INDUSTRIAL G.SERIES

LAYER 3 ETHERNET

SWITCH MANUAL

Covering models

RM 3 - 24-TXP-8S-4X-G

RM 3 – 8TXP – 24S-4X-G

Rev 1.0 September 2022

This page left blank intentionally

General Notes

Appendices

Version	Date	Modification
V1.0	20.9.2022	First Release

Federal Communication Commission Interference Statement

For further certification information, please contact Case Communications.

Declaration of Conformity CE

This product has passed the CE test for environmental specifications when shielded cables are used for external wiring. We recommend the use of shielded cables. Shielded cables are available from Case Communications . Please contact your local supplier for ordering information.

This product has passed the CE test for environmental specifications. Test conditions for passing included the equipment being operated within an industrial enclosure.
In order to protect the product from being damaged by ESD (Electrostatic Discharge) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products. FCC Class A

This equipment has been tested and found to comply with the limits for a ‘Class A’ digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Safety Instructions

- Read these safety instructions carefully.
- Keep this user manual for later reference.
- Disconnect this equipment from any AC outlet before cleaning. Use damp cloth. Do not use liquid or spray detergents for cleaning.
- For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
- Keep this equipment away from humidity.
- Put this equipment on a reliable surface during installation. Dropping it or letting it fall may cause damage.
- The openings on the enclosure are for air convection. Protect the equipment from overheating. **DO NOT COVER THE OPENINGS.**
- Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
- Position the power cord so that people cannot step on it. Do not place anything over the power cord.

All warnings on the equipment should be noted.

- If the equipment is not to be used for a long time, disconnect it from the power source to avoid damage by transient over voltage.
- Never pour any liquid into an opening. This may cause fire or electrical shock.
- Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
- If one of the following situations arises, get the equipment checked by service personnel:
- The power cord or plug is damaged.
- Liquid has penetrated into the equipment.
- The equipment has been exposed to moisture.
- The equipment does not work well, or you cannot get it to work according to the user
- manual
- The equipment has been dropped and damaged.
- The equipment has obvious signs of breakage.

- Instructions for installation in a pollution Degree 2 environment or equivalent statement.
- PoE requirements:

This product was designed for in-door used and not to be used outside. The user manual shall have the description as below or equivalent:

“The equipment is to be connected only to PoE networks without routing to outside plant.”

- DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO BELOW -40°C(-40°F) OR ABOVE 75°C(167°F) THIS COULD DAMAGE THE EQUIPMENT. THE EQUIPMENT SHOULD BE IN A CONTROLLED ENVIRONMENT.

Conventions

⚠ Warning signs are used to identify immediate hazards for property damage, injury or death.

⚠ CAUTION SIGNS ARE USED TO WARN AGAINST POTENTIAL HAZARDS OR TO CAUTION AGAINST UNSAFE PRACTICES

✏ Note signs are used to provide additional information or settings

Product Warranty

Company Address: Case Communications. Unit12E Norths Estate, Piddington, High Wycombe, Bucks HP14 3BE, Great Britain.

Case Communications warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for two years from the date of purchase. This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Case Communications, or which have been subject to misuse, abuse, accident or improper installation. Case Communications assumes no liability under the terms of this warranty as a consequence of such events. Because of Case Communications 's high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If a Case Communications product is defective, it will be repaired or replaced at no charge during the warranty period. For out of-warranty repairs, you will be billed according to the cost of replacement materials, service time and freight. Please consult your dealer for more details. If you think you have a defective product, follow these steps:

1. Collect all the information about the problem encountered. (For example, CPU speed, Case Communications products used, other hardware and software used, etc.) Note anything abnormal and list any on screen messages you get when the problem occurs.

2. Call your local dealer and describe the problem. Please have your manual, product, and any helpful information readily available.

3. If your product is diagnosed as defective, obtain an RMA (return merchandize authorization) number from your dealer. This allows us to process your return more quickly.

4. Carefully pack the defective product, a fully-completed Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.

5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Copyright

Technical Support and Assistance

1. Visit the Case Communications web site at www.casecomms.com where you can find the latest information about the product.

2. Contract your distributor, sales representative, or Case Communications 's customer service centre for technical support if you need additional assistance. Please have the following information ready before you call:

- Product name and serial number of your peripheral attachment.
- Description of your software (operating system, version, application software, etc.)
- A complete description of the problem
- The exact wording of any error messages
- Warning signs are used to identify immediate hazards for property damage, injury or death.

CAUTION SIGNS ARE USED WARN AGAINST POTENTIAL HAZARDS OR TO CAUTION AGAINST UNSAFE PRACTICES.

This page left blank intentionally

1. Product Introduction

1.1. Product Introduction

The Case Communications RM3 XX Series are a family of high-end industrial core Layer 3 (L3) switch's.

- The RM3-24TxP-8S-4X-G provides 24x10/100/1000-TxP PoE ports, 8x 10/100/1000 TxP PoE ports and 4x10Gbps SFP Ports.
- The RM3 -8TxP-24S-4X-G provides 8x10/100/1000 TxP PoE Ports and 24x100 /1000 SFP Ports and 4x10Gbps SFP Ports

The switch series supports SNMP v1/v2 v3 (Simple Network Management Protocol), CLI command line, Web net tube, and TELNET for Management. An ACL (Access Control List) makes the management more secure

The series complies with FCC and CE standards. Using a mute fan, the switches can work in environments from - 40 ℃ to 75 ℃.

1.2. RM3 Features

- IEEE802.3, IEEE802.3u, IEEE802.3ab, IEEE802.3z, IEEE802.3ae
- The switch supports G.8032 (ERPS) redundancy technology. Self-healing time for a looped network is less than 50 ms
- Support PoE management, POE load timing restart and on-off.
- Support IGMP Snooping, Static multicast filtering, MLD Snooping filtering
- Support DHCP Snooping, protect from ARP attack, attack of illegal DHCP server access
- Support NTP, easy for real-time synchronization of network time
- Support SNMP v1/v2/v3
- Support LLDP
- Support ACL, enhance the flexibility and safety of network management
- Support QoS, enhance the stability of network
- Support port mirror, convenient for online debug
- Support cable testing, convenient for the examining cable length in a project
- Support STP/RSTP/MSTP, enhance the stability of network
- Support IEEE802.1Q VLAN, IEEE802.1ad QINQ
- Support 802.1x authentication to port and MAC
- Support static routing L3 switching technology
- Operation temperature range: -40℃ ~ +75℃
- Storage temperature range: -40C~+85C

1.3. Overview

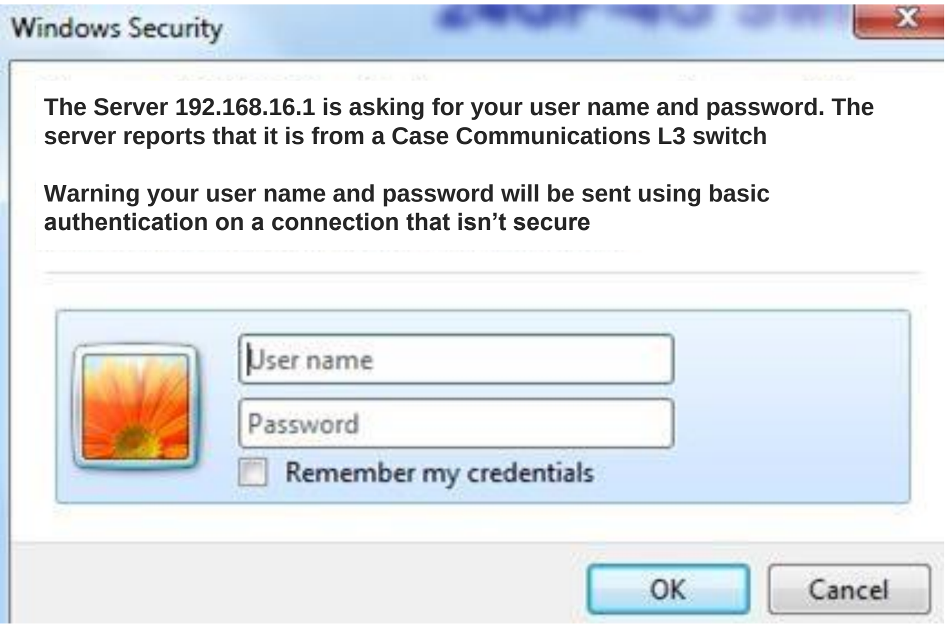
Thank you for purchasing your Case Communications L3 managed switch.

