ovolink

User Manual

Web Interface Access

OL-S1000 series

CONTENT

PREFEACE

This user manual describes the configuration procedures to help for properly using of the OL-S1000 series switches. It contains descriptions on performance and characteristics of the switches as well as detailed description on settings. Please carefully read this manual before installation of the switch.

This documentation is suggested to use as a guideline for:

• Network planners.

• Field technical support and servicing engineers.

• Network administrators.

The following information describes the conventions used in the documentation

-Examples provided in this document might be using devices that different from your device model or software version. It is normal that the port numbers, sample outputs, screenshots, and other information in the examples differ from your device.

ACCESSING THE SWITCH

Web Interface Access

The switch’ s web interface is accessible through the web-based authentication.

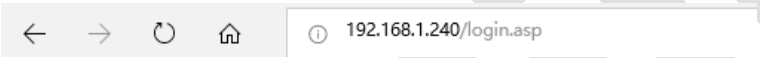
To manage your switch through a web browser in the host PC:

1) Make sure that the route between the host PC and the switch is available.

2) Launch a web browser.

3) Enter the switch’ s IP address in the web browser’ s address bar.

Default IP address is 192.168.1.240.

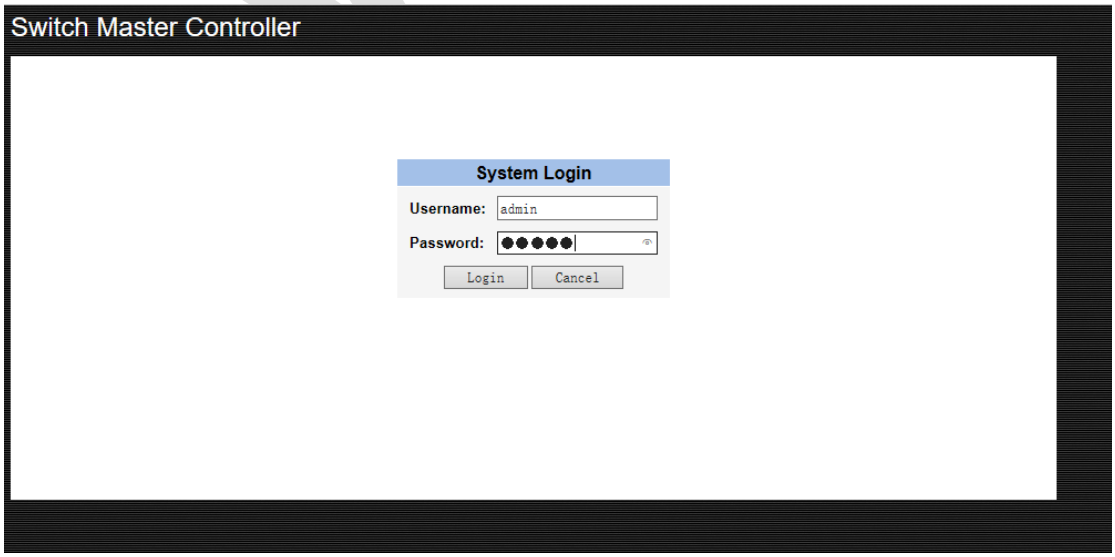


4) Enter the username and password in the pop-up login window.

Use **admin** for both，case sensitive，username and password in lower case letters.

5) Single click <Log in> or press Enter directly to enter the Web setting page

6) The typical web interface displays as below:



--View the switch’ s running status and configure it in this interface.

For security, please modify the default login password after first time login.

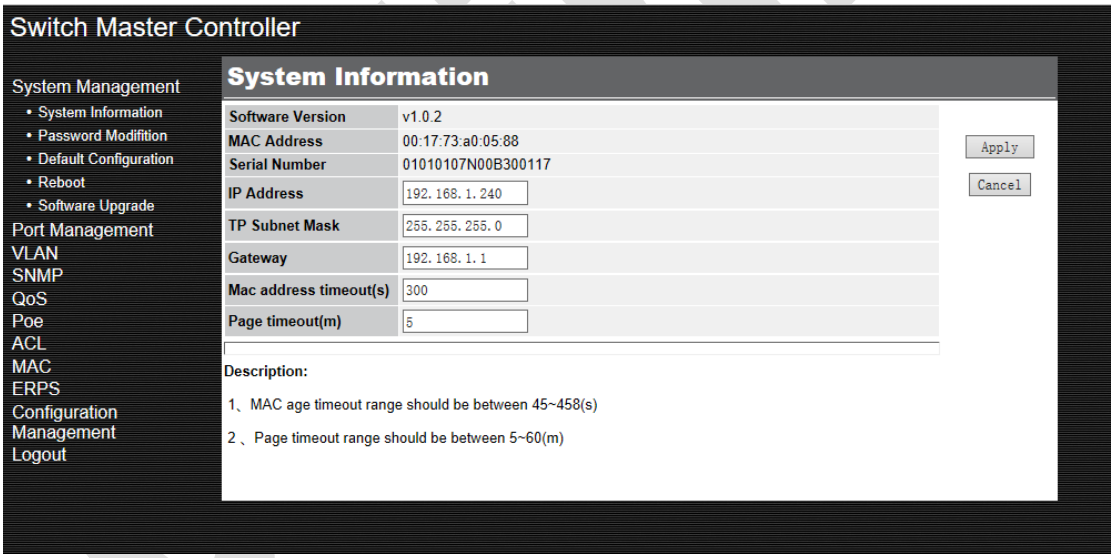
SWITCH MASTER CONTROLLER

In Switch Master Controller, the system information and configuration of the system parameters and features can be viewed.

• System Management

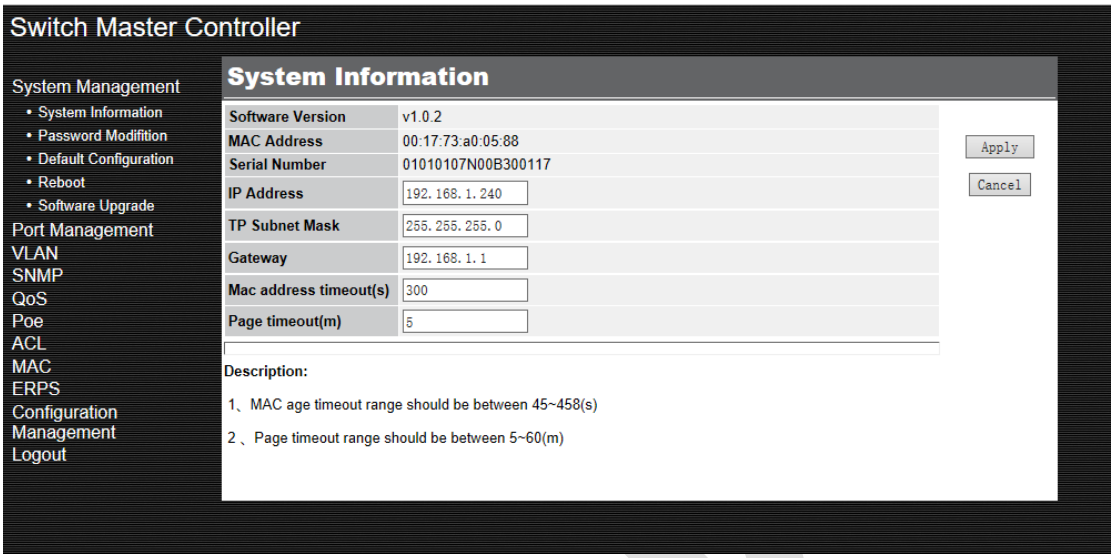
Main functions provided on this page:

View the current software version, compilation time, MAC address and Serial Number; set up relevant parameters of the system, such as IP address, Subnet Mask, MAC address timeout, page timeout, etc.



1.1 System Information

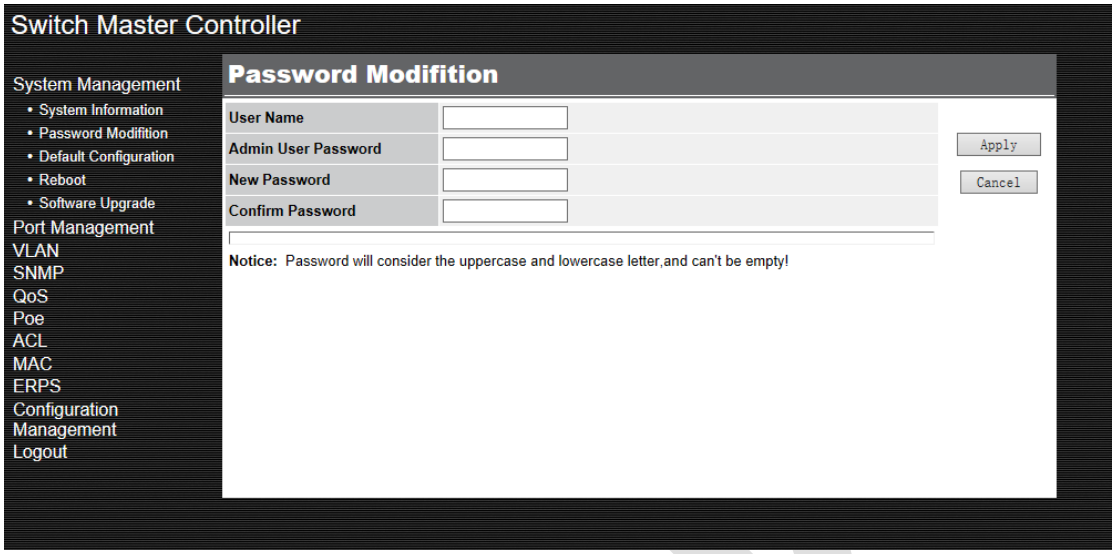
Port and system status, information, configuration description and system time can be viewed here.



