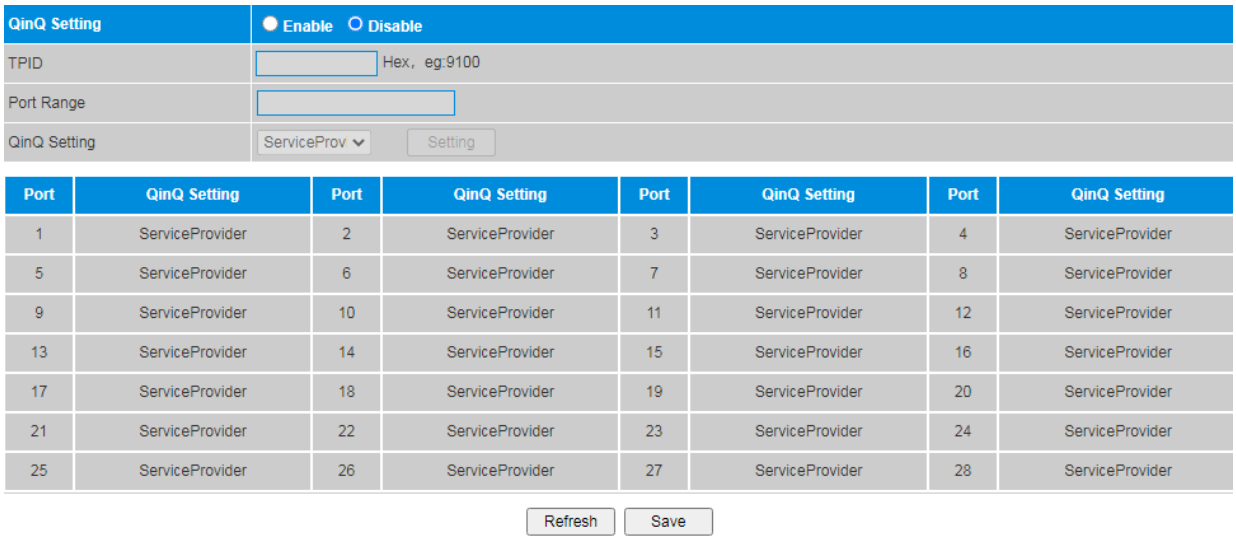
  Click <Delete>.

  Click <Save>.

8.5 QinQ

The switch supports QinQ function.

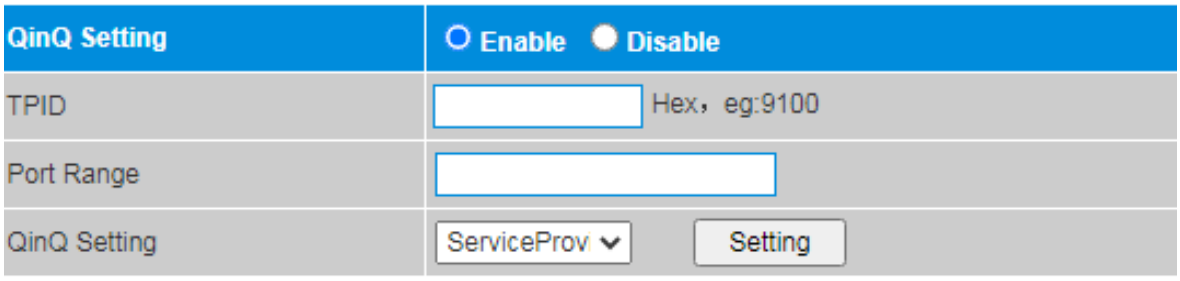
802.1Q-in-802.1Q (QinQ) technology improves VLAN utilization by adding another 802.1Q tag to a frame with an 802.1Q tag. In this case, frames from private VLAN tags can be transparently transmitted on the public network. A frame transmitted on the backbone network has double 802.1Q tags (one for the public network and the other for the private network), that is, 802.1Q-in-802.1Q (QinQ).



Procedure

Choose <VLAN> <GVRP> in the navigation tree to open the page.

- Enable the function.



- Set ports QinQ function.

Items	Descriptions	Default value
TPID	Tag Protocol Identifier. The TPID supports customization. Input the TPID.	Null
Port Range	Select the ports that need to be set.	Null
QinQ Setting	Choose which does the VLAN belong, including: · Service Provider: operator's VLAN	Service Provider

	· Customer: user's VLAN	

Click <Setting>.

Click <Save>.

8.6 PVLAN

The switch supports to divide PVLAN (private VLAN).

Two kinds of VLAN of PVLAN:

- Primary VLAN: Transmit traffic from the promiscuous port to the isolation, community, and other main promiscuous ports within the same VLAN.
- Secondary VLAN: Secondary VLAN includes two VLAN types:

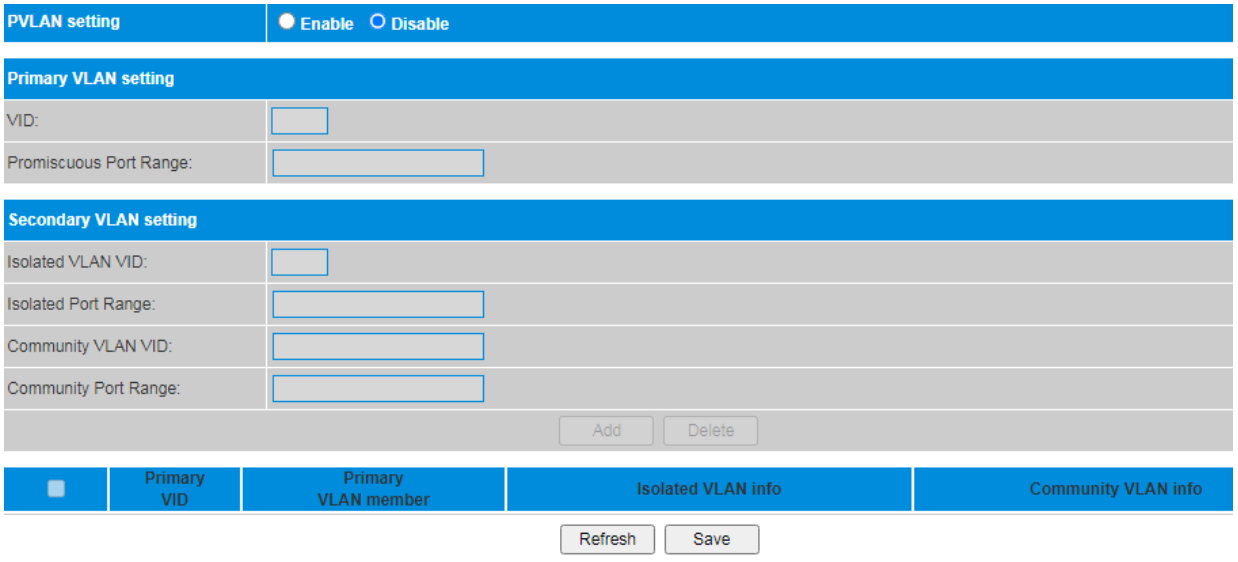
  Isolated VLAN: Transfer traffic from an isolated port to a promiscuous port. Isolate the port in the VLAN so that it cannot communicate with any other ports inside the PVLAN (another community VLAN port or a port in the same isolated VLAN). To communicate with other ports, you must traverse the promiscuous port.

  Community VLAN: Transmit traffic between the community ports in the same community VLAN and send it to the promiscuous port. The ports in the community VLAN can communicate with each other at layer 2 (only in the same community VLAN), but cannot communicate with ports of other community or isolated VLAN. To communicate with other ports, you must traverse the promiscuous port.

The PVLAN function is disable by default.

CAUTION

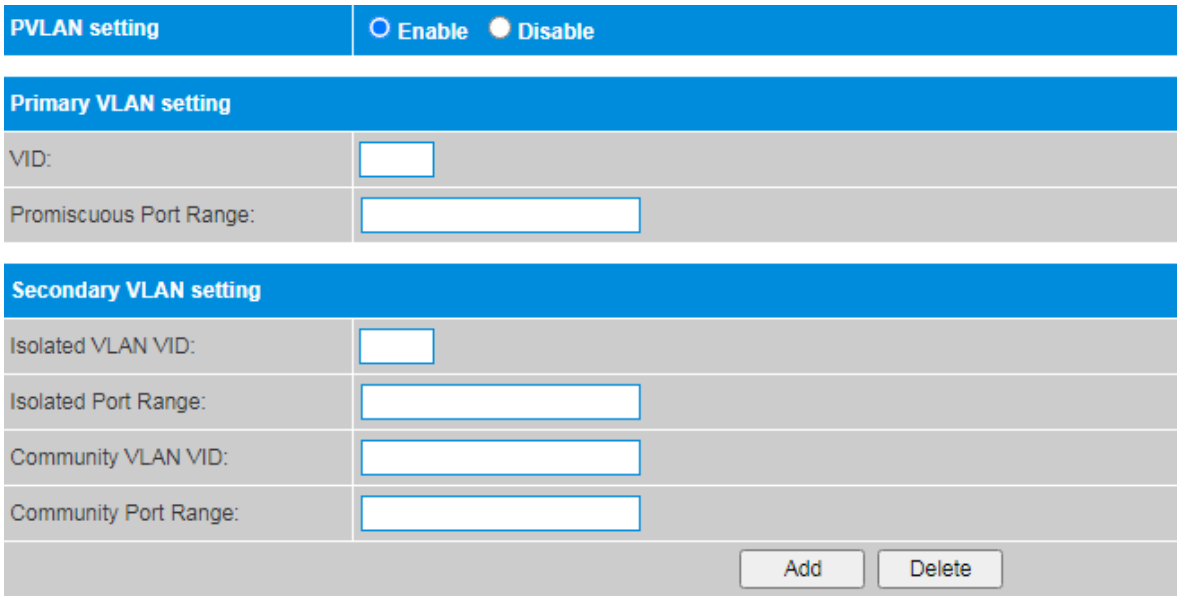
The PVLAN must be set with VLAN Forwarding List. The port or VLANID in PVLAN and VLAN Forwarding List can't be the same. Or the PVLAN would remove the port or delete the VLANID from the VLAN Forwarding List.



Procedure

Choose <VLAN> <PVLAN> in the navigation tree to open the page.

- Enable the PVLAN function.



- Add a primary VLAN.

Items	Descriptions	Default value
Primary VLAN Setting		
VID	Input the VLAN ID of primary VLAN. The value ranges from 1 to 4094.	Null
Promiscuous Port Range	Select the port range of the promiscuous VLAN. Belonging to "Primary VLAN", a promiscuous port can communicate with all interfaces, including isolated and community ports in PVLAN; the function of promiscuous port is to transfer traffic between the community and the isolated VLAN ports.	Null
Secondary VLAN Setting		
Isolated VLAN VID	Input the VLAN ID of the isolated VLAN.	Null
Isolated Port Range	Select the port range of the isolated VLAN. It is separated from all other ports in the PVLAN, except the promiscuous port; the traffic from the isolated port is only transmitted to the promiscuous port.	Null
Community VLAN VID	Input the VLAN ID of the community VLAN.	Null
Community Port Range	Select the port range of the community VLAN. It logically combines the various ports and promiscuous ports in the same area, and traffic can be transmitted between them.	Null

Click <Add>.

Click <Save>.

- Delete a primary VLAN.

Select the VLAN that need to be deleted.

Click <Delete>.

Click <Save>.

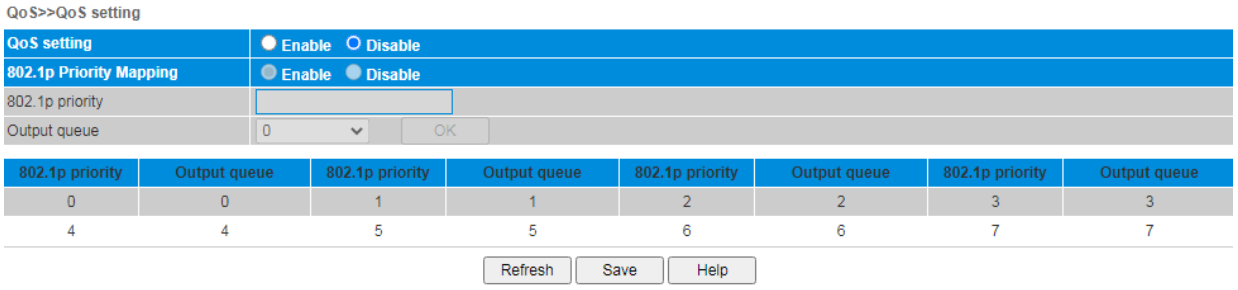
9 QoS

This chapter describes QoS (Quality of Service) and DSCP (Differentiated Services Code Point) configuration.

9.1 QoS Setting

QoS is a common concept in various occasions where there is a relationship between supply and demand of services. It evaluates the ability of service providers to meet customer needs. In Internet, QoS evaluates the service capability of network forwarding packet. Since the services provided by the network are diverse, the evaluation of QoS can be based on different aspects. QoS, as commonly referred to, is the evaluation of the service capability to support core requirements such as delay, jitter and packet loss rate in the process of packet forwarding.