These switches can be managed, configured and monitored via an embedded Web-based (HTML) interface, using a standard browser, allowing you to manage the switch at any remote site in the network.

1.4. Web Management Login

Open a web browser on your PC, input the switch’s IP address in this manner, http://xxx.xxx.xxx.xxx, then open that URL to login to the web management.

Note: The IP address of switch is 192.168.16.1 by default. So please input http://192.168.16.1 in the browser.
When the login window appears, please enter the default username
“root” and default password **“case”** Then click OK to login. On some version of software the user name maybe ‘admin’ and password ‘system’

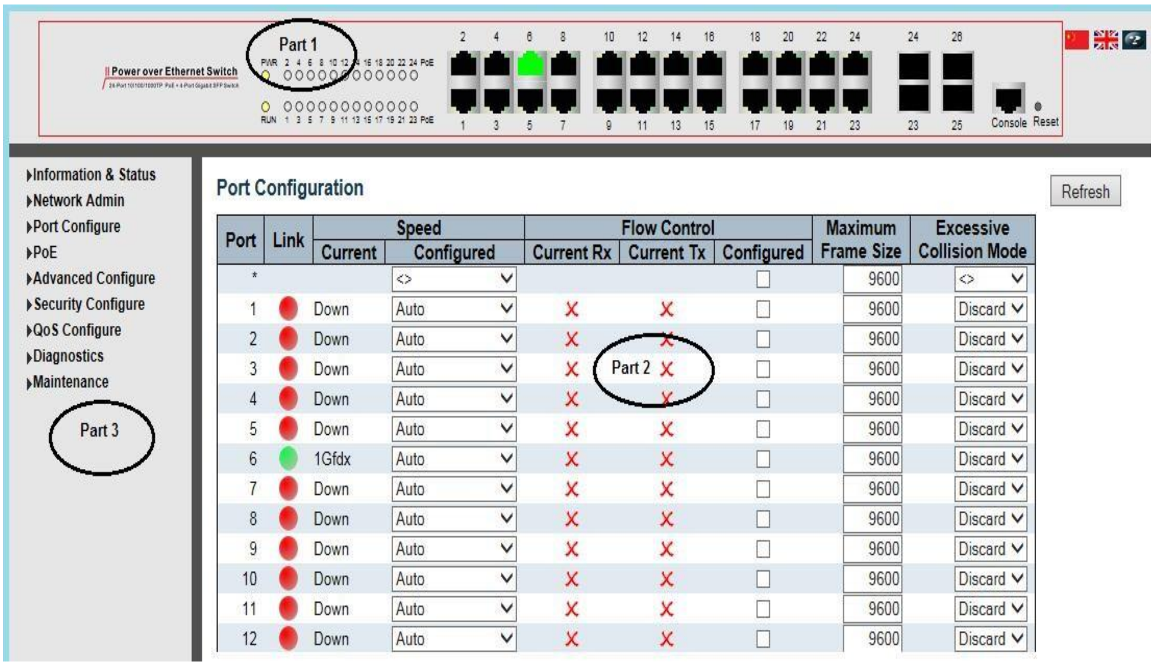


The Server 192.168.16.1 is asking for your user name and password. The server reports that it is from a Case Communications L3 switch

Warning your user name and password will be sent using basic authentication on a connection that isn’t secure

1.5. Web-based User Interface

After entering the username and password, the main screen appears as shown in Figure1-2 below



Port Configuration

Port	Link	Speed		Flow Control			Maximum	Excessive
		Current	Configured	Current Rx	Current Tx	Configured	Frame Size	Collision Mode
*			<>			□	9600	<>
1	🔴	Down	Auto	✗	✗	□	9600	Discard
2	🔴	Down	Auto	✗	✗	□	9600	Discard
3	🔴	Down	Auto	✗	✗	□	9600	Discard
4	🔴	Down	Auto	✗	✗	□	9600	Discard
5	🔴	Down	Auto	✗	✗	□	9600	Discard
6	🟢	1Gfdx	Auto	✗	✗	□	9600	Discard
7	🔴	Down	Auto	✗	✗	□	9600	Discard
8	🔴	Down	Auto	✗	✗	□	9600	Discard
9	🔴	Down	Auto	✗	✗	□	9600	Discard
10	🔴	Down	Auto	✗	✗	□	9600	Discard
11	🔴	Down	Auto	✗	✗	□	9600	Discard
12	🔴	Down	Auto	✗	✗	□	9600	Discard

This top level page includes main 3 parts. These are described below

Part	Description
Part 1	Panel display; Port indicators, including PoE and Link working status; Language selection button; Help document
Part 2	The Main Menu, lets you access all the commands and statistics
Part 3	Main Screen, showing ghe sub menus

The Web agent displays an image of the Managed Switch's ports. Different colors mean different states, they are illustrated as follows:

🟨 100Mbps Link	🟩 1000Mbps Link	⬛ No Link

1.6. Main Menu

Using the onboard Web interface, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. Using the web-management, the administrator can set up the switch by selecting the functions listed in the Main Menu. The following is brief description of the functions available:

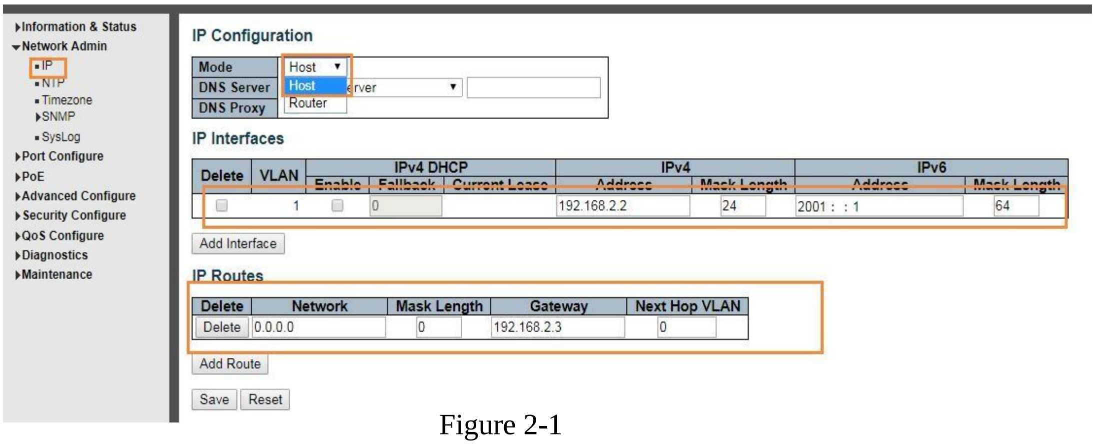
- **Information & Status** - Users can check switch information and working status under this menu.
- **Network Admin** - Users can check and configure network admin parameters under this menu.
- **Port Configure** - Users can check and configure ports specification using this menu.
- **PoE** - Users can check and configure Power-over-Ethernet (PoE) unsing this menu.
- **Advanced Configure** - Users can check and configure L2 advanced features under thismenu. **Security Configure** - Users can check and configure security features using this menu.
- **QoS Configure** - Users can check and configure the QoS features of the switch under this menu.

