WEB Management User Manual

ESMGS4-P2-B

ESMGS8-P4-B

ESMGS8-C2-B

ESMGS24-P4-B

ESMGN4-P2-B

ESMGN8-C2-B

ESMPN8-N2-B

ESMGN8-P4-B

ESMPN24-C4-RX-B

ESMGS24-P4-RXN-B

Table of content

1 WEB Configuration

1.1 Preparing and Entry

Configure the switch through Web pages, this chapter will take you through the equipment configuration process. After completing the hardware installation, you need to ensure that the computer networks parameters to meet certain conditions before accessing the Settings page.

1.1.1 Switch Default Configuration

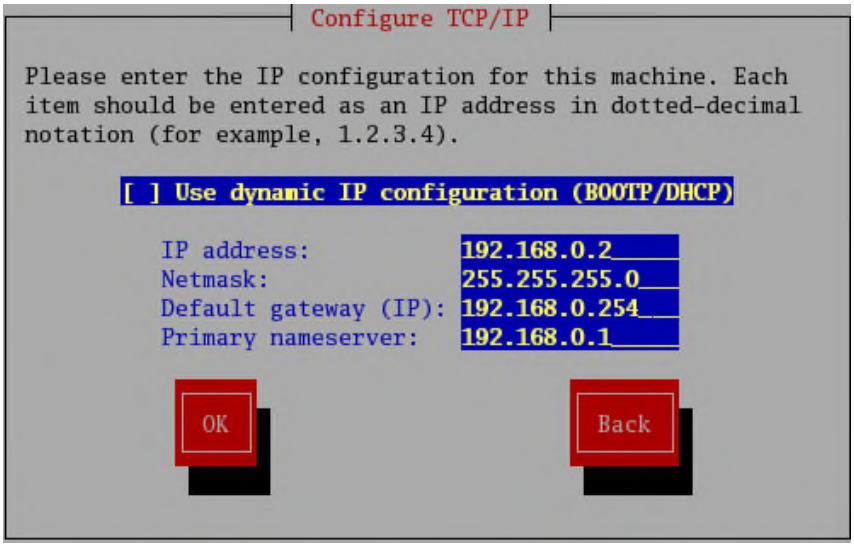
The system default IP address is: 192.168.0.240, user name: admin; password: admin

1.1.2 Computer basic configuration requirement

Ethernet card installed, you can access the Internet through a network port. we recommend using a Computer (or better), minimum display resolution support 1024 * 768 pixels for better view.

1.1.3 Establish network connection

Open network parameter configuration of computer shown as below。



Select the Internet Protocol (TCP / IP), enter the Internet Protocol (TCP / IP) Properties window. Select the input IP address in addition to the default IP address and subnet mask (255.255.255.0), click on the OK button to complete the operation. (Note: The IP address and switch must be in the same subnet.)

1.1.4 Check network whether connect between computer and switch

Use the ping command of Operating System, enter switch's IP address, if reply normally, then network connectivity; otherwise, check the network connection.

```
PING 192.168.0.240 (192.168.0.240) 56(84) bytes of data.
64 bytes from 192.168.0.240: icmp_seq=1 ttl=128 time=13.4 ms
64 bytes from 192.168.0.240: icmp_seq=2 ttl=128 time=14.5 ms
64 bytes from 192.168.0.240: icmp_seq=3 ttl=128 time=5.95 ms
64 bytes from 192.168.0.240: icmp_seq=4 ttl=128 time=1.12 ms
64 bytes from 192.168.0.240: icmp_seq=5 ttl=128 time=1.37 ms
64 bytes from 192.168.0.240: icmp_seq=6 ttl=128 time=8.12 ms
64 bytes from 192.168.0.240: icmp_seq=7 ttl=128 time=1.32 ms
64 bytes from 192.168.0.240: icmp_seq=8 ttl=128 time=1.25 ms

--- 192.168.0.240 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7059ms
rtt min/avg/max/mdev = 1.126/5.898/14.588/5.281 ms
```

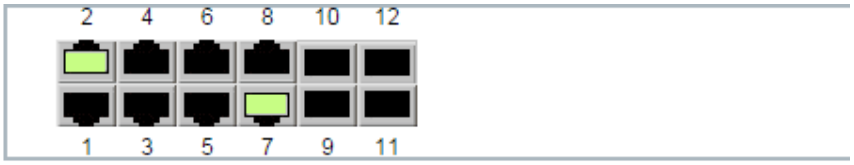
1.1.5 Login switch management interface

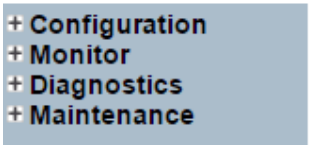
Running the browser, enter the switch default IP address (192.168.0.240) in address column, click Enter. Login dialog box, as shown below, enter your user name and password (the default user name: admin, password: admin), click the OK button or directly enter into the system configuration page. After a successful login interface as follows:

1.2 Web management interface

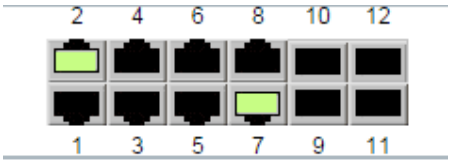
1.2.1 Basic information

Switch Configuration page is divided into Configuration, Manager, Diagnostics, Maintenance of four parts. As below：

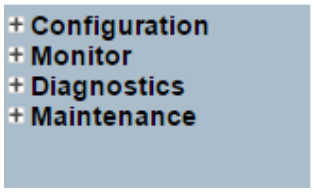




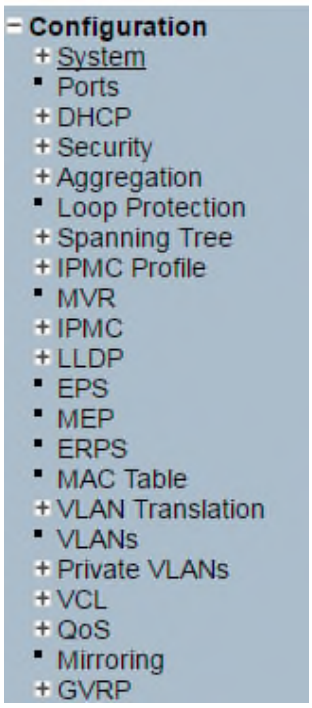
Port State Overview：This area displays the current status of the device connection port. When the indicator is green indicates that the corresponding port is connected, the indicator is gray, indicating the port not connected or enabled, as shown below:



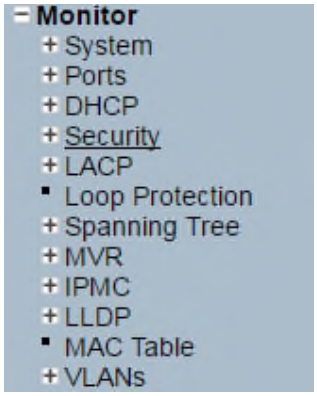
Navigation column: Click on a navigation column entry, the user can make the appropriate feature set and view, as shown below:



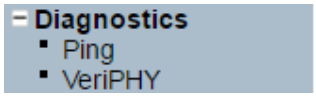
Configuration：Click the navigation column **Configuration** option, the system will expand to show the relevant configuration interface, users can set the interface-related functions.



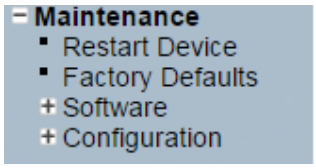
Monitor： Click on the navigation column **Monitor** option, the system will expand to show the relevant status interface, user-related functions can be provided in the interface.



Diagnostics： Click on the navigation column **Diagnostics** option, the system will expand the relevant components for switch device detection.



Maintenance： Click on the navigation column **Maintenance** option, the system will be displayed in the management area related to user management interface related functions can be provided in the interface.



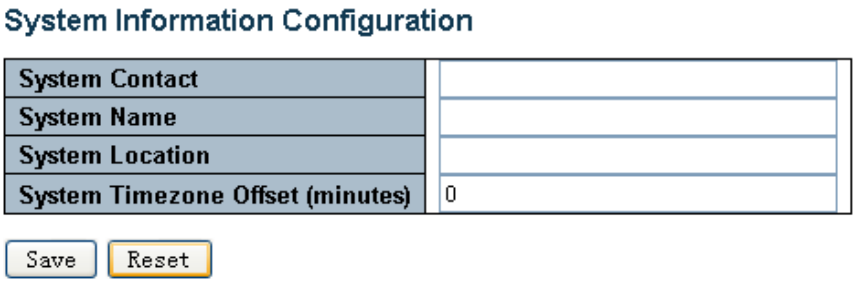
1.2.2 Configuration

1.2.2.1 System

A. System information

Enter 【**System**】→【**Information**】navigation column, enter the system contact, system name, system location, time zone offset system after setting, click **[Save]** button to complete the basic configuration information.

Click 【**Reset**】button, return to the data before system 【Save】



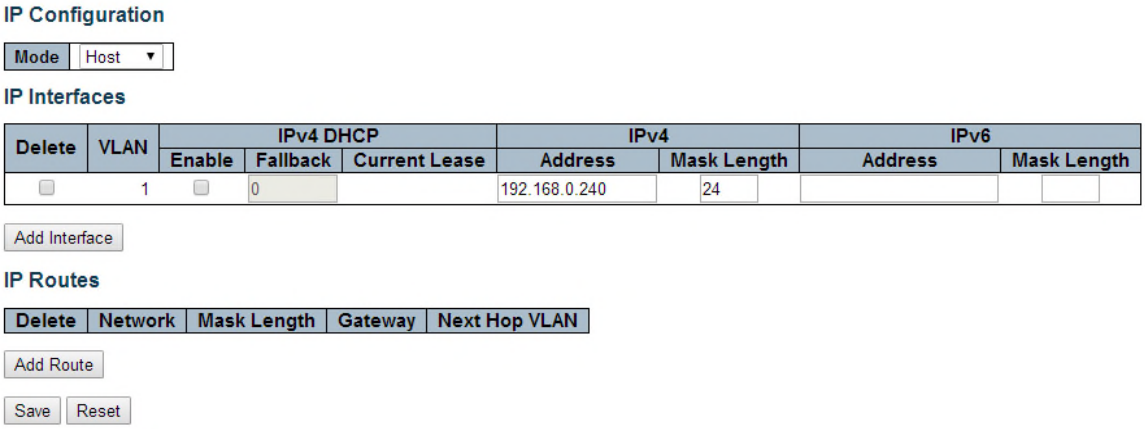
Interface items introduction：

Interface items	Configuration	Introduction	Factory configuration
System Contact	0~255 characters	Equipment maintenance personal contact information	No
System Name	0~255 characters	Switch name, is used to specify switch function (The first must be a letter, the last one cannot be a special sign)	No
System Location	0~255 characters	Describing the location information of device, such as production line 1	
System Time zone Offset	-720~720,unit:min	offset between equipment time zone and system time zone	0

B. IP address configuration

Enter **[System]** → **[IP]** navigation column, the page used to configure the address of the device management. The current status address of the device, a mask, router will be displayed in the form. After modifying the contents of the form, click **[Save]** button to complete the address modification or click **[Reset]**, it will be restored to the original value form content unmodified.

Router is optional item, default is empty. Set relevant parameters, click **[Save]** button to complete the configuration.



IP interface：interface items introduction(May different VLAN set different IP addresses, to meet the different hosts in VLAN access to the switch)

Interface items	configuration	Introduction	Factory setting
Delete	Select / not selected	Select this option to delete an existing IP interface.	not selected
VLAN	1~4095 number	The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating an new interface.	No
DHCP	Select / not selected	Enable the DHCP client by checking this box. If this option is enabled, the system will configure the IP address and mask of the interface using the DHCP protocol.	not selected
Address	Switch IP address	The IPv4 address of the interface in dotted decimal notation.	192.168.0.240

Mask Length	1-30	The destination IP network or host mask, in number of bits (prefix length).	24
Add Interface		Add an IP address settings	

Click **"Add Interface** "Add a new IP interface。

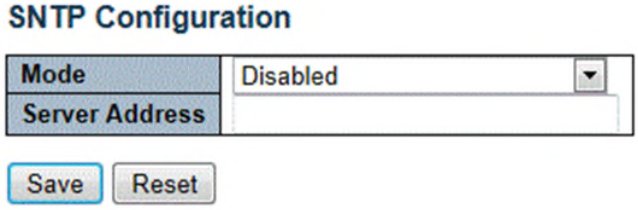
IP router： Interface items introduction：

Interface items	configuration	introduction	Factory setting
Delete	Select / not selected	Select this option to delete an existing IP route.	not selected
Network	IP address	The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0 or IPv6 :: notation.	NO
Mask Length	1-32	The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route.	24
Gateway	IP	The IP address of the IP gateway.	No
Add Route		Add a IP route configuration	

Click **"Add Route**r" to add a new IP route interface.

C. SNTP time server configuration

Enter【**System**】→【**SNTP**】Navigation, Time server configuration page, can be turned on when the remote NTP server, and configure remote SNTP time server, click **[Save]** button to complete time server configuration。

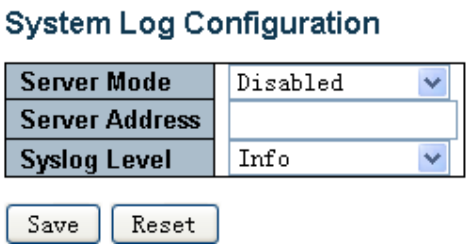


Interface items introduction：

Interface items	configuration	introduction	Factory setting
Mode	Disable/Enable	Indicates the NTP mode operation.	Disable
Server Address	Time server IP address	Provide the IPv4 or IPv6 address of a NTP server.	No

D. Log Server Configuration

Enter **[System]** → **[Log]** navigation column, log configuration page, you can configure a remote logging server information, the device logs information [Save] to a remote server, providing backup viewing. Select the server mode, set the server address, select the log level, click [Save] button to complete the system logging configuration.



Interface items introduction：

Interface items	Configuration	Introduction	Factory setting
Server Mode	Disable/Enable	Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server.	Disable
Server Address	Log configuration IP address	Configure log server IP address	No
Syslog Level	Info/Warning/Error	Indicates what kind of message will send to syslog server.	Info

5.2.2.2 Ports

Enter the **[Ports]** navigation column, you can view the connection status of each port, including: link connection, speed, flow control and maximum frame size and other information, No 1-6 for the front panel port 100M / 1000M

RJ45 ports, No 7-8 port for the data connection port, No 9-10 port Gigabit optical interfaces. Link status indication red indicates that the link down state; green indicates that the link up state.

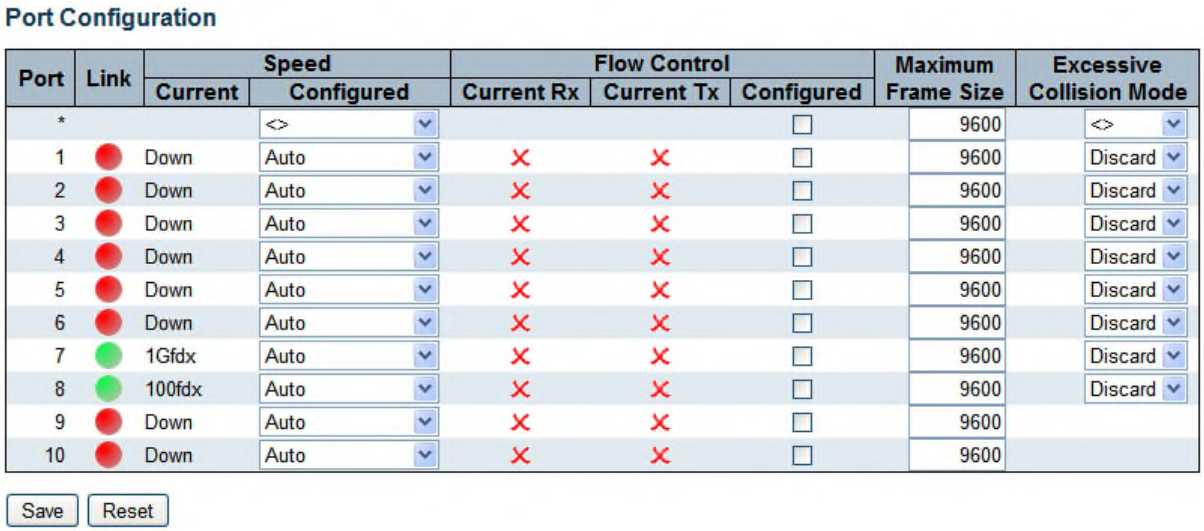
Port rate mode：

Ports can be selected as "Auto", "Disabled", "10mbps HDX", "10mbps FDX", "100Mpbs HDX", "100Mpbs FDX", "1Gbps FDX";

This option may be set directly: Auto can automatic identification access type.

Flow Control: enable the port flow control, implement port flow control

The maximum frame size that can be configured port maximum transmission unit, the default is 9600. Select the relevant parameters, click **[Save]** button to complete the port configuration. Also Click **[Save]** button to save changes. Click **[Reset]**to cancel any changes made locally and return to previously saved values.



Interface items introduction：

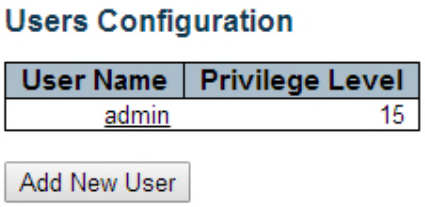
Interface items	Configuration	Introduction	Factory setting
Port		Physical port number	
Link		Port status display, a red light indicates that the link is disconnected status, green indicates normal connection link	
Speed Current	Info/Warning/Error	Display port status and mode	Info
Speed Configured	Disable	Prohibition to transfer data through the port	Disable

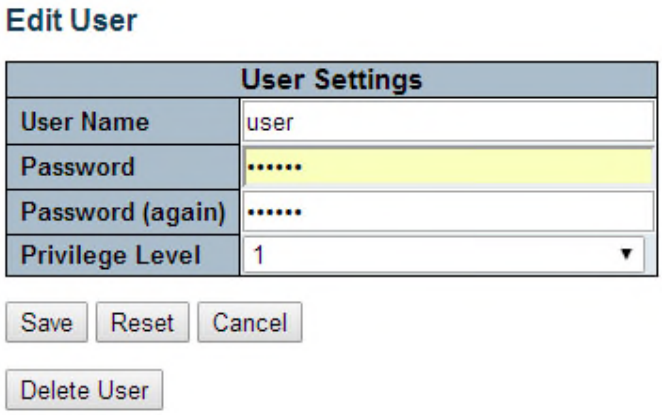
	Auto	Allows the port and the connected devices automatically adjust speed according to IEEE 802.3u	
	10Mbps HDX	In accordance with the rate selection, full / half duplex communication rate and to determine its mode of operation.	
	10Mbps FDX		
	100Mbps HDX		
	100Mbps FDX		
	1Gbps FDX		
Flow Control Current Rx		Indicates whether received the port flow control pause frames	X
Flow Control Current Rx		Indicate port whether send the flow control pause frames	X
Flow Control Configured	Check / uncheck	On / off flow control	uncheck
Maximum Frame Size	64-10056Byte	Set the port of the maximum data frame length	9600
Excessive Collision Mode	Discard/Restart	When the transfer conflict, whether retransmission of dropped packets: discard / retransmission	Discard

5.2.2.3 Security

A. System password configuration

Enter **[Switch]** → **[User]** navigation column, this page is used to add users, change user account password; important to remember the new password, the password is lost login prevent equipment failure.



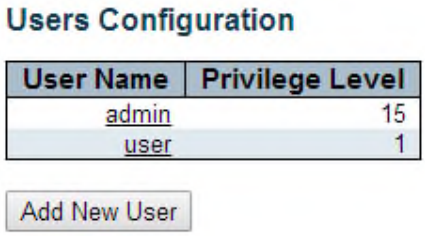


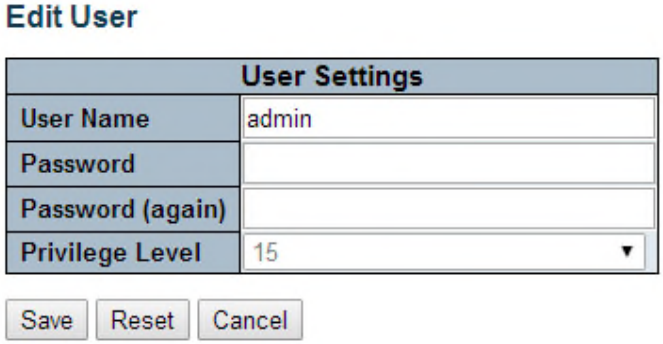
Interface items introduction：

Interface items	**Introduction**
Add New User	Add new user
User Name	User name
Password	password
Password(again)	Confirm password
Privilege Level	Level（The higher the value, the greater the level)

Modify the account password

In the User Interface, click the account that you want to modify;



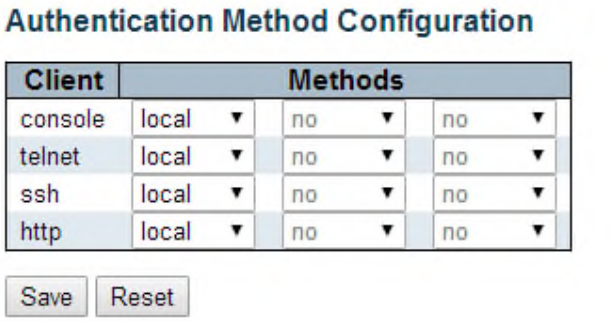


Interface items introduction：

Interface items	Introduction
Old Password	Enter the password currently used, if the old password is entered incorrectly, the new password is not enabled
New Password	Enter the new password, the length of the bit characters <0-30> characters
Confirm New Password	Re-enter the same new password, or cannot be enabled

B. Login authentication mode setting

Enter **[Switch]** → **[Auth Method]** navigation column, this page is used to set the manner in which authentication when users access the switch .



When you select the authentication mode is "none", no authentication enabled, you cannot login into the system.

When you select the authentication mode is "local", enable user name and password to log in the system's local user database.

When you select the authentication mode is "radius", enable remote server for authentication.

Set relevant parameters, click **[Save]**to save changes.

Click **[Reset]** to undo any changes made locally and revert to previously saved values.