Key items	Description
Software version	Display the version number of the currently running software and the software compilation time
MAC address	Display equipment MAC address
IP address	Set up equipment static IP address (192.168.1.240 by default)
Subnet mask	Set up subnet mask of equipment static IP address (255.255.255.0 by default)
Gateway	Set up the equipment gateway IP address (192.168.1.1 by default)
MAC address timeout	Set up dynamic MAC address table's aging time (300s by default)
Page timeout	WEB page timeout and exit time (5m by default)

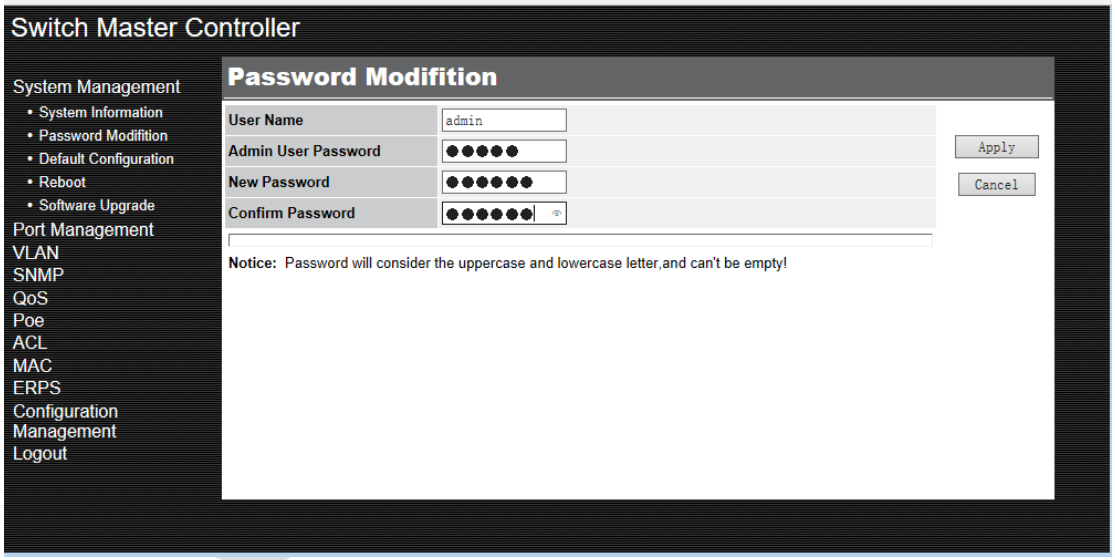
1.2 Password modification

Click on *System Management* > *Password modification* to load the following page:

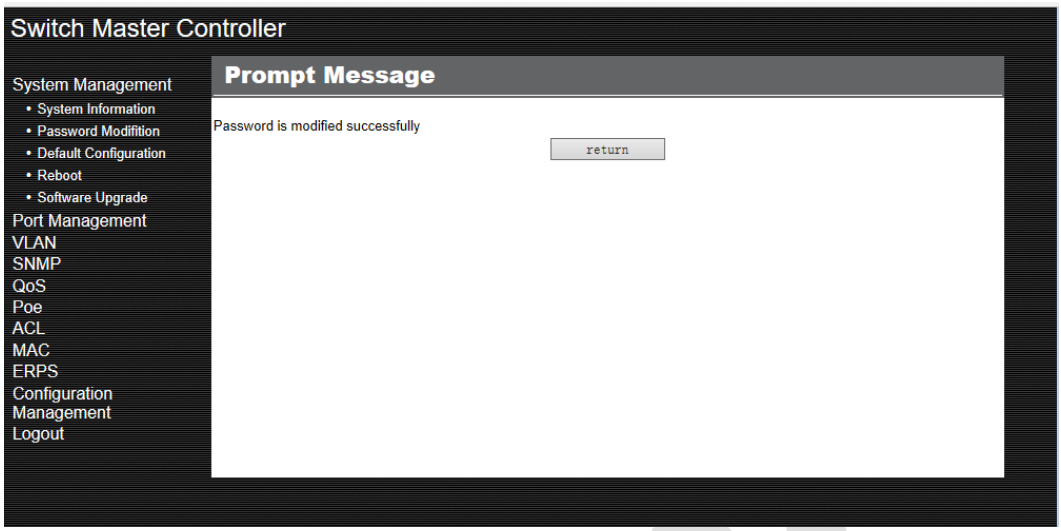


Change WEB page log in password.

The passwords are case sensitive and should compose 3-12 characters and cannot be left blank.

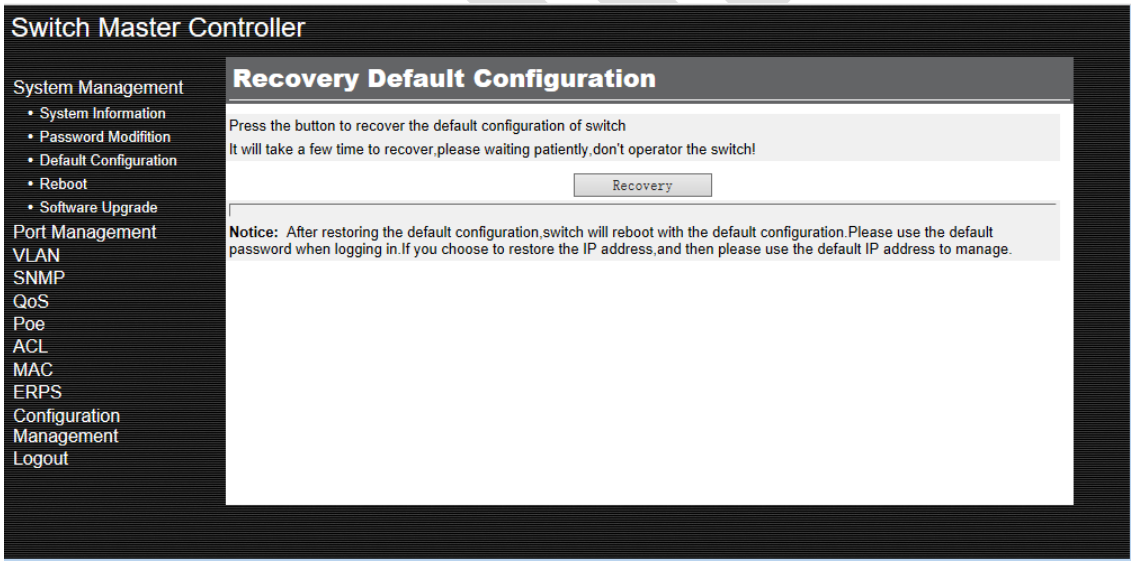


After created new password, Click " **Apply** " and the following window will pop up.



1.3 Default Configuration

Click on *System Management* > *Default Configuration* to load the following page:



Press **"Recovery"** to recover the default configuration of switch.

It takes a few minutes to recover, please waiting patiently without operate the switch.

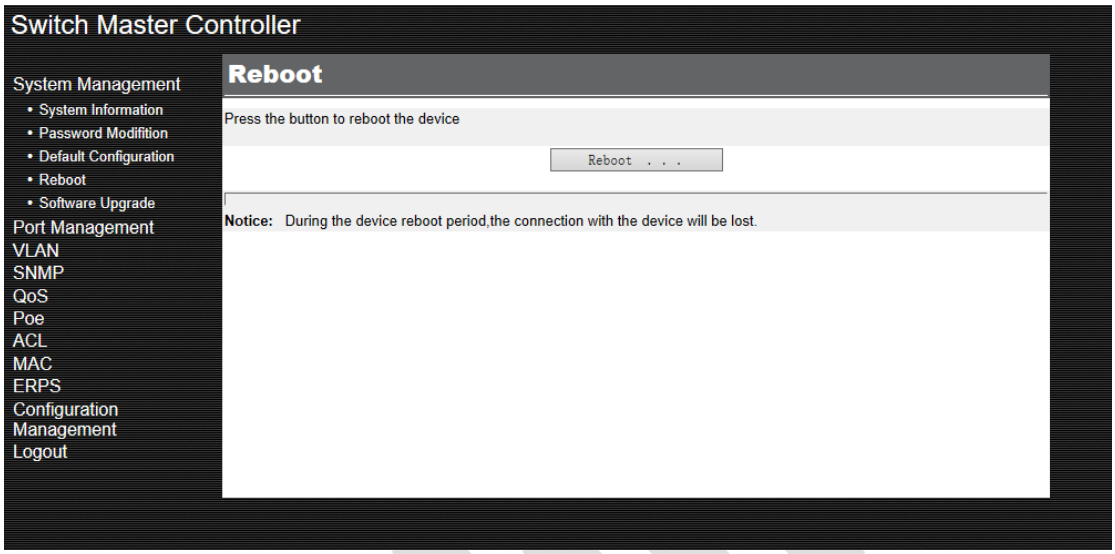
After restoring the default configuration, switch will reboot with the default configuration. Use the default configuration when logging in.

To restore the IP address will need the default IP address to manage.

1.4 Reboot the switch

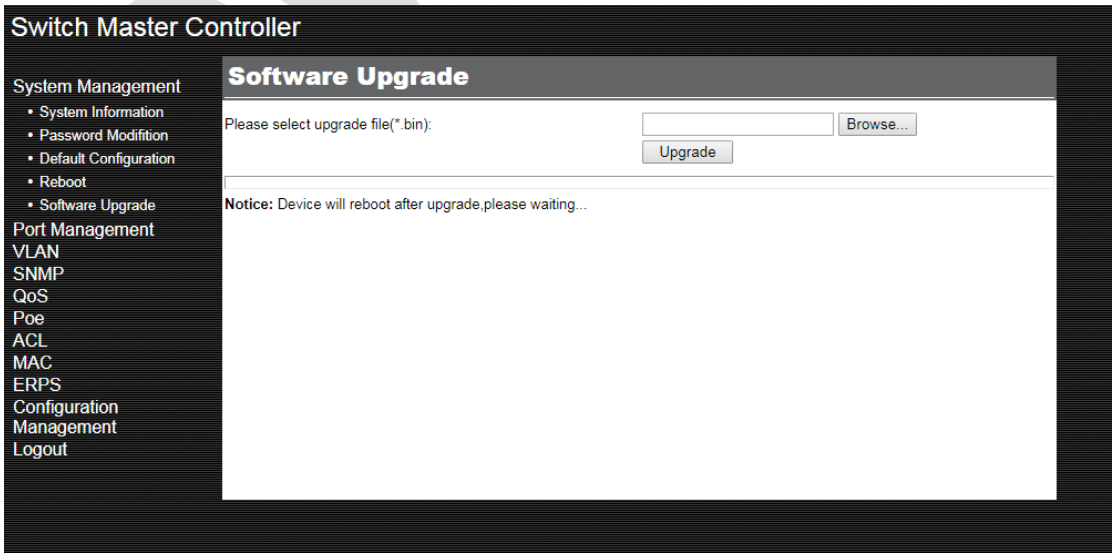
Click on *System Management > Reboot* to load the following page:

Save the current configuration before reboot the device.



1.5 Upgrading the software

Click on *Switch Master Controller > System Management> Software Upgrade* to load the following page:



Software version displayed on this page:

Follow these steps to upgrade the software:

1) Click <**Browse**> and select the proper firmware upgrade file.

2) Click <**Upgrade**> to upgrade the system.

3) Device will reboot after upgrade.

Note:

• It takes a few minutes to upgrade, please waiting patiently without operate the switch.

• It is recommended to back up your configuration before to upgrade.

• New software will validate only after the switch rebooted.

• Avoid power off or closing the upgrading page during the software upgrading process. If the system cannot automatically jump to the upgrading access prompt page after the completion of upgrading (consider at 5-10mins depends on the network condition), please open a new page and enter IP address to log in the device.