2. Network Management

2.1. IP Configuration

Note: Default IP address of switch is 192.168.16.1 by default, and the default sub netmask is 255.255.255.0(24)

Select "Network Admin">"IP", and the screen will shows as:



IP Configuration

Mode	Host ▾ (Host / Router)
DNS Server	…erver ▾
DNS Proxy	

IP Interfaces

Delete	VLAN	IPv4 DHCP			IPv4		IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Address	Mask Length
□	1	□	0		192.168.2.2	24	2001 : : 1	64

Add Interface

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
Delete	0.0.0.0	0	192.168.2.3	0

Add Route

Save Reset

Figure 2-1

The following is a description of the IP configuration:

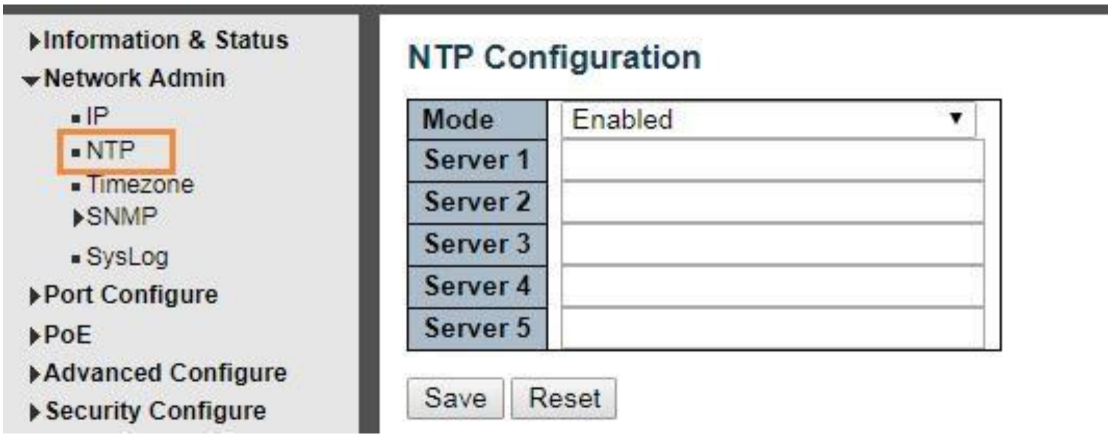
Port Name	Display system’s port name
VLAN	VLAN for access and management of switch
IPv4 DHCP	If enabled, it means that VLAN port will start the IPv4 DHCP client, to dynamically get IPv4 addresses from the switch. Otherwise, it will use switch’s static IP configuration. **Fallback (Seconds):** means the waiting time for switch to get dynamic IP address via DHCP. The value of "0" here means never over the time. Current Lease, means the IP address get from DHCP
IPv4	**Address**: static IPv4 address entered by user. **Mask Length:** static IPv4subnetmask entered by user
IPv6	**IP Address:** Users can input the static IPv6 address **IP Mask:** Users can input the static IPv6 subnet mask
IP Routes	**Destination:** Users can input the IPv4 address of destination **IP Mask:** Users can static IPv4 subnet mask **Next address:** Users can input next IPv4 address

Click "Add Interface" to create a new management for VLAN and IP address. Click "Save' 'to save settings.

Note: The switch creates VLAN1 by default. If the user needs to use other VLAN’s for switch management, please first add the VLAN in the VLAN module, and add the relevant port to the VLAN.

2.2. NTP Configuration

NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. You can specify NTP Servers and set GMT Time zone. The NTP Configuration screens will appear after you click "Network Admin">"NTP".



NTP Configuration

Mode	Enabled
Server 1	
Server 2	
Server 3	
Server 4	
Server 5	

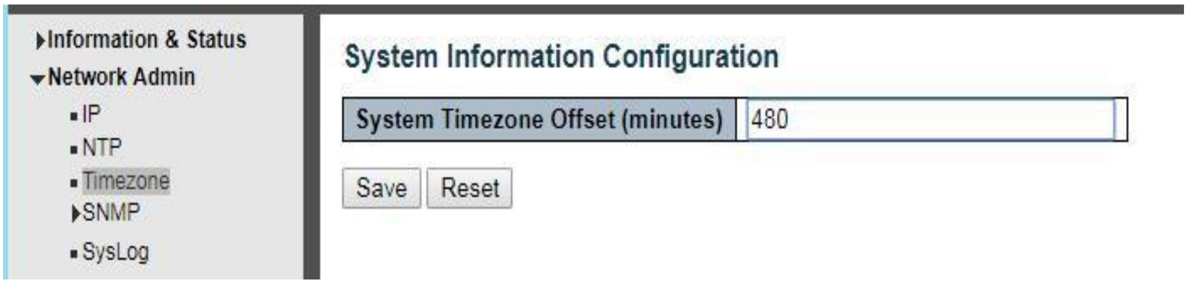
Figure 2-2 NTP Setting Screen

Mode	Click drop-down menu to select "Enabled" or "Disabled"NTP. **Enabled**: Enable NTP mode operation. When enabling NTP mode operation, the agent forwards and transfers NTP messages between the clients and the server when they are not on the same subnet domain. **Disabled**: Disable NTP mode operation.
NTP Sever	After inputting the NTP server IP address, the switch will obtain NTP information from that server.

After configuration has been set, please click "Save" to save the setting.

2.3. Timezone

Timezone allows you to set the time of the switch, users can set the time according to their locations. You can access the timezone through “Network admin” > “Timezone”, as shown in figure 2-3 below



System Information Configuration

System Timezone Offset (minutes): 480

Figure 2-3 NTP Setting

Item	Action
Time Zone Setting	Input the time

Click ‘Save’ to save your changes

2.4. SNMP Configuration

Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol / Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.
This Case Communications Layer 3 switch support SNMPv1, v2c,v3. Different versions of SNMP provide different security level for management stations and network devices.

SNMP’s v1 and v2c, use the "Community String" for user authentication. That string is similar to a password function. SNMP application in the remote users and SNMP in the Switch must use the same community string. SNMP packets from any unauthorised sites will be ignored (discarded).

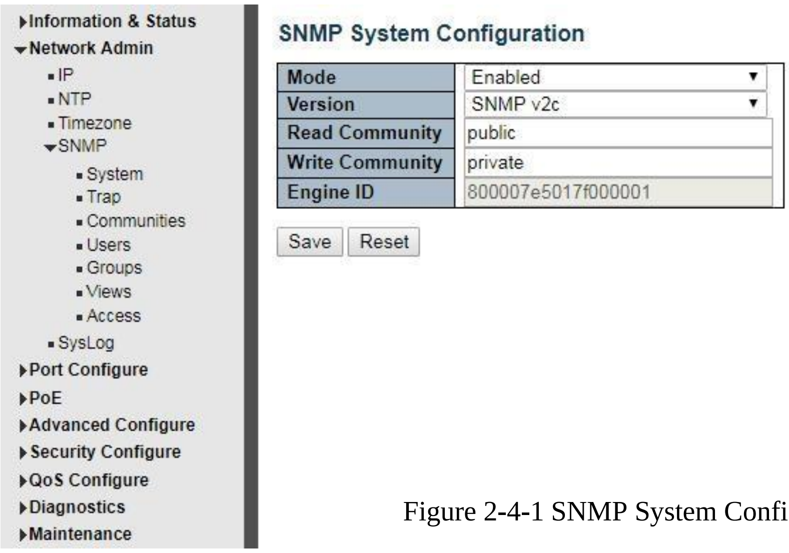
1. **Public** - allow authentication management station to read MIB objects.
2. **Private** - – allow authentication management station to read, write and edit MIB objects.

Trap – A trap is used by the agent (ie device on the network) to asynchronously inform the NMS of some event. These events may be very serious, such as reboot (someone accidentally turned off switch), or just general information, such as port status change. In these cases, the switch creates trap information and sends them to a NMS or PC on the network. Typical trap includes authentication failure, networking changes and cold/hot start trap.

MIB - A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules. The Case Communications switch uses standard MIB-II information management module. So, MIB object value can be read by any SNMP web-managed software.

2.4.1. SNMP System Configuration

You can enable or disable the SNMP System Configuration. Its screen will appear after you select "Network Admin">"SNMP">"System"



SNMP System Configuration

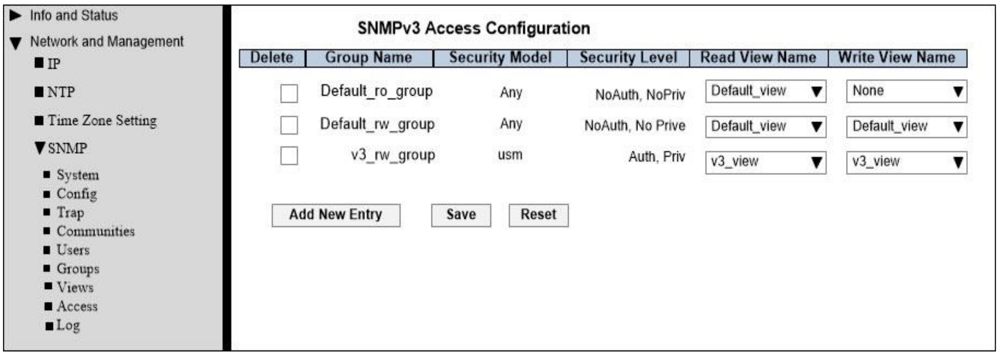
Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

Figure 2-4-1 SNMP System Configuration

Object	Description
Mode	Enabled or Disable SNMP function
Version	Click drop-down menu to select SNMP v2c or SNMP v1 version
Read Community	Public: allow authentication management station to read MIB objects
Write Community	Private: allow authentication management station to read and write MIB objects.