Interface items introduction：

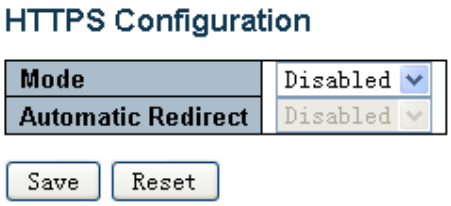
Interface items	configuration	introduction	Factory setting
Client	Console/http	As client user in console / web / telnet / ssh mode access system	
Methods	none/local/radius	After users access the system the authentication modes: non-authentication / local authentication / remote server authentication, you can select local authentication and remote authentication server certificate as the same time	local

C. HTTPS Configuration

Enter 【**Switch**】→【**HTTPS configuration**】navigation column, This page is used to enable the system's web connection is HTTP / HTTPS (secure HTTP). When users enable the HTTPS Meanwhile enable HTTPS automatic redirection function, the system will automatically select web mode into the system.

When the user closes the HTTPS mode, the system will select HTTP mode into the system. It must enable HTTPS mode to enable "automatic redirection" feature.

Select the relevant parameters, click [Save] to complete the HTTPS configuration; click [Reset] settings to the default values.

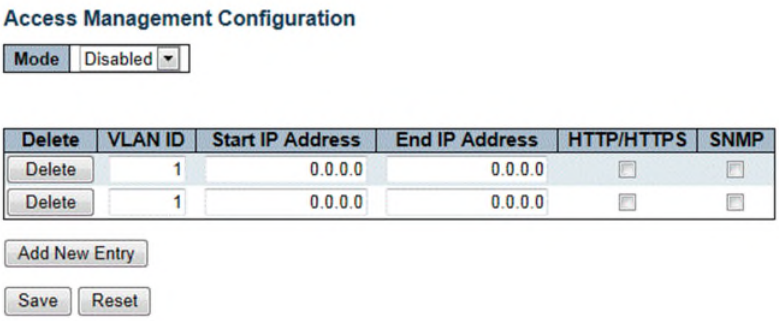


Interface items	configuration	introduction	Factory setting
Mode	Disable/Enable	Off / On HTTPS access switch	Disable
Automatic Redirect	Disable/Enable	Off / On automatic redirection between HTTP / HTTPS	Disable

D. Access management configuration

Enter 【**Switch**】→【**Access Management**】navigation column,Page is used to regulate the access management. Select Open access control management mode, click on the "Add New Entry" button, typing "Start IP Address (beginning IP address)", "End IP Address (End IP address)", select "HTTP / HTTPS", "SNMP", at least select a permissible service.

Click [Save] button to complete the access management configuration. Check delete selection on the corresponding clause, click the check box to complete the deletion.



Interface items introduction：

Interface items	Configuration	Introduction	Factory setting
Mode	Disable/Enable	off/one access control management	Disable
VLAN ID	1-4095	IP segment belongs VLAN	1
Start IP Address	IP Address	Access the start IP address	0.0.0.0
End IP Address	IP address	Access the end IP address	0.0.0.0
HTTP/HTTPS	Select / not selected	Selected, The IP address can accessed through HTTP/HTTPS	Not selected
SNMP	Select / not selected	Selected, The IP address can accessed through SNMP	Not selected

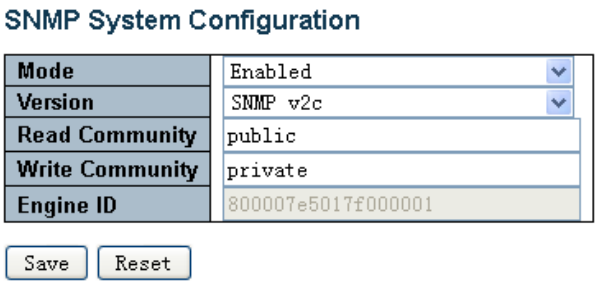
Add New Entry: Click to add a new interface.

Delete:

5.2.2.4 SNMP Configuration

A. SNMP system configuration

Enter 【**SNMP configuration**】→【**System**】navigation column,If your network is configured with the SNMP server, the switch can configure SNMP parameters, connect the SNMP server. When selected SNMP v3 version needs to be configured for specific functional parameters about SNMP v3 security certification, groups, views and so on.

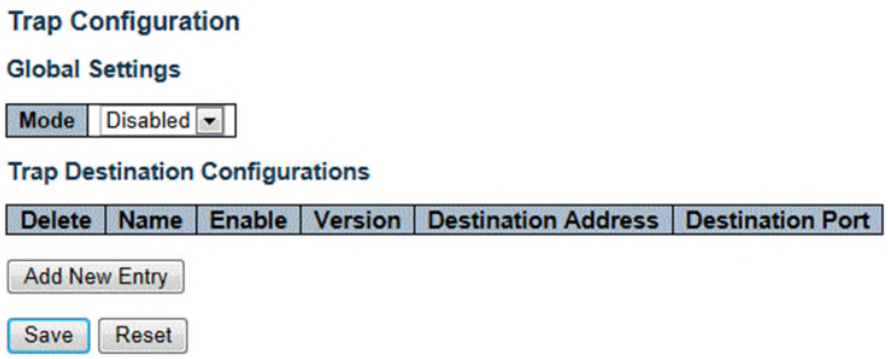


Interface items introduction:

Interface items	configuration	introduction	Factory setting
Mode	Disable/Enable	Indicates the SNMP mode operation.	Enable
Version	SNMP V1/SNMP V2C/SNMP V3	Indicates the SNMP supported version.	SNMP V2C
Read Community	0-255 string	Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.	Public
Write Community	0-255 string	Indicates the community write access string to permit access to SNMP agent.	private
Engine ID	16Decimal	Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.	800007e5017f000001

B. SNMP Trap Configuration

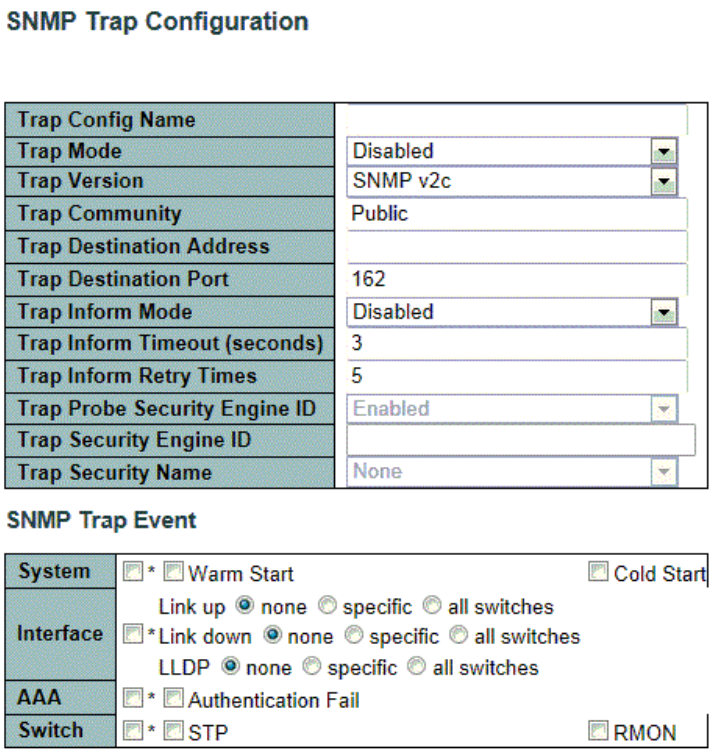
Enter 【SNMP configuration】→【**Trap**】,This page is used to configure the SNMP Trap function. The feature set SNMP Trap Active upload function followed protocol version, community, destination IP address, port number, and whether to use the Trap Inform, if you use Trap Inform, the corresponding timeout, retransmission parameters, and safety Engine ID. While providing local support for those events triggered Trap, such as: switch hot start, cold start, port status, authentication fails.



Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Mode	Disable/Enable	Indicates the trap mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.	Disable

Add New Entry: add button, Click to expand Trap configuration view



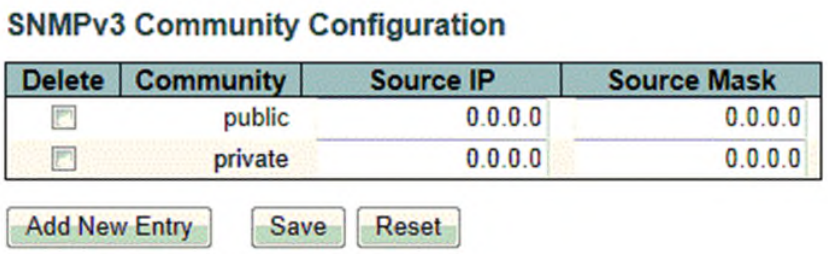
Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Trap Config name	0~255 Byte	Indicates which trap Configuration's name for configuring. The allowed string length is 1 to 255, and the allowed content is ASCII characters from 33 to 126.	No
Trap Mode	Disable/Enable	Indicates the SNMP mode operation.	Disable
Trap Version	SNMP V1/SNMP V2C/SNMP V3	Indicates the SNMP supported version.	SNMP V2C
Trap Community	Public/private String	Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.	Public
Trap Destination Address	IP address	Indicates the SNMP trap destination	No

		address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').	
Trap Destination Port	Port address	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.	162
Trap Inform Mode	Disable/Enable	Indicates the SNMP trap inform mode operation.	Disable
Trap Inform Timeout	0-2147 second	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.	3
Trap Inform Retry Times	0-255 time	Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.	5
Trap Probe Security Engine ID	Disable/Enable	Indicates the SNMP trap probe security engine ID mode of operation.	
Trap Security Engine ID	10-64 hexadecimal digits, not allowed all 0, all 1	Indicates the SNMP trap security engine ID.	ProbeFail
Trap Security Name		Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.	None
Trap Event		Configure SNMP trap on this page.	

C. SNMP Community Configuration

Enter【**SNMP Configuration**】→【**Community**】navigation column，Configure SNMPv3 community table on this page. This function is used for only one IP address to restrict the information requested or received.

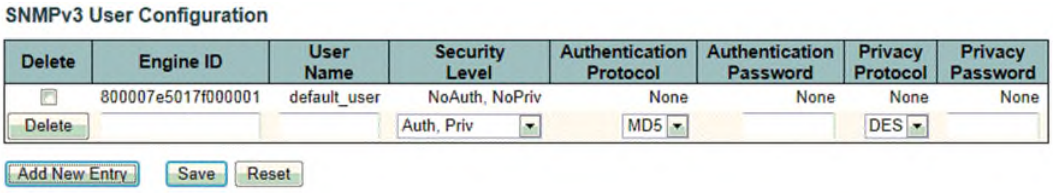


Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Community	0~255 byte	Community (Authenticate string)	No
Source IP	IP address	Community Source IP address	0.0.0.0
Source Mask	Subnet Mask	Community Source Mask	0.0.0.0

D. SNMP Users Configuration

Enter【**SNMP Configuration**】→【**Users**】navigation column, Configure SNMPv3 user table on this page. Configure Authentication security mode, security level, and data reported level of security, encryption mode for particular user when access identity verification when accessing



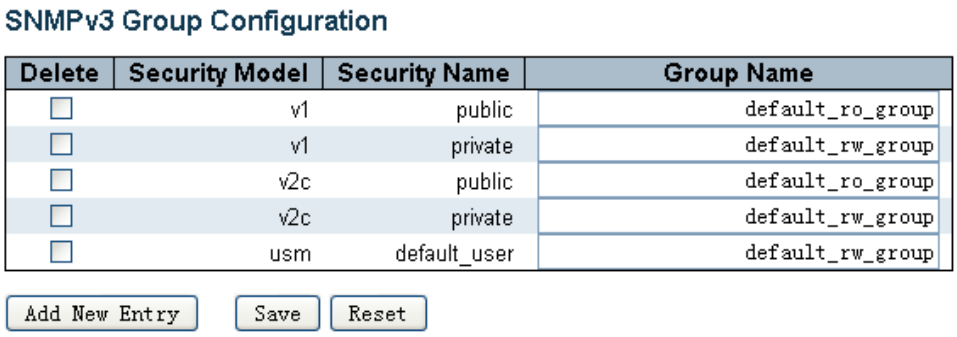
Interface items Introduction:

Interface items	Configuration	Introduction	Factory setting
Engine ID	16Decimal	Engine IDAs Engine ID authoritative SNMP it used to identify SNMP entities, authentication and encryption	800007e5017f000001
User Name	0-32 byte	User name	0.0.0.0
Security Level	NoAuth，NoPriv	Security levels: no authentication, no privacy	NoAuth，NoPriv
	Auth，NoPriv	authentication, no Privacy	

	Auth，Priv	authentication, Privacy	
Authentication Protocol	MD5/SHA	Select the authentication encryption algorithm	MD5
Authentication Password	8-32 characters	Authentication Password	NO
Privacy Protocol	DES/AES	Choose packet encryption algorithm	DES
Privacy Password	8-32 characters	Packet encryption password	NO

E. SNMP Group Configuration

Enter【**SNMP configuration**】→【**Groups**】navigation column, configure SNMPv3 group table on this page, This function is used to set some of these groups and the security model, the authentication name. The Page Setup group, as can select use group in SNMP-Access (SNMP Access Settings) page, out in option "Group Name" column, the configuration options for the user to use SNMP access.

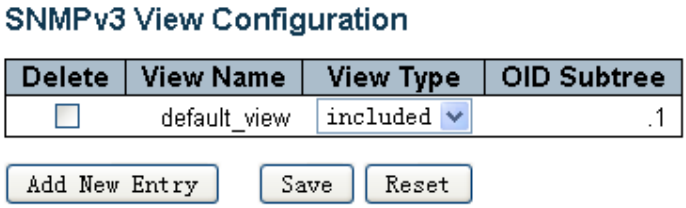


Interface items Introduction:

Interface items	Configuration	Introduction	Factory setting
Security Model	v1/v2c/usm	SNMP group safety mode	v1 group, v2c group，usm group
Security Name	Public/Private	SNMP group access permission	public permission, private permission, default user permission
Group Name	0-255 byte	SNMP group name	Default_ro_group Default_rw_group

F. SNMP View Configuration

Enter 【**SNMP configuration**】→【**Views**】navigation column, Configure SNMPv3 view table on this page. The main configuration items are: the view name, OID subtree, include or exclude the OID subtree.

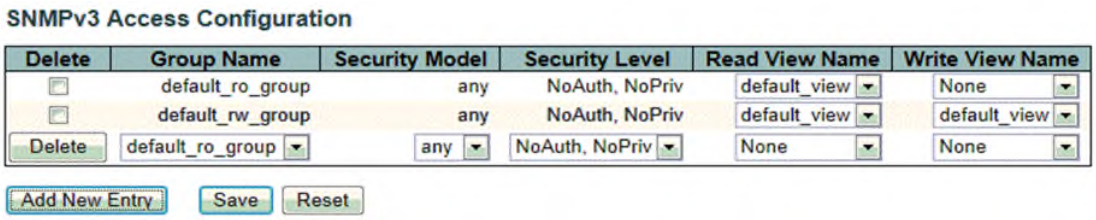


Interface items Introduction:

Interface items	Configuration	Introduction	Factory setting
View Name	0-255 byte	View name	default_view
View Type	Included/excluded	View only included/exclude OID subtree node	Included
OID Subtree	Use "," separated string of numbers	OID Mark	.1

G. SNMP Access Configuration

Enter【**SNMP configuration**】→【**Access**】navigation column,Configure SNMPv3 access table on this page. Configure when a group users access of the security mode , security levels, read-only view and read-write view. Click **[Save]**to save changes. Click **[Reset]** to return to the default values.



Interface items Introduction:

Interface items	Configuration	Introduction	Factory setting
Group Name	0-255 byte	User group name to access	default_ro_group default_rw_group
Security Model	any/v1/v2c/usm	Select the security mode, any mode / v1 / v2c / usm for user group	any
Security Level	NoAuth，NoPriv	Select security level for user group: No authentication and no privacy	NoAuth，NoPriv

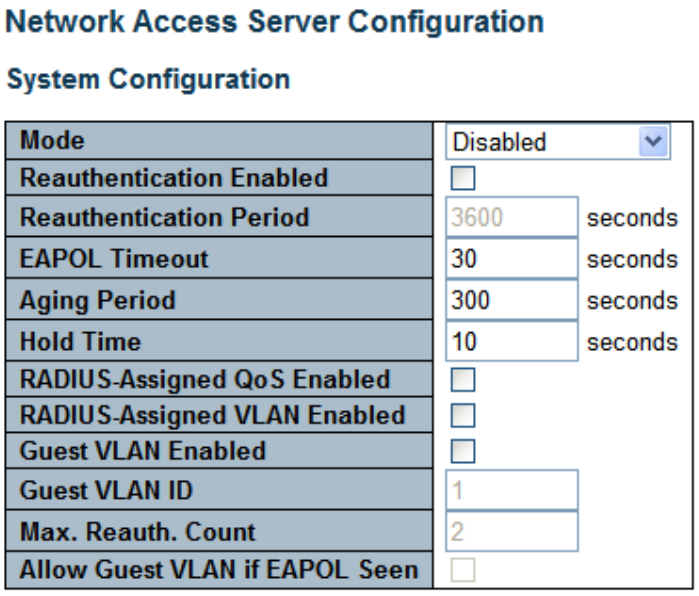
	Auth，NoPriv	Authentication and no privacy.	
	Auth，Priv	Authentication and privacy.	
Read View Name	None/view configuration	Select the desired view name for user	Default view
Write View Name	None/view configuration	Select the desired write view name for user	None Default view

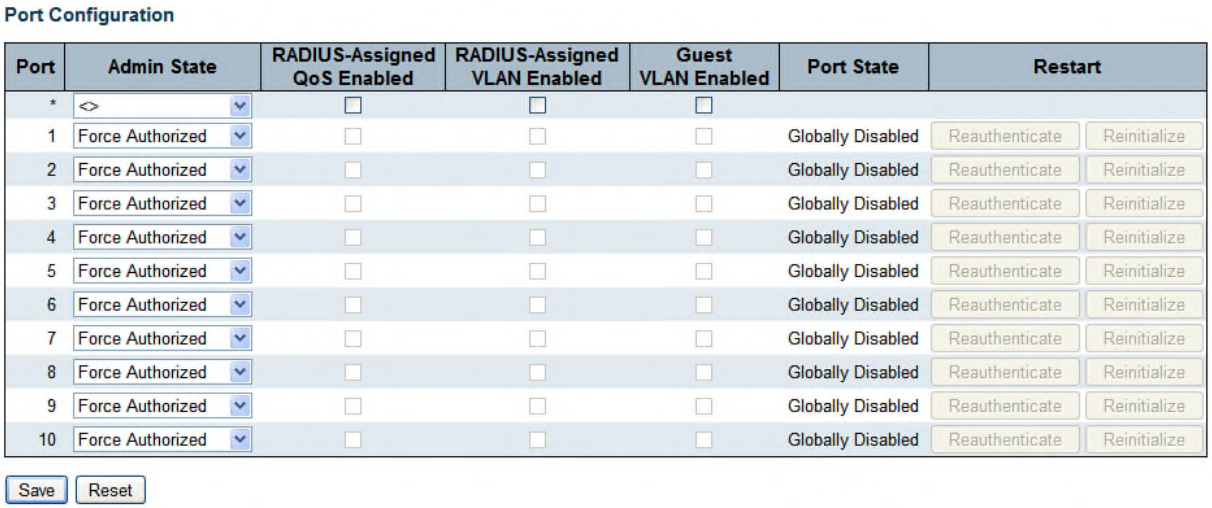
5.2.2.5 Network

A. NAS Configuration

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings. The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

Enter【**Network**】→【**NAS configuration**】navigation column





System configuration interface items introduction;

Interface items	Configuration	Introduction	Factory setting
Mode	Disabled/Enabled	Indicates if NAS is globally enabled or disabled on the switch stack.	Disabled
Reauthentication Enabled	Check / uncheck	Once selected, after the authentication is successful, a set time after the Reauthentication Period, will be certified again	uncheck
Reauthentication Period	1-3600 second	Recertification interval	3600
EAPOL Timeout	1-65535 second	Identity EAPOL defined time frame resend request, and this time on the MAC-based authentication is invalid	30
Aging Period	10-1000000 second	Certification aging time, after authentication, within Aging Period of time no longer detect the device, the authentication will automatically lapse	300
Hold Time	10-1000000 second	After the authentication fails, the re-certification intervals, during this time do not accept the authentication request of the terminal	10

Port configuration interface items introduction

Interface items	Configuration	Introduction	Factory setting
Port	1-n(Number of physical ports)	To configure the switch port number port	1-n
Admin State	Force Authorized	In this mode, when a client is connected to the port, the switch will automatically send an EAPOL success frame, you can access the network without authentication	Force Authorized **Note:** If set to a non Force Authorized port, you cannot open the port Spanning tree, and Aggregation functions
	Force Unauthorized	In this mode, when a client is connected to the port, the switch will automatically send an EAPOL frame failure, any client cant access the network	
	802.1X	Using 802.1X authentication mode	
	MAC-Based Auth.	Using MAC-Based authentication mode	
Port State	Globally Disabled	NAS all Disabled	
	Link Down	NAS all Enabled, but port cant connected	
	Authorized	Port operates in Force Authorized mode, or work in only one request mode, and the request authentication success	
	Unauthorized	Port operates in Force Unauthorized mode, or work in only one request mode, and the request authentication not success	
	X Auth/YUnauth	The port is a plurality of request mode, X client successfully authenticates, Y client authentication is unsuccessful	
Restart	Reauthorized	Authorized buttons only when the authentication mode in the open, while the port state of 802.1X / MAC-Based Auth. When it is enabled, click Reauthorized immediately for certification has passed recertification	

	Reinitialize	Reinitialize button only when the authentication mode in the open, while the port state of 802.1X / MAC-Based Auth. When it is enabled, click Reinitialize initialize the client immediately forced to cut off the last certification, recertification	

B. ACL（Access Control List ）Configuration

ACL Port Configuration

Enter 【**ACL configuration**】→【**Ports**】navigation column, Configure the ACL parameters (ACE) of each switch port. port only can receive the frames matching ACE parameter. Also define eight per port policy number, each policy is defined different content, you can configure the following parameters Series: Action , Permit / Deny to specify the type of data packet forwarding, Rate Limiter ID , Port Redirect , 16 bandwidth control policies for network security configuration page definitions; Logging (logging): Enable / Disable logging;

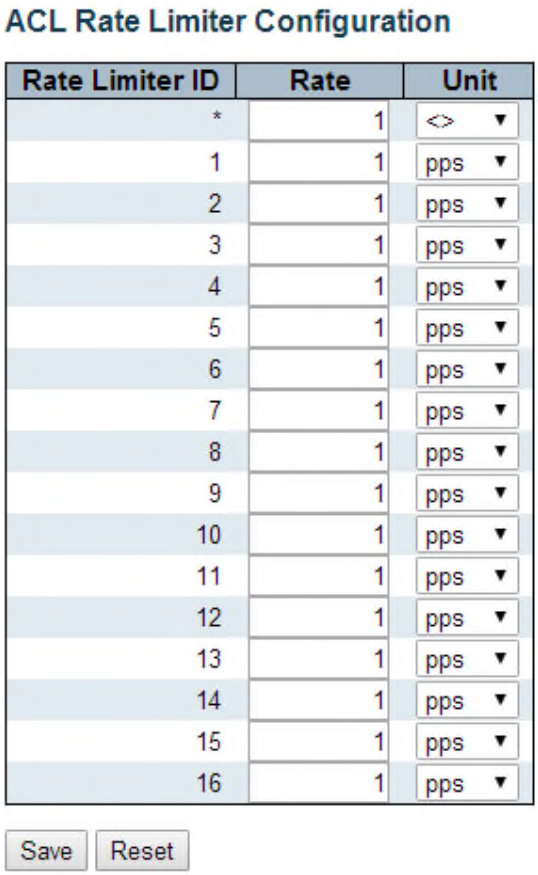
Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Port	1-n(Number of physical ports)	number for Switch To configure the port	1-n

Policy ID	0-255	Select the policy to apply to this port	0
Action	Permit/Deny	Select filter out traffic is forwarded or blocked	Permit
Rate Limiter ID	Disabled/0-16	Select which rate limiter ID to apply on this port	Disabled
Port Redirect	Disabled/port Number	Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".	Disabled
Mirror	Disabled/Enabled	Frames received on the port are mirrored or not mirrored.	Disabled
Logging	Disabled/Enabled	Frames received on the port are stored in the System Log or not logged.	Disabled
Shutdown	Disabled/Enabled	If a frame is received on the port, the port will be disabled or Enabled	
State	Disabled/Enabled	When you select Enabled, when changing the port you are using ACL user module, open ports When you select Disabled, when changing the port you are using ACL User Module, shut down the port	Enabled
Counter		Counts the number of frames that match this ACE.	0

ACL Rate Limiter Configuration

Enter 【**ACL configuration**】→【**Rate Limiters**】navigation column, is the ACL rate limiter configuration of port,The system supports 16 broadband strategy, speed range: 0-3276700 / PPS or 0,100,200,300 ... between 10000000kbps.