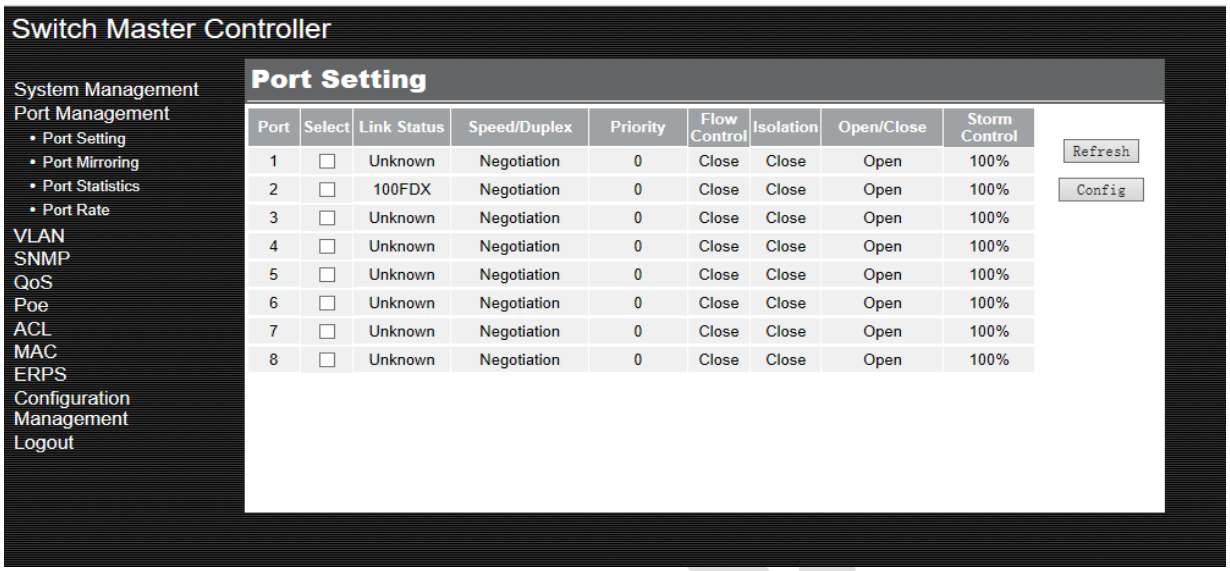
In case of power off or the upgrading page being closed in the upgrading process, please power on again and enter http://192.168.2.11 in the address bar to select the upgrading document for upgrading.

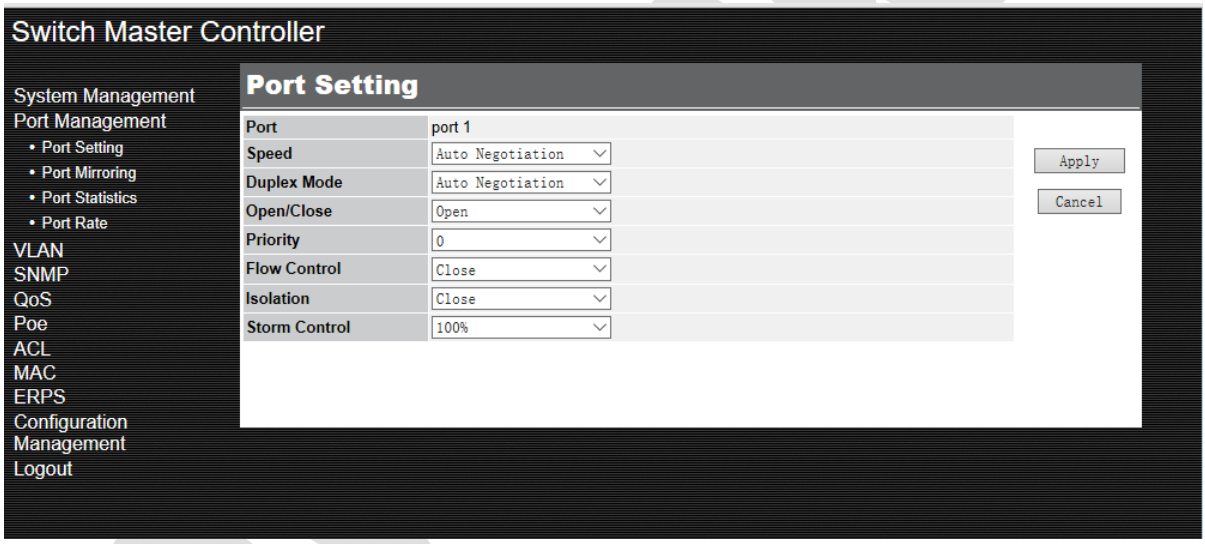
• Port Management

2.1 Port Setting

This page will display the state of attributes of ports.

Select the port for configuration and single click on <**Config**> to enter corresponding port setting page. Double click on boxes to do multiple selection on ports for batch configuration.





Parameter	Description
Link status	Actual work rate and mode of the port Unknow No Linked “100FDX” ： 100M Full Duplex 100M full duplex “100HDX” ： 100M Half Duplex “10FDX” ： 10M Full Duplex “10HDX” ： 10M Half Duplex

	Port rate can be selected: '10Mbps' : mandatory port rate at10M '100Mbps' : mandatory port rate at 100M 'Auto-negotiation' : the port rate is subject to automatic negotiation between the selected port and the end port
Speed/Duplex	Duplex mode of the port can be selected: 'Full Duplex' : the port can receive a message when sending a message 'Half Duplex' : the port can only sending or receiving a message at a time 'Auto-negotiation' : the duplex state of the port shall be subject to automatic negotiation between the selected port and the end port by default. Both the port rate and duplex state are for auto-negotiation
Priority	The priority of the port is divided into level 0~7. 0 for the lowest and 7 for the highest. For messages without 802.1Q heading tag, the equipment will use the port priority as the 802.1P priority for the port in receiving the message and search local priority mapping table. It is based on the priority to mark the local priority for the message. By default, the port priority is 0.
Flow Control	When flow control function is opened for both the equipment and the switch at the opposite terminal, if the port with flow control function open has the problem of congestion: the equipment will send flow control to the opposite terminal to inform the opposite terminal to reduce message sending speed. After receiving the flow control frame, the opposite terminal will reduce the rate for sending messages to the equipment so as to avoid loss of messages. By default, flow control function is closed.
Open/Close	When the port is closed, message forwarding cannot be realized. By default ,the port is open.
Storm Control	Default 100%

2.2 Port Mirroring

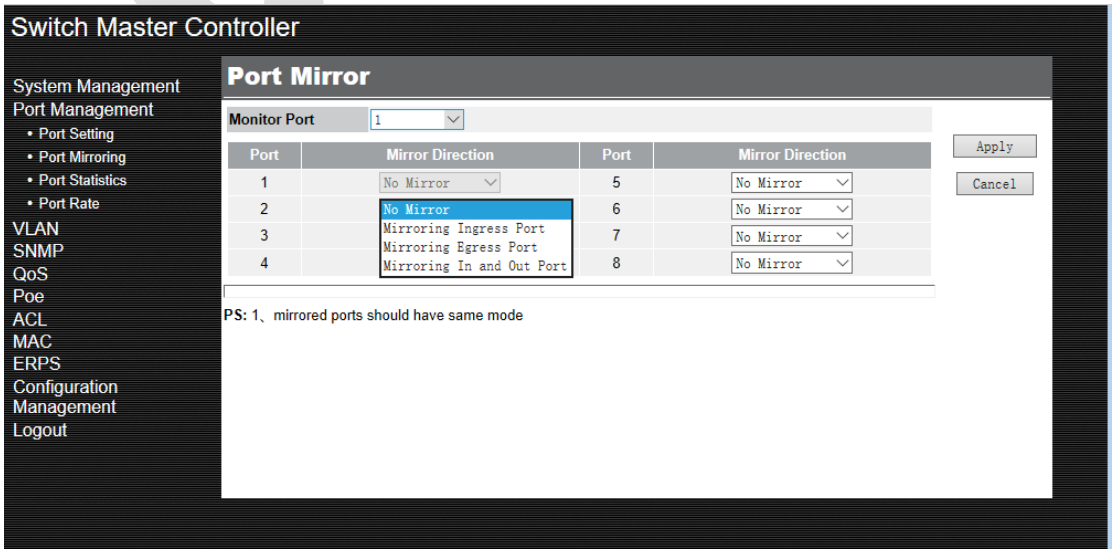
Network traffic analyzing and troubleshooting network problems by using Mirroring function.

Mirroring allows the switch to send a copy of the traffic that passes through specified sources (ports, LAGs or the CPU) to a destination port. It does not affect the switching of network traffic on source ports, LAGs or the CPU.

Click on *Port Management> Port Mirror* to load the following page:

Monitoring ports and mirrored ports can be done on this page. By default, mirroring function cannot be used.

The above page displays a mirroring session. Chose Monitor Port, Click <**Apply**> to configure this mirroring session on the following page:



Key items	Description
Monitoring port	'Un-mirroring' means not to use the equipment mirroring function. A port once being set up as the monitoring port cannot be set up as the mirroring port.
Mirroring direction	'Un-mirroring' means that the port will not be mirrored; 'Mirroring ingress port' : only messages received by this port can be mirrored to the monitoring port; 'Mirroring egress port' : only messages sent by this port can be mirrored to the monitoring port; 'Mirroring ingress and egress port' : messages received and sent by the port will be mirrored to the monitoring port;

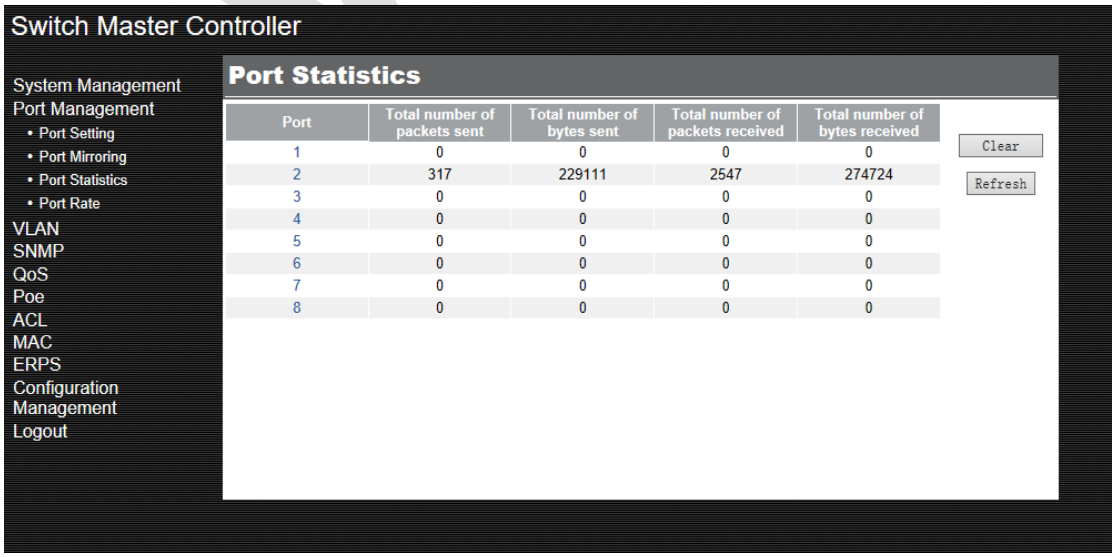
2.3 Port statistics

Viewing IPv4 Multicast Statistics on Each Port.