2.4.2. SNMP Trap Configuration

Users can enable or disable the SNMP Trap function and configure SNMP Access, select "Network Admin">"SNMP">"Trap" , then the screen as shown in figure 2-4-2 below will appear.



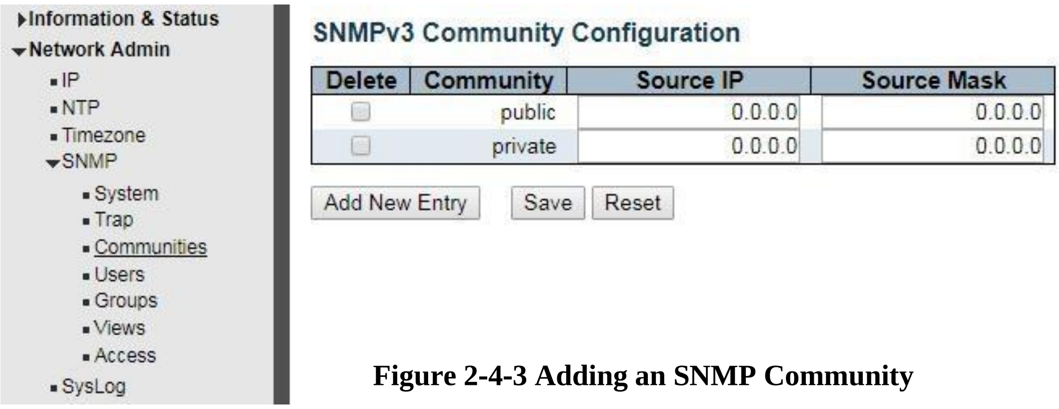
SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	Default_ro_group	Any	NoAuth, NoPriv	Default_view ▼	None ▼
□	Default_rw_group	Any	NoAuth, No Prive	Default_view ▼	Default_view ▼
□	v3_rw_group	usm	Auth, Priv	v3_view ▼	v3_view ▼

Figure 2-4-2

2.4.3. Communities

Users can set the new community name through “Network admin” > “SNMP” > “Communities”, as shown below in figure 2-4-3



SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
□	public	0.0.0.0	0.0.0.0
□	private	0.0.0.0	0.0.0.0

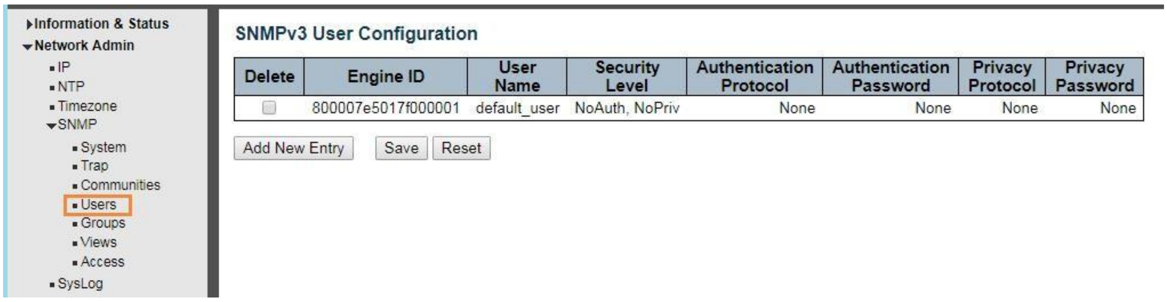
Figure 2-4-3 Adding an SNMP Community

Item	Description
Community	Input the name of the new community
Source IP	Input IPv4 source address
Source Mask	Input IPv4 subnet mask

Click “Save” to enable your changes

2.4.4. Users

SNMP v3 is a USM (User-Based Security Model) authentication mechanism. The administrator can set authentication and Encryption functions. The authentication is used to verify the validity of a message sender and to avoid illegal user access. Encryption is used to provide secure communications between the NMS and Agents. Using these two functions, it provides greater security for communication between an NMS and Agent.
Users can set an SNMP v3 account and Encry Mode. Click “Network Admin” > “SNMP” > “Users”, as below :



SNMPv3 User Configuration

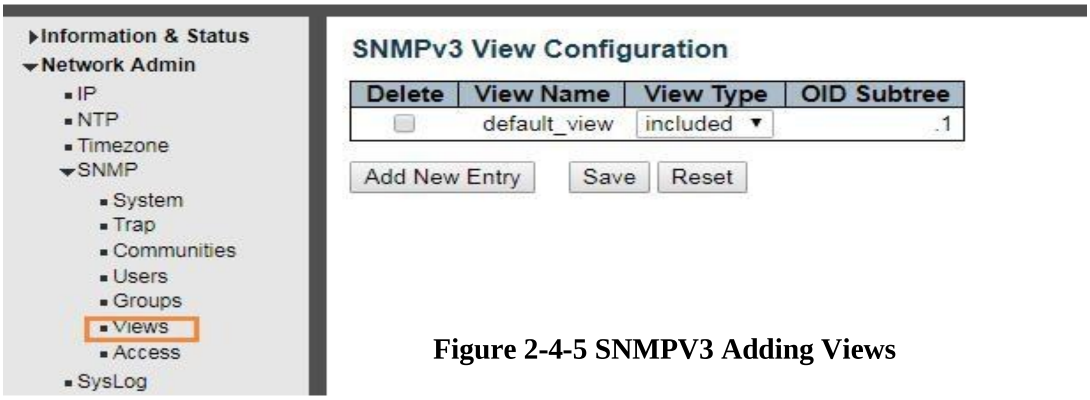
Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
□	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

Object	Instruction
Engine ID	Default Value 800007e5017f000001. The switch default value is recommended
User Name	Input the new account name of SNMPv3
Security Level	Three EncryModes, NoAuth, NoPriv, Auth, NoPriv, Auth, Priv, choosing by the drop down menu
Authentication Protocol	Select MD5 or SHA
Authentication Password	Input the encrypted password
Privacy Protocol	Select the encryption you want to use DES or AES
Privacy Password	Input the encrypted password

Click “Save” to enable your settings.

2.4.5. Adding Views

Users can set the SNMPv3 View. Select “Network Admin” > “SNMP” > “View”. As below:



SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
□	default_view	included ▾	.1

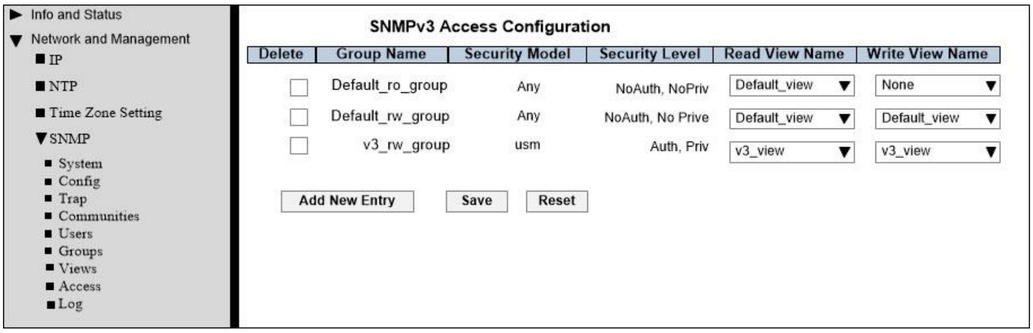
Figure 2-4-5 SNMPV3 Adding Views

Object	Instruction
Views Name	Input the name of Views
Views Type	Choose for included and excluded
OID Subtree	Input OID subtree, such as 1.2

Click "Saving" to enable your settings.