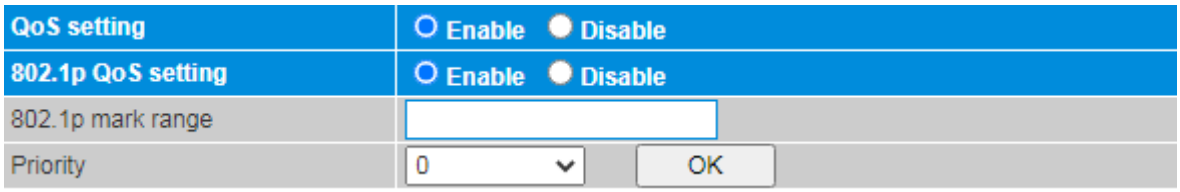
The function is disable by default.



Procedure

Choose <QoS> <QoS Setting> in the navigation tree to open the page.

- Enable the QoS setting function.
- Enable the 802.1p QoS Setting.



- Set the function.

Items	Descriptions	Default value
802.1p Mark Priority	Identify the priority. It includes 8 levels, from 0~7. By default the value is 0.	0
Priority	Choose the output queue. The switch supports setting 8 priorities, and the option is from 0 to 7.	0

Click <OK>.

Click <Save>.

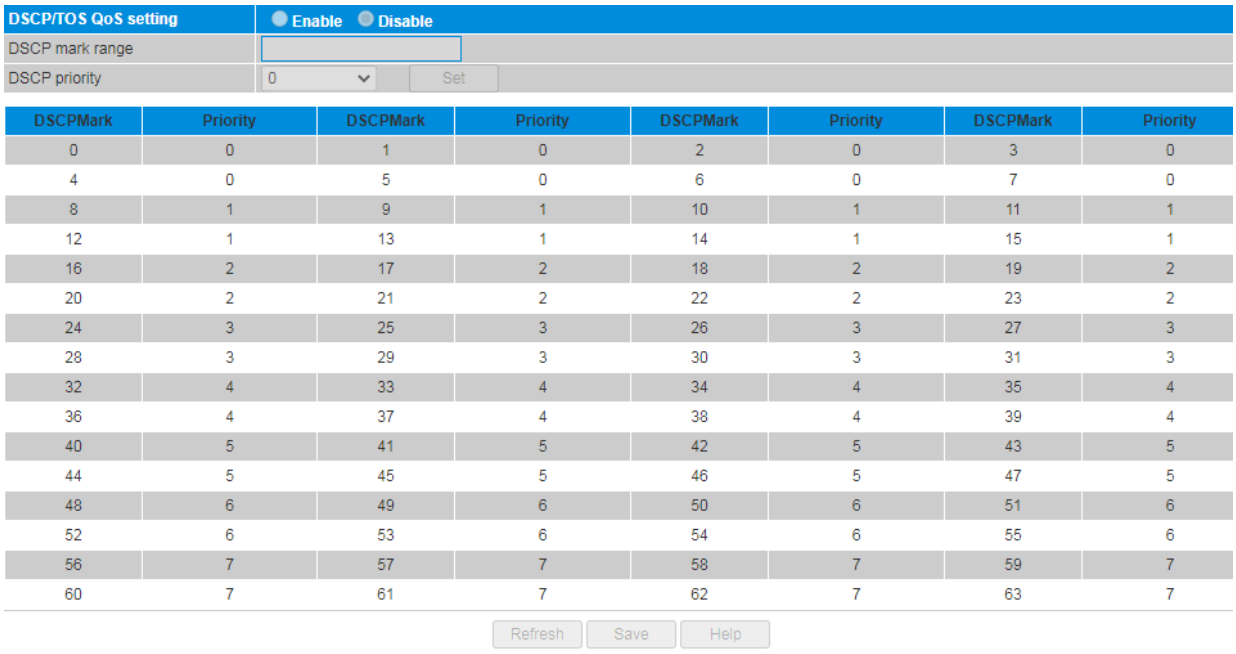
9.2 DSCP

Configure DSCP to maps DSCP priorities of packets to new DSCP priorities so that it can provide differentiated services.

The function is disable by default.

CAUTION

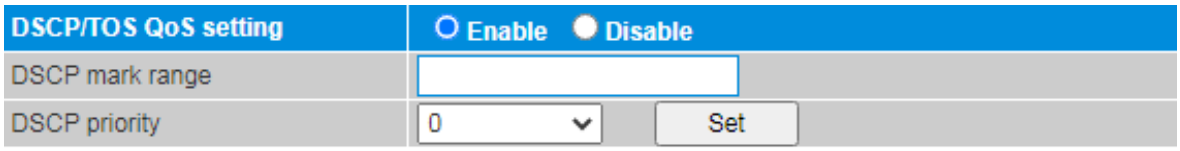
This function does not supports setting when the QoS setting and 802.1p Priority Mapping function are disable. Please enable the functions first.



Procedure

Choose <QoS> <DSCP> in the navigation tree to open the page.

- Enable the DSCP Priority Mapping function.



- Set the DSCP function.

Items	Descriptions	Default value
DSCP Mark Range	Identifies DSCP value range. The value ranges from 0~63. Format as “2” or “1-5” or “3, 1-5”.	Null
DSCP Priority	Choose the output queue. The switch supports setting 8 priorities, and the option is from 0 to 7.	0

Click <Set>.

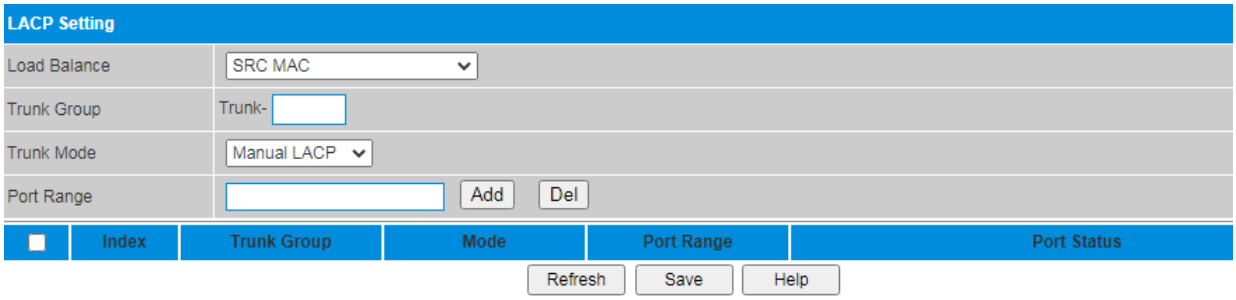
Click <Save>.

10 LACP

10.1 TRUNK

Link aggregation is a technology that bundles multiple Ethernet links into a logical link to increase bandwidth, improve reliability, and load balance traffic.

The switch supports manual LACP and static LACP trunk mode. Users can create link aggregation group, configure load pattern mode, working mode and members of link aggregation group, and delete the group.



Procedure

Choose <LACP> <TRUNK> in the navigation tree to open the page.

- Create link aggregation group and configuration.

Items	Descriptions	Default value
Load Balance	Choose the aggregation load pattern, including · SRC MAC: Source MAC · DST MAC: Destination MAC · SRC MAC + DST MAC: Source and Destination MAC · SRC IP: Source IP · DST IP: Destination IP Address · SRC IP + DST IP: Source and Destination IP Address	SRC MAC
Trunk Group	Indicates the trunk number. The value ranges from 1 to 8.	Null
Trunk Mode	Choose the aggregation pattern, including · Manual Aggregation: not under LACP protocol, by setting register to make aggregation. · Static LACP Aggregation: under LACP protocol, manually configured by the user, and the system is not allowed to automatically add or delete ports in the aggregation group.	Manual Aggregation
Port Range	Input the port number. Multiple interfaces can be selected. The value ranges from 1 to the max port number. Format as “2” or “1-5” or “3, 1-5”.	Null

Click <Add>.

Click <Save>.

- Delete trunk.

  Choose the trunk that need to be deleted.

  Click <Delete>.

  Click <Save>.

10.2 RSTP

The switch supports STP and RSTP.

The Spanning Tree Protocol (STP) trims a ring network into a loop-free tree network. It prevents replication and circular propagation of packets. The Rapid Spanning Tree Protocol (RSTP) was developed based on STP to implement faster convergence. RSTP defines edge ports and provides protection functions.

Loops often occur on a complex network. On a complex network, to implement redundancy, network designers tend to deploy multiple physical links between two devices, one of which is the master and the others are the backup.

Loops cause broadcast storms. Consequently, network resources are exhausted and the network breaks down. Loops also damage MAC addresses.

To remove loops, run STP at the data link layer. Devices running STP exchange STP BPDUs to discover loops on the network and block some ports to prune the network into a loop-free tree network. STP prevents infinite looping of packets to ensure packet processing capabilities of switches.

Because STP provides slow convergence, IEEE 802.1w released RSTP in 2001. RSTP enhances STP and speeds up network convergence.

Users can configure global parameter and ports parameters of Rapid Spanning Tree.

RSTP setting	Enable Disable				
STP Version					
Device priority	32768				
Sending message interval	2	second (1-10)			
Maximum message lifetime	6	second (6-40)			
Changing port status delay	4	second (4-30)			
Network bridge information	RSTP				

Modify configuration	Path expenditure	Port priority	Point to point port	Edge port
	0	0	No	Yes
Port range		Modify		

	Port	Por mark	Path expenditure	Port priority	Point to point port	Edge port
	1	port1	automatic detection	128	automatic detection	NO
	2	port2	automatic detection	128	automatic detection	NO
	3	port3	automatic detection	128	automatic detection	NO
	4	port4	automatic detection	128	automatic detection	NO
	5	port5	automatic detection	128	automatic detection	NO
	6	port6	automatic detection	128	automatic detection	NO
	7	port7	automatic detection	128	automatic detection	NO
	8	port8	automatic detection	128	automatic detection	NO
	9	port9	automatic detection	128	automatic detection	NO
	10	port10	automatic detection	128	automatic detection	NO
	11	port11	automatic detection	128	automatic detection	NO
	12	port12	automatic detection	128	automatic detection	NO
	13	port13	automatic detection	128	automatic detection	NO
	14	port14	automatic detection	128	automatic detection	NO
	15	port15	automatic detection	128	automatic detection	NO
	16	port16	automatic detection	128	automatic detection	NO
	17	port17	automatic detection	128	automatic detection	NO
	18	port18	automatic detection	128	automatic detection	NO
	19	port19	automatic detection	128	automatic detection	NO
	20	port20	automatic detection	128	automatic detection	NO
	21	port21	automatic detection	128	automatic detection	NO
	22	port22	automatic detection	128	automatic detection	NO
	23	port23	automatic detection	128	automatic detection	NO
	24	port24	automatic detection	128	automatic detection	NO
	25	port25	automatic detection	128	automatic detection	NO
	26	port26	automatic detection	128	automatic detection	NO
	27	port27	automatic detection	128	automatic detection	NO
	28	port28	automatic detection	128	automatic detection	NO

Refresh Save Help

Procedure

Choose <LACP> <RSTP> in the navigation tree to open the page.

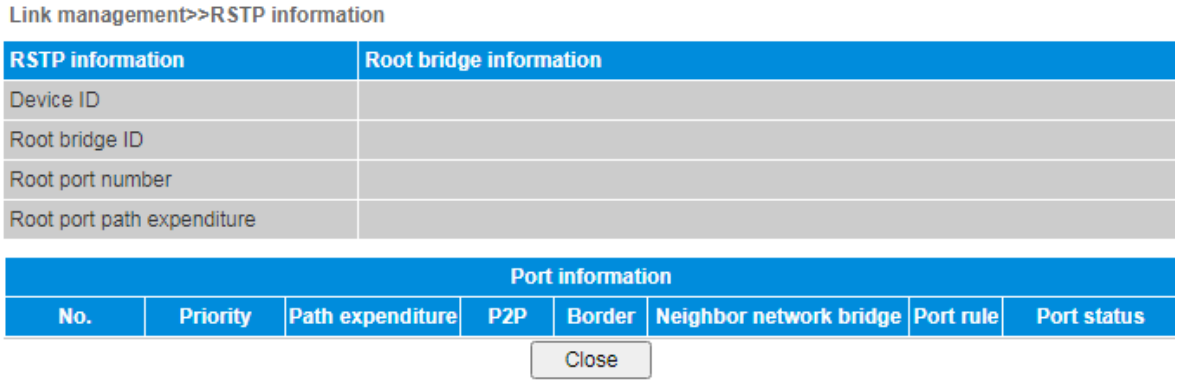
- Enable the function.

RSTP setting	Enable Disable	
STP Version		
Device priority	32768	
Sending message interval	2	second (1-10)
Maximum message lifetime	6	second (6-40)
Changing port status delay	4	second (4-30)
Network bridge information	RSTP	

- Configure global parameters.