Interface items introduction:

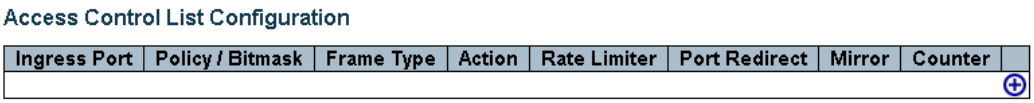
Interface items	Configuration	Introduction	Factory setting
Rate Limiter ID	1-16	ACL rate limiter ID in use	1-16
Rate	0-3276700/PPS 0,100,200,300…10000000kbps	Rate value configure	1
Unit	pps/kbps	Rate unit: pps: packets / sec Kbps: kilobytes / sec.	pps

Click **[Save]** button when the configuration is complete ; Click **[Reset]** to return to the default values.

ACL Access control List

Enter【**ACL configuration**】→【**Access Control List**】navigation column, Check system access control lists.

Click ⊕ to add ACE term of list



Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Ingress Port	All/Port1-n(Number of physical ports)	All: ACE matching all Ingress port Port1-n: ACE matching a Ingress port	All
Policy / Bitmask	Policy: 0-255 Bitmask: 0x0-0xff	Designation ACE strategies code and bit mask	Any
Frame Type	Any	ACE match all frame types	Any
	EType	ACE matching the Ethernet frame type, not match IP and ARP frames	
	ARP	ACE matching ARP / RARP frame	
	IPV4	ACE match all IPV4 frame	
	IPV4/ICMP	ACE matchingIPV4 frames with the ICMP protocol	
	IPV4/UDP	ACE matchingIPV4 frames with the UDP protocol	
	IPV4/TCP	ACE matchingIPV4 frames with the TCP protocol	
	IPV4/other	ACE matching the otherIPV4 frames except ICMP / UDP / TCP protocol	
	IPV6	ACE match all IPV6 frame	
Action	Permit	Forwarding and Learning with ACE matching frame	Permit
	Deny	Discard the ACE matching frame	
	Filter	Filtering the ACE matching frame	
Rate Limiter	Disabled/0-16	Select this port to be used for rate limiting	Disabled

		ID number	
Port Redirect	Disabled/port no	select a port frame whether redirected, if redirected, set the redirection port, if Action is selected Permit, you cannot choose to redirect	Disabled
Mirror	Disabled/Enabled	In the frame of this port is not receiving Mirror / mirrored	Disabled
Counter		The counter of frames and port settings match ACE	0

List Change button:

+: ACE insert an item in the current row;

e: Edit ACE;

↑: Move the list ACE;

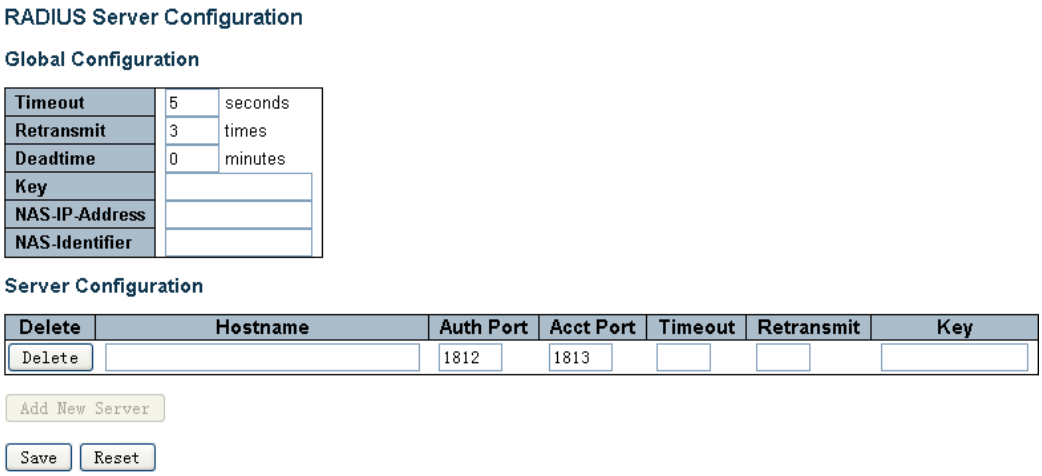
↓: Down ACE in the list

X: Delete ACE

+: In the bottom of the list to add an ACE item

5.2.2.6 AAA authentication authorization accounting configuration

Enter【**AAA configuration**】navigation column. If you use a remote RADIUS authentication server, you can configure corresponding RADIUS server parameters via this page, also can configure multiple servers, parameters include common parameters for all servers and each server's private parameters.



General parameters configuration

Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Timeout	1-1000 second	wait for the server response time before Retransmission request	5
Retransmit	1-1000	The maximum number of retransmissions request	3
Deadtime	0-1440 min	intervals of a request after the request fails	0
Key	0-63 byte	Previous common password of RADIUS server and switch	No
NAS-IP-Address	IP address	NAS logical IP address	No
NAS-Identifier	0-255 byte	NAS authentication string	No

Privacy server configuration

Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Delete			

Hostname	IP address	RADIUS server IP address	1812
Auth Port	Port No	RADIUS server UDP port used for authentication	1813
Acct Port	Port No	RADIUS server UDP port used for accounting	NO
Timeout	1-1000 second	wait for the server response time before Retransmission request(instead of generic parameters inside Timeout, if this parameter is empty, then common timeout use timeout parameter))	NO
Retransmit	1-1000	The maximum number of retransmission request	NO
Key	0-63 byte	Previous common password of RADIUS server and switch	

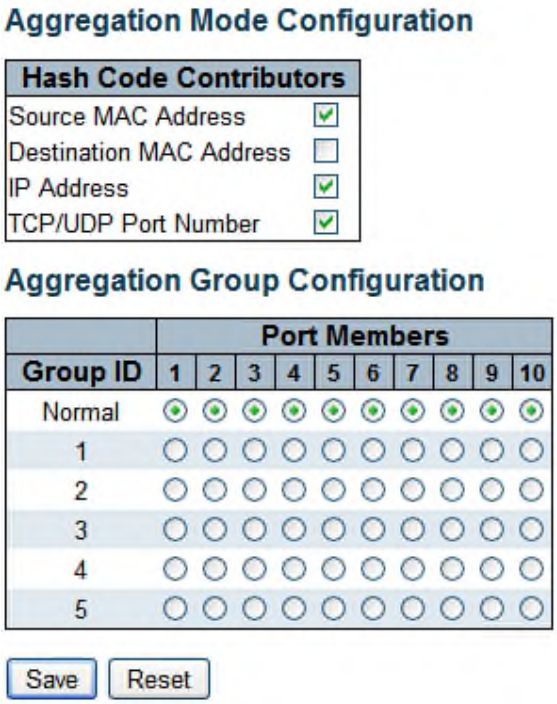
click “Add New Server” to add a new RADIUS server.

5.2.2.7 Aggregation

A. Static Aggregation

Enter【**Aggregation**】→【**Static**】navigation column, The switch supports four kind Hash algorithm, four kinds of algorithms mode can check, combination computing. Support 5 groups aggregation, each supports up to 10 ports. as shown: 1-2 opening set of aggregation; 3-4 opening set of aggregation and so on. Aggregation group member ports Please keep configuration consistency, such as port speed mode, owned vlan information.

If some ports are open LACP dynamic convergence protocol, it cannot manually configure the static convergence.



Aggregation algorithm mode： Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Source MAC Address	Select/not select	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.	not select
Destination MAC Address	Select/not select	The Destination MAC Address can be used to calculate the destination port for the frame.	not select
IP Address	Select/not select	The IP address can be used to calculate the destination port for the frame.	not select
TCP/UDP Port Number	Select/not select	The TCP/UDP port number can be used to calculate the destination port for the frame.	not select

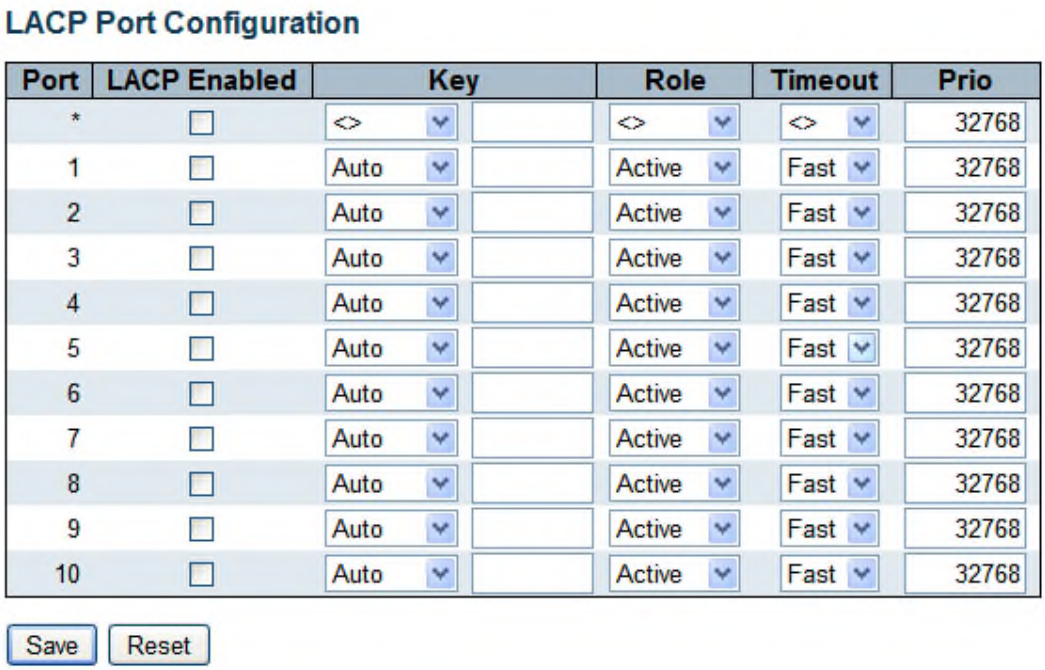
Aggregation configuration： this configuration is used to configure the Aggregation hash mode and the aggregation group. The aggregation hash mode settings are global, whereas the aggregation group relate to the currently selected stack unit, as reflected by the page header.

Interface items	Configuration	Introduction	Factory setting
Group ID	Normal/1-5	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.	Normal
Port Members	Select/not select	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.	not select

B. LACP

Enter 【**Aggregation**】→【**LACP**】navigation column, The switch supports dynamic aggregation port, after port enable LACP, Aggregation of both devices via protocol interaction gathering information, according to the parameters and status, automatic matching link aggregation together send and receive data. After forming aggregation, switching equipment maintenance aggregation link state, when the two sides configuration changes, automatically adjust or dissolve aggregated links.

If some ports have been static port aggregation, LACP dynamic convergence cannot be achieved.



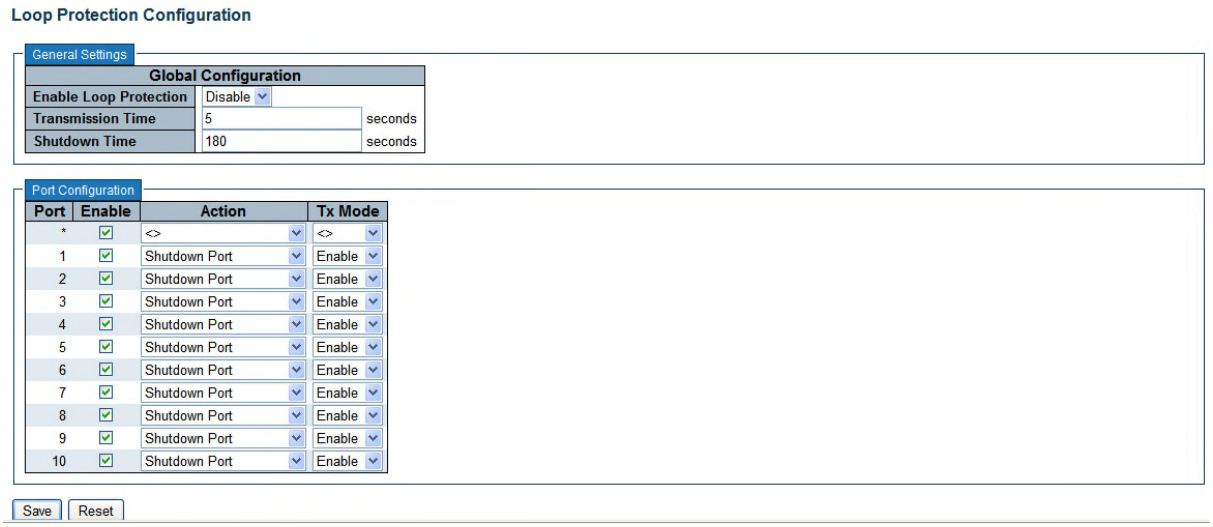
Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Port	1-n(Number of physical ports)	The switch port number.	1-n
LACP Enabled	Select/not select	Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner.	not select
Key	Auto/Specific(1-65535)	The Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can	Auto

		participate in the same aggregation group, while ports with different keys cannot.	
Role	Active/Passive	The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).	Not select
Timeout	Fast/slow	The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.	Fast
Prio	1-65535	The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.	32768

5.2.2.8 Loop Protection

Enter【**Loop Protection**】navigation column. This page allows the user to inspect the current Loop Protection configurations and set relevant parameters, click **[Save]** button to save changes.



General Settings： Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Enable Loop Protection	Disabled/Enabled	Controls whether loop protection is enabled on this switch port.	Disabled
Transmission Time	1-10 second	The interval between each loop protection PDU sent on each port. valid values are 1 to 10 seconds.	5
Shutdown Time	0-604800 second	The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until nextdevice restart).	180

Port Configuration ： Interface items introduction:

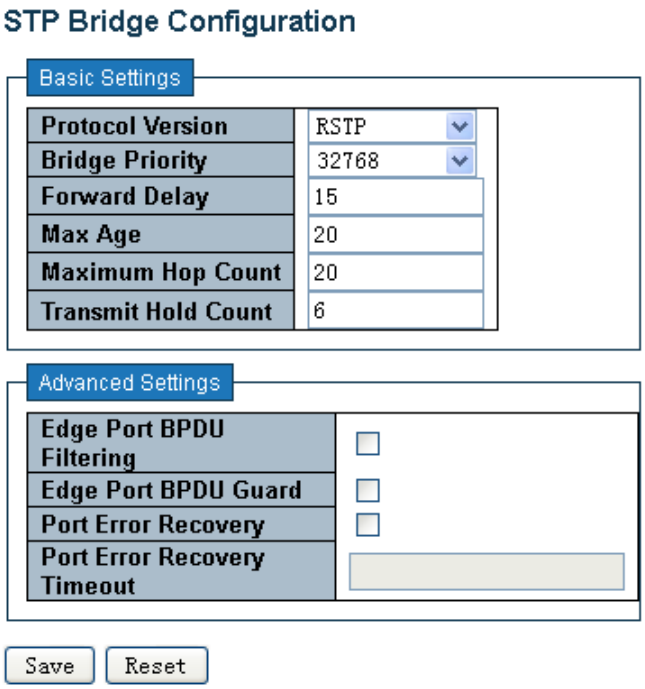
Interface items	Configuration	Introduction	Factory setting
Port	1- n	The switch port number of Switch.	1-n
Enable	Select/not select	Controls whether loop protection is enabled on this switch port.	Select
Action	Shutdown Port	loop is detected on a port, Shutdown the Port	Shutdown Port
	Shutdown Port and Log	Loop detected, shutdown port and log	
	Log Only	Loop detected, not shutdown port and log	
Tx Mode	Disabled/Enabled	Select the port is send port of protected PDU, or the receiving end, Enabled as the sender, Disabled receiving end	Enabled

5.2.2.9 Spanning Tree

A. STP Configuration

Enter【**Spanning Tree**】→【**Bridge Settings**】navigation column, configure the system spanning tree on this page, prevent loop. Enable RSTP protocol defaulted by system. All configured parameters are applied to all STP of switch configuration.

Set relevant parameters, click **[Save]** button to complete the spanning tree protocol bridge configuration. Click **[Reset]** button to restore the default settings.



Basic configuration: Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Protocol Version	STP/RSTP	Spanning tree protocol version	RSTP
Bridge Priority	0/4096/…../61440	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.	32768
Forward Delay	4-30 second	The delay used by STP Bridges to transit Root and Designated Ports to	15

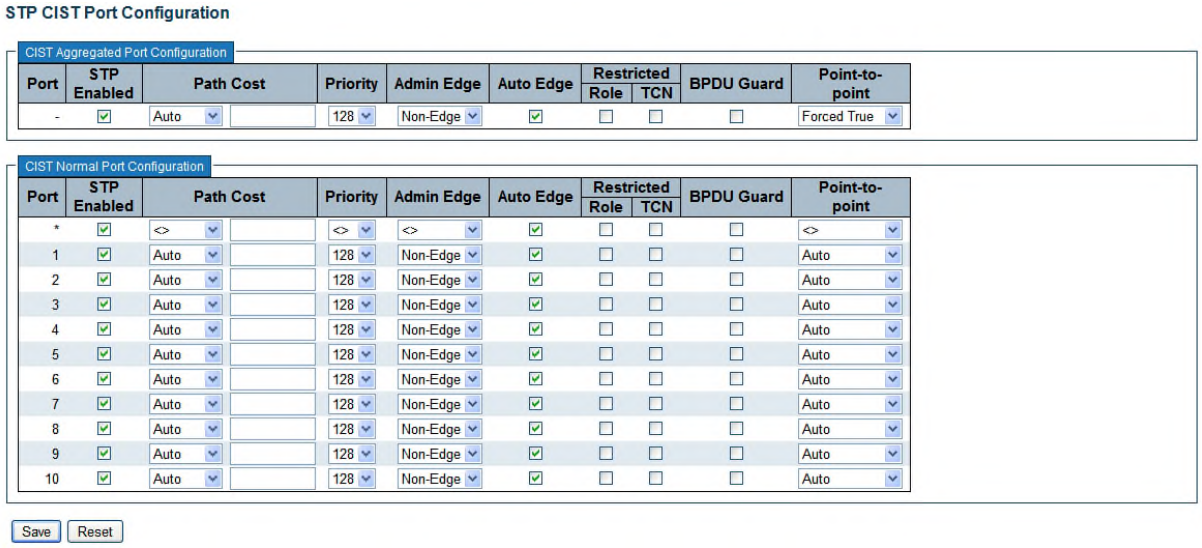
		Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.	
Max Age	6-40second And <=(Forward Delay-1) X 2	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and Max Age must be	20
Maximum Hop Count	6-40	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.	20
Transmit Hold Count	1-10	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.	6

Advanced configuration：

Interface items	Configuration	Introduction	Factory setting
Edge Port BPDU Filtering	Select/not select	Control whether a port explicitly configured as Edge will transmit and receive BPDUs.	not select
Edge Port BPDU Guard	Select/not select	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.	not select
Port Error Recovery	Select/not select	Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.	not select
Port Error Recovery Timeout	30-86400 second	The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).	No

B. STP port configuration

Enter【**Spanning Tree configuration**】→【**CIST Ports**】navigation column, All ports by default are run Spanning Tree Protocol to prevent loops. Port path cost default is Auto, users can manually specify, among 1-200000000, the smaller the value the more priority path. Port priority, use in the spanning tree calculation process for 0/16/32/48 / ... / 224/240, the default is 128. Edge port is use for switch connected to computer or connect network device without the spanning tree function. At this port directly into the forwarding state, will not participate in the logical topology calculations.