Click on *Port Management> port statistics* to load the following page:

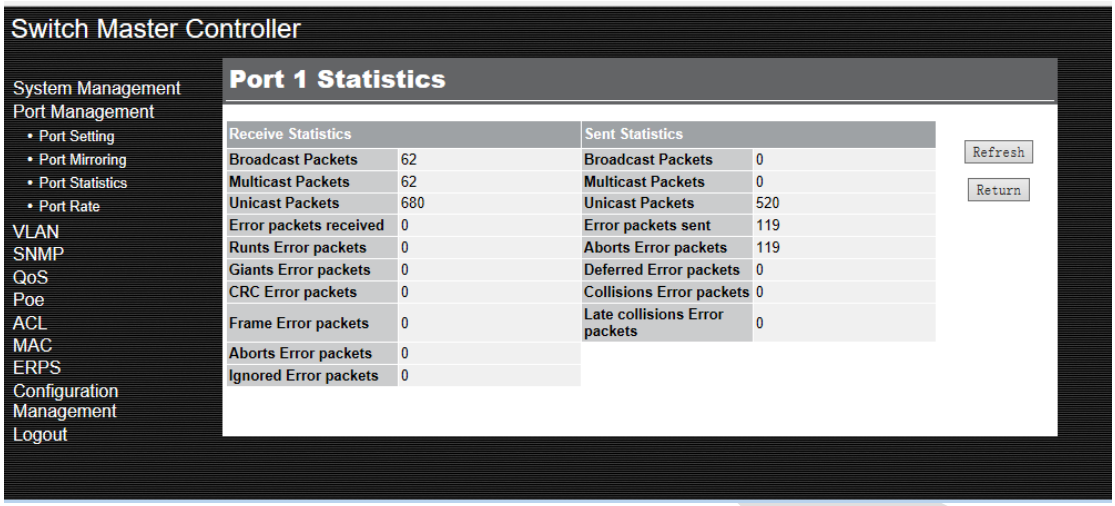
View information on total data package received/sent by various ports of the device.

(Main stage)



View the number of error packages received/ sent on the designated port by single

clicking on items corresponding to the port on the main page to enter corresponding statistic information page.

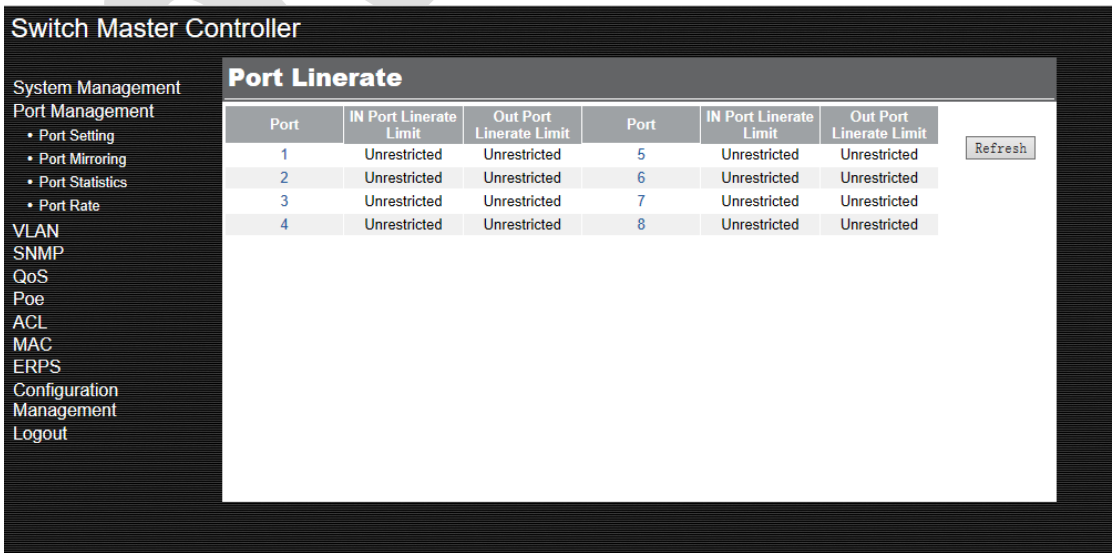


Follow these steps to view port statistics on each port:

To get the real-time multicast statistics, enable Auto Refresh, or click <**Refresh**> to enable Auto Refresh or disable Auto Refresh. When enabled, the switch will automatically refresh the multicast statistics. Refresh Interval after Auto Refresh is enabled, specify the time interval for the switch to refresh the multicast statistics.

2.4 Port Rate

Click on *Port Management> port rate* to load the following page:



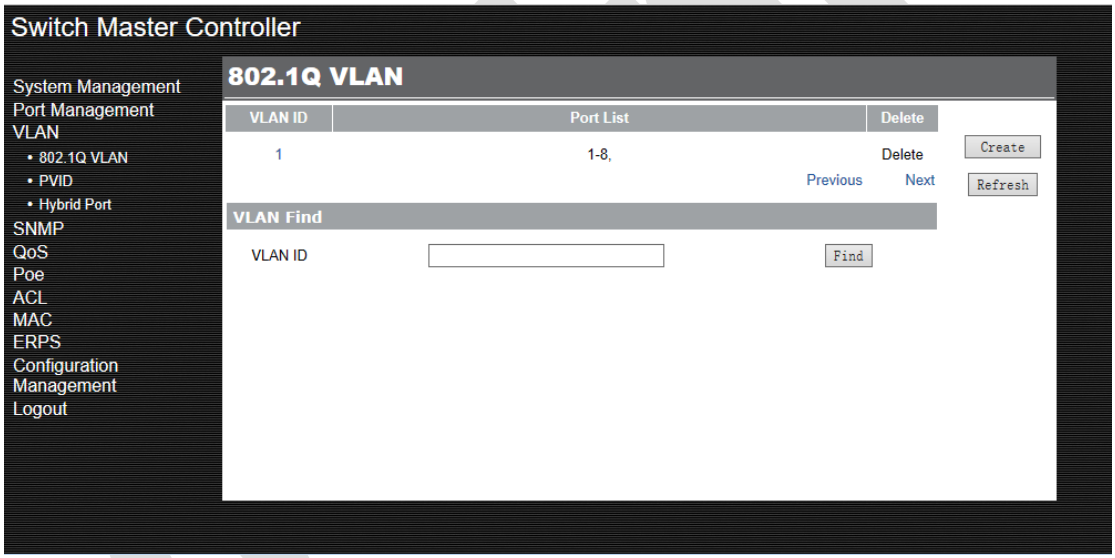
Explanation: port rate limit function cannot be used by default. Rate limit level is the level for rate limit at the port.

Rate limit level: range (0-127), 0 refers to no rate limit;

Actual rate: the port rate after rate limit. It is calculated based on the port rate limit level.

- VLAN

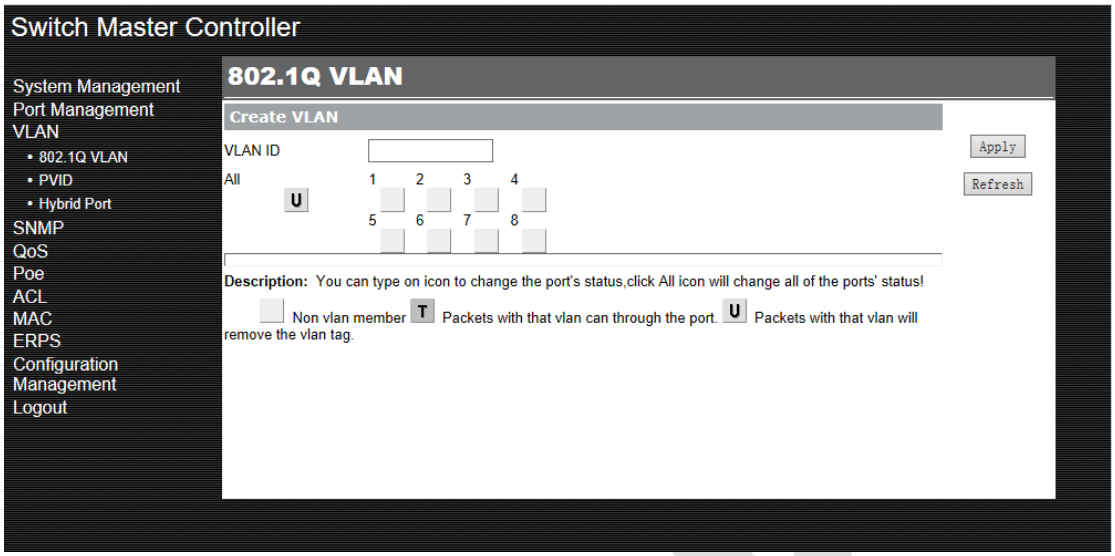
In the VLAN Config section, Click on *Switch Master Controller> VLAN* to load the following page:



3.1 802.1Q VLAN:

802.1Q Standard defines a kind of new frame format. A Tag field is added behind the standard Ethernet frame source address. This field refers to VLAN ID of different VLANs for identification. When data frame passing the switch, the switch will identify their VLAN based on the VLAN ID information tag.

Data frame of the VLAN will be communicated only in this VLAN.



New VLAN (single click on '**Create**' button on the main page to enter the corresponding page. Enter the created VLAN info in the 'VLAN ID' textbox. Click on **'Apply'** to take effect.

Select to define if the port belongs to VLAN or not.

'T' means Packets with VLAN through port

'U' means Packets with VLAN will remove the VLAN tag

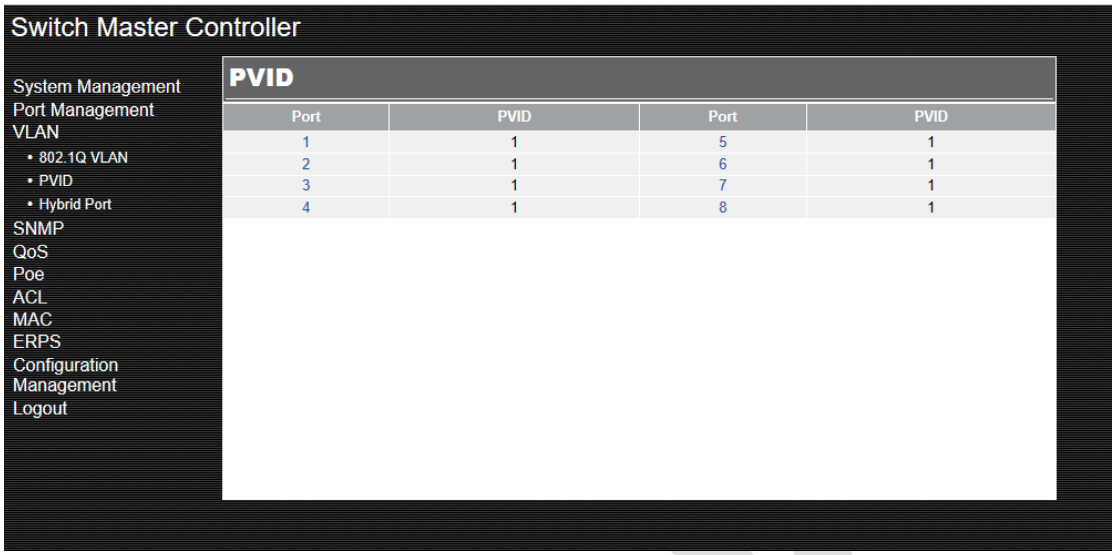
Blank means it does not belong to VLAN.