Items	Descriptions	Default value
STP Version	Choose the STP version, including two types: · STP · RSTP	Disable
Device Priority	Choose the priority of the switch. The lager number takes lower priority. Step length: 4096.	32768
Sending Message Interval	Input the interval time to send message. The value ranges from 1 to 10.	2s
Maximum Message Lifetime	Input the maximum lifetime of the message. The value ranges from 6 to 40.	20s
Changing Port Status Delay	Input the interval time of state transition delay for the ports. The value ranges from 4 to 30.	15s

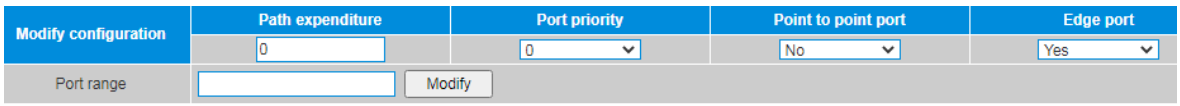
Click <RSTP> button to view the current RSTP information for the bridge.



Click <Close> to exit.

Click <Save>.

- Configure ports parameters.



Items	Descriptions	Default value
Path Expenditure	Indicates the path cost of local port and target port. The value ranges from 0 to 200,000,000. 0 means auto detect. On an STP/RSTP network, the accumulated cost of path from a port to the root bridge consists of all path costs of ports on the passed bridges. This cost is called root path cost, which determines root port selection.	0
Port Priority	Choose the priority of the port. The lager number takes lower priority. Step length: 16.	128
Point to Point Port	Choose the state of point-to-point, including · No. · Yes.	No

	· Auto Detect	
Edge Port	Choose <Yes> to enable the edge port. Choose <No> to disable the edge port.	No
Port Range	Select the ports that need to be set. Multiple interfaces can be selected.	Null

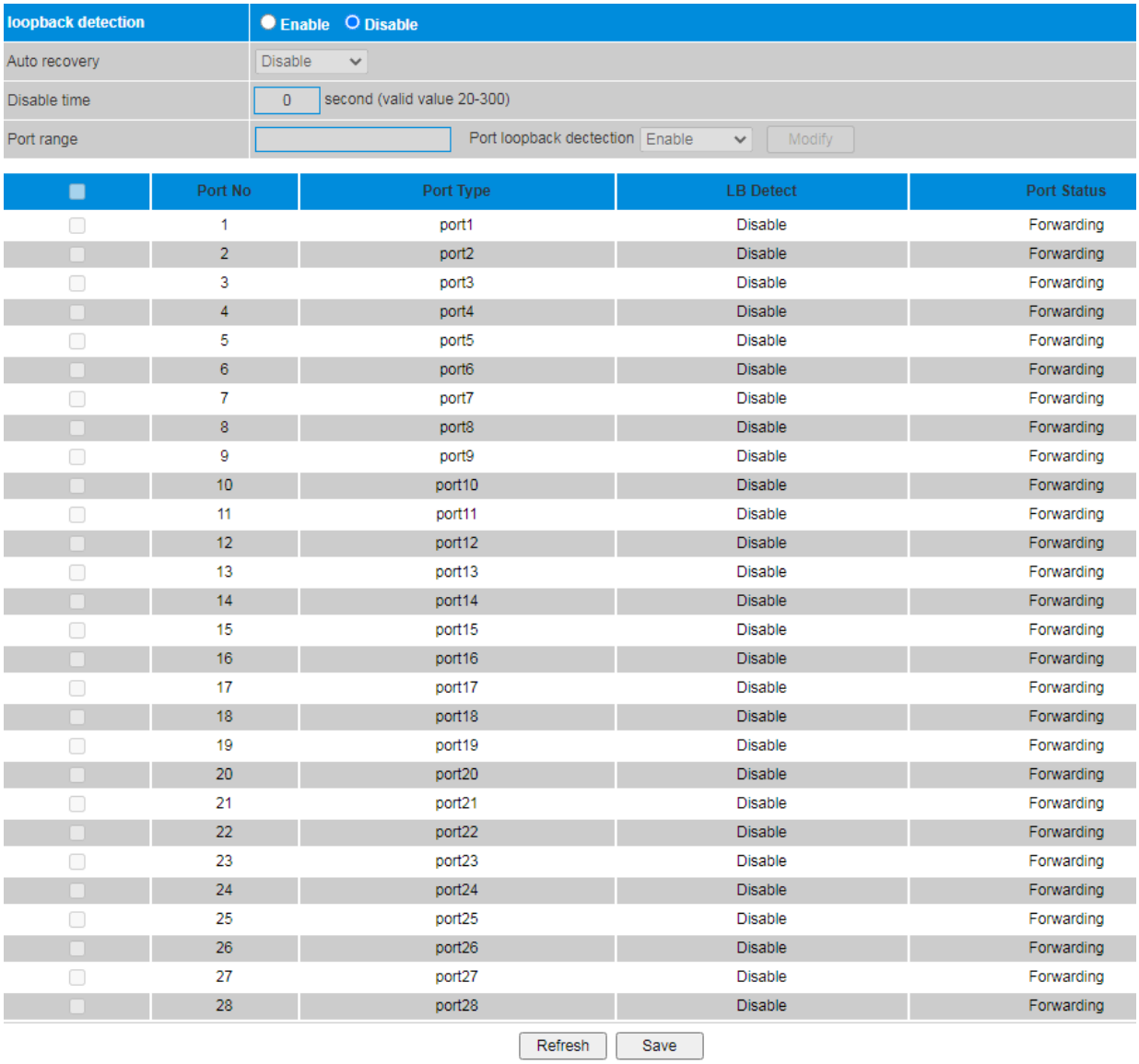
Click <Modify>.

Click <Save>.

10.3 Loopback

The switch supports loopback protection function.

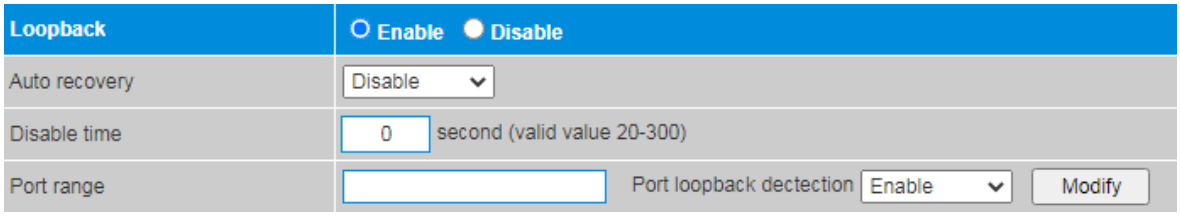
While the function is turned on, users can check if there is a loopback for the switch under this port. If there is loopback, the port will be shutdown.



Procedure

Choose <LACP> <Loopback Protect> in the navigation tree to open the page.

- Enable the function.



- Configure the loopback function.

Items	Descriptions	Default value
Auto Recovery	Choose <Enable> to enable the protection automatic recovery function. The ports will be recovered automatically.	Disable
Disable Time	Indicate the disable loop protect time. The port will be recovered automatically, if the port detection no loopback packet after the time range, when <Protect Automatic Recovery> is enable. The port will keep shutdown, if the port detection no loopback packet after the time range, when <Protect Automatic Recovery> is disable. The value ranges from 20 to 300s.	20s
Port Range	Select the ports that need to be set. Multiple interfaces can be selected.	Null
Port Loop Detection	The switch supports to enable or disable the loopback function of each port. Choose <Enable> to enable the function of the ports needed to be set.	Enable

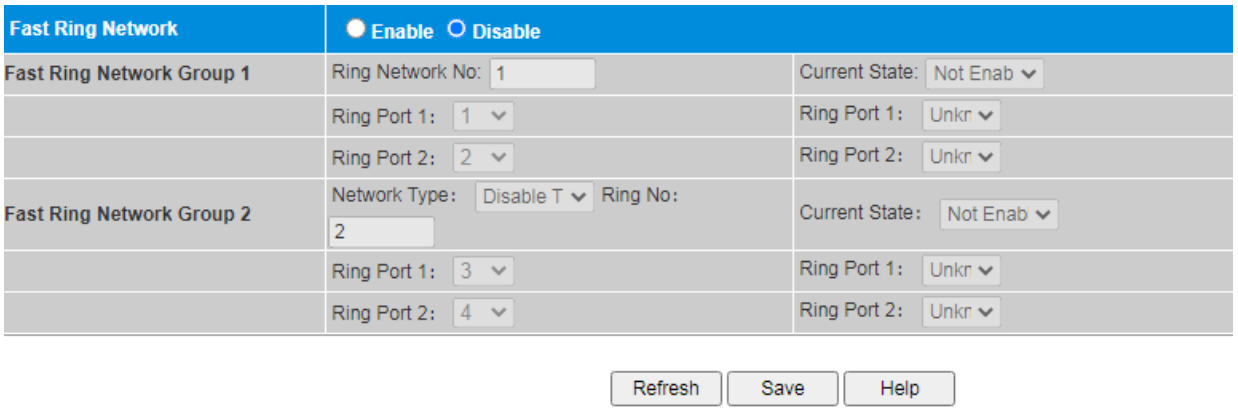
Click <Modify>.

Click <Save>.

10.4 Fast Ring

The switch supports to configure the Fast Ring protect function. Fast Ring is a private protocol applied on Ethernet loop protection to provide fast recovery switching for Ethernet traffic in ring topology.

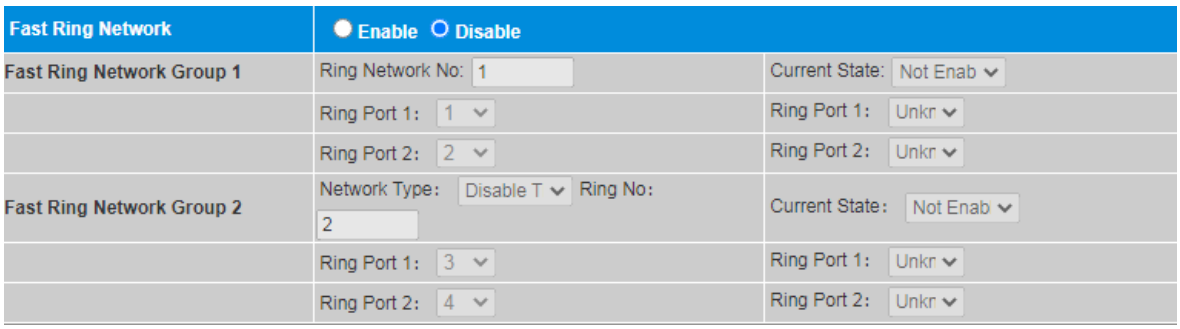
Fast Ring provides a faster redundant recovery than spanning tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same. In the ring topology, every switch should support fast ring and be enabled with Fast Ring and two ports should be assigned as the member ports in the fast ring group. When the failure of network connection occurs, the traffic will go through via the backup link.



Procedure

Choose <LACP> <Fast Ring> in the navigation tree to open the page.

- Enable the function.



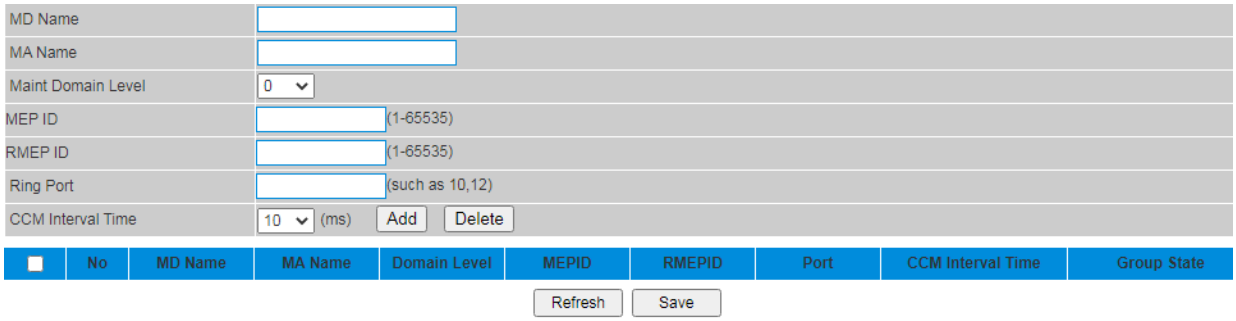
- Configure the Fast Ring.

Items	Descriptions	Default value
Fast Ring Network Group 1		
Ring Network No.	Indicates the number of main ring network the switch accesses. The value ranges from 0 to 255.	0
Ring Port 1	Choose the port that access the ring network.	26
Ring Port 2	Choose the port that access the ring network. The port can't be the same if it is used in other ring network.	28
Current State	Actual status of the ring network group 1. This parameter is not able to be set.	Disable
Ring Port 1	Actual port number that being accessing the network. This parameter is not able to be set.	Unknown
Ring Port 2	Actual port number that being accessing the network. This parameter is not able to be set.	Unknown
Fast Ring Network Group 2		
Network Type	Choose the network type of the sub ring network, including: · Double · Coupling Click <Disable>, the function of sub ring network is disabled.	Disable
Ring ID	Indicates the number of sub ring network the switch accesses. The value ranges from 0 to 255.	0
Ring Port 1	Choose the port that access the ring network.	25
Ring Port 2	Choose the port that access the ring network. The port number can't be the same if it is used in other ring network.	27
Current State	Actual status of the ring network group 2. This parameter is not able to be set.	Disable
Ring Port 1	Actual port number that being accessing the network. This parameter is not able to be set.	Unknown
Ring Port 2	Actual port number that being accessing the network. This parameter is not able to be set.	Unknown

Click <Save>.