Interface Items Introduction:

Interface items	Configuration	Introduction	Factory setting
Port	1- n	Switch port number	1-n
STP Enabled	Select/not Select	off/ on port STP Enabled	Select
Path Cost	Auto/ Specific:1- 200000000	Path cost, when selecting Auto the system will be based on the connection speed to use STP recommended values. When you select Specific, enter a value between 1-200000000 only as a path overhead	Auto
Priority	0/16/32….240	Port Priority	128
AdminEdge	Non-Edge/Edge	Set the port connected device is STP bridge device or a non-bridge device, if non-bridge device, configured as Edge, will speed forwarding rate	Non-Edge
AutoEdge	Select/not Select	When selected enter the auto detect whether the port is an edge port,	Select

		according to the results of the monitoring configuration itself edge port	
Restricted Role	Select/not Select	When Selected, the device serves as limit state, not select to the root port	not Select
Restricted TCN	Select/not Select	When Selected, TCP packet forwarding equipment limitations, namely, it does not forward the received TCN (Topology Change Notification) message to other ports	
BPDU Guard	Select/not Select	When Selected, the port does not receive a valid BPDU	not Select
Point-to-Point	Auto	Device Automatic detection link is connected to this port is point to point	Auto
	Forced True	Set this port to connect the device to force the link to point	
	Forced False	Set this port to connect the device to force non-point link	

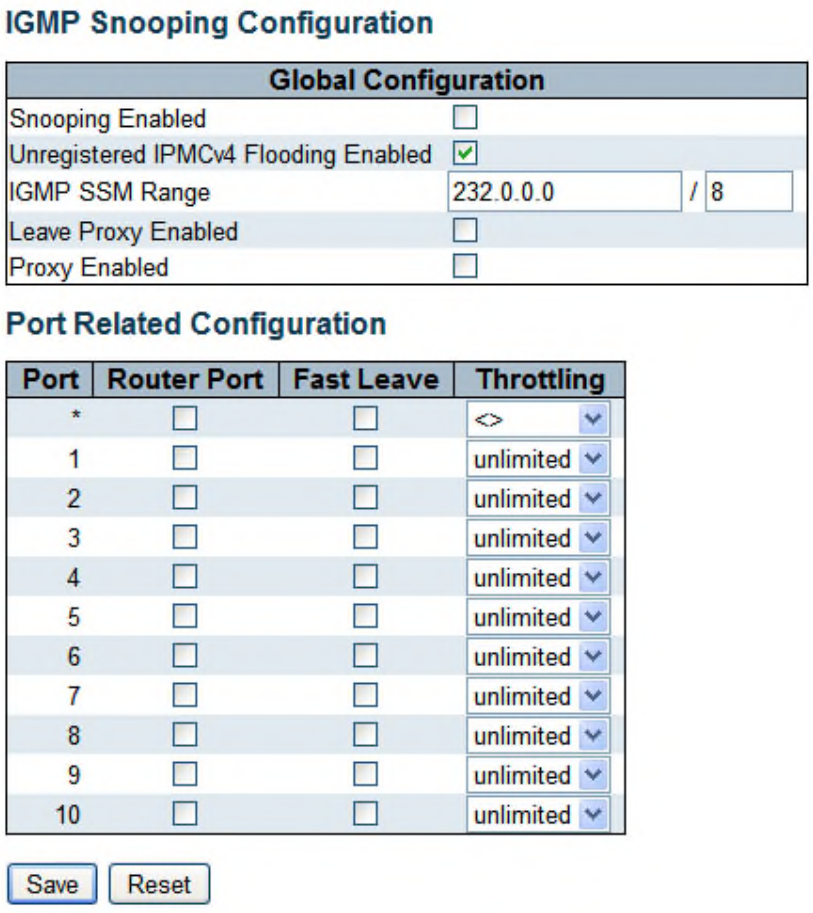
5.2.2.10 IPMC Configuration

A. IGMP Snooping basic configuration

Enter【**IGMP Snooping configuration**】→【**Basic**】navigation column, Common configuration can enable the multicast listener function to achieve the IGMP packet detection, and for the host and corresponding port and establish the corresponding multicast group address mappings. Broadcast unknown multicast function is configured for unregistered multicast packets discarded or broadcast operations.

Port can be configured router port, does not age. When receiving an IGMP query is not configured for the port on the router port, the switch that the port is connected with IGMP router (direct or indirect), on the port recorded as dynamic routing port. When the switch receives IGMP reports will be forwarded to the router port.

Tick Snooping enabled, the port 1-2 routing port, fast leave options, click **[Save]** button to complete the IGMP Snooping, Port configurations.



Interface items introduction:

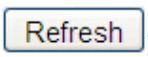
Interface items	Configuration	Introduction	Factory setting
Snooping Enabled	tick/not tick	Enable the Global IGMP Snooping, disabled by default	not tick
Unregistered IPMCv4 Flooding Enabled	tick/not tick	ON / OFF port flooding control, when IGMP Snooping is enabled, the flood control takes effect, when IGMP Snooping feature is disabled, cannot be controlled flooding	tick
IGMP SSM Range		IGMP SSM range	
Leave Proxy Enabled	tick/not tick	Leaving the Proxy enable / disable	not tick
Proxy Enabled	tick/not tick	Proxy On / Off	not tick
Router Port	tick/not tick	Set the port to route / non-routing port	not tick
Fast Leave	tick/not tick	Enable / disable IGMP fast leave	not tick

B. IGMP Snooping VLAN Configuration

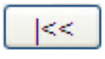
Enter【**IGMP Snooping Configuration**】→【**VLAN Configuration**】navigation column, Click Add New IGMP VLAN button, enter VLAN ID 1-2, tick Snooping enable option, click [Save] button to complete the IGMP Snooping VLAN configuration.

Click the Delete button before corresponding VLAN ID, click [Save] button to complete the IGMP Snooping vlan deleted.

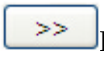
IGMP Snooping VLAN number on the page displayed shows up to 99, 20 per default .by the following three keys can be updated, view the list



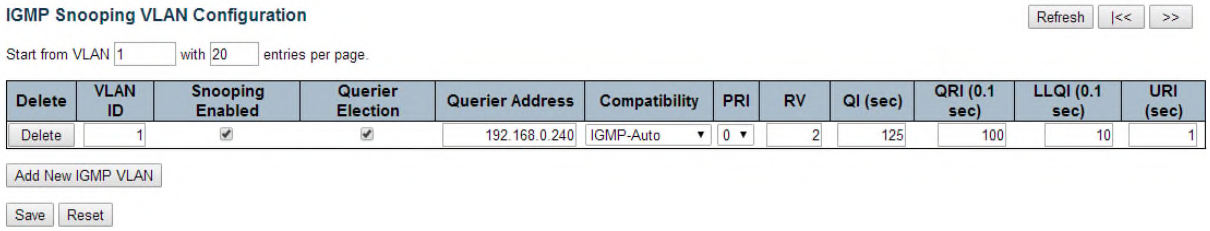
Refresh the display list



Previous displays list



Back displays list

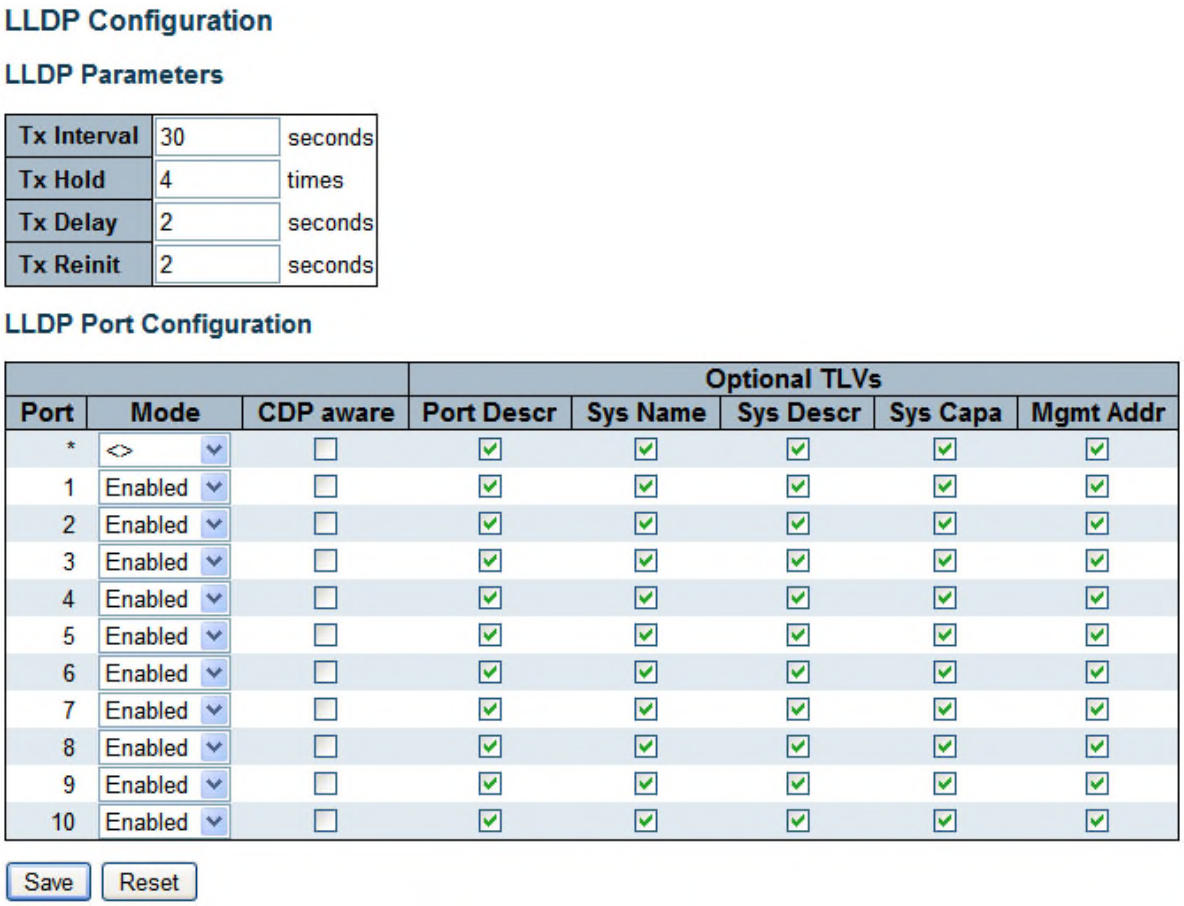


Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Delete		Delete the corresponding IGMP Snooping VLAN list	
VLAN ID	1-4095	Setting IGMP Snooping VLAN, range: 1-4095	No
Snooping Enabled	Tick/not tick	On / Off the corresponding VLAN Snooping function, VLAN up to make the function 32	not tick
Querier Election	Tick/not tick	Enable / Disable IGMP querier after opening can be selected as the interrogator, after closing will not be selected for the query is	tick
Querier Address	IP address	Setting IGMP query IP address, if not , the default address for the VLAN management, if the corresponding management address is not set, it defaults to the first VLAN management address, if not VLAN management address, the system defaults to 192.0 .2.1	0.0.0.0

5.2.2.11 LLDP Configuration

Enter**【LLDP Configuration】→【LLDP】**navigation column, The switch supports LLDP (Link Layer Discovery Protocol), can be major capacity of the terminal equipment, management addresses, device identification, interface identifications and other information organized into different TLV (Type / Length / Value: type / length / value) and Package (: link layer discovery protocol data unit link Layer Discovery Protocol Data Unit) published its standard MIB will give its directly connected neighbors, neighbors receive this information in LLDP (Management Information Base: MIB) in the form save up for NMS inquiry and determine the communication status of the link.



LLDP Parameter configuration： Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Tx Interval	5-32768 second	The time interval of switch to send LLDP frames to the neighbor	30
Tx Hold	2-10 times	Multiple frame interval for configuring LLDP frame effective time, the effective time = Tx Hold x Tx Interval	4
Tx Delay	1-8192 second	After LLDP configuration change, time to re-transmission and the last time interval between frames LLDP, <= 1/4 Tx Interval	2
TxReinit	1-10 second	Time interval between LLDP stop frame and a new start frame	2

LLDP port configuration: Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Port	1-n	Switch port number	1-n
Mode	Disabled	The port is configured to not send or accept LLDP frame	Disabled
	Enabled	Port is configured as both sending and receiving LLDP frame	
	Rx Only	Port is configured to only receive not send LLDP frame	
	Tx Only	Port is configured to only transmit LLDP frames	
Port Descr	Tick/Not tick	When ticked, the port description information transmit contained TLV in LLDP frame, and did not tick the TLV information is not included in LLDP frame, transmission	Tick
Sys Name	Tick/Not tick	When ticked, the "System Name" will be included in LLDP frame transmission, and did not tick the "System Name" is not included in LLDP frame, transmission	Tick
Sys Descr	Tick/Not tick	When ticked, the "System Description" will be included in LLDP frame transmission, and did not tick the "System Description" is not included in LLDP frame, transmission	Tick
Sys Capa	Tick/Not tick	When ticked, the "System Properties" will be included in LLDP frame transmission, and did not tick the "System Properties" does not contain the transmission in LLDP frame,	Tick
MgmtAddr	Tick/Not tick	When ticked, "Managing Address" will be included in LLDP frame transmission, and did not tick the "Manage Addresses" are not included in LLDP frame, transmission	Tick

5.2.2.12 POE

Enter【**POE**】navigation column, Set the value of the PoE.

Power Over Ethernet Configuration

Reserved Power determined by	(•) Class ( ) Allocation ( ) LLDP-MED
Power Management Mode	( ) Actual Consumption (•) Reserved Power

PoE Power Supply Configuration

Primary Power Supply [W]
2000

PoE Port Configuration

Port	PoE Mode	Priority	Maximum Power [W]
*	<>	<>	15.4
1	Disabled	Low	15.4
2	Disabled	Low	15.4
3	Disabled	Low	15.4
4	Disabled	Low	15.4
5	Disabled	Low	15.4
6	Disabled	Low	15.4
7	Disabled	Low	15.4
8	Disabled	Low	15.4
9	Disabled	Low	15.4
10	Disabled	Low	15.4
11	Disabled	Low	15.4
12	Disabled	Low	15.4

Save Reset

Power Over Ethernet Configuration：Interface items introduction:

Interface items	Introduction	Factory setting
Reserved Power determined by	Class/Allocating /LLDP-MED	Class
Power Management Mode	Actual Consumption/Reserved Power	Reserved Power

PoE Power Supply Configuration

Interface items	Introduction	Factory setting
Primary Power Supply[W]	2000	2000

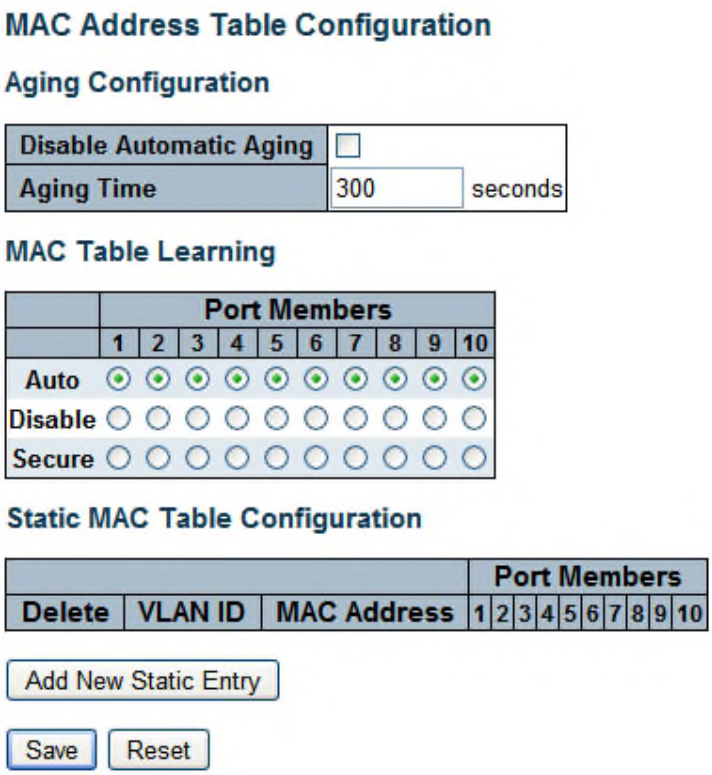
PoE Port Configuration

Interface items	Introduction	Factory setting
PoE Mode	Disabled/PoE/PoE+	Disabled
Priority	Low/High	Low
Maximum Power[W]		15.4

5.2.2.13 MAC Table

Enter【**MAC Table**】navigation column, set the MAC address table dynamically updated timeout, MAC address table learning mode, and manually add static MAC address table. Static MAC address table can add up to 64 MAC addresses.

Click<**Add New Static Entry**> button, enter the VLAN ID, a legitimate MAC address, select the port member, click [Save] button to complete the configuration MAC address table.

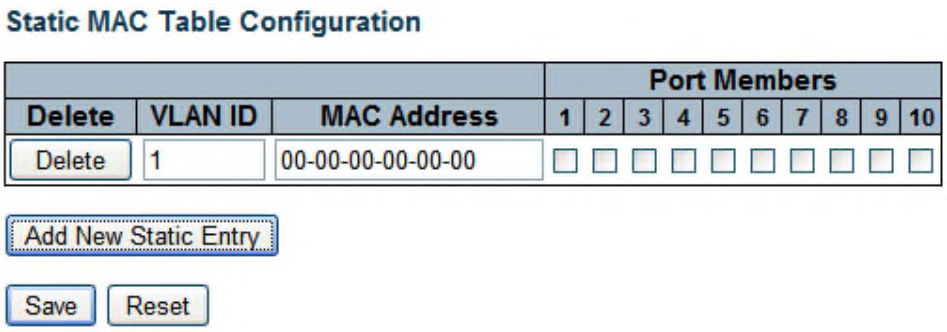


Timeout configuration：Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Disable automatic aging.	Tick/not tick	After tick the switch a certain time is not automatically remove the MAC address not used in MAC address table	not tick
Age time	10-1000000 second	MAC address table dynamically updated timeout	300

MAC address table configuration: Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Auto	Select	Open port MAC address auto-learning function	Selected
Disable	Select	Cancel port MAC address auto-learning function	Not Selected
Secure	Select	Only static MAC address table can be learned, discard other MAC addresses.	Not Selected



Static MAC address configuration： Interface items introduction:

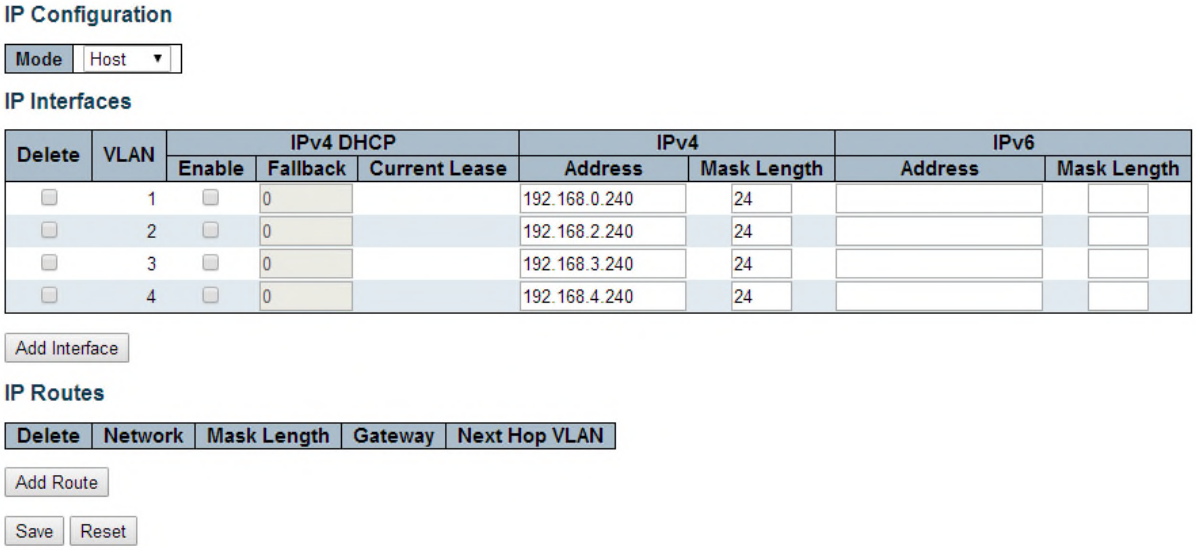
Interface items	Configuration	Introduction	Factory setting
Delete		Click, delete the corresponding table	
VLAN ID	1-4095	Added MAC address belong to VLAN ID	1
MAC Address	MAC address	MAC address add to MAC address table	00-00-00-00-00-00
Port Members	Recheck 1-n port	After selecting the port, MAC Address in the MAC address table added to the corresponding port in MAC address table	All not selected

Click on "Add a New Static Entry" to add a new static MAC address entries to the MAC address table.

5.2.2.14 VLANs Configuration

A. VLAN member IP configuration

Enter the [System Configuration] → [IP] navigation column, Vlan can create / delete IP, click [Save] button to save the current configuration, click [Delete] button to delete VLAN entries. Click [Reset] button to restore the data before storage.



Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Delete		Click, delete the corresponding entries	
VLAN	1-4095	To configure the specified VLAN ID	1
IPv4	Address	TCP/IP address	
	Mask Length	Subnet mask significant digits, such as: 24 represents: 255.255.255.0 namely11111111. 11111111.11111111.00000000	

click “Add Interface ” to add a new VLAN IP.

B. VLAN Configuration

Enter【Configuration】→【**VLANs** Configuration】navigation column, can create / modify VLAN, and added / edited the port to the appropriate VLAN.