3.2 Port PVID under 802.1QVLAN mode

PVID: Designate tag vid for untagged messages in port inlet direction; such messages when going out from tag port will be tagged.

Tag vid=PVID.

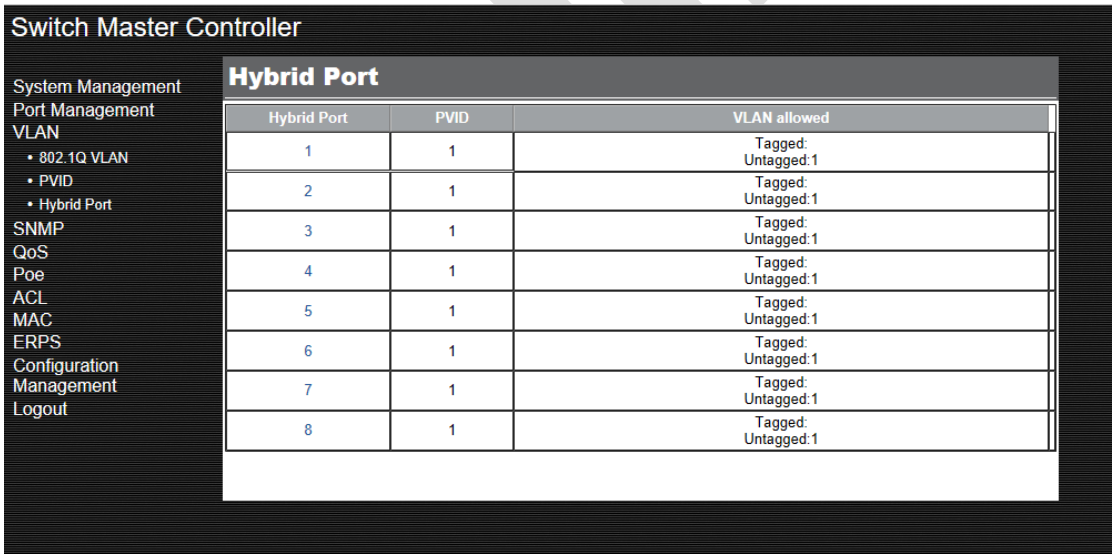
By default, the port PVID is 1.



3.3 Hybrid port.

All the ports of the device are Hybrid ports.

Following page shows VLAN allowed and tag control.



Enter VLAN ID in the 'tagged VLAN' textbox and messages of such VLAN will allow passing the port and messages will have VLAN Tag when going out of the port;

Enter VLAN ID in the 'untagged VLAN' textbox and messages of such VLAN will allow passing the port. The message will NOT have VLAN Tag when going out the port.

PVID and VLAN allow passing must use the existing VLAN.

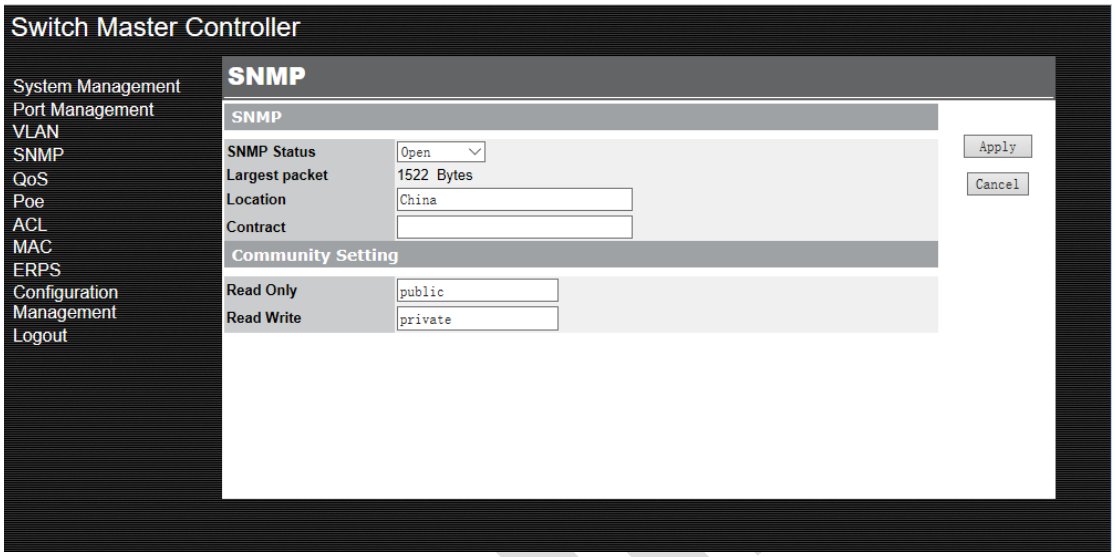
PVID is the default VLAN ID.

- SNMP

Access Interface

Select the interface to control the methods for users' accessing.

Manage the network devices via NMS.



Item	Description
SNMP Status	Open/close SNMP function; it is open by default.
Largest Packet	Set up the size of the largest SNMP message package that can be received/sent by SNMP Agent.
Location	In case of any fault of the switch, maintenance personnel is able to fast locate the failure, thus ensuring fast problem solving. System maintenance contact information is 'Blank' by default and physical location information of the equipment is originally set as 'China'.
Contact	The contact personnel that manages the device.
Read Only	Community with read only rights can only inquire equipment information; by default, it is set as 'public'.
Read Write	Community with read and write rights can

	configure the equipment; by default, it is 'private' .

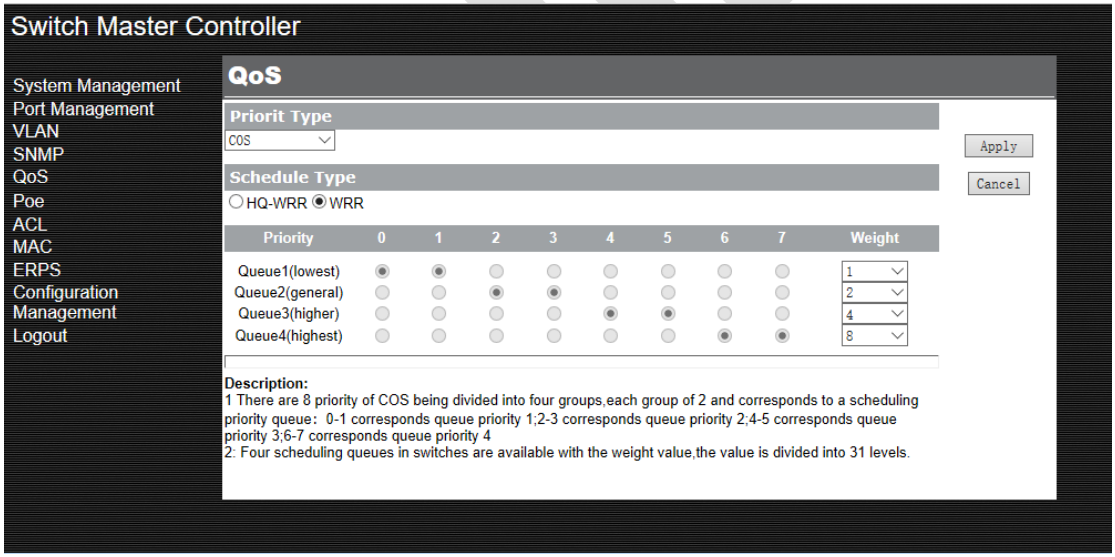
• QoS

The device supports simple QoS function. In case of network congestion, the system will control message forwarding order based on user settings on message priority trust mode and queue scheduling algorithm.

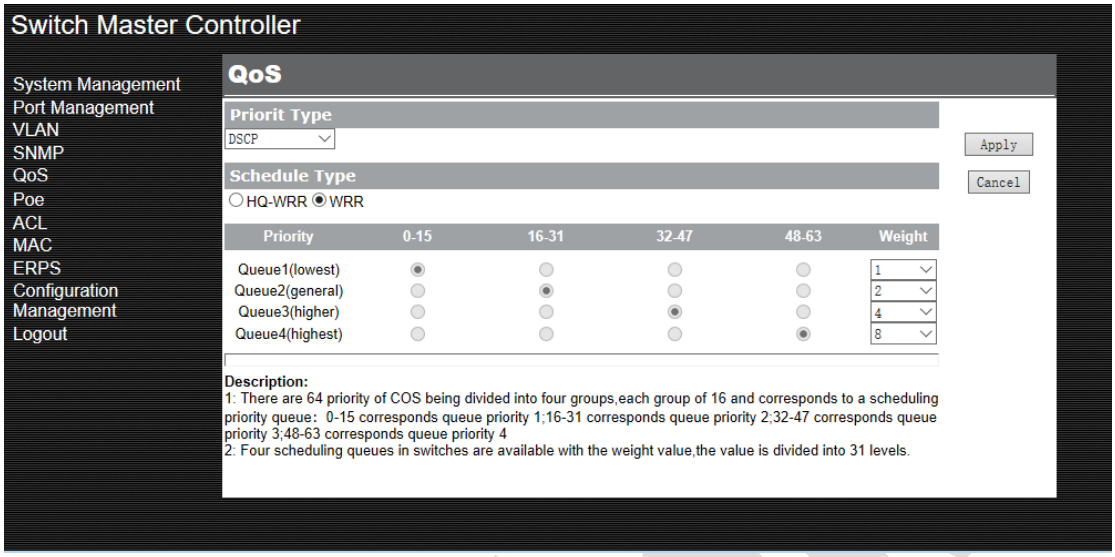
The device supports two kinds of message priority trust: 802.1p priority (COS) and DSCP. The equipment will map the messages to the designated queue based on the trust priority that being selected :

Four queues are supported in total;

Queue 1 at the lowest priority, whereby queue 4 at the highest priority.



802.1Q priority Type(COS)	Queue
0、1	0
2、3	1
4、5	2
6、7	3



The four scheduled queues are available with 31 levels of weight value.

DSCP Priority	Queue
0~15	1
16~31	2
32~47	3
48~63	4

Key Item	Explanation
Priority Type	Select priority trust mode of messages 1. COS: according to 802.1p priority, key the message into the export queue of the port at corresponding priority 2. DSCP: according to DSCP priority, key the message into the export queue of the port at corresponding priority By default, the device will place messages into the export queue of the port at

	corresponding priority according to 802.1p
Schedule Type	Select the queue scheduling mode E.g.: if the weight ratio of queue 1, queue 2, queue 3 and queue 4 is 1: 2: 4: 8 and the queue scheduling mode is WRR, the port will send messages by the flow ratio of 1: 2: 4:8 in case of data message congestion in the queue 1, 2, 3 and 4 at a port; if the scheduling mode is selected to be HQ-WRR, the equipment will at first to guarantee the prior sending of messages in queue 4 and then apply WRR scheduling for other 3 queues. By default, the equipment will use WRR queue scheduling mode
Weight	Set up the priority weight of the queue It is 1: 2: 4: 8 by default

• PoE Configurations

PoE Only for products that support PoE feature.