10.5 CCM

CC monitors connectivity of links between MEPs. A MEP periodically sends multicast continuity check messages (CCMs) to an RMEP in the same MA. If an RMEP does not receive a CCM within a period three times the timeout interval at which CCMs are sent, the RMEP considers the path between itself and the MEP faulty. A MEP generates and sends CCMs. They are enabled to send CCMs to one another at the same interval. Each CCM carries a level equal to the MEP level.



Procedure

Choose <LACP> <CCM> in the navigation tree to open the page.

· Configure CCM.

Items	Descriptions	Default value
MD Name	Indicate the Maintenance Domain.	Null
MA Name	Indicate the Maintenance Association.	Null
Main Domain Level	Level of an MD. The value ranges from 0 to 7. A greater value indicates a higher level.	0
MEP ID	Maintenance association End Point ID. MEPs are located at the edge of an MD and MA. The value ranges from 1 to 65535.	Null
RMEP ID	Remote Maintenance association End Point ID. A MEP configured on a CFM-enabled device is called a local MEP. MEPs configured on other devices in the same MA are called remote maintenance association end points The value ranges from 1 to 65535.	Null
Ring Port	Select the ports that need to set.	Null
CCM Interval Time	Time interval for sending messages. The value could be 10/100/1000/10000ms.	10ms

Click <Add>.

Click <Save>.

· Delete CCM.

Choose the item that need to be deleted.

Click <Delete>.

Click <Save>.

11 Port Security

11.1 Static Address Lock

The switch supports to set the static MAC table.

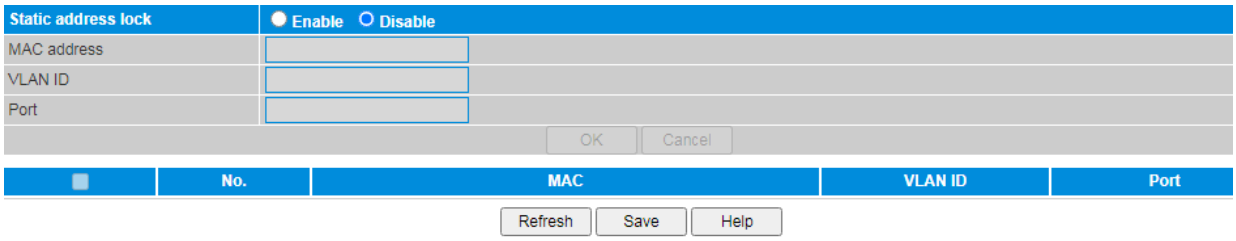
A MAC address table records the MAC address, interface number, and VLAN ID of the device connected to the device.

Each device maintains a MAC address table. A MAC address table records the MAC address, interface number, and VLAN ID of the connected devices. When forwarding a data frame, the device searches the MAC table for the outbound interface according to the destination MAC address in the frame. This helps the device reduce broadcasting.

The static entry is set by users and is delivered to each SIC. It does not age.

The static entry will not be lost after the system is reset or the interface board is hot swapped or reset.

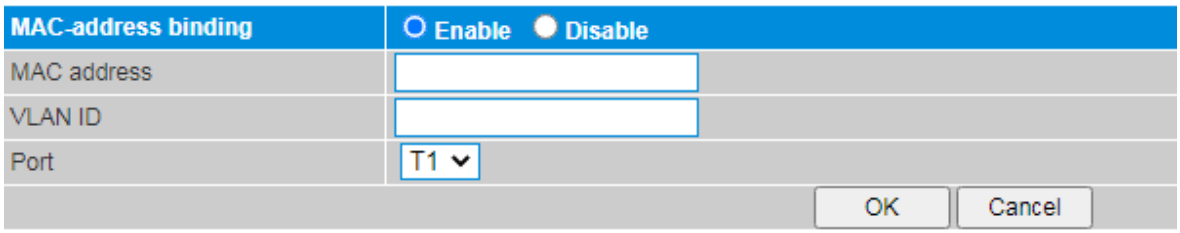
The function is disable by default.



Procedure

Choose <Port Security> <Static Address Lock> in the navigation tree to open the page.

- Enable the function.



- Configure the static MAC table.

Items	Descriptions	Default value
MAC Address	Input the 48 bit mac address.	Null
VLAN ID	Input the VLAN ID. The value ranges from 1 to 4094.	Null
Port	Select the ports that need to be set.	Null

Click <Add>.

Click <Save>.

- Delete the static MAC table.

Select the record that need to be deleted.

Click <Delete>.

Click <Save>.

11.2 802.1x Authentication

IEEE802.1x Authentication system adopted the "controllable ports" and "uncontrolled ports" logic functions. It can realize the separation of business and certification. After passing certification, the business flow and the certification flow separation, it has no special requirement for the following subsequent packets. Business can be flexible, especially in develop broadband multicast business, it has a lot of advantages. All the business are not restricted by authentication.

Three Main Parts of 802.1x Authentication:

- Application supplicant: User and Client which want to get the certification.
- Authentication server: A typical example for the RADIUS server.
- Certification system authenticator: Between the end devices, such as wireless access points, switches, etc. We can play at the same time equipment system and authentication server two characters, you can also use the additional authentication server, at the same time support the billing system.

The function is disable by default.

Global setting	Enable Disable
Timing update certification	3600 Second [60 - 40,000,000]
Radius server	Local Remote
Radius server setting	IP address
	Share secret key
Server port setting	Billing server port [0 - 65535]
	Certification server port [0 - 65535]

Port setting	Control mode	Port control method	Maximum user quantity
	Authorized-force	MAC Based	[1 - 4096]
Port range	Edit		

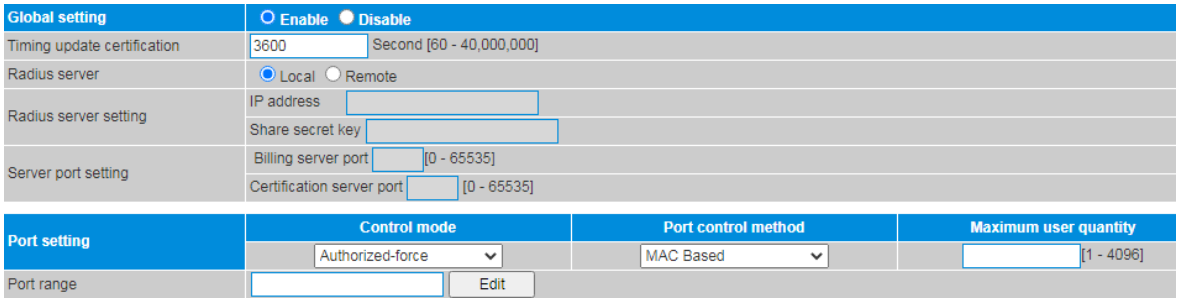
	Port	Port mark	Setting status		
			Control mode	Control method	Maximum user quantity
	1	port1	Authorized-force	MAC Based	4096
	2	port2	Authorized-force	MAC Based	4096
	3	port3	Authorized-force	MAC Based	4096
	4	port4	Authorized-force	MAC Based	4096
	5	port5	Authorized-force	MAC Based	4096
	6	port6	Authorized-force	MAC Based	4096
	7	port7	Authorized-force	MAC Based	4096
	8	port8	Authorized-force	MAC Based	4096
	9	port9	Authorized-force	MAC Based	4096
	10	port10	Authorized-force	MAC Based	4096
	11	port11	Authorized-force	MAC Based	4096
	12	port12	Authorized-force	MAC Based	4096
	13	port13	Authorized-force	MAC Based	4096
	14	port14	Authorized-force	MAC Based	4096
	15	port15	Authorized-force	MAC Based	4096
	16	port16	Authorized-force	MAC Based	4096
	17	port17	Authorized-force	MAC Based	4096
	18	port18	Authorized-force	MAC Based	4096
	19	port19	Authorized-force	MAC Based	4096
	20	port20	Authorized-force	MAC Based	4096
	21	port21	Authorized-force	MAC Based	4096
	22	port22	Authorized-force	MAC Based	4096
	23	port23	Authorized-force	MAC Based	4096
	24	port24	Authorized-force	MAC Based	4096
	25	port25	Authorized-force	MAC Based	4096
	26	port26	Authorized-force	MAC Based	4096
	27	port27	Authorized-force	MAC Based	4096
	28	port28	Authorized-force	MAC Based	4096

Refresh Save Help

Procedure

Choose <Port Security> <802.1x Authentication> in the navigation tree to open the page.

- Enable the function.



- Configure the global parameters.

  Set the parameters as required.

Items	Descriptions		Default value
Timing Update Certification	Input the authentication timer, the value ranges from 60~40,000,000s.		3600s
Radius Server	Choose the radius server, including two types: · Local: local radius server. · Remote: remote radius server.		Local
Remote Radius server			
Radius Server Setting	IP Address	Input the IP address of Radius server.	Null
	Secret Shared Key	Indicate the secret shared key of the IP address.	Null
Server Port Setting	Billing Server Port	Indicate the accounting port. The value ranges from 0 to 65535.	1813
	Certification Server Port	Indicate the authentication port. The value ranges from 0 to 65535.	1812

  Click <Save>.

- Configure the port parameters.

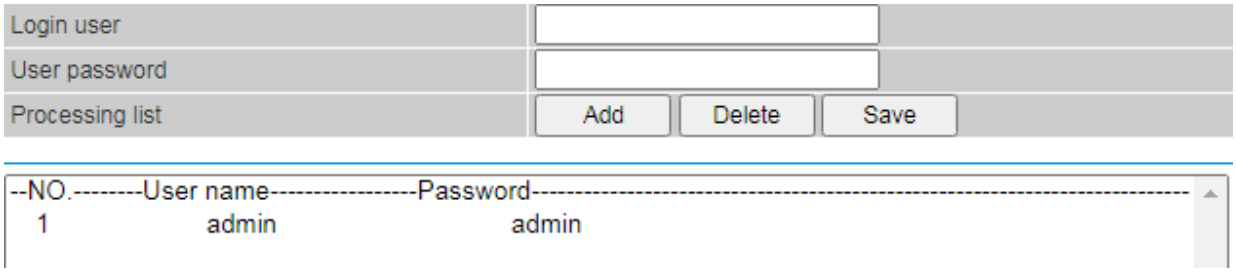
Items	Descriptions	Default value
Control Mode	Choose the control mode, including: · Authorized-force · Auto · Unauthorized-force	Null
Port Control Method	Port control mode, by default the value is MAC-based.	MAC-based
Maximum User Quantity	Input the maximum user quantity, the value ranges from 1 to 4096.	Null
Port Range	Select the ports that need to be set.	Null

  Click <Edit>.

  Click <Save>.

11.3 RADIUS Database

The switch supports to add or delete user name and password for local 802.1x authentication.



Procedure

Choose <Port Security> <RADIUS Database> in the navigation tree to open the page.

- Create an account.

Items	Descriptions	Default value
User Login	Input the user name.	Null
User Password	Indicate the password of the user name, the value support 5~16 bites string.	Null

  Click <Add>.

  Click <Save>.

- Delete an account.

  Select the account that need to be deleted.

  Click <Delete>.

  Click <Save>.

12 Network Management

12.1 SNMP

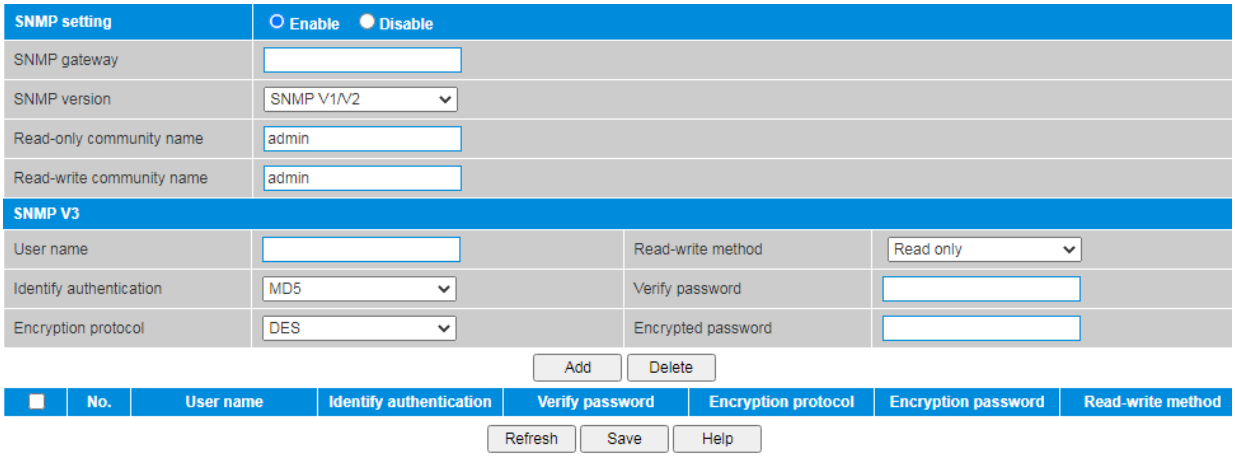
The switch supports SNMP.