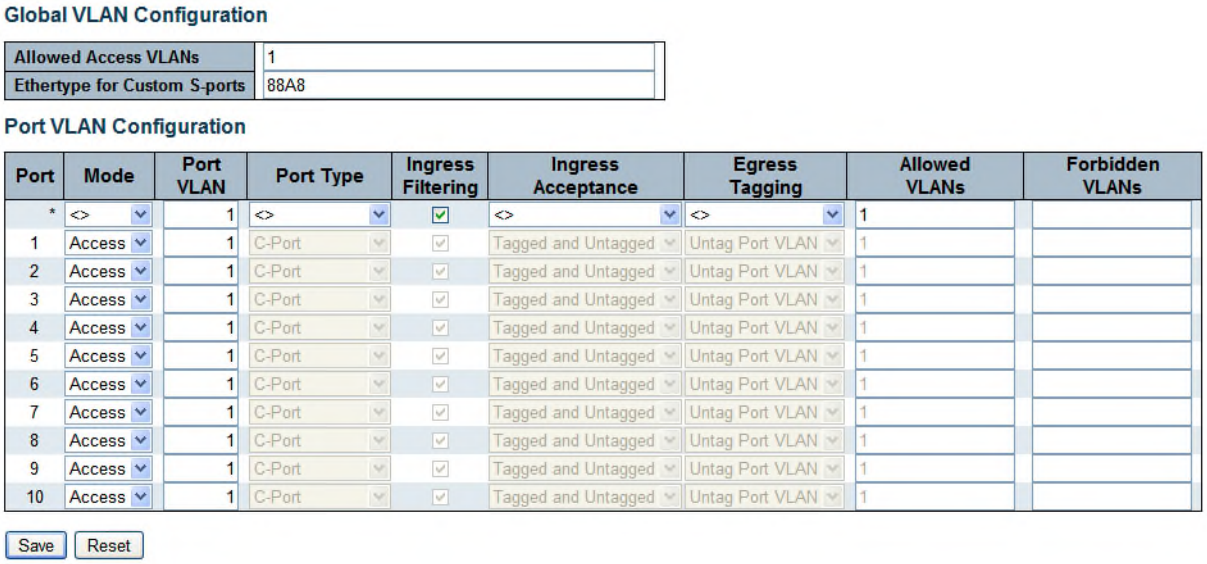
If just use common VLAN function, this page only need to configure the default VLAN number (Port VLAN) ,other functions without changes, except if you want to customize VLAN settings at Port VLAN , need to add a new VLAN number added to back inside of Allowed Access vlans ;

Ingress Filtering: refers to the port receives the packets that do not match choose to drop or forwarded, the default port input filtering function is disabled, that does not match the vlan packets received.

Frame Type: tag refers to the port receives packets with VLAN tag (and the VLAN ID tag should not be 0); untag refers to the port only receives packets without tag labels.

If configure advanced QINQ features, port optional: unaware lc / c-portls / s-port / s-custom-port type several modes to achieve different functions.

Click [Reset] button to return to the data before [Save]



Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Allowed Access vlans	VLAN port	Allowed access VLAN ID	1
Ether type for Custom S-ports	S-Ports definition mode	port when as service port the VLAN Ethernet type	88A8
Port	1~N	Ethernet port ID	
Mode	Access	access	√
	Trunk	Configure when VLAN need Trunk	
	HYbrid	Mixed (ring network use)	
Port VLAN	Range 1~4095	Configure the range of VLAN ID1~4095	1

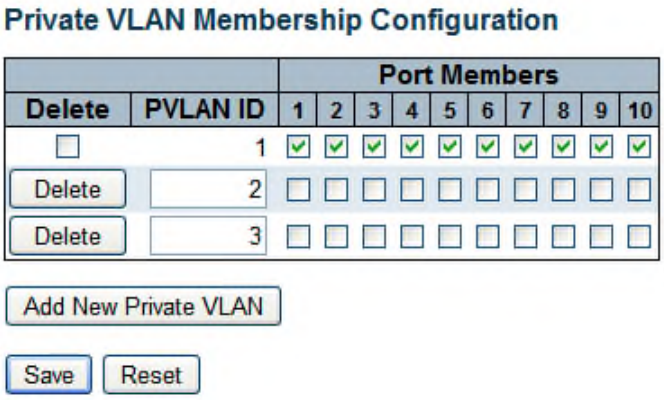
Port Type	Unaware	Port as unaware VLAN tag port	C-Port
	C-Port	Port as custom port	
	S-Port	Port as service port	
	S-Custom-Port	Port as service/custom port	
Ingress Filtering		Refers to the port receives the packets that do not match choose to drop or forwarded, the default port input filtering function is disabled, that does not match the vlan packets received	
Ingress Acceptance	Tagged And Untagged/ Tagged only/ Untagged only	Tagged And Untagged/ Tagged only/ Untagged only, When the input port and VLAN tag does not match the frame, the frame is dropped	
Egress Tagging	Untagged Port VLAN/Tagged All / Untagged All	Set the port receive the frame type, Untagged Port VLAN: VLAN port only receives untagged frames; Tagged ALL: port receives frames tagged for all, Untagged All: some frame labels are not applied,	All
Allowed VLANs		When setting the Trunk function need to set the allow the VLAN ID	1
Forbidden VLANs	Forbidden VLAN	Setting forbidden VLAN	

5.2.2.15 Private VLANs configuration

A. Private VLAN membership configuration

Enter **【Private VLANs configuration】→【PVLAN Membership】**navigation column, click**【Add New Private VLAN】**button, entry PVLAN ID to 2 and 3,select the port membership, click**【Save】**”button to compete the private VLAN membership configuration.

Select the Delete option in front of the corresponding VLAN ID, click [Save] button to delete the private VLAN members.



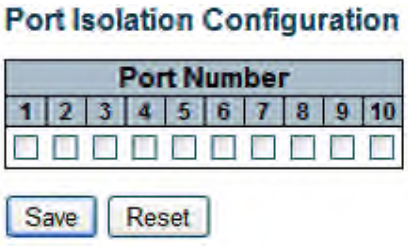
Interface items introduction：

Interface items	Configuration	Introduction	Factory setting
Delete		Click, delete the corresponding items	
Private VLAN ID	1-4095	Specifies to configure a private VLAN ID	1
Port Members	Tick/not tick	VLAN description information	tick

click “Add New Private VLAN ” to add a new private VLAN.

B. Private VLAN port isolation configuration

Enter【**Private VLANs configuration**】→【**Port Isolation**】navigation column, To implement Layer 2 isolation between packets, and different ports can be configured to different VLAN, but do not waste the limited VLAN resources, using port isolation feature, achieving isolation between ports within the same VLAN, users only need to put the port to the isolation group, you can achieve isolation between Layer 2 data within the isolation group port. Port isolation provides users with a more secure and flexible networking schemes.



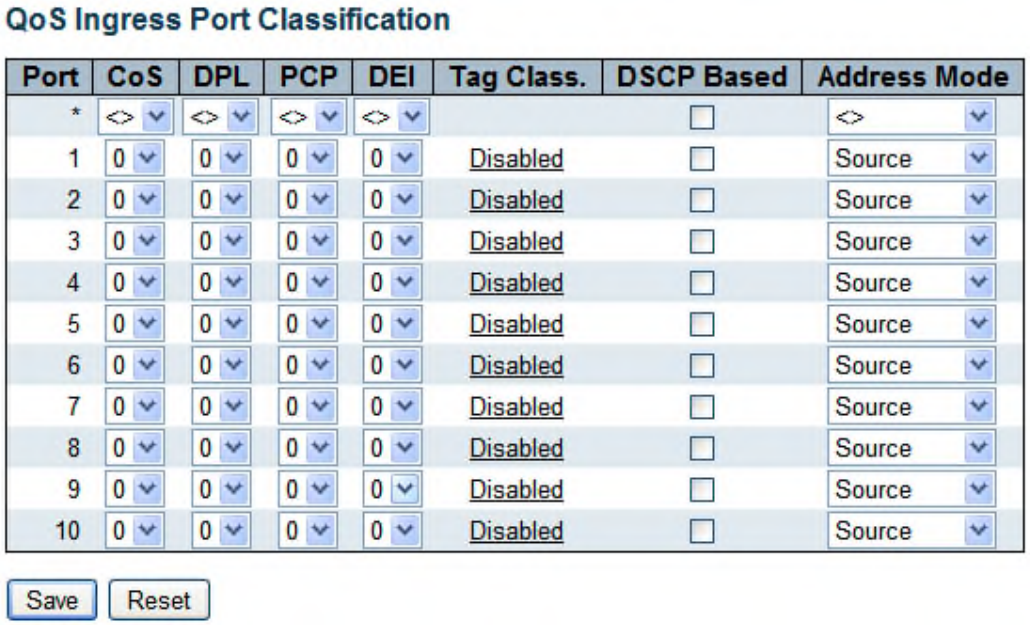
Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Port Members	Tick/not tick	after tick, the port isolated its VLAN and Private VLAN	Not tick

5.2.2.16 QoS configuration

A. Qos ingress Port classification

Enter【**Port Classification**】navigation column, this page allows you to configure the basic QoS Ingress Classification settings for all switch ports. The main configuration items as: Qos class (QoS category), DP level (DP level).

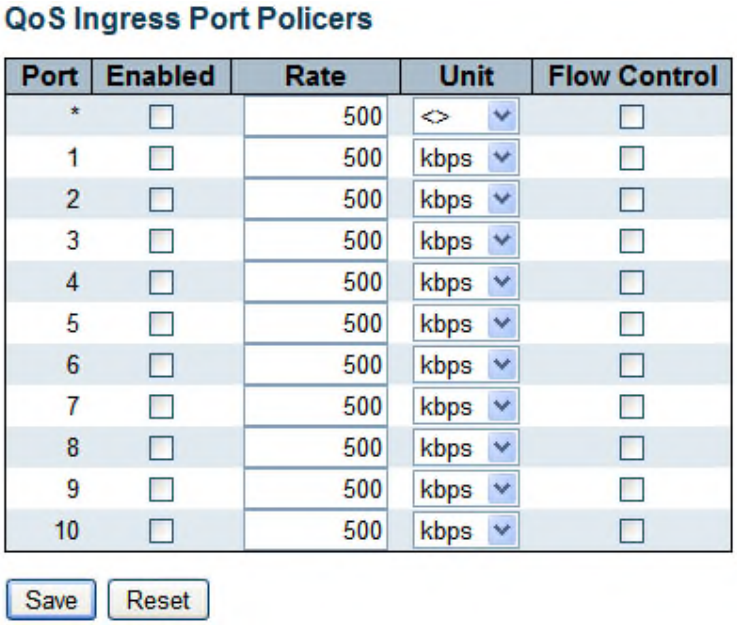


Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Port	1- n	configure the switch port number	1-n
QoS class	0-7	Qos class number, 0 is the lowest priority category	0
DP level	0/1	Frame discard class, 0: no dropped frames; 1: drop frames during congestion	0
PCP	0-7	802.1Q VLAN priority tag frames, if the port is VLAN aware and the frame has a VLAN tag, this value will be inserted into the VLAN priority bits field VLAN tag. Otherwise it will insert the default VLAN priority	0
DEI	0/1	VLAN discard frames rating, 0: VLAN frame is not discarded; 1: discard the VLAN frame congestion	0

B. Qos ingress port Policing

Enter【**Port Policing**】navigation column, Configure the port rate of Qos policing,main configure items:Rate(速率)、Flow Control.



Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Port	1- n	switch Port ID need to configure	1-n
Enabled	Select/not select	Qos policy enabled, select: enabled	Not select
Rate	100-1000000/ 1-3300	Rate value configure: 100-1000000Kbps or 1-3300pps	500
Unit	Kbps/pps	Rate unit： pps: packets / sec Kbps: kilobytes / sec.	kbps
Flow Control	Select/not select	On/off flow control	Not select

C. Qos egress port schedulers

Enter【**Port Scheduler**】navigation column, show QoS port data flow egress schedulers.

QoS Egress Port Schedulers

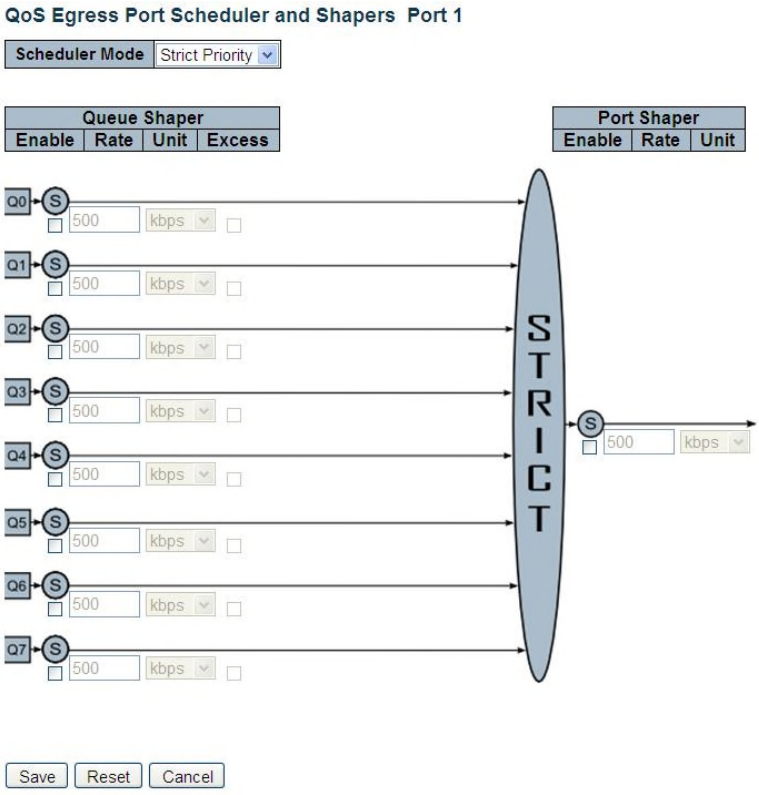
Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-

Interface items introduction:

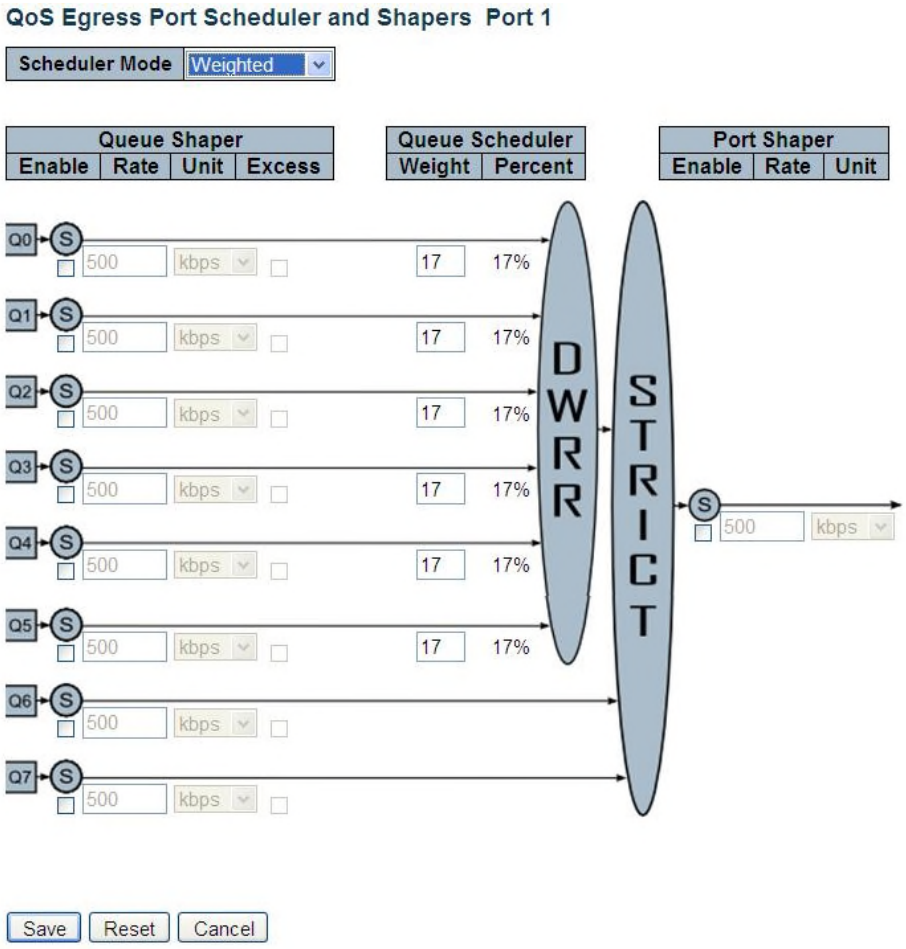
Interface items	Configuration	Introduction	Factory setting
Port	1- n	Switch Port ID need to configure	1-n
Mode	Strict Priority /Weighted	Port schedule mode	Strict Priority
Weight Qn		show line 1-5 weighted	500

Click port number 1、2、3、… 10 enter to specific configure page

Scheduler Mode configure to Strict priority, interface show as below:



Scheduler Mode configure to Weighted, interface show as below:



Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Scheduler Mode	Strict Priority /Weighted	Schedule mode optional	Strict Priority
Queue Shaper Enable	Select/not select	On / Off queue shaper enable	not select
Queue Shaper Rate	100-1000000/ 1-3300	Queue rate configure: 100-1000000Kbps or 1-3300pps	500
Queue Shaper Unit	Kbps/pps	Rate unit pps: packets / sec Kbps: kilobytes / sec.	kbps
Queue Shaper Excess	Select/not select	After select, queue can use excess bandwidth	not select

Queue Scheduler Weight	1-100%	Set the queue percentage weight	17
Queue Scheduler Percent		show the queue percentage weight	17%
Port Shaper Enable	Select/not select	On/off port module	Not select
Port Shaper Rate	100-1000000/ 1-3300	Port module rate: 100-1000000Kbps or 1-3300pps	500
Port Shaper Unit	Kbps/pps	Rate unit pps: packets / sec Kbps: kilobytes / sec.	Kbps

Change the option of the port number of upper right corner, you can configure all switch ports.

D. Qos Egress port shapers

Enter【**Port Shaping**】navigation column, show QoS port queue module configuration.

QoS Egress Port Shapers

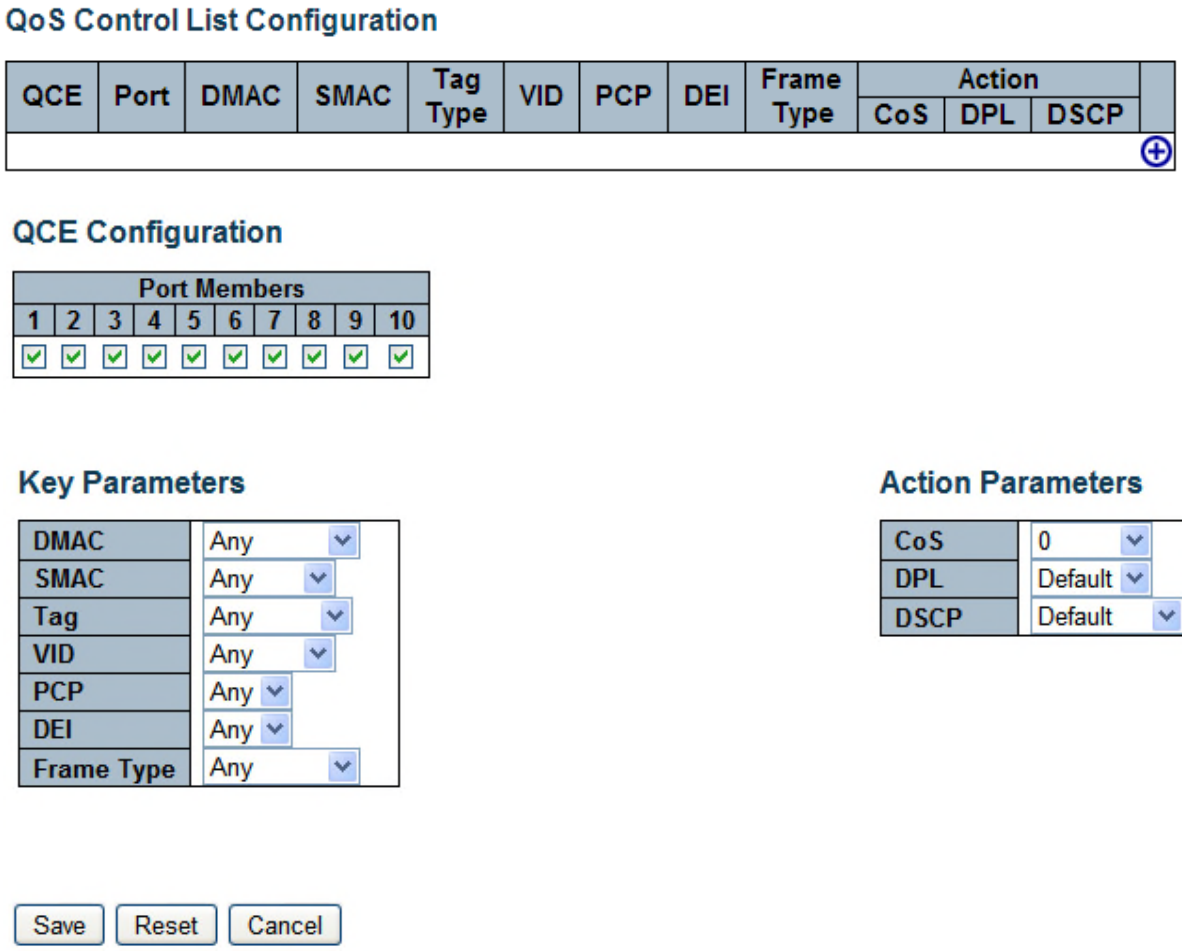
Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Port	Strict Priority /Weighted	Schedule mode selected	Strict Priority
Shapers Qn		shows each queue configuration	
Shapers Port		shows each port configuration	

E. Qos control list

Enter【**QoS Control List**】navigation column ,configure QoS control list. Click on the table rightmost button, the page will go to a particular list item configuration interface.



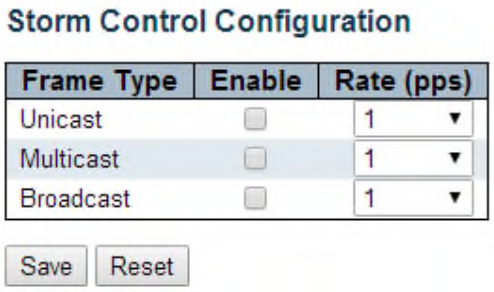
Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
QCE#		QoS list item Index	
Port	All/ port no	Includ port	
Key Parameters Frame Type	Any/Ethernet/LLC/SNAP/IPV4/IPV6	Select the recognized frame type for the input data flow	Any
Key Parameters SMAC	Any/Specific	Select the recognized MAC address OUI (Organization ID) for the input data flow	Any
Key Parameters DMAC	Any/UC/MC/BC	Select a frame input data stream to identify the destination MAC address type: Any: Destination can be any type of MAC UC: Destination only to allow unicast MAC MC: Destination only to allow multicast MAC	Any

		BC：Destination MAC only to allow broadcast	
Key Parameters VID	Any/Specific(1-4095)/Range(VID1~VID2)	The frame VLAN ID range to be recognized of the input data stream, Any: All VLAN Specific: a specific VLAN Range: a VLAN range	Any
Key Parameters PCP	Any/0,1,2,3,4,5,6,7/0-1,2-3,4-5,6-7,0-3,4-7	Select the recognized priority for the input data flow	Any
Key Parameters DEI	Any/0/1	Select the recognized discard flag for the frame of input data flow	Any
Action Class	0-7	Add type value for frame matching key parameters	0
Action DPL	Default/0/1	Add discard value for frame matching key parameters（Default：Retain the original DPL）	Default
Action DSCP	Default/0-63	Add DSCP value for frame matching key parameters （Default： Retain the original DSCP）	Default

F. Qos storm control configuration

Enter【**Storm Control**】navigation column, configure QoS port storm control, open for unicast, multicast, rate limit broadcast storms, and set rate. The main configuration items : Unicast (unicast frames), Multicast (multicast frames), Broadcast (broadcast frames).