Allow all PoE-related traps, including:

Over-max-pwr-budget: Triggered when the total power required by the connected PDs exceed the maximum power defined by the PoE switch.

Port-pwr-change: Triggered when a port starts to supply power or stops supplying power.

Port-pwr-deny: Triggered when the switch powers off PDs on low-priority PoE ports. When the total power required by the connected PDs exceed the system power limit, the switch will power off PDs on low-priority PoE ports to ensure stable running of the other PDs.

Port-pwr-over-30w: Triggered when the power required by the connected PD exceeds

30 watts.

Port-pwr-overload: Triggered when the power required by the connected PD exceeds the maximum power of the port can supply.

Port-short-circuit: Triggered when a short circuit is detected on a port.

Thermal-shutdown: Triggered when the PSE chip overheats. The switch will stop supplying power in this case.

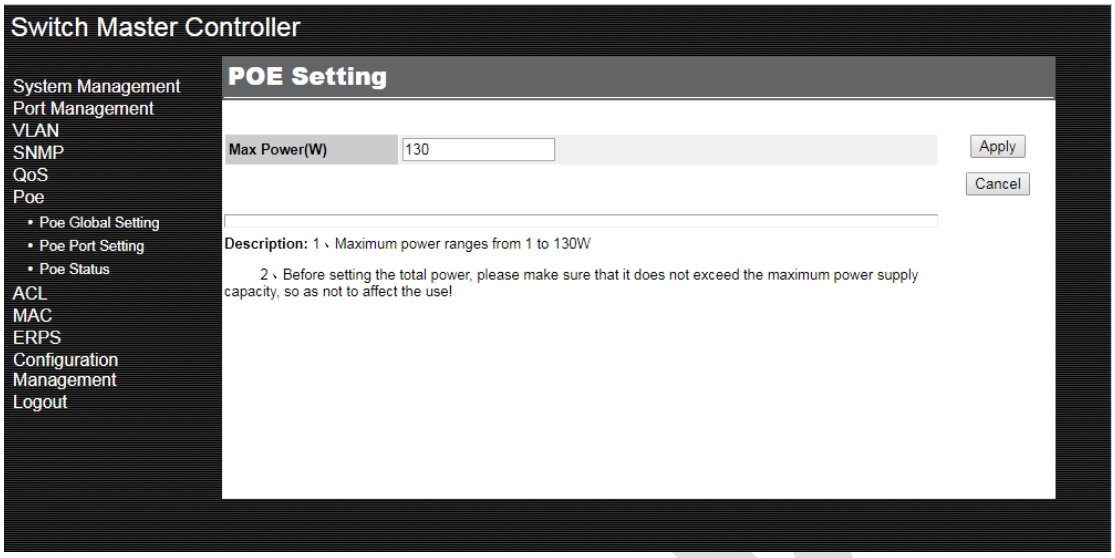
Power over Ethernet (PoE) is a remote power supply function. With this function, the switch can supply power to the connected devices over twisted-pair cable. Some devices such as IP phones, access points (APs) and cameras may be located far away from the AC power source in the actual use. PoE can provide power for these devices without requiring to deploy power cables but a single cable to provide both data connection and electric powers.

IEEE 802.3af and 802.3at are both PoE standards. The standard process of PoE power supply contains powered-device discovery, power administration, disconnect detection and optional power-device power classification.

PSE Power sourcing equipment (PSE) is a device that provides power for PDs on the Ethernet, for example, the PoE switch. PSE can detect the PDs and determine the device power requirements.

PD Powered device (PD) is a device receiving power from the PSE, for example, IP phones and access points. According to whether PDs comply with IEEE standard, they can be classified into standard PDs and non-standard PDs. Both standard POE and Non-standard PDs can be powered via our switches.

Choose the menu Switch Master Controller> PoE > PoE Global to load the following page.



6.1 POE Global Setting

In the PoE Global setting section, you can view the Maximum power.

The Maximum power

Displays the maximum power the PoE switch can supply.

In addition, you can configure the global power. Click <**Apply**>.

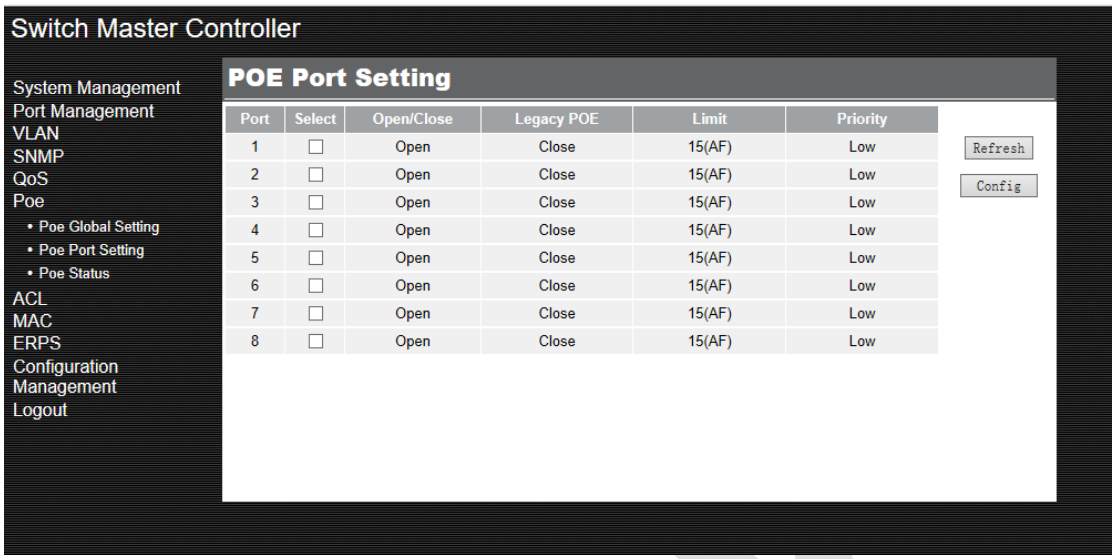
Note: please make sure power not exceed global power limit.

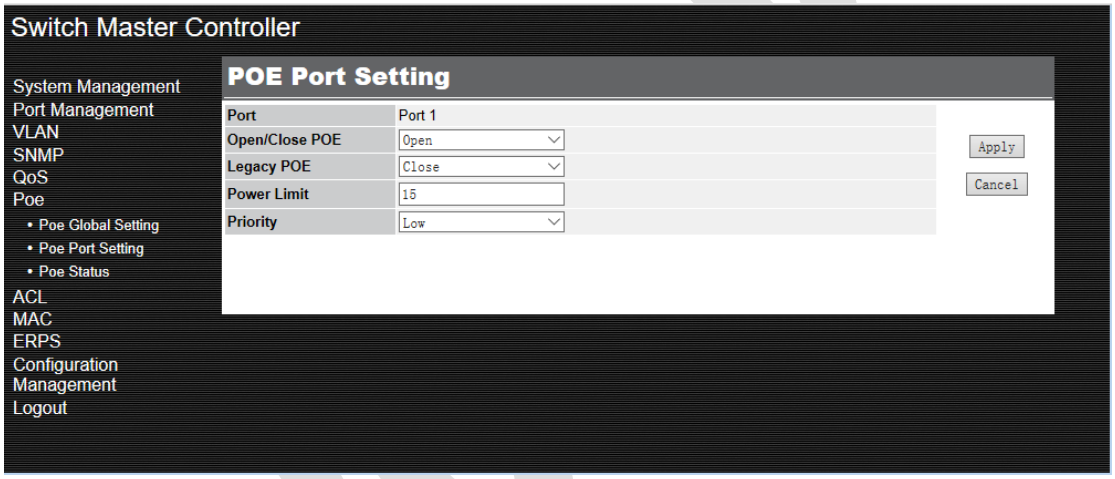
.

6.2 POE port Setting

To set POE port, follow these steps:

1) Select the port that you want to configure
2) Click <**Config**>
3) Specify the parameters.
4) Click <**Apply**>





- Open/Close PoE

  Enable or disable the PoE function for the corresponding port. The port can supply power to the PD when its status is OPEN.

- PoE Priority

  Select the priority level for the corresponding port.

When the supply power exceeds the system power limit, the switch will power off PDs on low-priority ports to ensure stable running of other PDs.

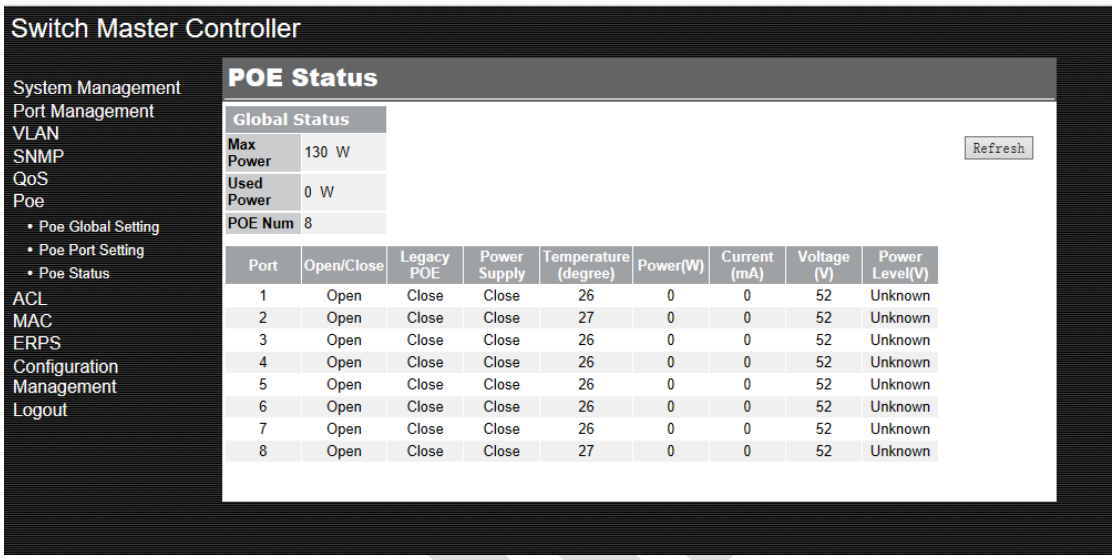
- Power Limit

  Specify the maximum power the corresponding port can supply.

- Power Limit Value (0.1w-30w)

6.3 PoE status

Click on Switch Master Controller> PoE > PoE Status to load the following



- Max Power

  Specify the maximum power on the PoE switch.

- Used Power (w)

  Displays the port’ s real-time power supply.

- POE Num:

  Displays the number of POE ports.

- Open/Close

  PoE Status displays the PoE function for corresponding port. The port can supply power to the PD when its status is OPEN.

- Legacy PoE

  Displays Legacy PoE Open or Close

- Power Supply

  Displays current Power Supply Open or Close

- Temperature

  Displays the port’ s real-time temperature

- Power

  Displays the real-time system power consumption of the PoE switch.

- Current (mA)

  Displays the port’ s real-time current.

- Voltage (v)

  Displays the port’ s real-time voltage.

- Power Level

  Displays the class of the linked PD. PoE Priority displays the priority level for the corresponding port.