As a network management standard protocol used on TCP/IP networks, SNMP uses a central computer (NMS) that runs network management software to manage network elements.

In a large network, it is very difficult for network administrator to detect, locate and rectify the fault as the switch does not report the fault. This affects maintenance efficiency and increases maintenance workload. To solve this problem, equipment vendors have provided network management functions in some products. The NMS then can query the status of remote devices, and devices can send traps to the NMS in the case of particular events.

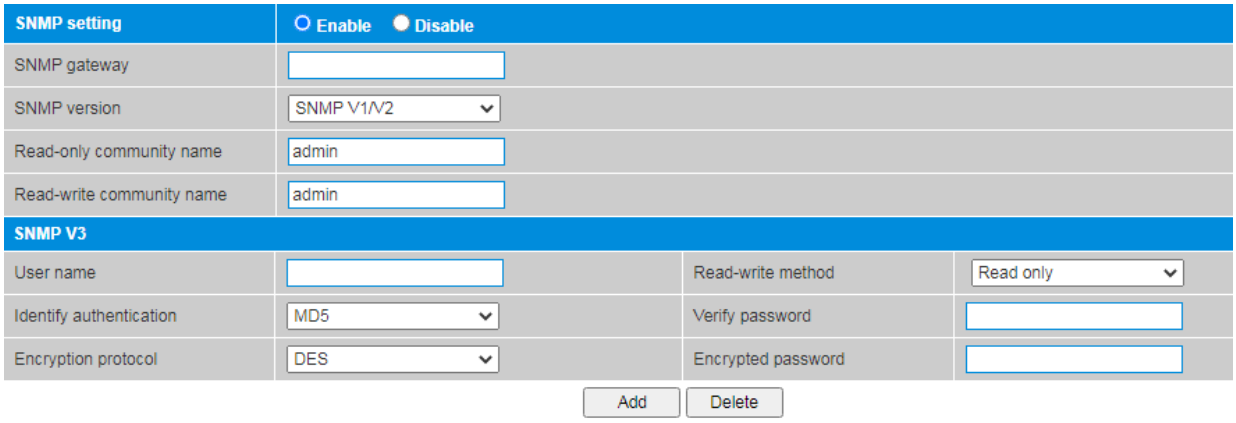
Users can configure the function of the SNMP community permission and SNMP V3.

The function is enable by default.



Procedure

Choose <Network Management> <SNMP> in the navigation tree to open the page.



- Configure SNMP community permission.

Items	Descriptions	Default value
SNMP Gateway	Input the IP address of the server.	Null
SNMP Version	Choose the SNMP version, by default the value is SNMP V1/V2.	SNMP V1/V2
Read-only Community Name	Indicate the name of SNMP community for read-only permission. The group only has permission to operate. The value supports strings.	public
Read and Write Community Name	Indicate the name of SNMP community for read and write permission. The group has permission to get and set operations. The value supports strings.	private

Click <Add>.

Click <Save>.

- Configure SNMP V3.

Items	Descriptions	Default value
User name	Indicates the user name. The value supports 31 stings.	Null
Read and Write Mode	Choose the read and write mode, including · Read-only · Read and Write	Read-only
Identify Authentication	Choose the identity authentication, including · MD5 · SHA	MD5
Verify Password	Indicates the Authentication password, supporting 8~32 digits strings.	Null
Encryption Protocol	Choose the Encryption Protocol, including · DES · AES · 3DES	DES
Encrypted Password	Indicates the Encryption password, supporting 8~32 digits strings.	Null

Click <Add>.

Click <Save>.

- Delete SNMP V3 .

Select the item that need to be deleted.

Click <Delete>.

Click <Save>.

12.2 Port Mirror

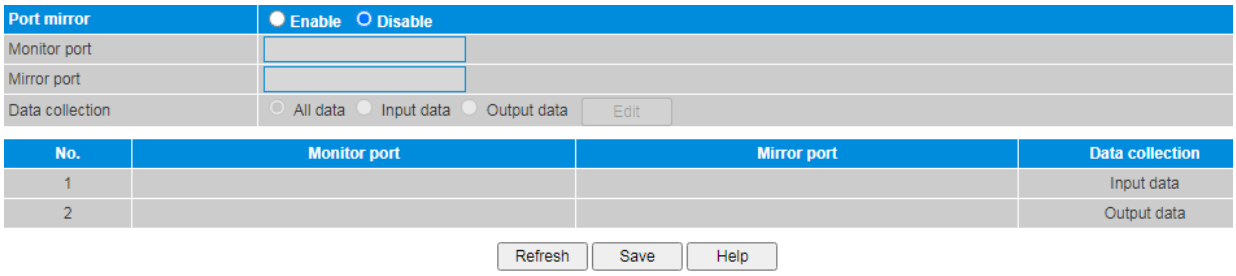
The switch supports monitoring the ports data transferring.

Packet mirroring copies the packets on a mirrored port (source port) to an observing port (destination port).

During network maintenance, maintenance personnel need to capture and analyze packets (for example, when there are suspicious attack packets). However, these operations always affect packet forwarding.

Packet mirroring copies packets on a mirrored port to an observing port so that users can analyze packets copied to the destination port by a monitoring device to monitor the network and rectify faults.

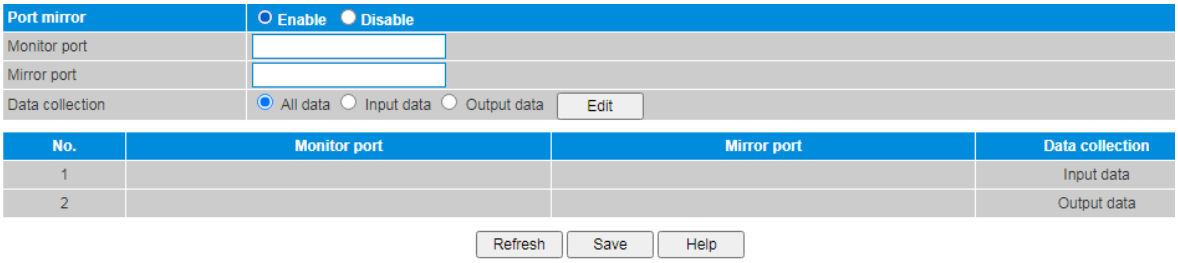
Users can configure the source interface and target interface of mirror. The function supports 1 to 1 and many to 1 modes.



Procedure

Choose <Network Management> <Port mirroring> in the navigation tree to open the page.

- Enable the function.



- Configure the port mirroring.

Items	Descriptions	Default value
Monitor Port	Choose the monitor port.	Null
Mirror Port	Select the port range of mirror ports, Multiple ports can be selected.	Null
Data Collection	The packets that the need to be copied and monitored on the mirrored ports, including · All Data: input and output data · Input Data · Output Data	All Data

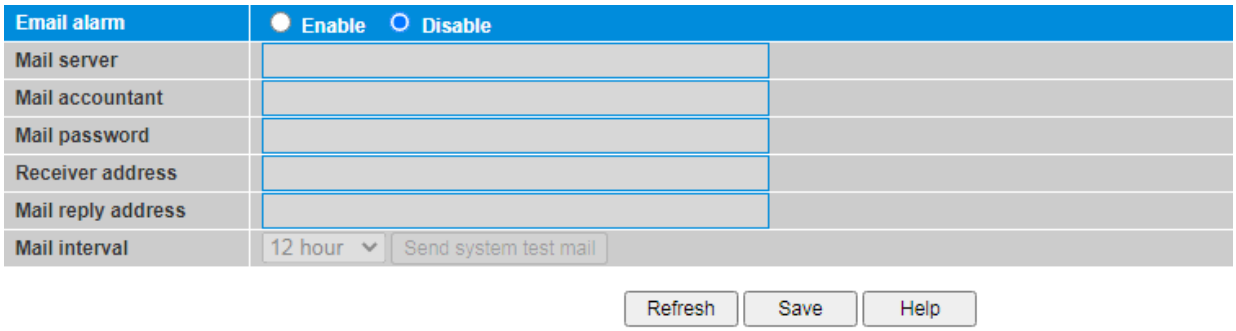
Click <Edit>.

Click <Save>.

12.3 Email Alarm

When the device is running an event supervision, the supervision sends an alert message to defined mail recipients when something wrong about defining time and some abnormal event occurs. Supervision also periodically send all log messages to predefined recipients.

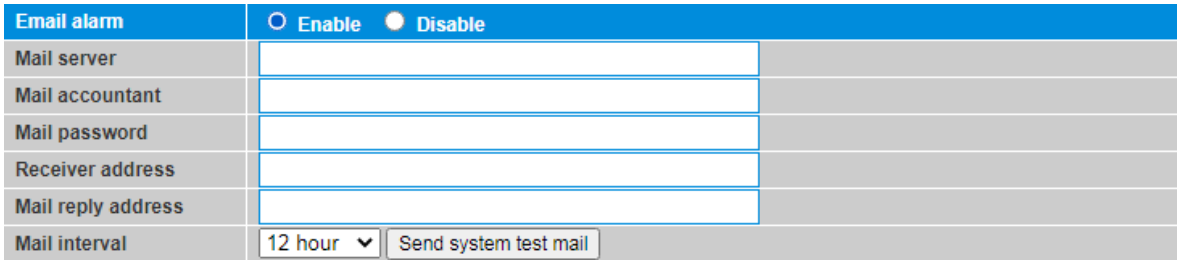
The function is disable by default.



Procedure

Choose <Network Management> <Email Alarm> in the navigation tree to open the page.

- Enable the function.



- Configure the email alarm.

Items	Descriptions	Default value
Mail server	Input the host computer's IP address, or the host computer that provides POP3 mail delivery service to the switch.	Null
Mail Accountant	Input the user name for account logging in email server.	Null
Mail Password	The password of the account logging in email sever.	Null
Receiver Address	The email address used to inform recipients of abnormal events.	Null
Mail Reply Address	The email address that can help solve abnormal events.	Null
Mail Interval	The interval that regularly send log and weekly reports. The sending interval supports 6 types interval: any time, 1h, 2h, 4h, 12h and 24h. When the interval is set as any time, the system will send email once there is alarm.	Null

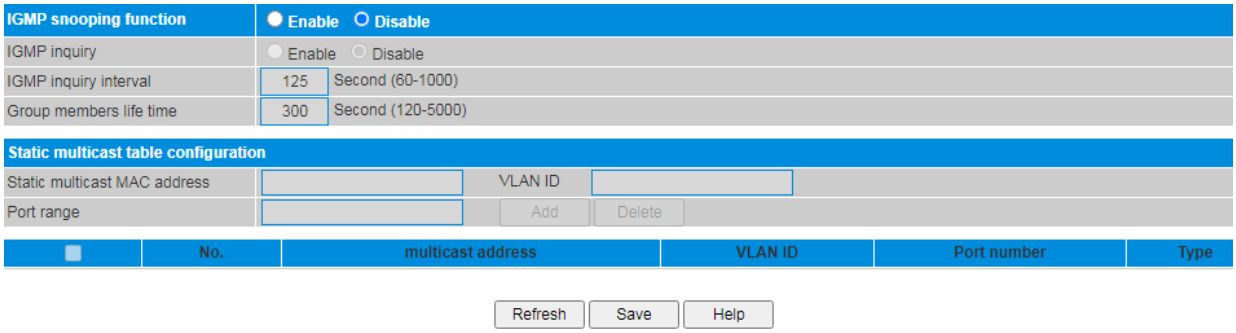
Click <Save>.

Click <Send system test mail>, check if the configuration is succeed.

12.4 IGMP Snooping

Internet Group Management Protocol Snooping (IGMP-Snooping) is a Layer 2 IPv4 multicast protocol. The IGMP-Snooping protocol maintains information about the outgoing interfaces of multicast packets by snooping multicast protocol packets exchanged between the Layer 3 multicast device and user hosts. The IGMP-Snooping protocol manages and controls the forwarding of multicast packets at the data link layer.

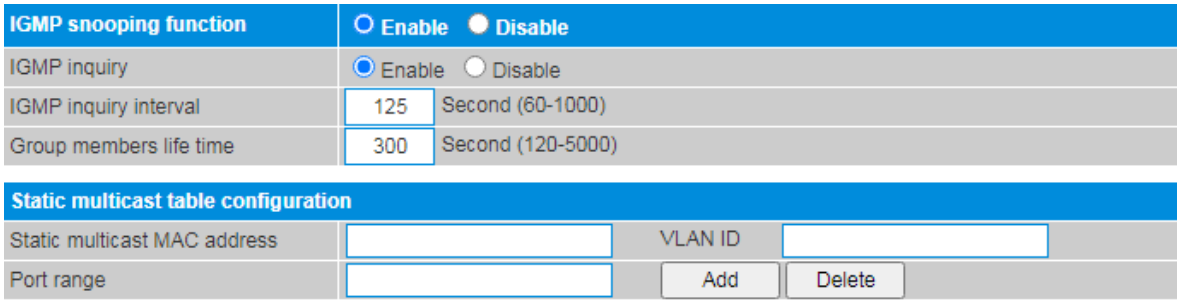
Users could turn on/off the IGMP-Snooping function and configure the IGMP-Snooping Timer.