2.4.6. SNMP Access Configuration- SNMP Access Configuration

Uses can set an Access to load a built Views. Click "Network Admin" > "SNMP" > "Access", as below:



SNMPv3 Access Configuration

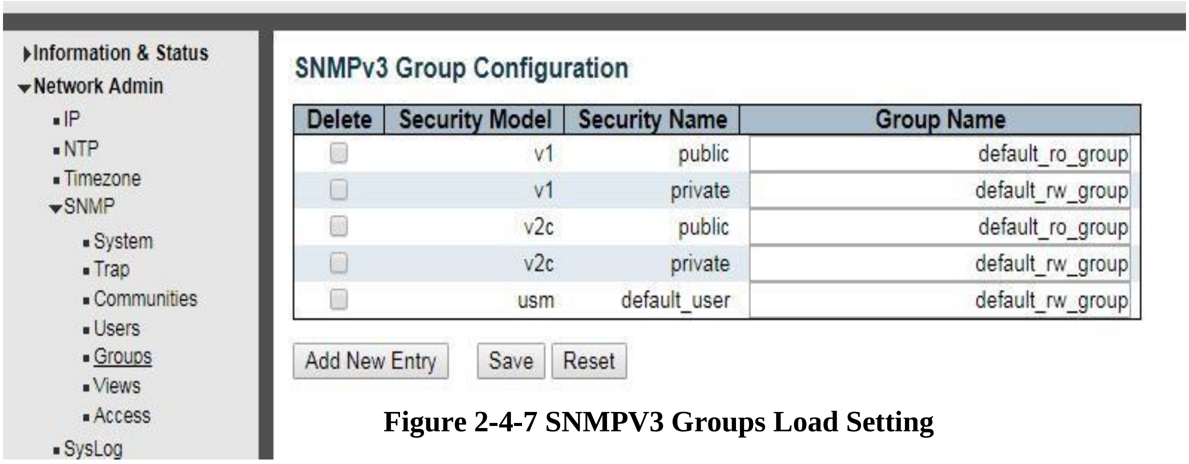
Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	Default_ro_group	Any	NoAuth, NoPriv	Default_view ▼	None ▼
□	Default_rw_group	Any	NoAuth, No Prive	Default_view ▼	Default_view ▼
□	v3_rw_group	usm	Auth, Priv	v3_view ▼	v3_view ▼

Object	Instruction
Group Name	Input the name of group
Security Model	Choose from v1 v2c usm
Security Level	Three EncryModes, NoAuth, NoPriv, Auth, NoPriv, Auth, Priv, choosing by using the drop down the menu
Read View Name	Chose the built views
Write View Name	Chose the built views

Click "Save" to enable your settings.

2.4.7. SNMP v3 Group Configuration

Users can set Groups to load built Users and Access. Click "Network Admin" > "SNMP" > "Groups", as shown below



SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group
□	usm	default_user	default_rw_group

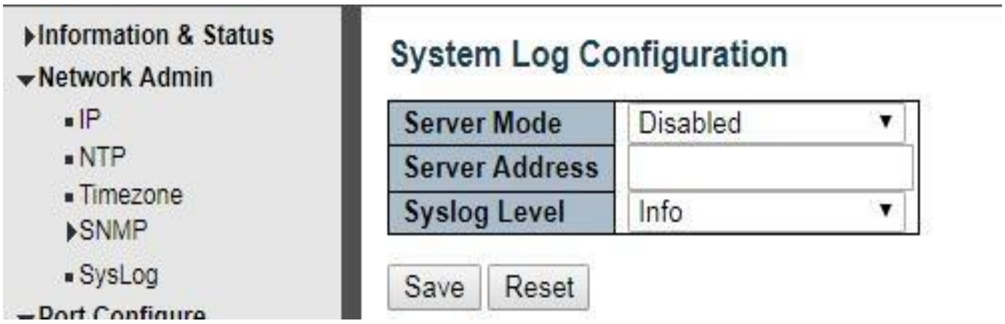
Figure 2-4-7 SNMPV3 Groups Load Setting

Object	Instruction
Security Model	Select v1 v2c usm
Security Name	Choose the built account name. For the team built under v1 v2c, or built account name under usm
Group Name	Input built group name

Click "Save" to enable settings.

2.5 System Log Configuration

User can configure switch's system log, via the following screen after click "Network Admin">"Syslog"



System Log Configuration

Server Mode	Disabled ▼
Server Address	
Syslog Level	Info ▼

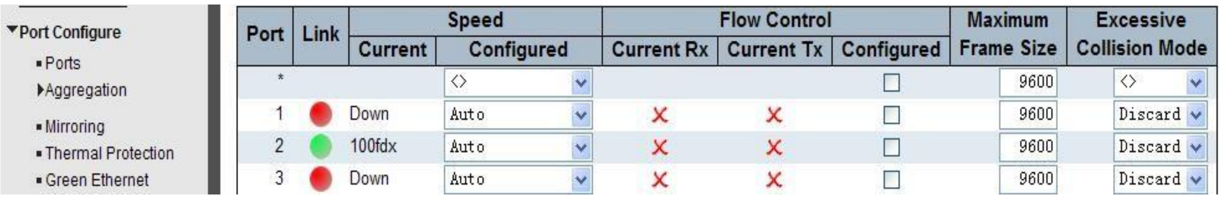
Figure 2-5 - System Log Configuration Screen Configuration object and description is:

Object	Description
Server Mode	Enabled or Disable SNMP System Log function. If "Enable" is selected, the switch will send System Log Information to defined Sys Log server.
Server Address	Defined server IP address
Syslog Level	To define level of System Log, including: **Info**: Information, warnings and errors. **Warning**: warnings and errors. **Error**: errors.

3. Port Configuration

3.1. Port Configuration

This page is for configuring port specifications of the switch. After selecting "Port Configure">"Ports", the following screen will appear:



▾Port Configure
- ▪Ports
- ▸Aggregation
- ▪Mirroring
- ▪Thermal Protection
- ▪Green Ethernet

Port	Link	Speed		Flow Control			Maximum	Excessive
		Current	Configured	Current Rx	Current Tx	Configured	Frame Size	Collision Mode
*			<>			□	9600	<>
1	🔴	Down	Auto	✗	✗	□	9600	Discard
2	🟢	100fdx	Auto	✗	✗	□	9600	Discard
3	🔴	Down	Auto	✗	✗	□	9600	Discard

Figure 3-1 Port Configuration Screen

Object	Description
Link	Red indicates the Link is Down, Green means the Link is Up
Speed	Select the port speed and full / half duplex mode. **"Disabled"** means that port is disabled. **"Auto"meaning** in full-duplex (FDX) or half-duplex mode (HDX) (1000mbps always in full-duplex mode) auto negotiate among 10,100,1000Mbps devices. **"Auto" setting allows** the port to automatically determine the fastest settings for the device connected, and to apply these settings. "**1000-X_AMS**" means that port is Ethernet/Optical combo port, and optical port is prioritized. Other options are10M HDX, 10M FDX, 100M HDX, 100M FDX, 1000M FDX, 1000-X.
Flow Control	802.3x is a flow control mechanism for a variety of port configurations. Full-duplex ports use 802.3x flow control, half-duplex ports use back pressure flow control. It is disabled by default. Check to enable flow control.
Maximum Frame Size	It is used to set the maximum frame size for Ethernet. The default setting is 9600, which supports Jumbo frames.