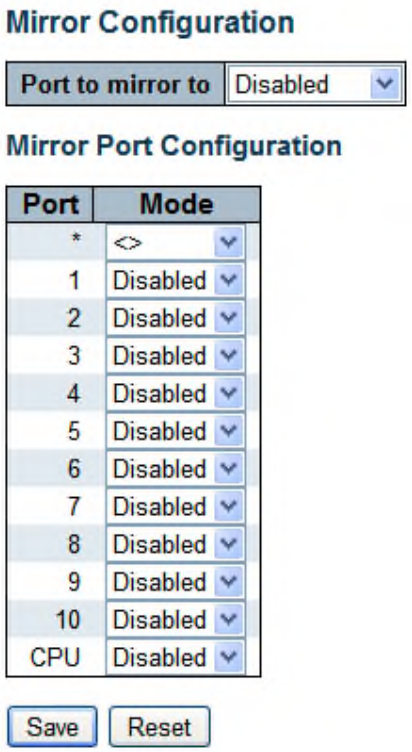
Interface items introduction:

Interface items	Configuration	Introduction	Factory setting

Frame Type		Data frame type, Unicast; Multicast: Broadcast	
Enable	Select/not select	On/off storm control	Not select
Rate	1-1024Kpps	Select the data rate upper limit	1pps

5.2.2.17 Mirroring configuration

Enter【**Mirroring**】configuration navigation column, Port mirroring, will complete mapping to the specified port for some port or control packets flow, the designated port as the destination port, the port is mapped source port mirroring, port mirroring connected to the network analytical instruments , you can clear analysis mirroring port packets without disrupting the business of mirroring source port. Port mirroring is a convenient re-line monitoring. All ports system can be configured as a mirrored port, but the destination port mirroring can only configure one. When a port is configured as a mirrored port, the corresponding port cannot be configured as a source port. Source port means that mirrored port, you can configure multiple destination port mirroring to only configure one.



Interface items introduction:

Interface items	Configuration	Introduction	Factory setting
Port to mirror to	Disabled/1- n	Disabled Close mirroring function, 1-n	Disabled

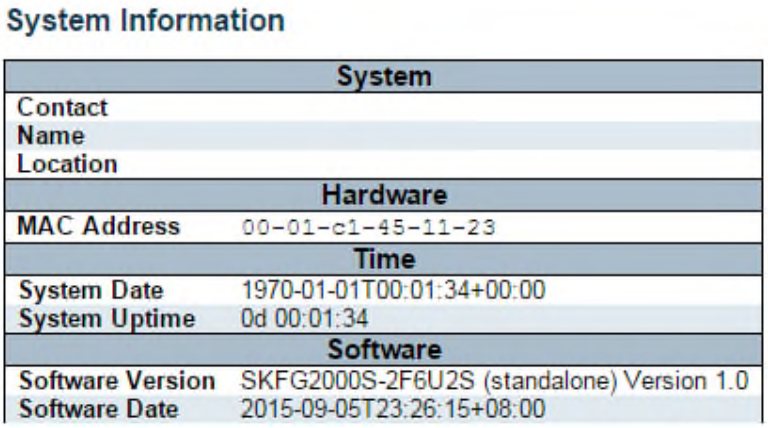
		select the destination port	
Port	1- n	Switch physical port number	1-n
Mode	Disabled	Close Port Mirroring	Disabled
	Rx Only	Only received frames are mirrored	
	Tx Only	Only transmit frames are mirrored	
	Enabled	Transmit and received frame are mirrored	

5.2.3 Monitor(Status Display)

5.2.3.1 System

A. System information

Enter【**System**】→【**Information**】navigation column, view system information on page.



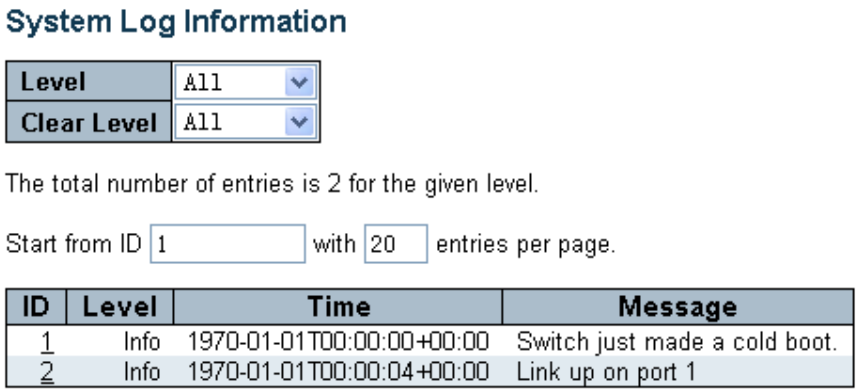
Interface items introduction:

Interface items	Introduction
Contact	System Configuration menu configure: maintenance personnel contact
Name	System Configuration menu configure: switch name
Location	System Configuration menu configure: switch location
MAC Address	Switch MAC address
Chip ID	Switch chip ID
System Date	System date

System Uptime	System uptime
Software Version	Software version
Software Date	Software date

B. System log

Enter【**System**】→【**Log**】navigation column, on system log page, view some log information during the running equipment process that is easy for the maintenance personnel analyze the problem.



Interface items introduction:

Interface items	Introduction
Level	Select log level:ALL;Info:;Warning;Error
Clear Level	Remove log level:ALL;Info;Warning;Error;
ID	Log index ID
Level	Log level
Time	Log Time date
Message	Log message

Page operating button:

Refresh

Clear

|<<：view the first log

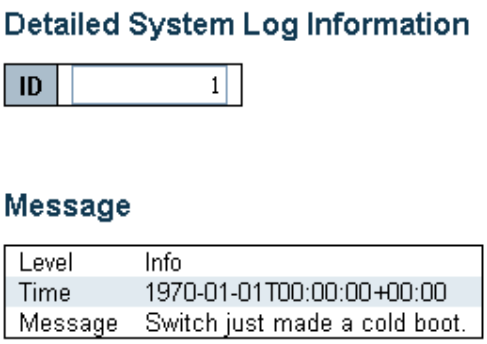
<<: view the Previous log

>>: view the next log

>>|: view the last log

C. Log detail

Enter【**System**】→【**Detailed Log**】navigation column, entrylog, display system log detail on page.



Interface items introduction:

Interface items	Introduction
ID	Select the log index to view
Level	Log level
Time	Log generate time
Message	Log message

5.2.3.2 Thermal Protection

Enter【**Thermal Protection**】,display the status information of device temperature on page.

Thermal Protection Status

Thermal Protection Port Status

Port	Temperature		Port status
1	62	°C	Port link is thermal protected (Link is down)
2	62	°C	Port link is thermal protected (Link is down)
3	63	°C	Port link is thermal protected (Link is down)
4	62	°C	Port link is thermal protected (Link is down)
5	62	°C	Port link is thermal protected (Link is down)
6	62	°C	Port link is thermal protected (Link is down)
7	63	°C	Port link is thermal protected (Link is down)
8	62	°C	Port link is thermal protected (Link is down)
9	63	°C	Port link is thermal protected (Link is down)
10	62	°C	Port link is thermal protected (Link is down)

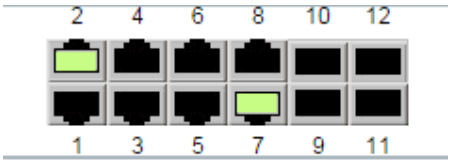
Interface items introduction:

Interface items	Introduction
Local Port	Switch physical port number
Temperature	Temperature
Port status	Display the port link status

5.2.3.3 Ports

A. **Port status**

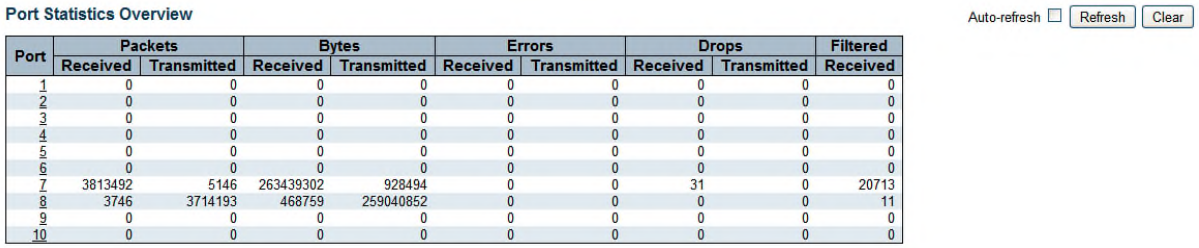
Enter【Ports】→【State】navigation column, entry port state overview page, a graphical interface that shows the connection status of the switch ports:



B. Port data traffic overview

Enter【**Ports**】→【**Traffic Overview**】navigation column, In the Port Statistics page, you can see the number of packets transmitted and received for each port, the number of bytes transmitted and received error packets. When have too many error message it indicates the working status of the port is poor, you need to check the cable connected to the port or other side card if there are problems.

In this function, the user can check the <Auto Refresh> to refresh the data in real time, can also be manually Click <Refresh> button to see the new data, <Clear> button to clear the statistics function provides.



Port Statistics Overview

Auto-refresh ☐ Refresh Clear

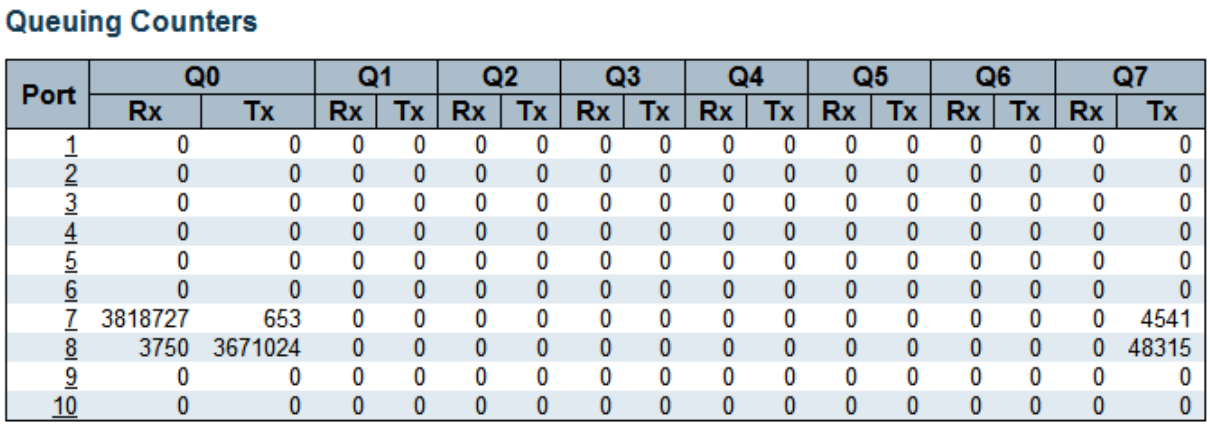
Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	3813492	5146	263439302	928494	0	0	31	0	20713
8	3746	3714193	468759	259040852	0	0	0	0	11
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0

Interface items introduction:

Interface items	Introduction
Port	Switch physical port number
Packets Received	Packets Received
Packets Transmitted	Packets Transmitted
Bytes Received	Bytes Received
Bytes Transmitted	Bytes Transmitted
Errors Received	Errors Received
Errors Transmitted	Errors Transmitted
Drops Received	Drops Received
Drops Transmitted	Drops Transmitted
Fitered Received	Fitered Received

C. Port QoS Statistics

Enter【**Ports**】→【**QoS Statistics**】navigation column, Displays status in different queues of each port on page.



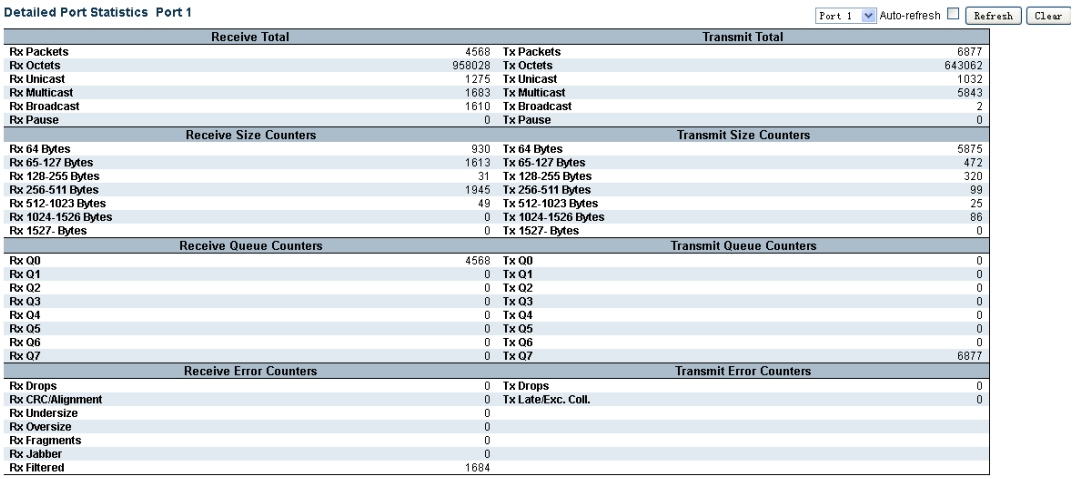
Queuing Counters

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	3818727	653	0	0	0	0	0	0	0	0	0	0	0	0	0	4541
8	3750	3671024	0	0	0	0	0	0	0	0	0	0	0	0	0	48315
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Interface items introduction:

Interface items	Introduction
Port	Port ID
Qn Rx	The number of queue received frame
QnTr	The number of queue transmit frame

Click the port number, enter the corresponding port QoS status in the detailed statistics page, you can query detailed operation of each port, including receiving the transmitted packets, broadcast packets, error packets, etc., to facilitate network management for network maintenance personnel. Drop-down navigation through the port to see the designated port traffic information, the user can check the <Auto-refresh> button to refresh the data in real-time information can also be manually Click <Refresh> to see the new data, <Clear> button to clear the statistical data provided Features.



Total of transmitting and receiving packets：Interface items introduction:

Interface items	Introduction
Rx Packages	Total Rx Packages
Rx Octets	Total Rx Octets
Rx Unicast	Total Rx Unicast
Rx Multicast	Total Rx Multicast
Rx Broadcast	Total Rx Broadcast
Rx Pause	Total Rx Pause
Tx Packages	Total Tx Packages
Tx Octets	Total Tx Octets

Tx Unicast	Total Tx Unicast
Tx Multicast	Total Tx Multicast
Tx Broadcast	Total Tx Broadcast
Tx Pause	Total Tx Pause

Frame number of Transmit and received of different frame length: The interface Item Description:

Interface items	Introduction
Rx 64 Bytes	Frame number of Rx 64 Bytes
Rx 65-127 Bytes	Frame number of Rx 65-127 Bytes
Rx 128-255 Bytes	Frame number of Rx 128-255 Bytes
Rx 256-511 Bytes	Frame number of Rx 256-511 Bytes
Rx 512-1023 Bytes	Frame number of Rx 512-1023 Bytes
Rx 1024-1526 Bytes	Frame number of Rx 1024-1526 Bytes
Rx 1527- Bytes	Frame number of Rx 1527- Bytes
Tx 64 Bytes	Frame number of Tx 64 Bytes
Tx 65-127 Bytes	Frame number of Tx 65-127 Bytes
Tx 128-255 Bytes	Frame number of Tx 128-255 Bytes
Tx 256-511 Bytes	Frame number of Tx 256-511 Bytes
Tx 512-1023 Bytes	Frame number of Tx 512-1023 Bytes
Tx 1024-1526 Bytes	Frame number of Tx 1024-1526 Bytes
Tx 1527- Bytes	Frame number of Tx 1527- Bytes

Transmit / receive queue transmit / receive the frame number: Interface Item Description:

Interface Item	Description
Qn Rx	Receiving frame number in queue
Qn Rx	Transmit frame number in queue

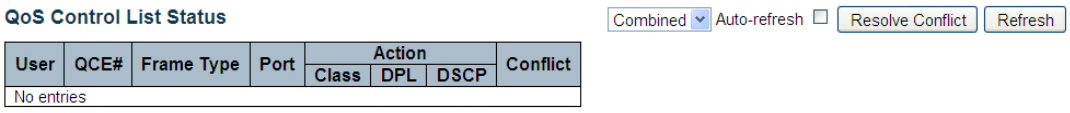
Transmitting / receiving error count: Interface Item Description:

Interface Item	Description

Rx Drops	Number of received frame due to insufficient cache or congestion drops
Rx CRC/Alignment	Number of received frame occurred CRC and alignment errors
Rx Undersize	The number of short frames received undersize 64 bytes
Rx Oversize	The number of frame received oversize the maximum frame
Rx Fragments	The number of received frame with invalid CRC, frame length less than 64
Rx Jabber	The number of received frame with invalid CRC, frame length over max frame
Rx Filtered	The number of filtered outframes during forwarding process
Tx Drops	Number of transmit frame due to insufficient cache or congestion drops
Tx Late/Exc. Coll.	The number of transmit frames conflict then drop during transmission

D. Port QoS Control list

Enter【Ports】→【QCL Status】navigation column, display all QoS control table on page.

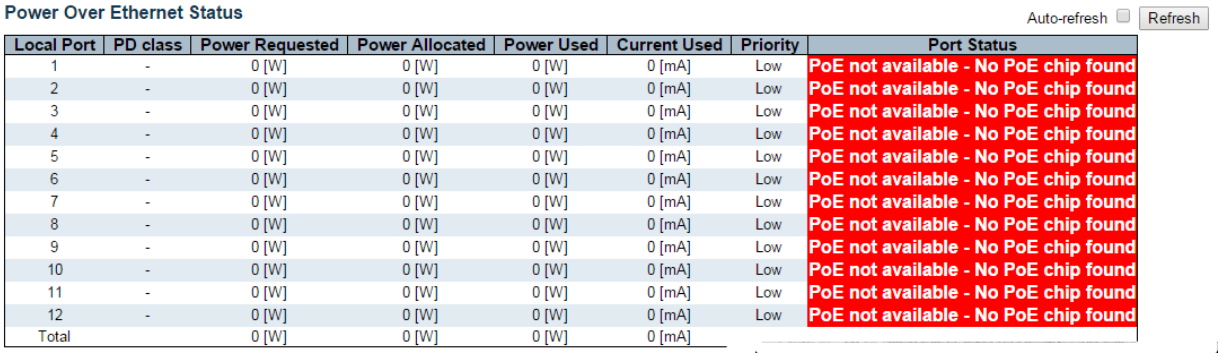


Interface items introduction:

Interface items	introduction
User	User name
QCE#	QoS list index
Frame Type	Identify the input frame type:Any/Ethernet/LLC/SNAP/IPV4/IPV6
Port	The Qos controls apply to which ports
Action Class	To add QoS type value for" parameter configuration to match the input frame,"
Action DPL	To add QoS discard flag for" parameter configuration to match the input frame,"

Action DSCP	To add DSCP value for" parameter configuration to match the input frame,"
Conflict	Status indicator whether conflict with other QoS control items

5.2.3.4 PoE



Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
3	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
7	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
9	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
10	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
11	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
12	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

Interface items introduction:

Interface items	introduction
PD class	1\2\3\4…
Power Requested	Required power dissipation
Power Allocated	**Power Allocated**
Power Used	Actual power usage
Current Used	Actual current usage
Priority	Low/High
Port Status	The PoE available is green, the PoE is not available is red

5.2.3.5 Security

A. Access Management Statistics

Enter【**Access Management Statistics**】navigation column, display access management statistics on page. Use can select<**Auto-refresh**>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data, <Clear> button to clear the statistics function provides.

Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0

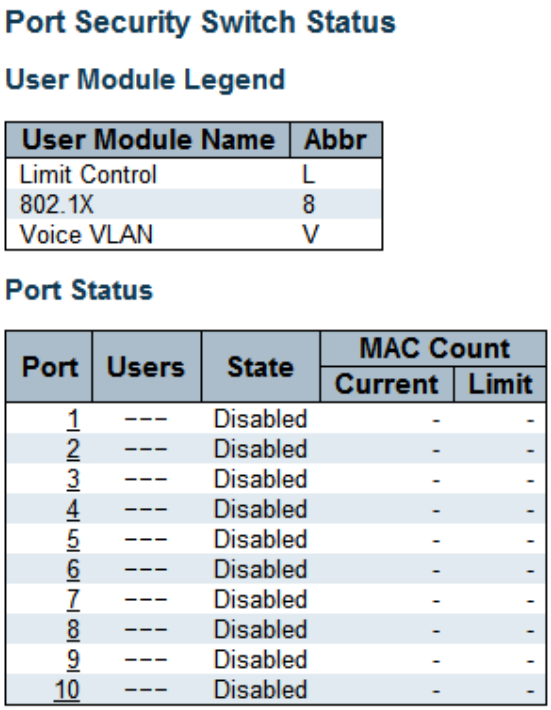
Interface items introduction:

Interface items	**Description**
Interface	Access management interface type: **HTTP/ HTTPS/SNMP**
Received Packets	Number of received packets from port after turned on access management mode
Allowed Packets	Number of allowed port after turned on access management mode
Discarded Packets	Number of discarded packets from port after turned on access management mode

B. Network

Port Security

Enter【**Port Security**】→【**Switch**】navigation column, display port switch security on page. User can select<**Auto-refresh**>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.