• ACL

Overview

ACL (Access Control List) filters traffic as it passes through a switch and permits/denies packet crossing specified interfaces or VLANs. It accurately identifies and processes the packets based on the ACL rules. ACL helps to limit network traffic, manage network access behaviors, forward packets to specified ports and more.

To configure ACL, follow these steps:

1) Configure a time range during which the ACL is running.

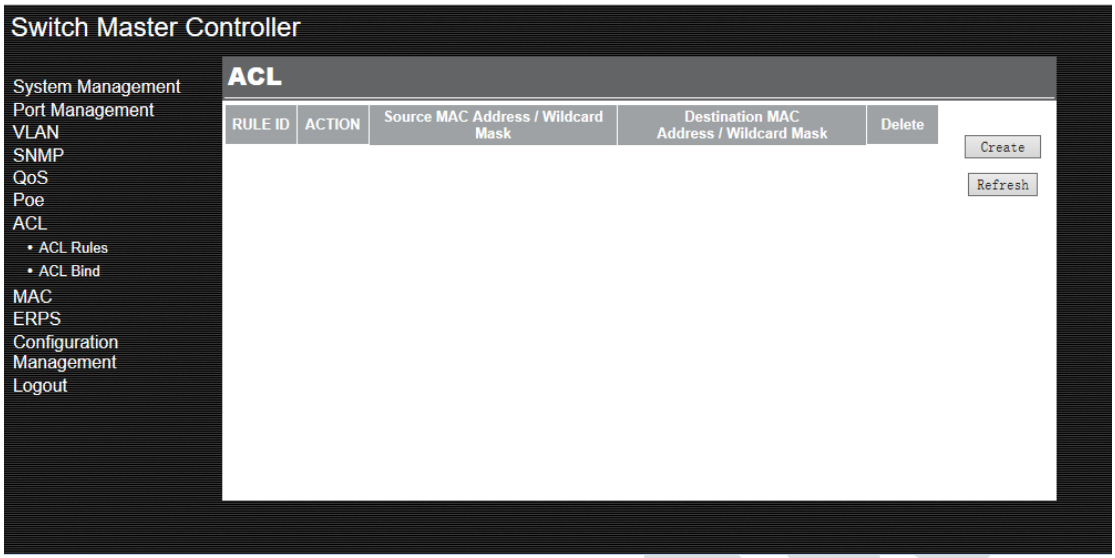
2) Create an ACL and configure the rules to filter different packets.

3) Bind the ACL to a port or VLAN to make it effective.

Configuration Guidelines

- A packet ‘matches’ an ACL rule when it meets the rule’ s matching criteria. The resulting action will be either to ‘permit’ or ‘deny’ the packet that matches the rule.
- If no ACL rule is configured, the packets will be forwarded without being processed

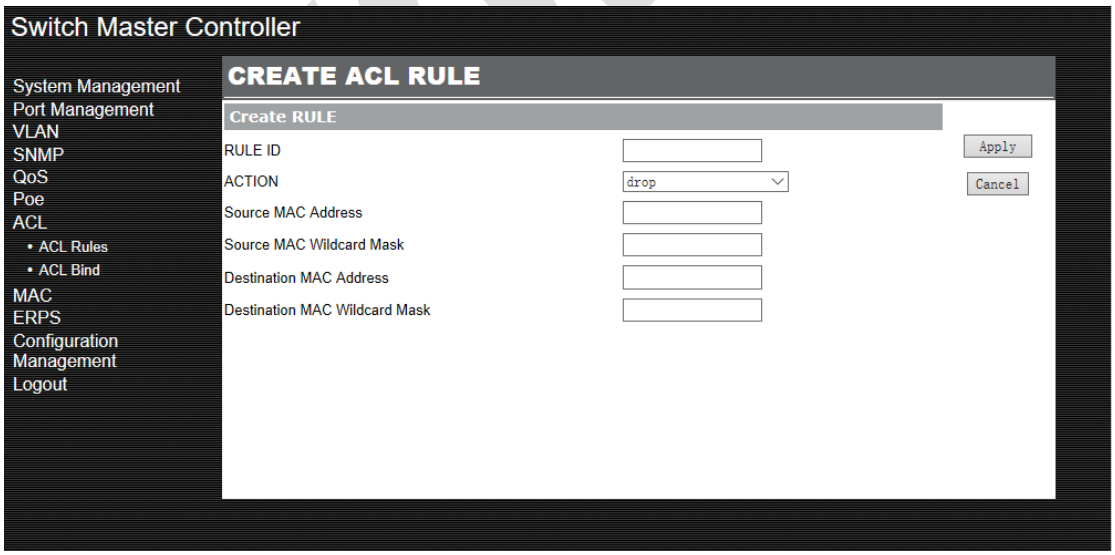
by the ACL. If there is configured ACL rules and no matching rule is found, the packets will be dropped.



7.1 Create ACL Rules

MAC ACL: MAC ACL uses source and destination MAC address for matching operations.

In ACL Rules Table section, click to open the following page.



Follow these steps to configure the MAC ACL rule:

1) In the MAC ACL Rule section, configure the following parameters:

Rule ID

Enter an ID number to identify the rule. It should not be the same as any current

rule ID in the same ACL. For the convenience of inserting new rules to an ACL, it is suggested to set the appropriate interval between rule IDs.

Action

Select an action to be taken when a packet matches the rule.

None: The packets will forward normally.

Drop: The packets will discard.

Source-MAC/Mask

Enter the source MAC address with a mask.

A value of 1 in the mask indicates that the corresponding bit in the address will be matched.

Destination-MAC/Mask

Enter the destination MAC address with a mask.

6) Click <**Apply**>.

7.2 ACL Bind

To bind the ACL to a port or a VLAN, the received packets on the port or in the VLAN will then match and process according to the ACL rules. An ACL takes effect only after it is bound to a port or VLAN.

Note:

• Different types of ACLs cannot be bound to the same port or VLAN.

• Multiple ACLs of the same type can be bound to the same port or VLAN. The switch matches the received packets using the ACLs in order.

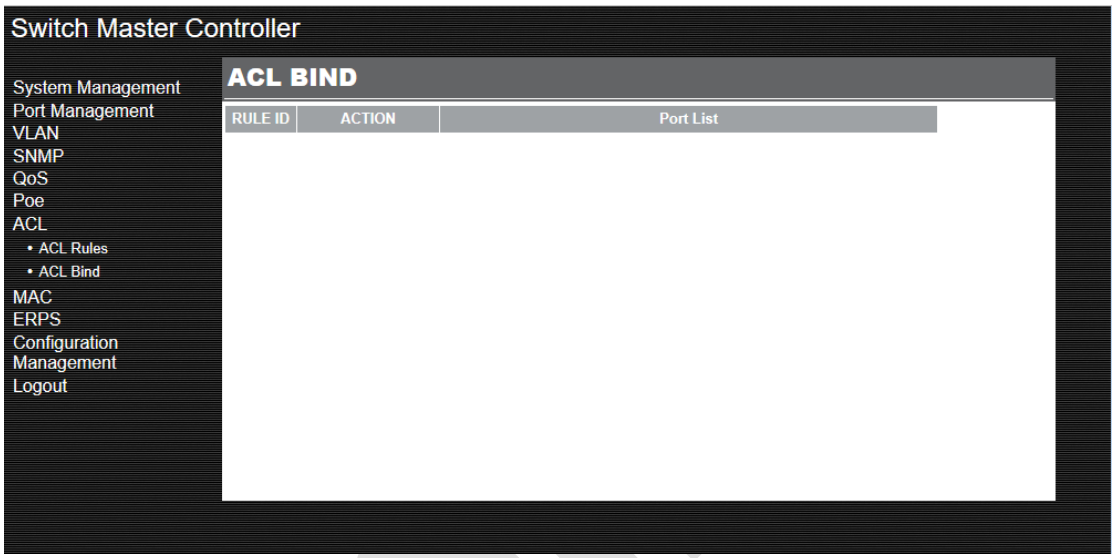
The ACL that is bound earlier has a higher priority.

Binding the ACL to a Port, Click on Switch Master Controller> ACL > ACL Bind > Port Binding and click to load the following page. Follow these steps to bind the ACL to a Port:

1) Choose ID or Name to be used for matching the ACL. Select an ACL from the drop-down list.

2) Specify the port to be bound.

3) Click <**Create**>.



- **MAC**

Mac Address Configurations

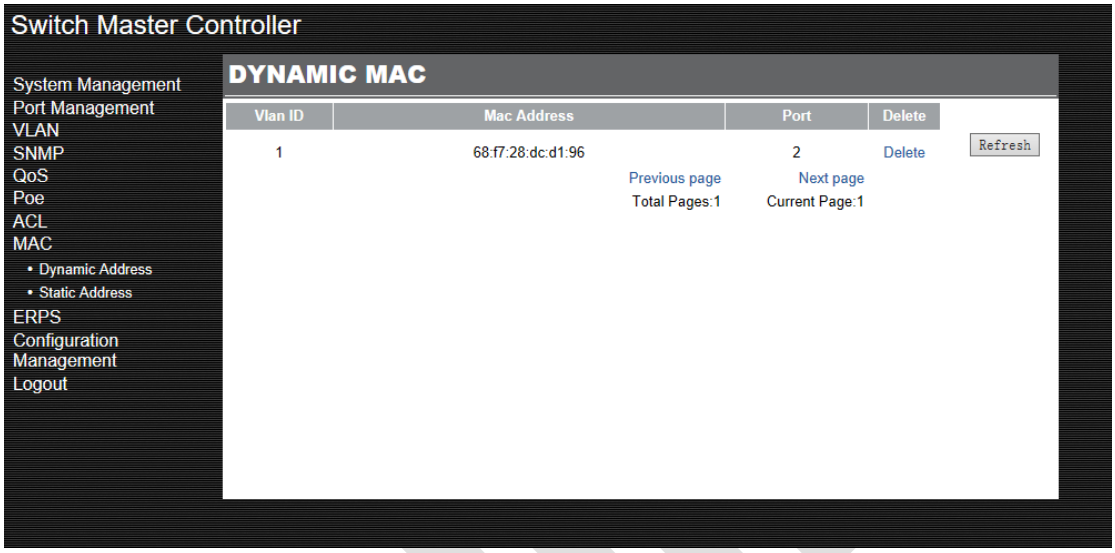
- Dynamic address

Dynamic addresses are addresses learned by the switch automatically and the switch regularly ages out those that are not in use. The switch removes the MAC address entries related to a network device if no packet is received from the device within the aging time. Specify the aging time if needed.