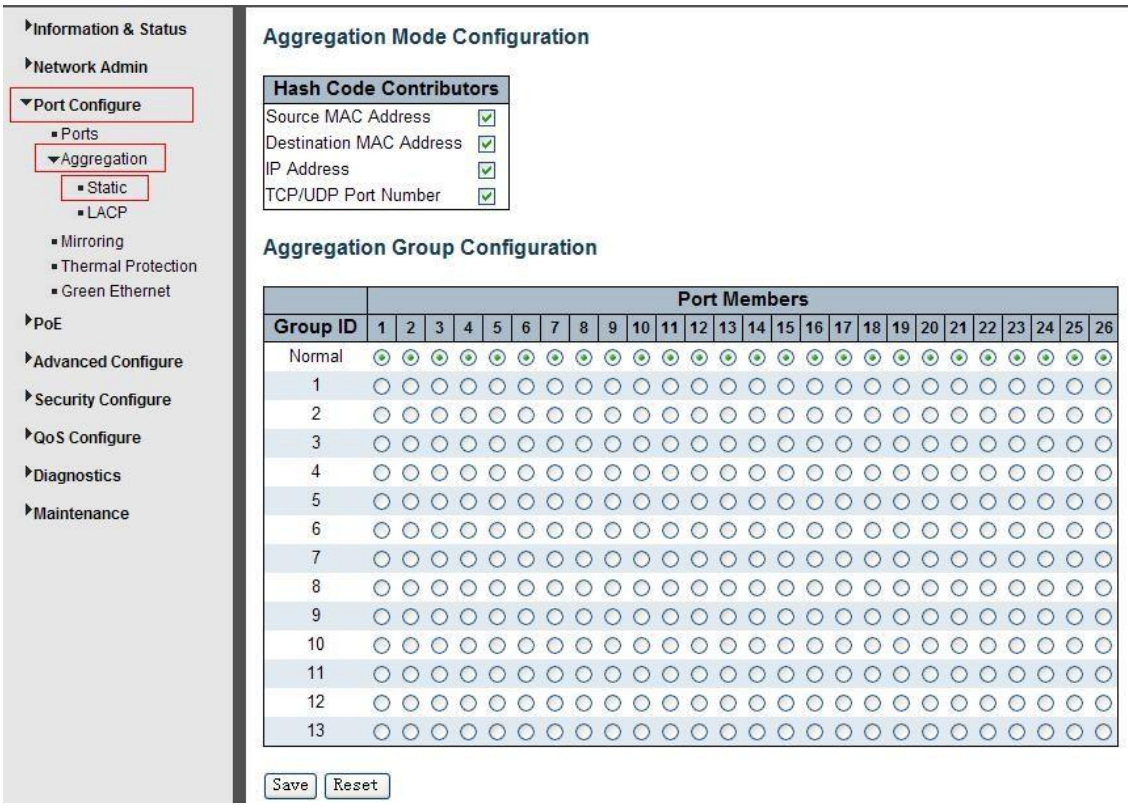
Click "Save" to store and active settings.

3.2. Link Aggregation

Users can set up multiple links between multiple switches. Link Aggregation, is a method that ties some physical ports together as one logic port, to enlarge bandwidth. Your Case Layer 3 switch supports up to 13 groups Link Aggregation, joining ports 2 to 8 as one group. **Note:** If any port in the link aggregation group is disconnected, data packets that were sent to the disconnected port will share the load with other connected ports in the aggregation group.

3.2.1. Static Aggregation

In this page, users can configure the static aggregation of the switch's ports. After selecting the menu "Port Configure">"Aggregation">"Static", the following window will appear allowing the network manager to make static aggregation settings.



Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	☑
Destination MAC Address	☑
IP Address	☑
TCP/UDP Port Number	☑

Aggregation Group Configuration

	Port Members																									
Group ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Normal	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
5	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
7	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
9	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
10	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
11	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
12	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
13	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Figure 3-2-1 Port Static Aggregation Configuration Screen

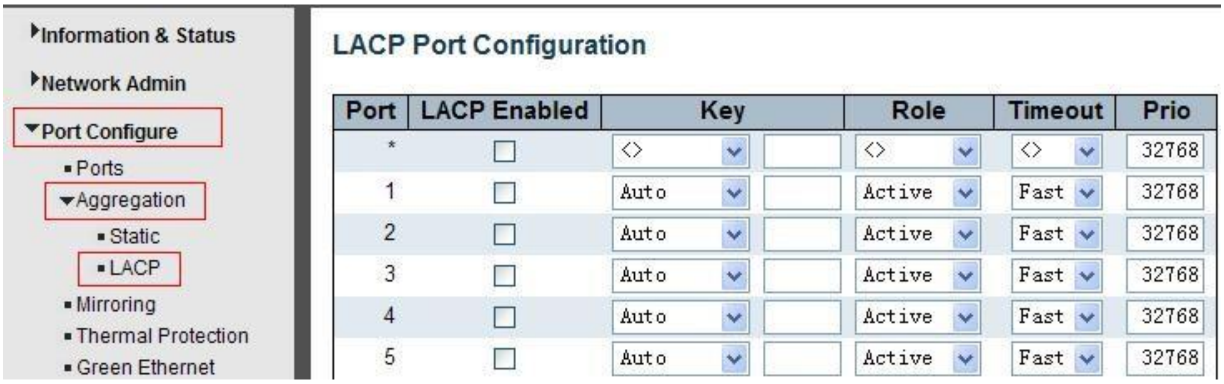
Object	Description
Aggregation Mode Configuration	This parameter is flow hash algorithm among LAG(Link Aggregated Group) ports.
Group ID	Static aggregation group ID
Port Members	This switch supports up to 13 groups Link Aggregation, 2 to 8 port as one group.

Click "Save" to store and active settings.

Note: It allows a maximum of 8 ports to be aggregated as 1 static trunk group at the same time.

3.2.2. LACP Aggregation

Link Aggregation Control Protocol (LACP) provides a standard means for exchanging information between Partner Systems that require high-speed redundant links. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode. For more detailed information, refer to the IEEE 802.3ad standard. Users can create a dynamic aggregation group for switches. After clicking on "Port Configure">"Aggregation">"LACP", users can set LACP configuration as shown in the screen below.



LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	32768
1	☐	Auto		Active	Fast	32768
2	☐	Auto		Active	Fast	32768
3	☐	Auto		Active	Fast	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768

Figure 3-2-2 LACP Configuration Screen Configuration

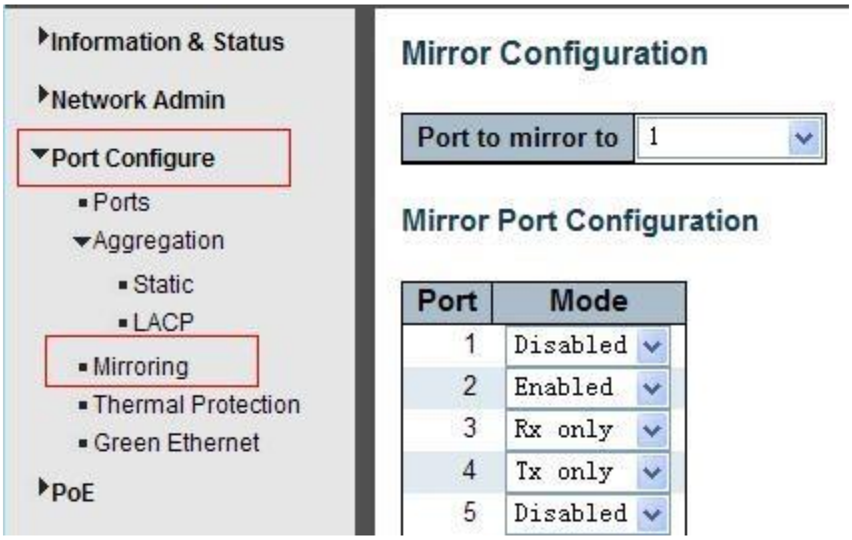
Object	Description
LACP	Enable or disable LACP function of that port.
Key	The Key value incurred by the port, range 1-65535 . **Auto** setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the **Specific** setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
Role	**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).
Timeout	**Timeout** controls the period between BPDU transmissions. **Fast** will transmit LACP packets each second, while **Slow** will wait for 30 seconds before sending an LACP Packet
Prio	**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.

Click "Save" to store and active settings.

3.2.3. Port Mirroring

This function provides monitoring of network traffic allowing the switch to forward a copy of each incoming or outgoing packet from one port of a network switch to another port where the packet can be studied. It enables the manager to keep close track of switch performance and alter it if necessary.