Procedure

Choose <Network Management> <IGMP Snooping> in the navigation tree to open the page.

- Enable IGMP snooping function.
- Enable IGMP Inquiry function.



- Configure the IGMP-Snooping function.

Items	Descriptions	Default value
IGMP General Query Interval	Indicate the query interval time. The value ranges from 60~1000 s.	125s
Maximum Response Time	Indicate the maximum survival time of equipment existing multicast members. The value ranges from 120~5000 s.	300s

Click <Save>.

- Configure the static multicast table.

Set the parameters as required.

Items	Descriptions	Default value
Static Multicast MAC Address	Input the static multicast MAC address	Null
VLAN ID	Indicate the survival time of group members. The value ranges from 120~5000 s.	Null
Port Range	Select the ports that need to be set. Multiple interfaces can be selected.	Null

Click <Save>.

CAUTION

- It is recommended that PC's Ethernet port should be allocated only one IP address.
- It is recommended that Network should not to have multiple IGMP inquirer.
- Choose all the port If the forwarding relationship to unknown multicast group is uncertain.

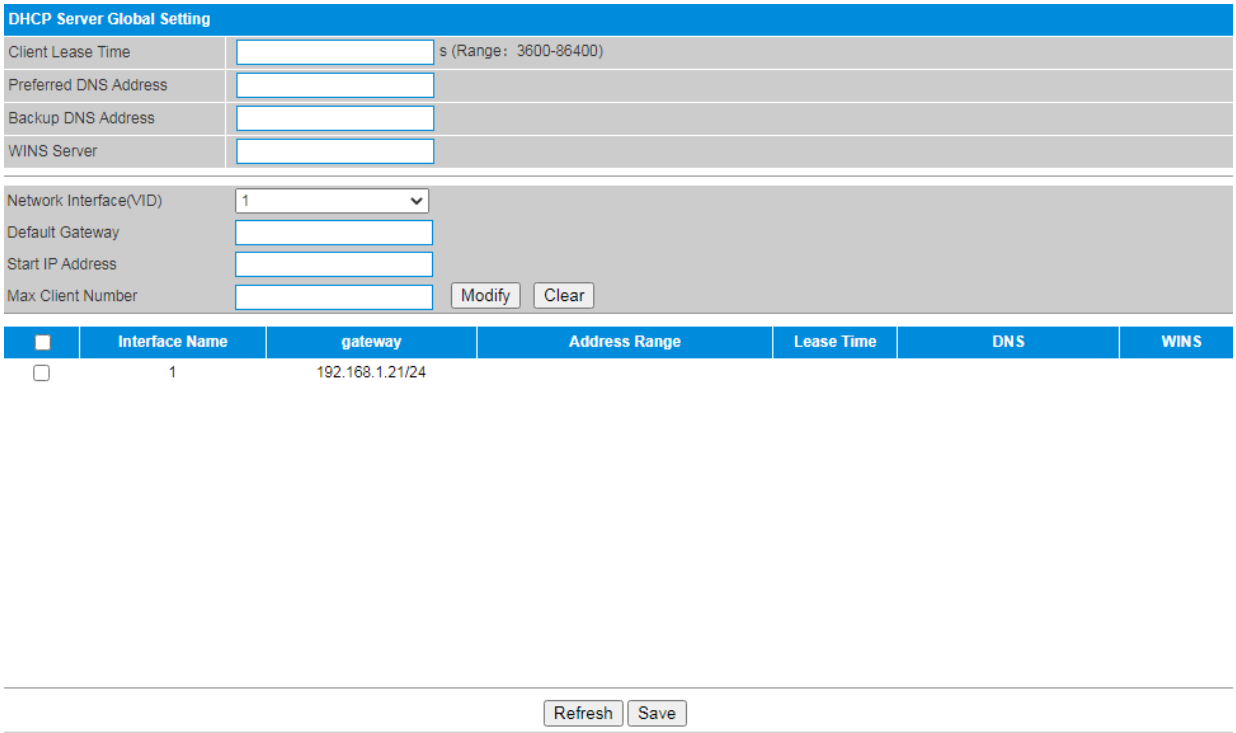
12.5 DHCP

DHCP is a technology used to dynamically manage and configure clients in a concentrated manner.

The client applies to the server for configurations such as the IP address, subnet mask, and default gateway, and the server replies with corresponding configurations according to policies.

Users need to configure a DHCP server based on the global address pool to enable computers to obtain IP addresses from the global address pool dynamically.

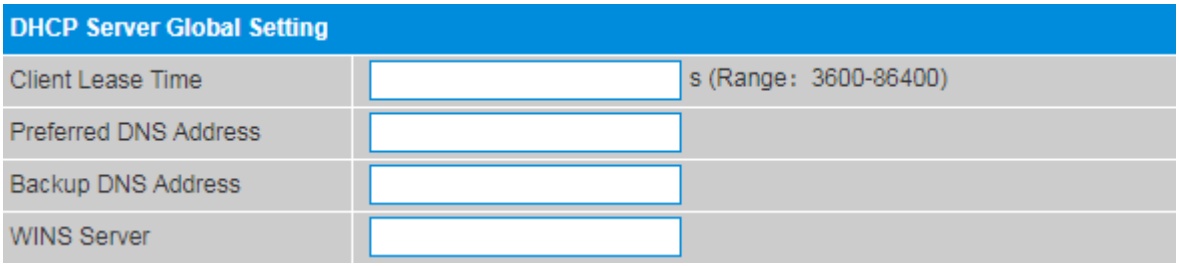
Users can configure an address pool on a VLAN when a device supports switched Ethernet interfaces. IP addresses cannot be configured on switched Ethernet interfaces directly; therefore, you need to create a VLAN and configure a DHCP address pool on the VLAN.



Procedure

Choose <Network Management> <DHCP Server> in the navigation tree to open the page.

- Select the existed record, and input information of DNS, Gateway, Start IP address, etc.

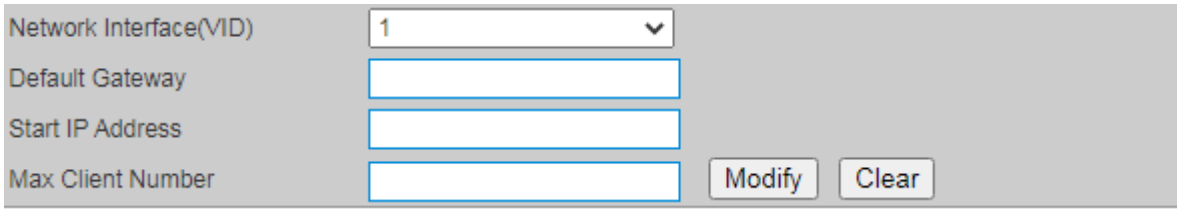


Items	Descriptions	Default value
Client Lease Time	Indicates the lease of dynamic IP addresses. The default lease is one day (86400s). The value ranges from 3600 to 86400 s.	14400
Preferred DNS Address	Indicates the main IP address of a DNS server.	Null
Backup DNS Address	Indicates the backup IP address of a DNS server.	Null
WINS Server	Indicates the IP address of a WINS server.	Null

Click <Modify>.

Click <Save>.

- Set an address pool on a VLAN.



Set the parameters as required.

Items	Descriptions	Default value
Network Interface (VID)	Select a record in the table to indicate the name of a VLNAIF interface. The VLANs in the table are created in the <Ethernet Switch> <802.1Q VLAN> and <IP Service> <Interface IP> modules.	1
Default Gateway	Indicates the default IP address and subnet mask of the selected VLAN. The value is displayed automatically after you select the <Network Interface (VID)>.	Null
Start IP Address	Indicate the start IP address of the interface.	Null
Max Client Number	Input the max client number. The value ranges from 2 to 255.	Null

Click <Modify>.

Click <Save>.

- Clear the record.

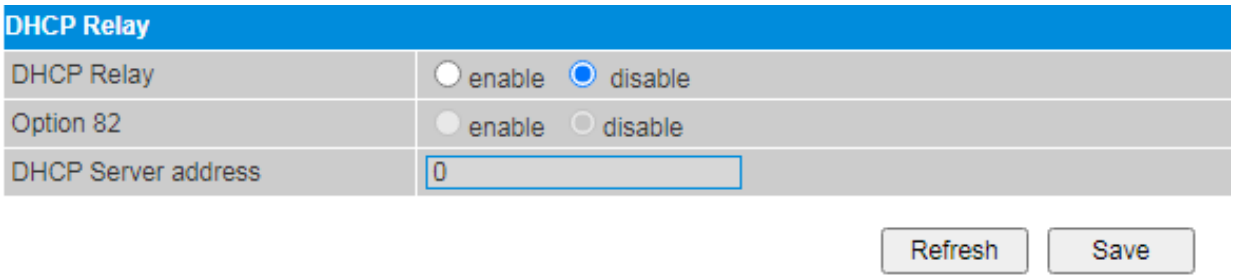
  Select the record that need to be cleared, multiple records can be selected.

  Click <Clear>.

  Click <Save>.

12.6 DHCP Relay

Through DHCP Relay, it can achieve the processing and forwarding for DHCP information between different subnets and physical network segments. If the DHCP client and DHCP server are in the same physical network segment, the DHCP client can correctly get the dynamically assigned IP address. If they are not in the same physical network segment, the DHCP Relay Agent is required, with which the information could be forwarded to DHCP client and DHCP sever in different physical subnets instead of requiring to set DHCP server in every physical segment.

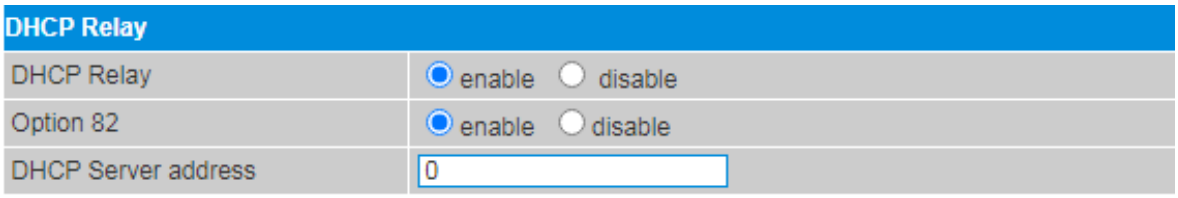


Procedure

Choose <Network Management> <DHCP Relay> in the navigation tree to open the page.

- Enable DHCP Relay.

  Enable Option 82.



  Input the DHCP Server Address.

Items	Descriptions	Default value
DHCP Server Address	Indicates the lease of dynamic IP addresses. The default lease is one day (86400s). The value ranges from 3600 to 86400 s.	0

  Click <Save>.

- Disable DHCP Relay.