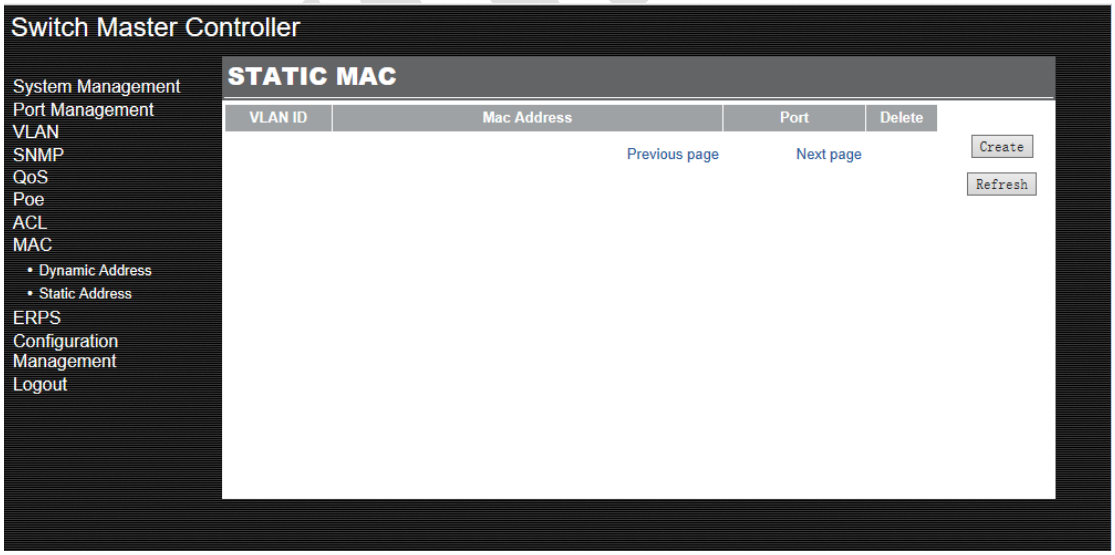
- Static address

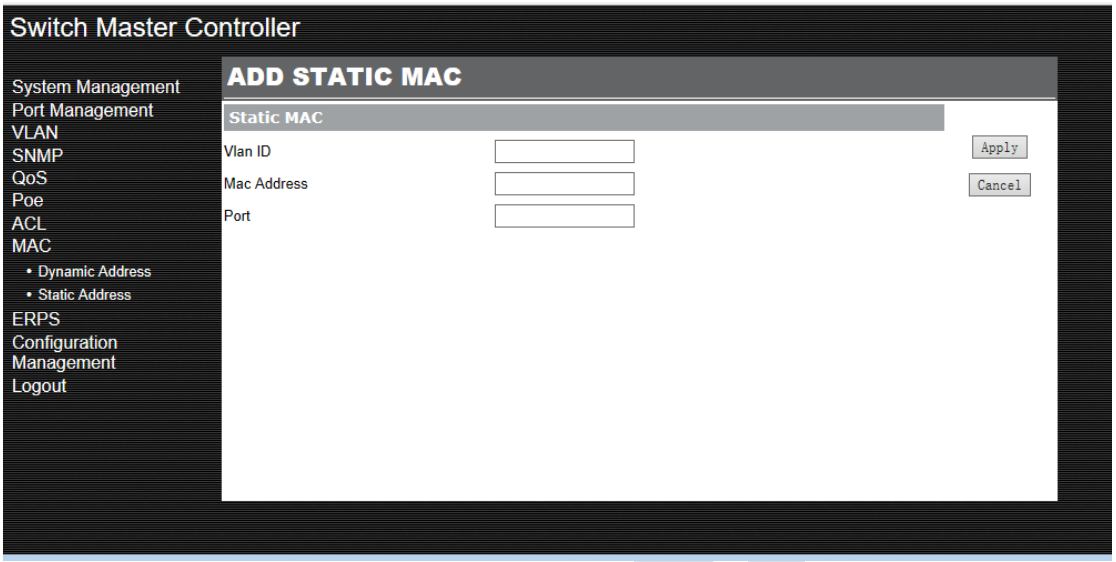
Static addresses are manually added to the address table and do not age. For relatively fixed connection and frequently visited server, to manually set the MAC address of the server as a static entry to enhance the forwarding efficiency of the switch.

8.1 Dynamic MAC



8.2 Static Mac





Note:

• In the same VLAN, once an address is configured as a static address, it cannot be set as a filtering address. Vice versa.

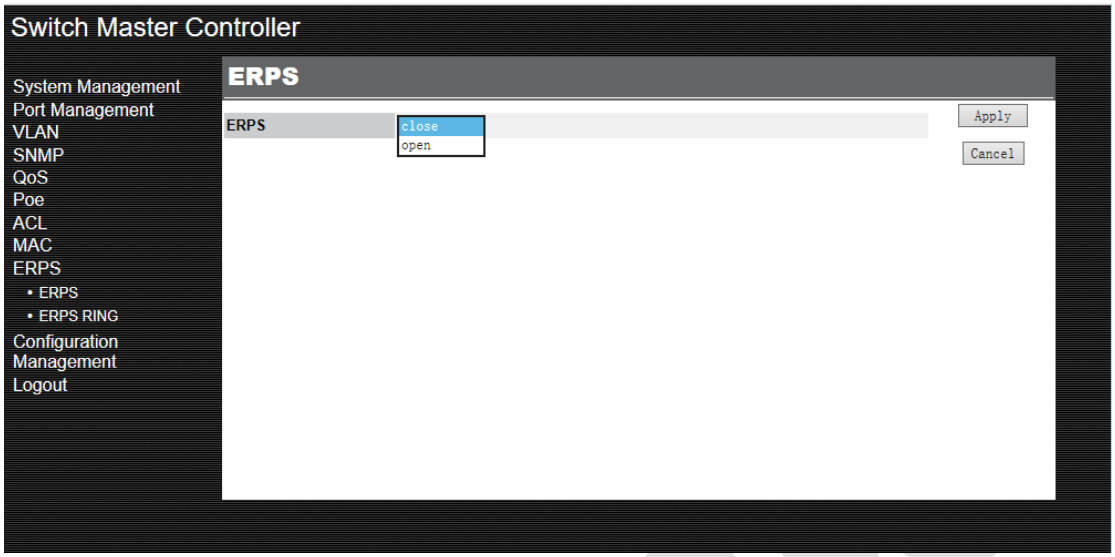
• Multicast or broadcast addresses cannot be set as static addresses.

• Ports in LAGs (Link Aggregation Group) are not supported for static address configuration

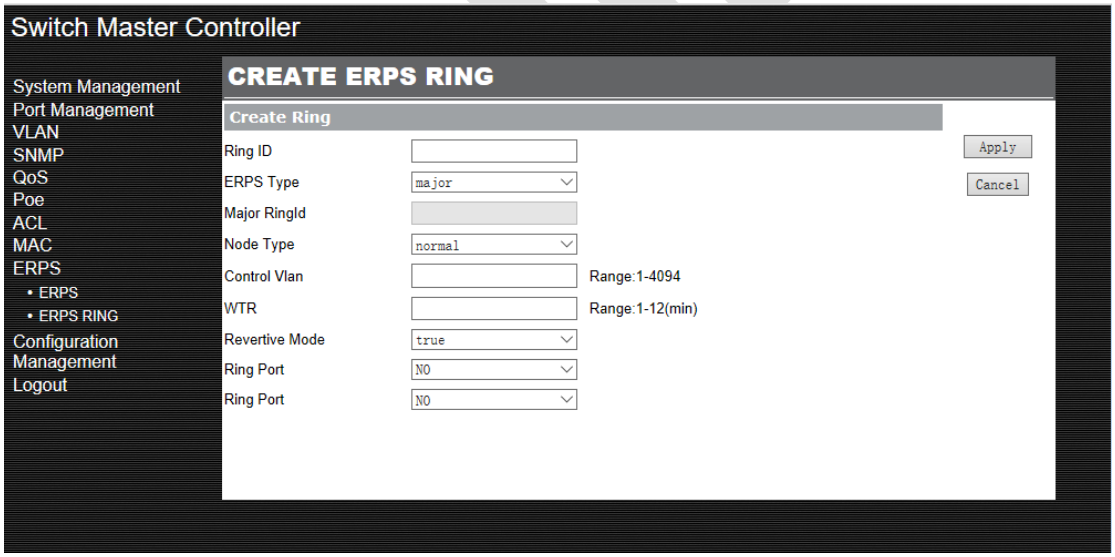
• ERPS

In a loop, data will be transmitted in cycle by ports in the loop, thus forming data congestion. When open the loop for detection, the port forming the loop will be automatically blocked off. Select to enable this function in the 'loop detection' drop box. By default, it is closed.

9.1 ERPS



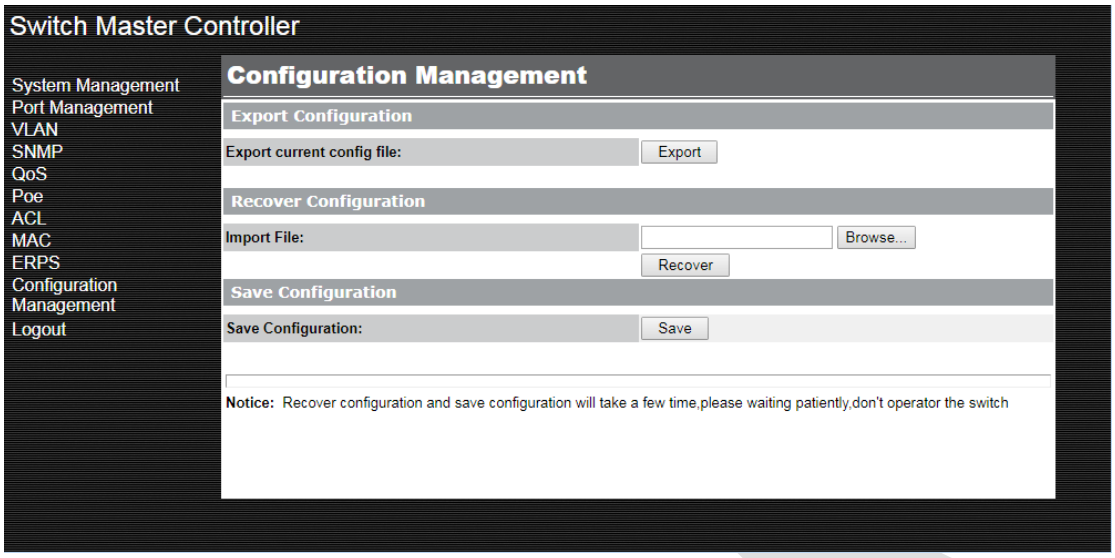
9.2 ERPS RING



- **Configuration Management**

After configuration of all items on the setting page, be sure to save your configuration.

Unsaved configuration will be lost due to reboot or other operation.



Item	Description
Export	Single click 'Export' to select the configuration file backup path to save the current equipment configuration in the computer. You may restore configuration by this fire (*.cfg) in the future)
Recover	Single click ' Browse...' to select formally backed up file (*.cfg). Single click 'restore' and confirm to restore the equipment to the previous configuration (the configuration takes effect after automatic reboot)
Save	Single click "Save" to save current configuration information so that it will not be lost after reboot

Note:

1. A long period of time may be required for configuration import and export. Please wait with patient and don' t operate the switch.

2. Please don' t close the power supply of the switch in the configuration import and export process.

- **Log out**

If you have completed the setting of all configuring items and completed the saving operation, you may single click "Logout" in the navigation bar and click "Yes" to exit the Web setting page.