To configure Mirror settings, please click "Port Configure">"Mirroring" . Then the following screen will appear as shown here:



Mirror Configuration

Port to mirror to	1

Mirror Port Configuration

Port	Mode
1	Disabled
2	Enabled
3	Rx only
4	Tx only
5	Disabled

Figure 3-3 Mirror Configuration Screen Configuration

Object	Description
Port Mirror To	Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. **Disabled** disables mirroring.
Mode	Select source port mirror mode. **Rx only** Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored. **Tx only** Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored. **Disabled** Neither frames transmitted nor frames received are mirrored. **Enabled** Frames received and frames transmitted are mirrored on the mirror port. Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror port Tx frames. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

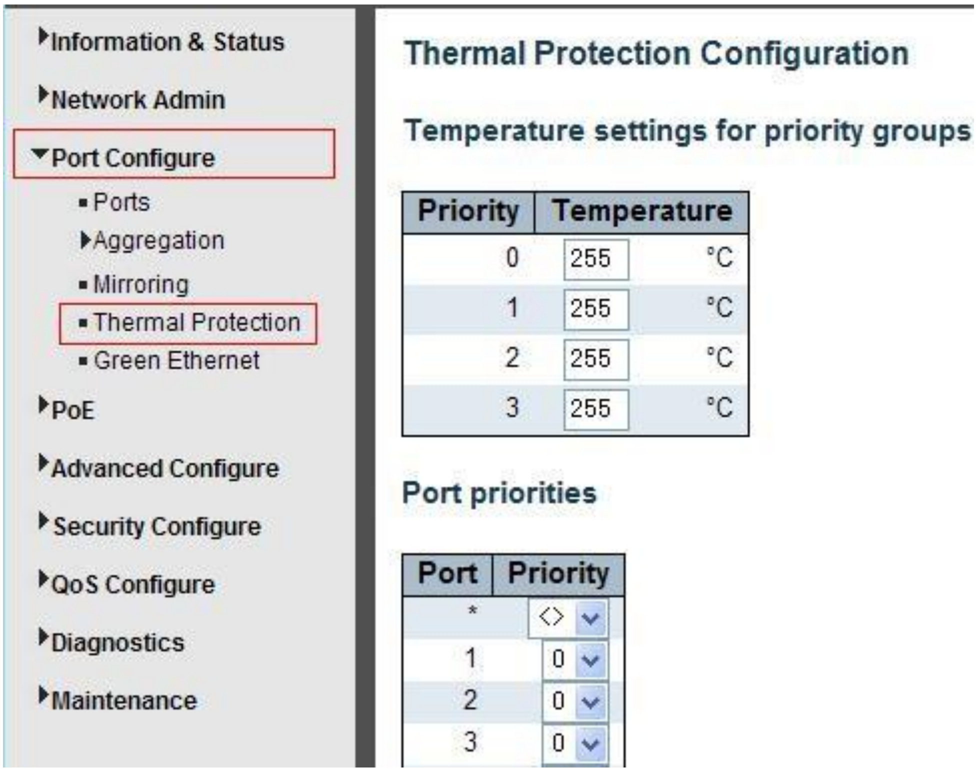
Click Save to store active settings

Note: You cannot set a higher speed port(s)to be mirrored by a lower speed port. For example, if you try to mirror 100Mbps port(s) to a 10 Mbps port. The destination port should be equal or a higher speed compared to the source port.

3.2.4. Thermal Protection Configuration

Thermal protection is for detecting and protecting the switch. When the switch detects that the port temperature is higher than the defined temperature, the system will disable the port, to protect the switch

After selecting "Port Configure">"Thermal Protection", the following screen will appear as shown below:



Thermal Protection Configuration

Temperature settings for priority groups

Priority	Temperature	
0	255	°C
1	255	°C
2	255	°C
3	255	°C

Port priorities

Port	Priority
*	<>
1	0
2	0
3	0

Figure 3-2-4 Thermal Protection Configuration Screen

Object	Description
Temperature settings for priority groups	This switch supports 4 Thermal Protection priority groups, and each of them can have a defined temperature for protection.
Port priorities	Define which priority group that the port belongs to.

Note: By default, all ports on the switch belong to Priority Group 0, with a protected temperature 225 degree C.

4. PoE Configuration

Power-over-Ethernet (PoE), means the Ethernet switch supplies power via its 100BASE-TX, 1000BASE-T interfaces The maximum power distance is 90 meters. PoE power system, based on Ethernet wiring using UTP Cat5 or higher Cable, and can provide power to IP camera's, VoIP phones, wireless AP, as well as transmitting data.

The switch PoE power supply system conforms to standards, IEEE 802.3af and 802.3at. Devices from different manufacturers should have no problems, as long as they are comply with these standards.

PD, refers to the Powered Devices attached to the switch. These generally include IP cameras, wireless Access Points, VoIP phones, and other IP-based terminal equipment.

The whole process of PoE:

1. **Detection:** At the beginning, the switch outputs a very small voltage, to detect if its linked PD is an IEEE802.3af / IEEE802.3at compliant device. If it detects that the PD is a compliant device, then it will go to next step.

2. **PD Classification**: After detecting the PD device, the switch will classify and recognise what power the device requires.

3. **Power up:** After the 2 steps above are complete, the switch start supplying power to the PD, within a range of 44~57VDC.

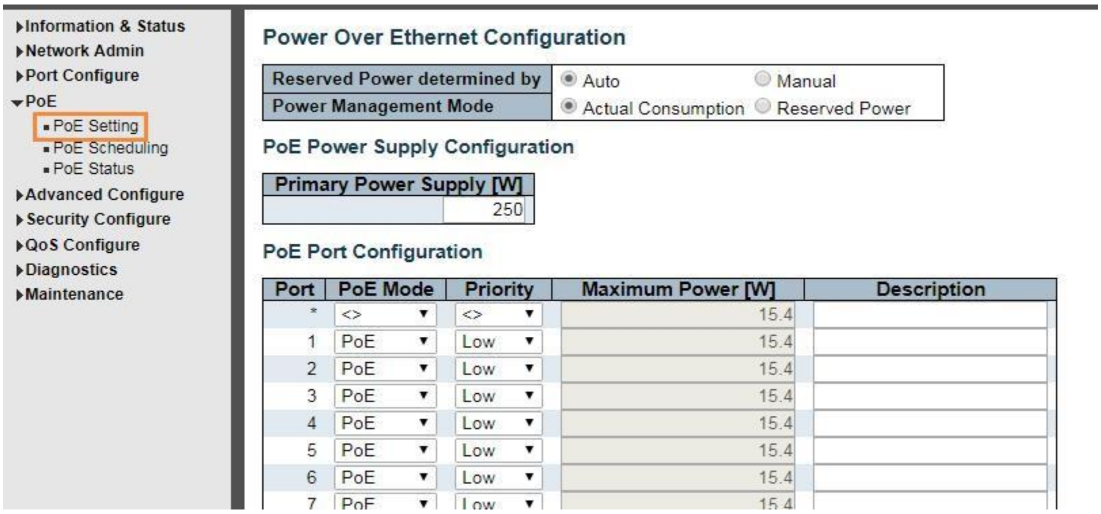
4. **Power supply**: The switch provides a stable 44~57V DC to PDs, and auto feeds power as required by the PDs. The maximum power of single PoE port for IEEE 802.3af devices: 15.4W; Maximum power of single PoE port for IEEE 802.3at devices: 25.5W.

5. **Disconnection:** If PD is disconnected or a user disables PoE from the management software, the switch will quickly(300- 400ms) stop powering the PD.

If at any time in the powering process, the switch stops working then it will restart from step1. If an abnormal situation happens, such as the PD short circuiting, or the power consumption is higher than the feeding power, etc. then restart from step 1.

4.1. PoE Setting

After selecting "PoE">"PoE Setting", user can make PoE settings in the following screen:



Power Over Ethernet Configuration

Reserved Power determined by	● Auto	○ Manual
Power Management Mode	● Actual Consumption	○ Reserved Power

PoE Power Supply Configuration

Primary Power Supply [W]
250

PoE Port Configuration

Port	PoE Mode	Priority	Maximum Power [W]	Description
*	<>	<>	15.4	
1	PoE	Low	15.4	
2	PoE	Low	15.4	
3	PoE	Low	15.4	
4	PoE	Low	15.4	
5	PoE	Low	15.4	
6	PoE	Low	15.4	
7	PoE	Low	15.4	