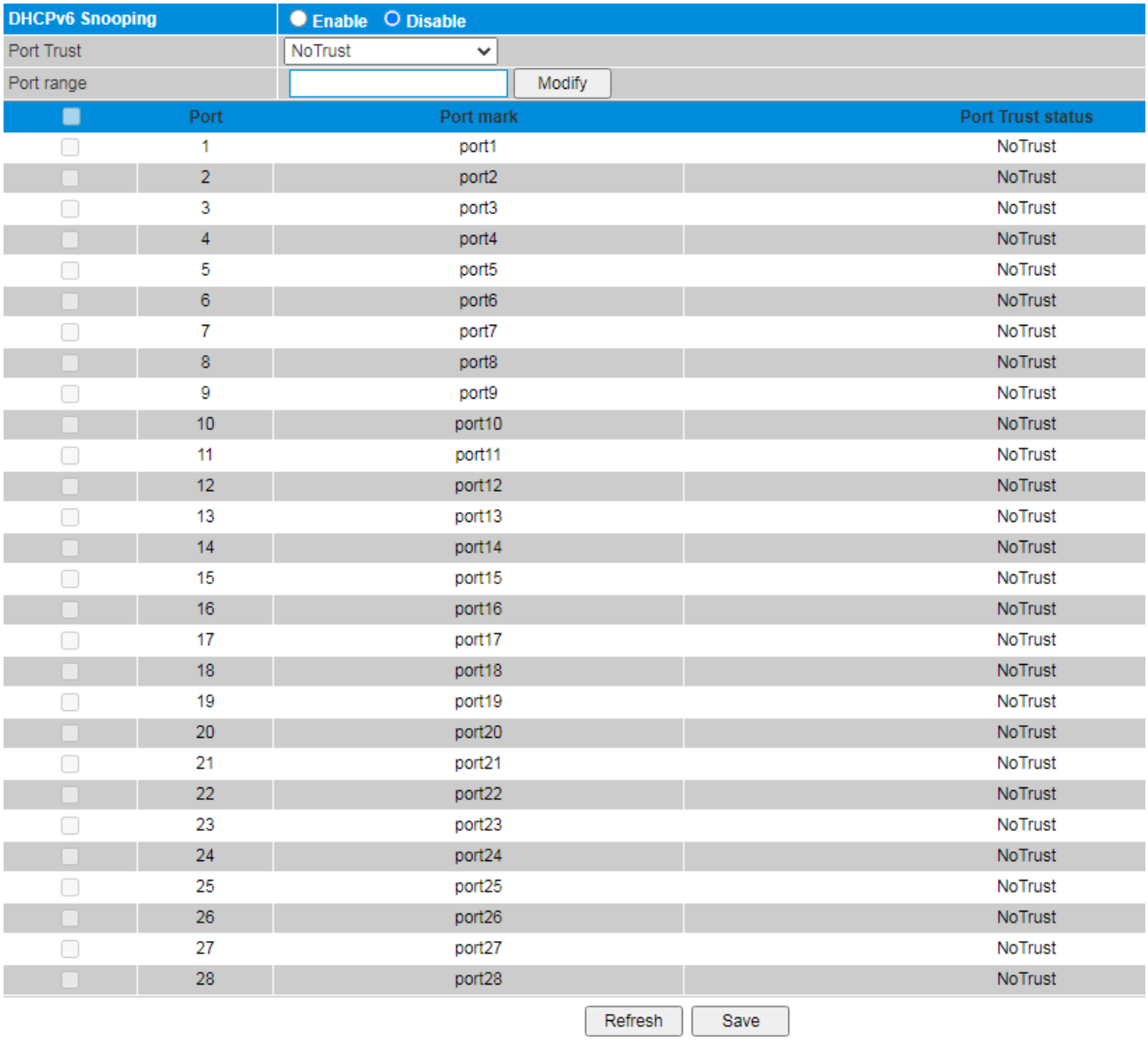
  Disable the DHCP Relay.

  Click <Save>.

12.7 DHCPv6 Snooping

In order to ensure DHCP clients to obtain IP addresses through legal DHCP servers, it should set the device ports, which are directly or indirectly connected with DHCP severs trusted by administrators, as the trust ports, and set other ports as untrusted ports. There into the trust ports could normally forward the received DHCP response message, and the untrusted ports would discard the DHCP Ack, DHCP Nak, DHCP Offer, and DHCP Decline packets from DHCP server. Thus, DHCP clients can only obtain IP addresses from legal DHCP servers, and the fake DHCP server set up privately cannot assign IP addresses to DHCP clients. Besides, it requests to configure the port connected to the DHCP server to be in "trust" mode after enabling DHCP Snooping under the user's port or VLAN. Through above configurations, the device would generate a DHCP Snooping dynamic binding table.

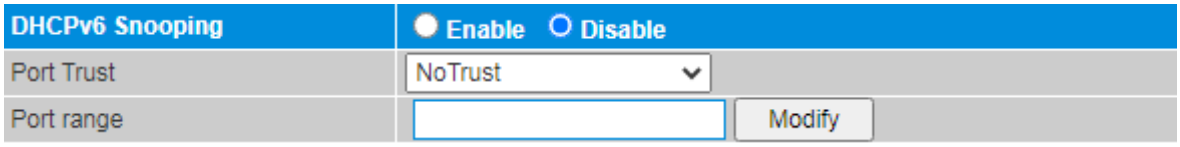
The function is disable by default.



Procedure

Choose <Network Management> <DHCP Snooping> in the navigation tree to open the page.

- Enable DHCPv6 Snooping and set the ports to trust.



Items	Descriptions	Default value
Port Trust	Set to trust the port or not.	0
Port Range	Input the port number. Multiple interfaces can be selected. The value ranges from 1 to the max port number. Format as “2” or “1-5” or “3, 1-5”.	Null

Click <Modify>.

Click <Save>.

- Disable DHCPv6 Snooping.

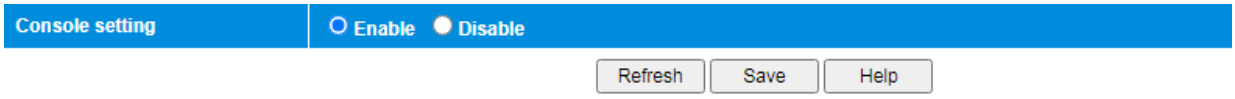
Disable the DHCPv6 Snooping.

Click <Save>.

12.8 Telnet Setting

The switch supports CLI configuration through console port. Set to allow telnet setting or not while configure the device by command lines.

By default the function is disable.



- Enable console port setting.

Enable console setting.

Click <Save>.

- Disable console port setting.

Disable console setting.

Click <Save>.

13 Network Information

13.1 Flow Statistics

View packets received and sent by the ports.

Choose <Network Information> <Flow Statistics> in the navigation tree to open the page.

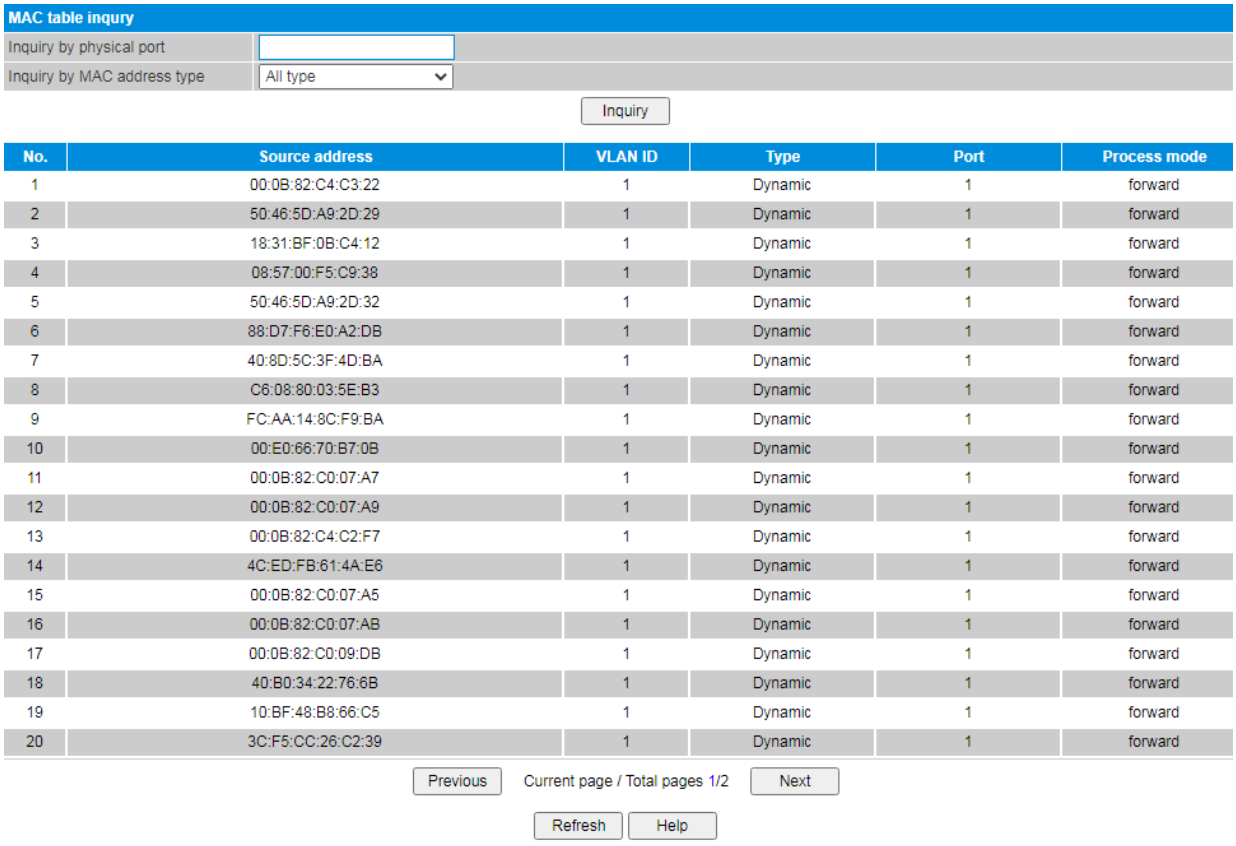
Port	Sent frame				Received frame			
Port	Singlecast package	Multicast package	Broadcast package	Error package	Singlecast package	Multicast package	Broadcast package	Error package
1	530	6	7	0	483	47362	29814	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0

Reset Refresh Help

13.2 MAC Table

Query and view the MAC table of the interfaces.

Choose <Network Information> <MAC Table> in the navigation tree to open the page.



Procedure

- Query MAC table

  Set the query conditions, Click <Inquiry>.

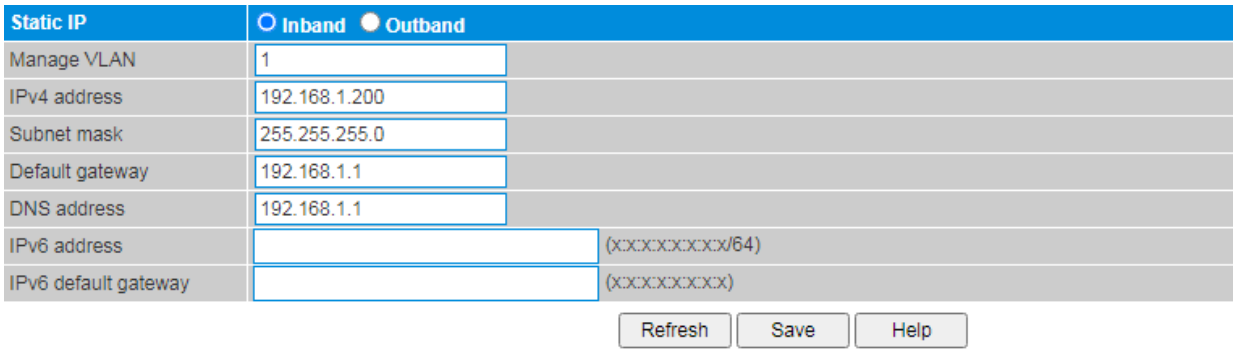
  By default, all the MAC table are displayed.

> **CAUTION**
>
> Multicast MAC address table is displayed in IGMP snooping table, all these address tables are unicast addresses. The permanent static address is configured in static MAC address port table. Users need to modify corresponding entries when the port changes. The aging time of MAC address is 300s by default, after port disconnected the upper port operation procedures clear all correspond port entries.

14 System Management

14.1 IP Address

User can view and modify the Manage VLAN, IPv4 address, IPv6 address, default gateway and DNS address.



Procedure

Choose < System Management> <IP Address> in the navigation tree to open the page.

- Configure the parameters.

Items	Descriptions	Default value
Manage VLAN	VLAN ID of the interface. The value ranges from 1 to 4094. Note: If the VLAN ID of the switch changes, the VLAN ID of managed PC linked with the switch must be changed to the same.	1
IPv4 Address	The IPv4 address of the IP address of the Ethernet interface.	192.168.1.200
Subnet Mask	The subnet mask of the IPv4 address.	255.255.255.0
Default Gateway	The default gateway the switch linking with.	192.168.1.1
DNS Address	The default DNS address the switch linking with. Please fill in correct DNS address when using it for NTP and alarm email.	192.168.1.1
IPv6 Address	The IPv6 Address of the IP address of the Ethernet interface.	Null
IPv6 default Gateway	The default gateway of the IPv6 address.	Null

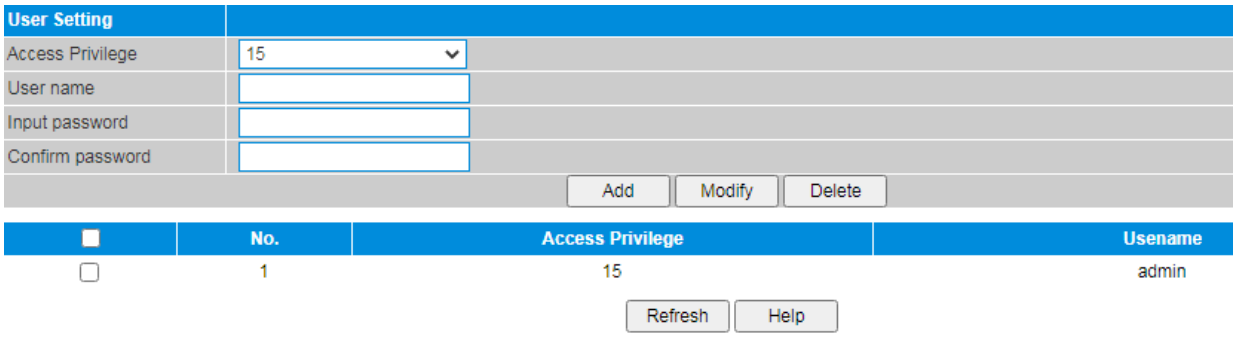
Click <Save>.