Port Security Switch Status

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

Port Status

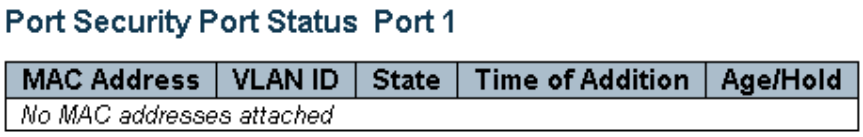
Port	Users	State	MAC Count	
			Current	Limit
1	---	Disabled	-	-
2	---	Disabled	-	-
3	---	Disabled	-	-
4	---	Disabled	-	-
5	---	Disabled	-	-
6	---	Disabled	-	-
7	---	Disabled	-	-
8	---	Disabled	-	-
9	---	Disabled	-	-
10	---	Disabled	-	-

Interface items introduction:

Interface items	Description
User Module Name	The module name can request a port security services
Abbr	User name Single-letter abbreviations
Port	Switch physical port number
Users	User module abbreviations
MAC Count	The current number of learned MAC addresses

Port state

Enter【**Port Security**】→【**Port**】navigation column, display specific port state on page, User can select<**Auto-refresh**>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.



Port Security Port Status Port 1

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached				

Interface items introduction:

Interface items	**Description**
MAC Address & VLAN ID	Port learned MAC address and VLAN ID

State	Indicates whether a matching MAC address of the frame is forwarded or blocked
Time of Addition	The first occurrence time on matching the MAC address
Age/Hold	MAC address hold time

NAS state

Enter【NAS state】→【**Switch**】navigation column, display switching state of network access server on page，User can select<**Auto-refresh**>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.

Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	
5	Force Authorized	Globally Disabled			-	
6	Force Authorized	Globally Disabled			-	
7	Force Authorized	Globally Disabled			-	
8	Force Authorized	Globally Disabled			-	
9	Force Authorized	Globally Disabled			-	
10	Force Authorized	Globally Disabled			-	

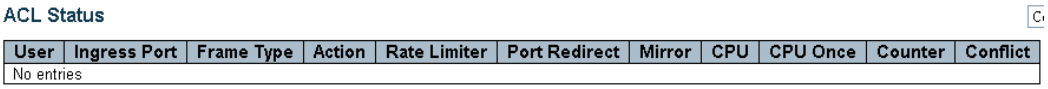
Interface items introduction:

Interface items	introduction:
Port	Switch physical port number, click to the details page
Admin State	**adopt authentication mode**
	Force Authorized: In this mode, when a client is connected to the port, the switch will automatically send an EAPOL success frame, you can access the network without authentication
	Force Unauthorized: In this mode, when a client is connected to the port, the switch will automatically send an EAPOL failure frame, any client can access the network
	802.1X: Using 802.1X authentication mode
	MAC-Based Auth.: Using MAC-based authentication mode
Port State	**Port state：**

	Globally Disabled: NAS all Disabled
	Link Down: NAS all Enabled, but port cant link
	Authorized: Port operates in Force Authorized mode, or work in only one request mode, and the request authentication success
	Unauthorized: Port operates in Force Unauthorized mode, or work in only one request mode, and the request authentication not success
	X Auth/Y Unauth: port in mange request mode,X user authentication success user authentication not success
Last Source	The last receiving source from EAPOL frame
Last ID	The last receiving user name from response authentication EAPOL frame

ACL Status

Enter【**ACL Status**】navigation column, on statistics page, can view related security information, Use view all kinds network security information through select the drop-down navigation Combined, Static, IPMC, LOOP, conflict. User can select<**Auto-refresh**>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.



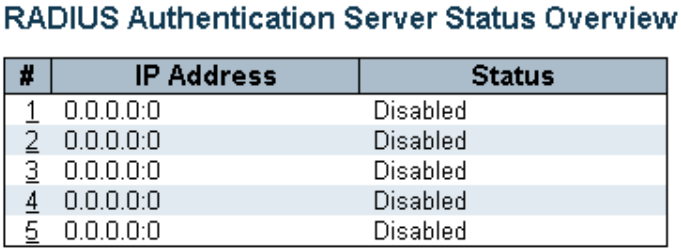
Interface items introduction:

Interface items	**Description**
User	Indicate to access list user
Ingress Port	Access ingress input port: All/Port1-n
Frame Type	Any: ACE matching all frame type
	Type: ACE matching Ethernet type frame not IP frame and ARP frame
	ARP: ACE matching ARP/RARP frame
	IPV4: ACE matching all IPV4 frame
	IPV4/ICMP: ACE matching IPV4 frame with ICMP protocol
	IPV4/UDP: ACE matching IPV4 frame with UDP protocol
	IPV4/TCP: ACE matching IPV4 frame with TCP protocol

	IPV4/other: ACE matching IPV4 frame with other protocol except ICMP/UDP/TCP
	IPV6: ACE matching all standard IPV6 frame
Action	Permit: forward and learn the frame matching ACE
	Deny: discard the frame matching ACE
	Filter: filter the frame matching ACE
Rate Limiter	Disabled/0-16: rate limit ID use on port
Port Redirect	Disabled/Port ID: Whether Port Frame is re-directed, if redirect ,redirect port
Mirror	Disabled/Enabled：The frame Be mirrored/not mirror receiving from the port
CPU	Packet matching ACE forward to CPU
CPU Once	The first packet matching ACE forward to CPU
Counter	Packet counter matching ACE
Conflict	Firmware state

C. AAAstatus

Enter【**AAA**】→【**RADIUS Overview**】navigation column, If the network has been configured remote server radius, you can view the relevant certification packet statistics from this page.



Interface items introduction:

Interface items	introduction
#	NAS service ID, click to detail
IP Address	Server IP address
Status	Disable: server off
	Not Ready: server on without IP packet
	Ready：server on operating IP packet, RADIUS module is ready to accept access

	Dead(X seconds Left): invalid time

Enter【**AAA**】→【**RADIUS Details**】navigation column, display the authentication state of RADIUS server on page, User can select<**Auto-refresh**>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.

RADIUS Authentication Statistics for Server #1

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address			0.0.0.0:0
State			Disabled
Round-Trip Time			0 ms

Accept packet：interface items description:

Interface items	description
Access Accepts	Receiving packet number from server
Access Rejects	Receiving packet number from server
Access Challenges	Receiving access password packets from server
Malformed Access Responses	Receiving packets number which non-compliant and unknown from server
Bad Authenticators	Receiving authentication response packets number which including invalid authentication name, invalid message, Invalid Certificate attributes from server
unknown Types	Authentication port receiving number of unknown packets which transmit from the server
Packets Dropped	Authentication port receiving number of discard packets which transmit from the server

Transmit packet: interface items description:

Interface items	description
Access Accepts	The number of access requests packets sent to the server
Access Retransmissions	The number of Access Retransmissions packets sent to the server
Pending Requests	The number of request packet sent to the server has not been a response but not overtime
Timeouts	Authentication timeout Number

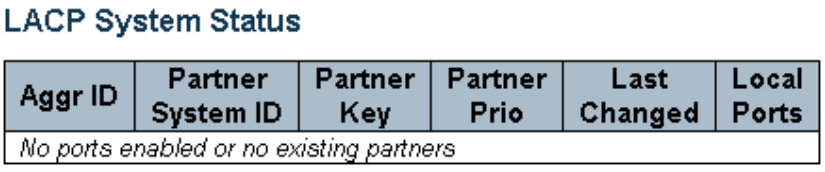
Other information: interface items description:

Interface Items	Description
IP Address	Authentication server IP address
State	**state：**
	Disable: server off
	Not Ready: server on without IP packet
	Ready：server on operating IP packet, RADIUS module is ready to accept access
	Dead(X seconds Left): invalid time
Round-Trip Time	Recent access response, access password, the access request interval

5.2.3.6 LACP state

A. LACP system status

Enter【**LACP**】→【**System Status**】navigation column, on this status page, can see the operating status on the port agreement, the group number of automatic aggregation, local port, peer communication key member number and other information.



Interface items introduction:

Interface items	Introduction
Aggr ID	Aggregation Examples ID
Partner System ID	Aggregation system ID
Partner Key	Communication key
Last changed	Aggregation changing time
Local Ports	indicator which ports including in aggregation port

B. LACP port status

Enter【**LACP**】→【**Port Status**】navigation column, This page displays LACP physical port information ,User can select<**Auto-refresh**>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.

LACP Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-

Interface items introduction:

Interface items	Introduction
Port	Switch physical port ID
LACP	LACP status， Yes: LACP on and connected port;No： LACP off and port disconnected
Key	Communication key
Aggr ID	Aggregation Examples ID
Partner System ID	Aggregation system ID
Partner Port	Including port in aggregation group
Partner Prio	The priority of port in aggregation group

C. LACP port statistics

Enter【**LACP**】→【**Port Statistics**】navigation column, This page displays the physical port LACP reception, transmission dropped packets, User can select<Auto-refresh>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.

LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

Interface items introduction:

Interface items	**Description**
Port	switch physical port ID
LACP Received	Port Received the number LACP frame
LACP Transmitted	Port transmitted the number LACP frame
Discarded	Port discard the number of illegal LACP frame

5.2.3.7 Loop Protection

Enter【**Loop Protection**】navigation column,display loop protection status on page,User can select<Auto-refresh>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.

Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
No ports enabled						

Interface items introduction:

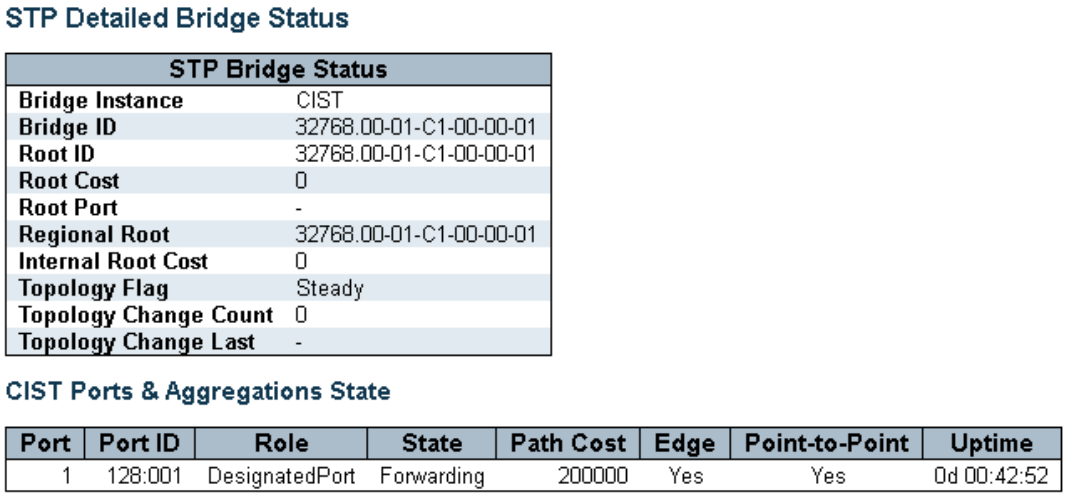
Interface items	**Description**
Port	Switch physical port number
Action	Protective action of port configuration
Transmit	Transmit mode of port configuration

Loops	loops time on port
Status	Current loop protective status
Loop	current port whether in loop status
Time of Last Loop	The last time detect the loop

5.2.3.8 Spanning Tree

A. Spanning Tree Bridge status

Enter【**Spanning Tree**】→【bridge status】navigation column, can view：bridge ID、Root bridge ID, port path cost and other information, User can select<Auto-refresh>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.



STP bridge status detail :Interface items description：

Interface items	Description
Bridge Instance	STP bridge instance type
Bridge ID	Bridge instance ID
Root ID	Current root ID
Root Cost	Root path cost
Root Port	Designated port for the root bridge
Regional Root	Be selected to regional root bridge ID
Internal Root Cost	Internal root bridge path cost

Topology Flag	Topology change status
Topology Change Count	Topology change count
Topology Change Last	Changing time for last topology

CIST port and aggr status： Interface items description

Interface items	description
Port	Switch STP valid port number
Port ID	Port ID to be used for STP
Role	The current use of STP port role
State	The current STP port status
Path Cost	The current STP port path cost
Edge	Edge port instructions, Yes: port edge port; No: ports are non-edge port
Point-to-Point	The current state of the STP is point to point
Uptime	The last uptime of bridge port

B. Spanning Tree Port status

Enter【**Spanning Tree**】→【**Port Status**】navigation column, can view each STP port status. Including STP role, the forwarding state, updated information, User can select<Auto-refresh>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.

STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	RootPort	Forwarding	1d 00:00:24
8	DesignatedPort	Forwarding	0d 22:31:09
9	Disabled	Discarding	-
10	Disabled	Discarding	-

Interface items introduction:

Interface items	Introduction:
Port	switch physical port no

CIST Role	current STP port role
CIST State	current STP port status
Uptime	The last uptime of bridge port

C. Spanning Tree Port statistics

Enter【**Spanning Tree**】→【**Port Statistics**】navigation column, this page shows the STP packet statistics, User can select<Auto-refresh>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.

STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	0	1405	0	0	0	0	0	0	0	0

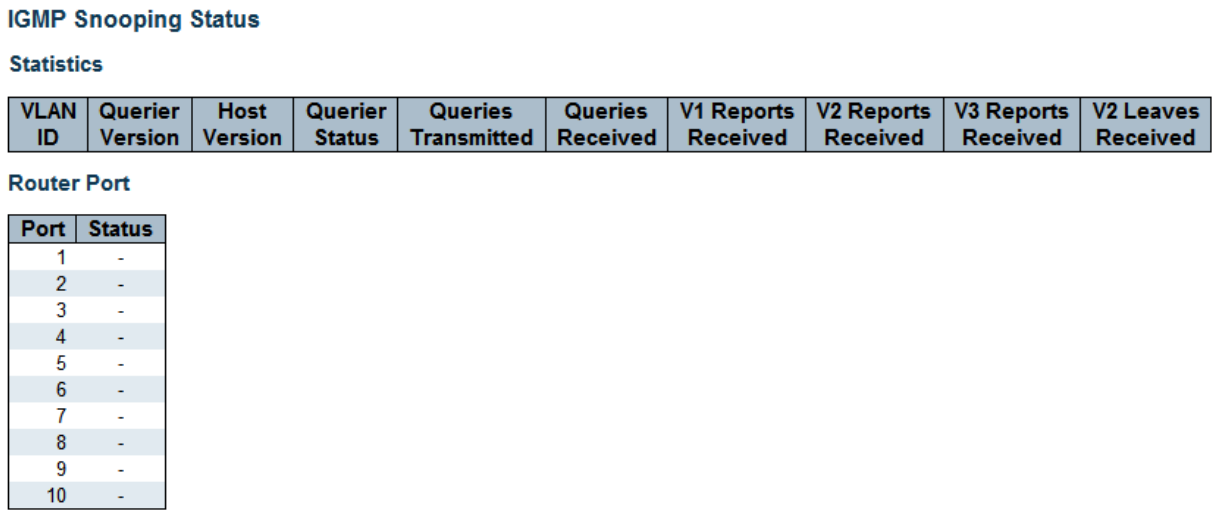
Interface items introduction:

Interface items	Introduction
Port	Switch physical port number
Transmitted MSTP	Port transmitted the number of MSTP BPDU
Transmitted RSTP	Port transmitted the number of RSTP BPDU
Transmitted STP	Port transmitted the number of STP BPDU
Transmitted TCN	Port transmitted the number of TCN BPDU
Received MSTP	Port received the number of MSTP BPDU
Received RSTP	Port received the number of RSTP BPDU
Received STP	Port received the number of STP BPDU
Received TCN	Port received the number of TCN BPDU
Discarded Unknown	Port discarded the number of unknown STP BPDU
Discarded Illegal	Port discarded the number of illegal STP BPDU

5.2.3.9 IPMC status

A. IGMP Snooping status

Enter【**IGMP Snooping**】→【**Status**】navigation column, show IGMP Snooping on page, User can select<Auto-refresh>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.



Statistics status: Interface items introduction：

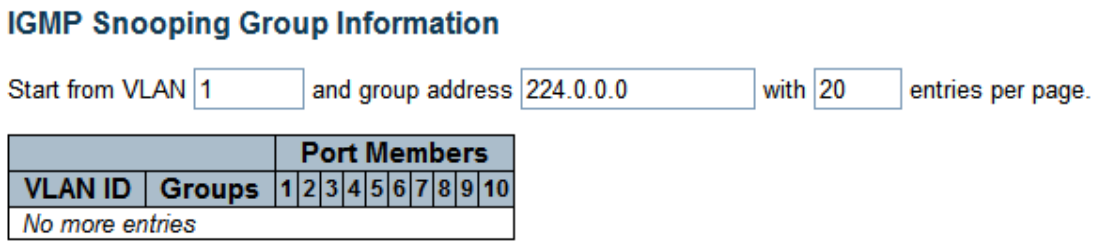
Interface items	Introduction
VLAN ID	VLAN ID
Querier Version	Working Query Version
Host Version	Working Host Version
Querier Status	Querier Status
Queries Transmitted	The number of transmitted query frame
Queries Received	The number of received query frame
V1 Reports Received	The number of received V1 Report frame
V2 Reports Received	The number of received V2 Report frame
V3 Reports Received	The number of received V3 Report frame
V2 Leaves Received	The number of received V2 leave frame

Router port：Interface items instruction:

Interface items	Instruction
Port	Switch port ID
Status	Indicator route port

B. IGMP Groups Information

Enter【**IGMP Snooping**】→【**Groups Information**】navigation column, show IGMP Snooping group information on page, User can select<Auto-refresh>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.



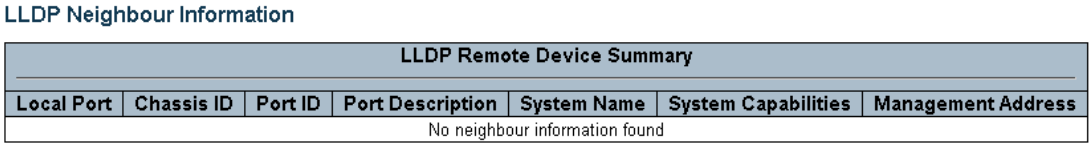
Interface items instruction:

Interface items	Instruction
VLAN ID	VLAN ID
Groups	Group address
Port Members	Group including port

5.2.3.10 LLDP status

A. LLDP neighbors

Enter【**LLDP**】→【**Neighbors**】navigation column, after the device switched LLDP (Link Layer Discovery Protocol) function, you can view the neighbor information on this page, including the port, the system name and other information. User can select<Auto-refresh>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.

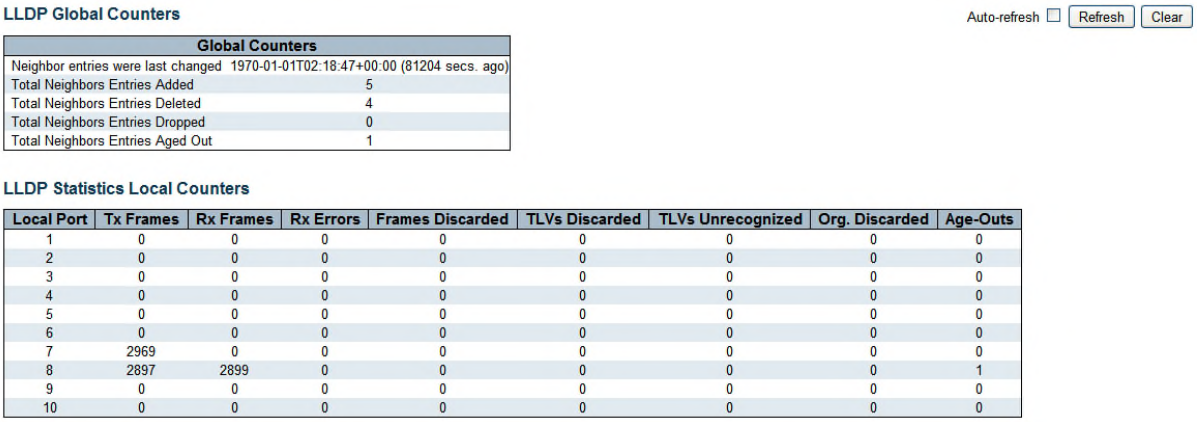


Interface items introduction

Interface items	Introduction
Local Port	Receiving the port number of LLDP frame
Chassis ID	Neighbor's LLDP frame included Chassis ID value
Port ID	Neighbor's LLDP frame included port No
Port Description	Neighbor transmitted the port description
System Name	Neighbor published system name
System Capabilities	Neighbor published system capabilities
Management Address	Neighbor IP address

B. LLDP Port status

Enter【**LLDP**】→【port status】navigation column, page show LLDP counter, User can select<Auto-refresh>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.



Global Counter：interface items instruction:

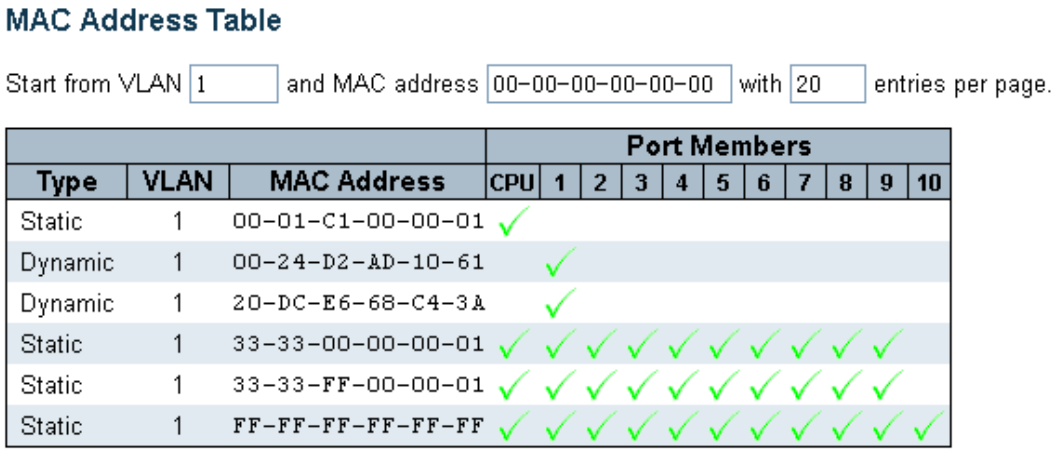
interface items	instruction
Neighbour entries were last changed	Receiving the port number of LLDP frame
Total Neighbours Entries Added	Neighbor's LLDP frame included Chassis ID value
Total Neighbours Entries Deleted	Neighbor's LLDP frame included port No
Total Neighbours Entries Dropped	Neighbor transmitted the port description
Total Neighbours Entries Aged Out	Neighbor published system name

Local counter：**Interface items instruction**：

Interface items	**instruction**
Local Port	Port of local received and transmitted frame
Tx Frames	The number of LLDP frames transmitted
Rx Frames	The number of LLDP frames received
Rx Errors	The number of wrong LLDP frames received
Frames Discarded	The number of after receiving the discard LLDP frames
TLVs Discarded	The number of discarded TLV information sheet
TLVs Unrecognized	The number of unrecognized TLV information
Org. Discarded	The number of Organized TLV information
Age-Outs	Valid time of LLDP

5.2.3.11 MAC Table

Enter【**MAC Table**】navigation column, On this page you can view all the Layer switch MAC address forwarding, port, MAC address, VLAN and other entries. User can select<Auto-refresh>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.



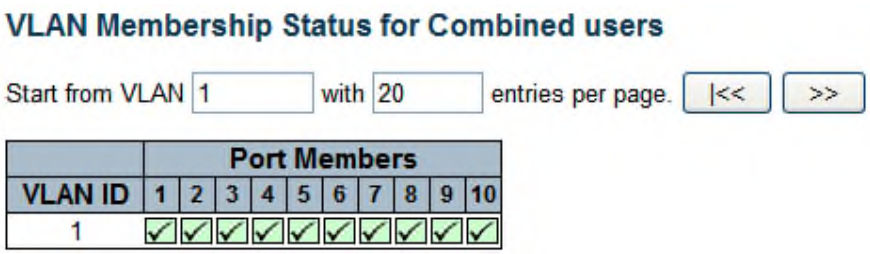
Interface items introduction:

Interface items	Introduction
Type	MAC address type of Related MAC items,Static;Dynamic
VLAN	VLAN ID of Related MAC items
MAC address	MAC address of Related MAC items
Port Members	Corresponding port of Related MAC items

5.2.3.12 VLANs status

A. VLAN membership

Enter【**VLANs**】→【**VLAN Membership**】navigation column, show VLAN membership information on page. User can select<Auto-refresh>button to refresh data in real time. Can also be manually Click <Refresh> button to see the new data.



Interface items introduction:

Interface items	Introduction
VLAN ID	VLAN ID of corresponding port
Port Members	VLAN ID including port

B. VLAN port

Enter【**VLANs**】→ 【**VLAN Port**】navigation column, page show VLAN port status, Dropdown navigation options Static, NAS, MSTP, Combined. User can select<Auto-refresh>button to refresh data in real time, Can also be manually Click <Refresh> button to see the new data.

VLAN Port Status for Combined users

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag PVID		No
2	C-Port	☑	All	1	Untag PVID		No
3	C-Port	☑	All	1	Untag PVID		No
4	C-Port	☑	All	1	Untag PVID		No
5	C-Port	☑	All	1	Untag PVID		No
6	C-Port	☑	All	1	Untag PVID		No
7	C-Port	☑	All	1	Untag PVID		No
8	C-Port	☑	All	1	Untag PVID		No
9	C-Port	☑	All	1	Untag PVID		No
10	C-Port	☑	All	1	Untag PVID		No

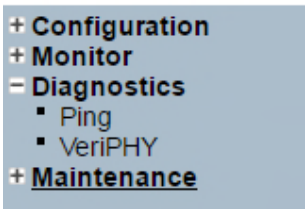
Interface items introduction:

Interface items	Introduction
Port	Switch port ID
Port Type	VLAN type indication port Unaware port as VLAN tag port which is not recognized C-Port port as user port S-Port port as service port S-Custom-Port as user/service port
Ingress Filtering	Indicates whether filter the ingress frame:

	Disabled: filtering Close Enabled: filtering function is enabled
Frame Type	port ingress the accepted frame type: ALL：port accepted all frame Tagged：port only accept frame with VLAN tag, Untagged: port only accept frame without VLAN tag
Tx Tag	transmit the status of filtering frame: tag/ remove tag
UVID	No label VLAN ID
Conflicts	It indicates whether there is a conflict VLAN

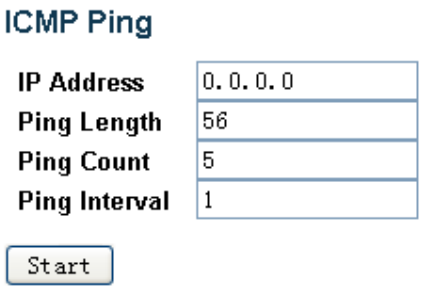
5.2.4 Diagnostics

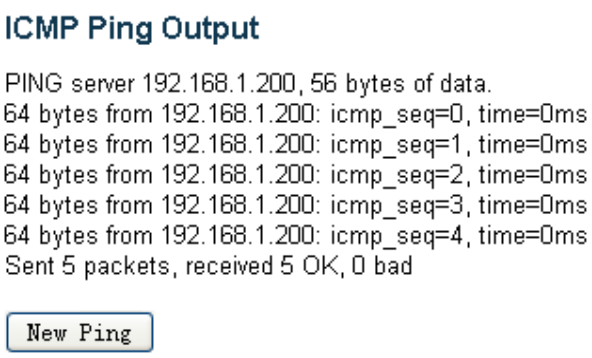
Diagnostics navigation column, including: ping and VeriPHY function.



5.2.4.1 Ping

Enter【**Ping**】navigation column, This can check the network connectivity, if the network is normal, ping detection will respond to ICMP echo packets. Enter the IP address, PING length, count, spacing parameters click <Start> button to start testing, you can display the information correctly.



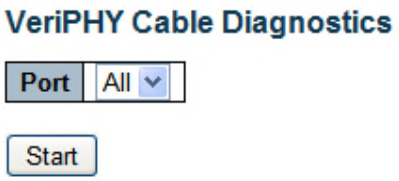


Interface items introduction:

Interface items	Introduction
IP Address	Set the tested destination IP address
Ping Length	Set Ping packet length, range: 2-1452, default is 56bytes
Ping Count	Set the count of send Ping packets, range: 1-60, default is 5
Ping Interval	Set Ping packet sending interval, range: 0-30, default is 1 second

5.2.4.2 VeriPHY Diagnostics

Enter【**VeriPHY diagnostics**】navigation column, It can detect electrical cable ,communication under normal will show Ok



Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--

.

Interface items introduction:

Interface items	**Description**
Port	Switch Ethernet port ID
Pair A（B、C、D）	Cable Differential pairs connected state OK：normal Open：Open circuit Short：Short circuit Short A（B、C、D）：short with A（B、C、D）cable Cross A（B、C、D）：Coupling with A（B、C、D）cable
Length A（B、C、D）	Cable length XXX m

5.2.5 Maintenance

5.2.5.1 Restart Device

Enter【**Restart Device**】Navigation Column, When restarted after set the system MAC address etc., it is recommended to restart the device to take effect.

5.2.5.2 Factory Defaults

Enter【**Factory Defaults**】Navigation Column, When need to revert to the original system defaults can choose to restore the factory configuration functions. The default configuration for all configuration and IP address will become equipment factory.

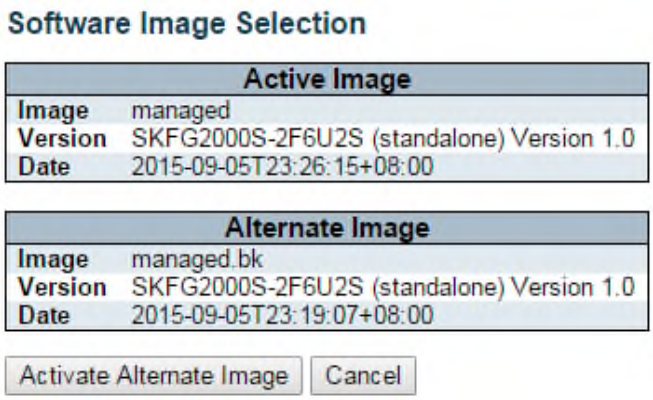
5.2.5.3 Software

A. Upload (firmware download)

Enter【**Software**】→【**Upload**】Navigation Column, Version Upgrade for upgrading switch version, after the upgrade need to restart the device.

B. Image Select

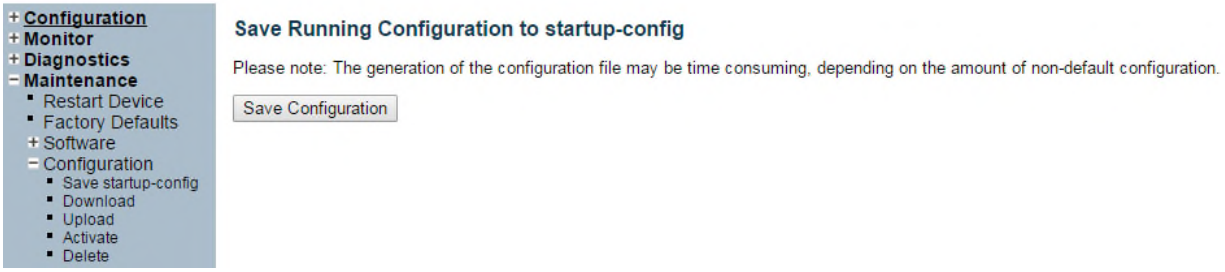
Enter【**Image Select**】can activate the backup image.



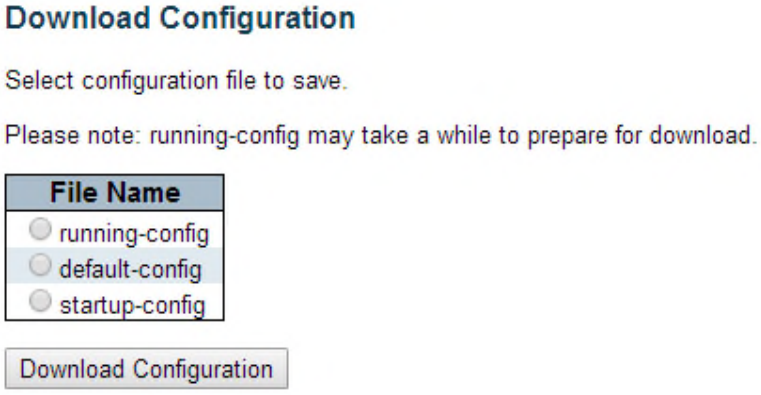
5.2.5.4 Configuration

Note: The device all changes need to be saved here, otherwise changes will not take effect.

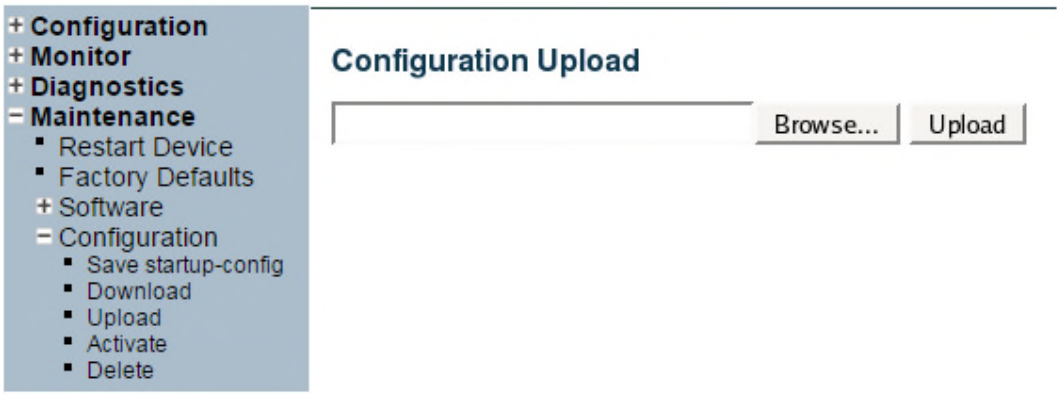
Enter【**Configuration**】→【**Save startup-config**】Navigation Column, Save the current configuration, if not save, restart device will not take effect on equipment configuration.



Enter【**Configuration**】→【**Download**】Navigation Column, can upload current equipment configuration.



Enter【**Configuration**】→【**Upload**】Navigation Column, can upload the previous configure file to switch by upload function to achieve configuration updates.



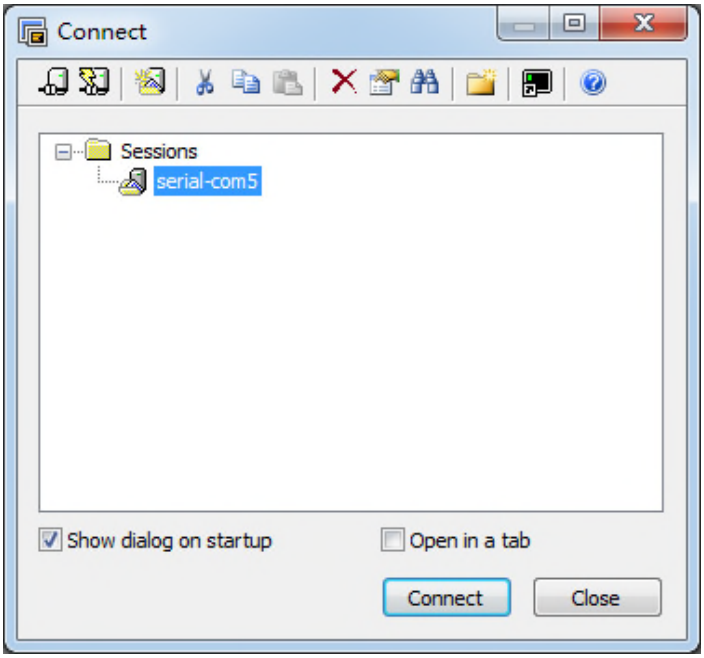
2 Command Line Management

Beside WEB management, Amber Series also support command line management

2.1 Configure HyperTerminal

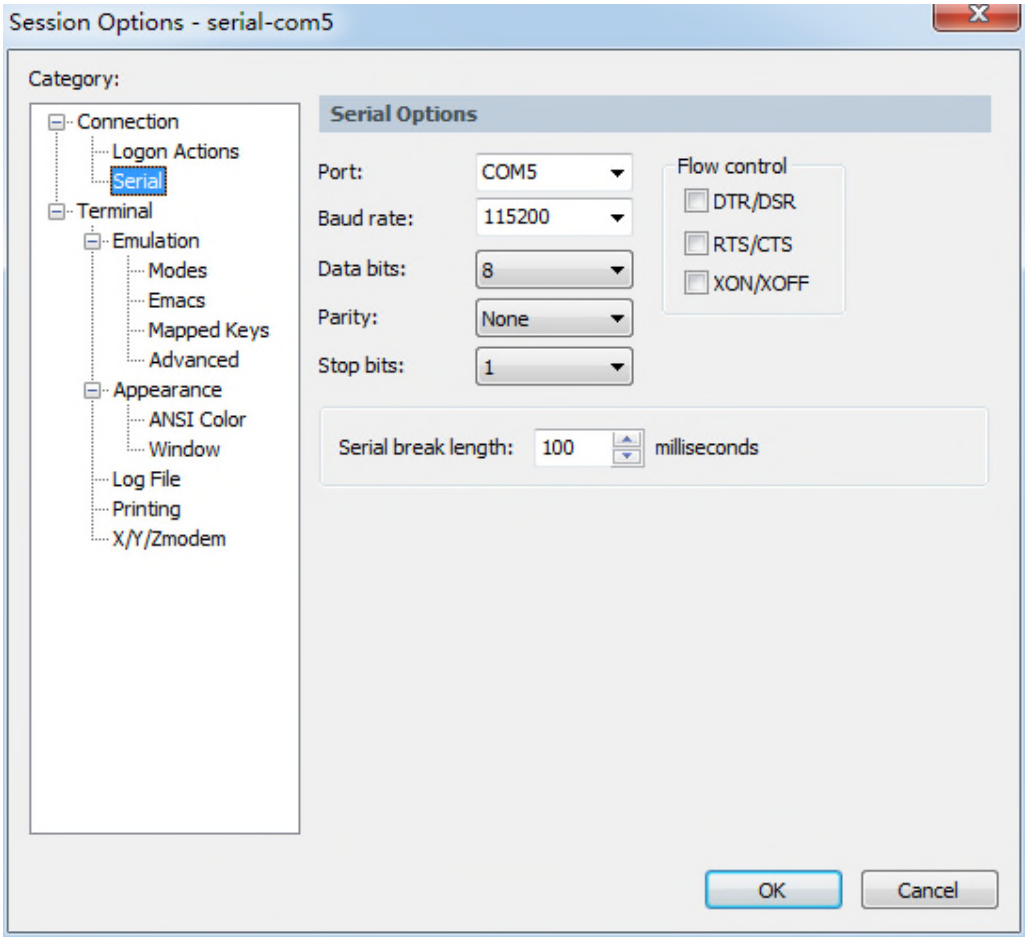
2.1.1 USB（115200-8-N-1）port connect with Device console port

1. There are many ways to access the serial management port of the Switch. For example, Hyper Terminal, SecureCRT, Putty and so on. SecureCRT software will be used in the description below.



2. Select the COM port to use and click "OK."

3. Set the appropriate serial port parameters as follows and then click "OK."



3. To power the switch, you will see the following prompt message in serial terminal interface:

```
Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Free Software Foundation, Inc.
RedBoot is free software, covered by the eCos license, derived from the
GNU General Public License. You are welcome to change it and/or distribute
copies of it under certain conditions. Under the license terms, RedBoot's
source code and full license terms must have been made available to you.
Redboot comes with ABSOLUTELY NO WARRANTY.

Platform: VCore-III (MIPS32 24KEc) LUTON26
RAM: 0x80000000-0x88000000 [0x80021c78-0x87fb0000 available]
FLASH: 0x40000000-0x40ffffff, 64 x 0x40000 blocks
== Executing boot script in 3.000 seconds - enter ^C to abort
RedBoot> fis load -d managed
Image loaded from 0x80040000-0x806e1068
RedBoot> go

Username:
```

2.2 Login equipment and basic command Query

Note: The command can be entered only the first four characters, the other can be used as usual omitted;

2.2.1 System Information Query

Command：Show version

```
Username: admin
Password:
# show version

MEMORY           : Total=90630 KBytes, Free=77429 KBytes, Max=77427 KBytes
FLASH            : 0x40000000-0x40ffffff, 64 x 0x40000 blocks
MAC Address      : 00-01-c1-15-01-02
Previous Restart : Cold

System Contact   :
System Name      :
System Location  :
System Time      : 1970-01-01T08:00:59+08:00
System Uptime    : 00:00:59
```

2.2.2 Recovery factory default

Command：reload defaults

```
# reload defaults
% Reloading defaults. Please stand by.
#
```

2.2.3 Logout

Enter "/" Return to the root directory of the command prompt; then enter "Logout", that is exit to the login screen

```
Active Image
------------
Image            : managed
Version          : SKFG2000S-2F6U2S (standalone) Version 1.0
Date             : 2015-09-05T23:26:15+08:00

Alternate Image
---------------
Image            : managed.bk
Version          : SKFG2000S-2F6U2S (standalone) Version 1.0
-- more --, next page: Space, continue: g, quit: ^C
```

2.2.4 Query / ModifyIP

Command-line prompt to enter a user name and password, enter the appropriate commands into the relevant settings and queries. (At the command prompt, type "?" or "help" to get help.)

The following equipment for the VLAN1 IP

```
Username: admin
Password:
# show interface vlan 1
VLAN1
  LINK: 00-01-c1-15-01-02 Mtu:1500 <BROADCAST MULTICAST>
  IPv4: 192.168.1.241/24 192.168.1.255
  IPv6: fe80::201:c1ff:fe15:102/64 <TENTATIVE>
```

Modify IP Address

NOTE: After modifying the IP to exit and save, otherwise the changes will not be effective;

```
# conf terminal
(config)# interface vlan 1
(config-if-vlan)# ip addr 192.168.1.247 255.255.255.0
(config-if-vlan)# exit
(config)# exit
# copy running-config startup-config
Building configuration...
% Saving 1965 bytes to flash:startup-config
#
```

2.2.5 Using own command help function

To sum up, configure other feature can be successfully logged the command prompt configure by the system prompts, enter the 'tab' key to display prompts information as below.

```
#
clear       configure   copy        debug       delete      dir         disable
do          dot1x       enable      erps        exit        firmware    help
ip          logout      more        no          ping        reload      send
show        terminal
#
```


```
#
clear       configure   copy        debug       delete      dir         disable
do          dot1x       enable      erps        exit        firmware    help
ip          logout      more        no          ping        reload      send
show        terminal
#
```

3 Technical Parameters

Technical	
Ethernet standard	802.3 - 10Base-T, 802.3u - 100Base-TX, 100Base-FX, 802.3z - 1000Base-LX/SX 802.3ab - 1000Base-TX, 802.3ad - Link Aggregation Control Protocol 802.3x - Flow Control 802.1D - Spanning Tree Protocol 802.1p - Class of Service, 802.1Q - VLAN Tagging 802.1w - Rapid Spanning Tree Protocol, 802.1X - Authentication 802.1ad - VLAN QinQ 802.1AB - LLDP 802.1s – MSTP
MAC address table	8192
Priority	8
flow control	IEEE 802.3x Flow Control and Back-pressure
Treatment	Store-and-Forward
Interface	
RJ45 Ports	10/100//1000 Base-T(X), Auto MDI/MDI-X
Fiber Ports	1000 Base-X 100 Base-FX
Power Supply	
Power input	PWR1: 45~57VDC PWR1: 45~57VDC
Power reverse protection	Present at terminal block
Power Consumption	10W (No POE)
POE/POE+	IEEE802.3af、802.3at
POE/POE+output power	Each POE port output range of 44-57V, 600mA， it can also be designed to provide 30W power to loads. V+ matched with data cable 1/2, and V- matched with data cable 3/6 gross power=POE ports*POE each power
Environment	
Operating temperature	-40 ~ 75ºC (-40~167ºF)

Storage temperature	-40 ~ 85°C (-40~185°F)
Operating humidity	5% to 95%, No condensation
Mechanical	
Dimensions (W x D x H)	62 mm(W) x 87 mm(D) x 100 mm(H)（DIN-rail）
Casing	IP40 protection