14.2 User Management

The Web system manages users at levels.

User levels are marked by numbers from 1 to 15, in ascending order.

The access privilege of user is determined by the level of this user.



Procedure

Choose <System Management> <User Setting> in the navigation tree to open the page.

- Create username.

Items	Descriptions	Default value
Access Privilege	Choose the user level, from 1~15. · With lower than 3 level, the users are only allowed the read permission. · With 3 and higher than 3 level, the users are allowed the read, create and delete permission.	15
User Name	Input the username, supporting 32 digits of letters or numbers.	Null
Input Password	Input the password, support 16 digits of letters or numbers.	Null
Confirm Password	Confirm the password. The value must be the same as <Input password>.	Null

  Click <Add>.

  Click <Save>.

- Delete username.

  Choose the username that need to be deleted.

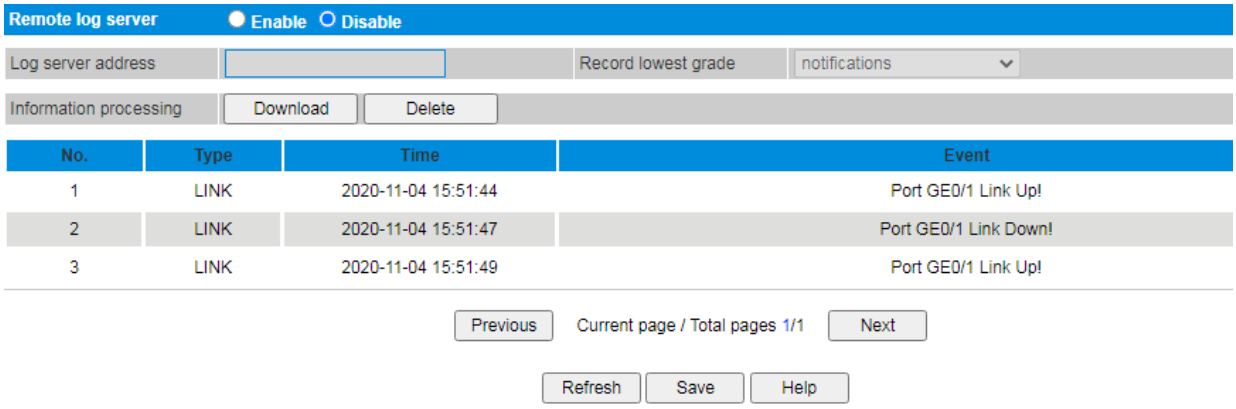
  Click <Delete>.

  Click <Save>.

14.3 Log Information

Users can view, download and clear the system log, including:

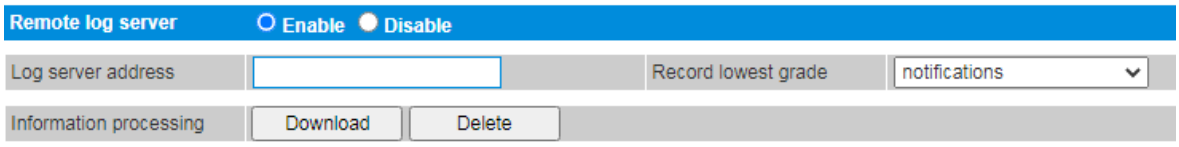
- System restart
- Port link down/up
- Power supply status
- login information
- Broadcast storm
- System action and operation record
- NTP time synchronization information
- Other system information



Procedure

Choose <System Management> <Log Information> in the navigation tree to open the page.

- Enable remote log server.



Configure system log function.

Items	Descriptions	Default value
Log Server Address	The server address that receiving log information.	Null
Record lowest grade	There are eight optional levels: · error information · notification information to be logged · information in need of quick reaction · serious information · information that can't be used in system · normal but important information · information in debug · warning information Choose the lowest record grade type.	Notifications

Click <Save>.

- Clear the system log records.

  Click <Delete> to delete the displayed log.

- Download the system log records.

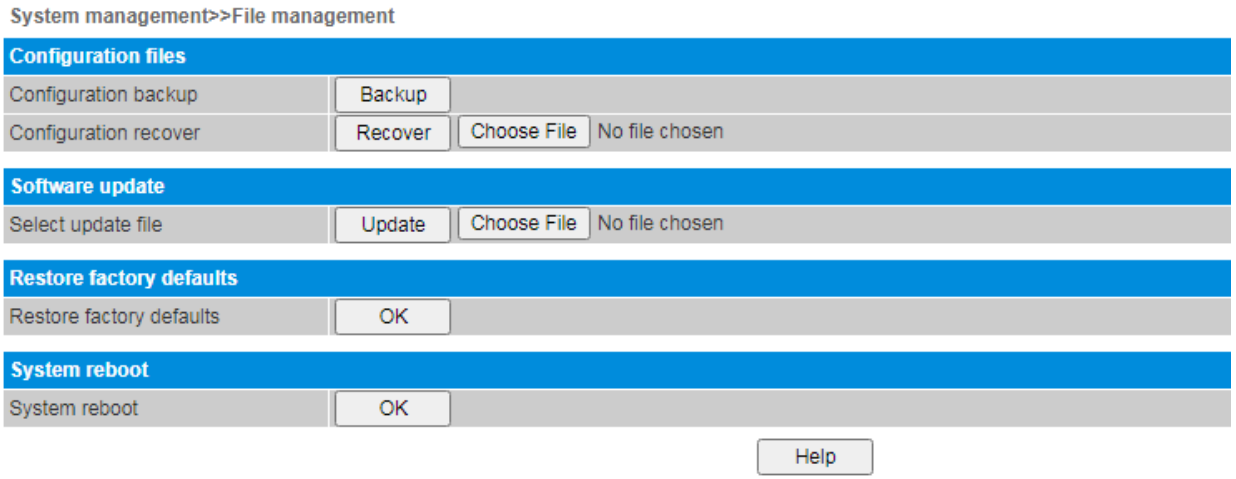
  Click <Download> to download the displayed log.

WARNNING

The system log can't be recovered after clear operation!

14.4 File Management

Users can restore the factory value, reboot the system, download the actual configuration file, upload configuration file, and upgrade the software version.



Procedure

Choose <System Management> <Management> in the navigation tree to open the page.

- Back up the configuration.

  Click <Backup> under <Configuration File>-< Configuration Backup >.

  The configuration file will be downloaded.

- Upload configuration file.

  Click <Choose File>, upload the configuration file.

  Click <Recover> under <Configuration File>-< Configuration Recover >.

  The configuration file will be uploaded

  WARNNING

  The actual configuration will be covered after uploading configuration file operation. Please download your configuration file before uploading, or the latest configuration can't be recovered.

- Upgrade the software.

  Click <Choose File> under <System Upgrade>.

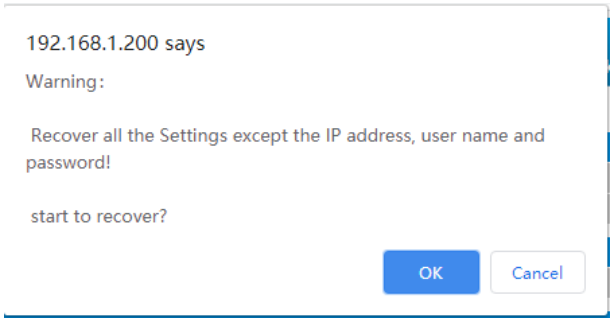
  Click <Upgrade>.

  WARNNING

- To upgrade the software version, please contact the seller to get the software package.
- After software upgrade, please press the <Init> key on the front panel for 5s, to make sure the new version software will work normally.

- Restore factory default value remotely.

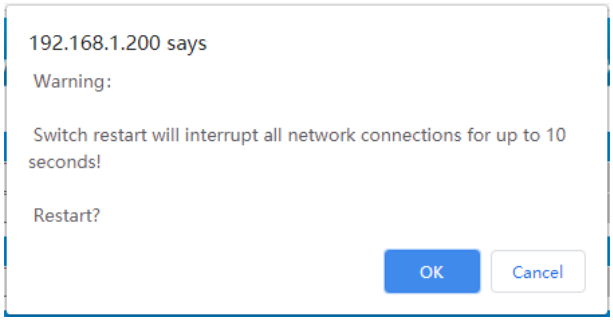
  Click <OK> under <Restore Factory defaults>.



  Click <OK>.

- Reboot the system remotely.

  Click <OK> under <System Reboot>.



  Click <OK>.

14.5 Web Access Control

The switch supports Web system management through http or https. The mode can be switched here.

By default it is http.

Choose <System Management> <Web Access Control> in the navigation tree to open the page.

- Enable http setting.

  Enable http setting.

  Click <Save>.

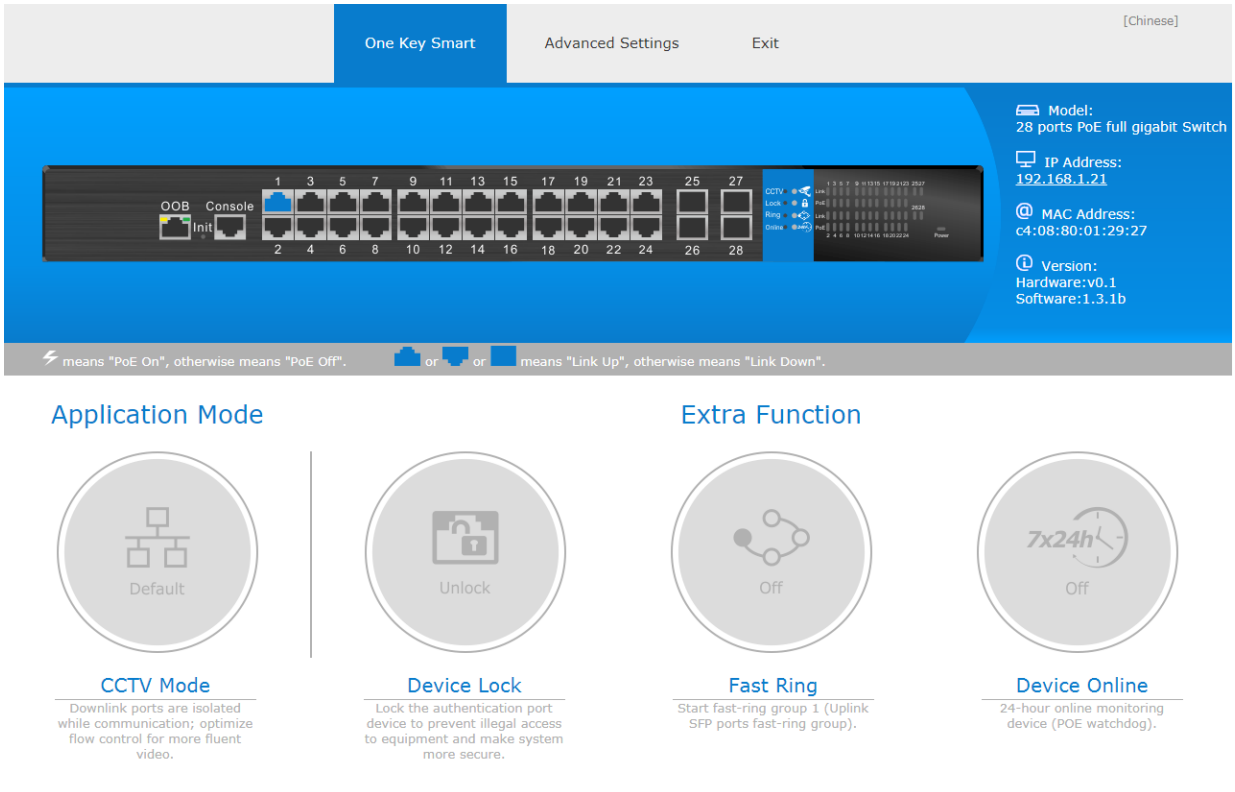
- Enable https setting.

  Enable https setting.

  Click <Save>.

14.6 One Key Smart

On this page, users could check up the main configuration and change the mode of the switch.



Procedure

Login the Web system or choose <System Management> <One Key Smart> in the navigation tree to open the page.

- View the main configuration.

Items	Descriptions
Model	The model of the switch.
IP Address	The IP address of the switch. It can be configured on <System Management> <IP Address> page.
MAC Address	The MAC address of the switch.
Version	Hardware and software version of the system.

- Switch the following mode of switch.

Items	Descriptions	Default value
CCTV Mode	Switch to this mode, downlink ports are isolated while communication; optimize flow control for more fluent video.	Disable
Device Lock	Lock the authentication port device to prevent illegal access to equipment and make system more secure.	Disable
Fast Ring	Start Fast Ring group 1 (Fast Ring group of X1.X2 ports).	Disable
Device Online	POE watchdog, 24-hour online monitoring switch.	Disable

VIDEOR E. Hartig GmbH
Carl-Zeiss-Straße 8
63322 Rödermark/Germany
Tel. +49 (0) 6074 / 888-0
Fax +49 (0) 6074 / 888-100
www.videor.com
www.eneo-security.com