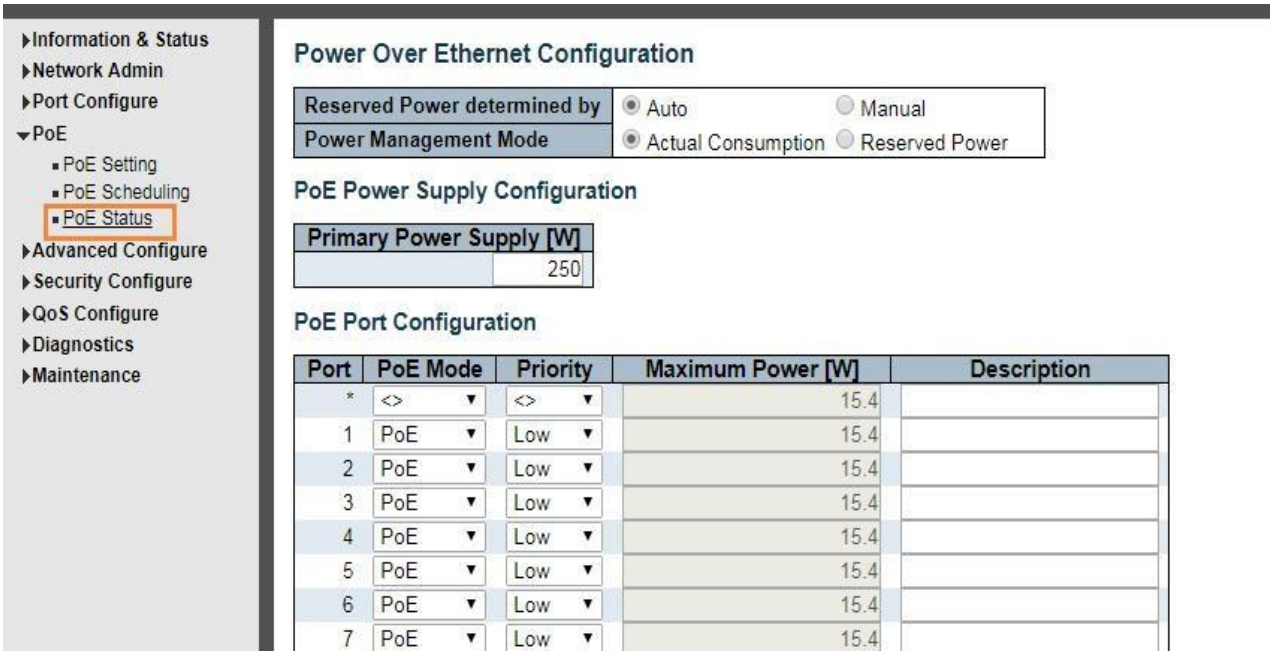
Figure 4.1 Power Over Ethernet Configuration

Object	Description
Reserved Power determined by	This switch supports 2 modes for reserved power determination. **Auto:** Switch automatically assigned maximum power of switch port according to detected PD class. About PD Class, please refer to the 802.3af / 802.3at definition. **Manual:** Maximum reserved power of the port is customise by the user.
Power Management Mode	This switch supports 2 modes for Power Management. **Actual Consumption**: In this mode, when the actual power consumption of all the ports exceeds the switch's power budget, the lowest priority port will be shut down. If all ports have the same priority, then the maximum port number would be shut down. **Reserved Power:** In this mode, when the reserved power consumption of all the ports exceeds the switch's power budget, the port that connect to new PD will not be enabled.
Primary Power Supply [W]	Users can set the maximum primary power of the whole switch. Default setting is 370W.
PoE Mode	This switch support 802.3af(PoE) and 802.3at(PoE+) mode. Default setting is 802.3at.
Priority	Define the priority of the PoE port. Priority from low to high is Low, High, Critical.
Maximum Power(W)	It is for define port's maximum Power when user set Manual as reserved power determination mode.

Click "Save" to store and active settings.

4.2. PoE Status

Using this page, users can check and look at the PoE status of all ports, after selecting "PoE">"PoE Status".



Power Over Ethernet Configuration

Reserved Power determined by	● Auto	○ Manual
Power Management Mode	● Actual Consumption	○ Reserved Power

PoE Power Supply Configuration

Primary Power Supply [W]
250

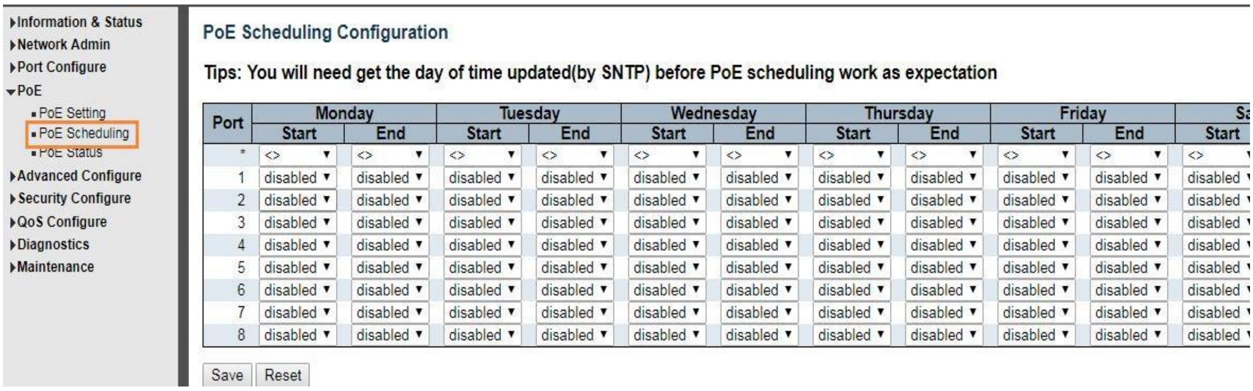
PoE Port Configuration

Port	PoE Mode	Priority	Maximum Power [W]	Description
*	<>	<>	15.4	
1	PoE	Low	15.4	
2	PoE	Low	15.4	
3	PoE	Low	15.4	
4	PoE	Low	15.4	
5	PoE	Low	15.4	
6	PoE	Low	15.4	
7	PoE	Low	15.4	

Figure 4-2 PoE Status Screen

4.3. PoE Scheduling

The switch support PoE scheduling, users can set timing PoE reboot and enable/disable PoE on time schedule. Click “PoE”> “PoE Scheduling”, as below:



PoE Scheduling Configuration

Tips: You will need get the day of time updated(by SNTP) before PoE scheduling work as expectation

Port	Monday		Tuesday		Wednesday		Thursday		Friday		Sa
	Start	End	Start	End	Start	End	Start	End	Start	End	Start
*	<>	<>	<>	<>	<>	<>	<>	<>	<>	<>	<>
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Figure 4.3 PoE Scheduling

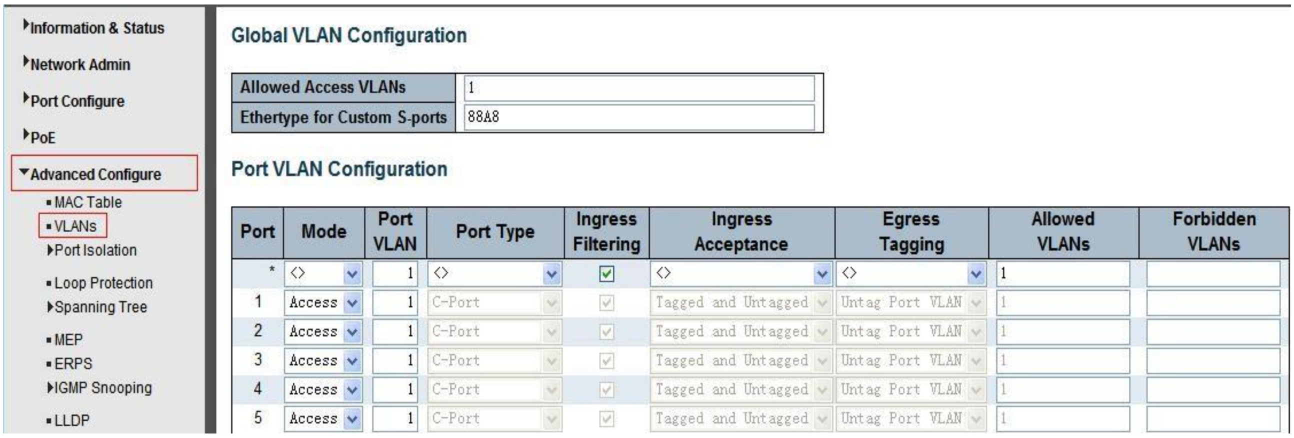
Object	Instruction
Cycle	Selection range: Monday to Sunday
Start	Restoration for PoE, Time range: 00:00-24:00
End	ange: 00:00-24:00

5. Advanced Configuration

5.1. VLAN

A VLAN (Virtual Local Area Network) is a communication technology that logically divides one physical LAN into multiple broadcast area networks (multiple VLANs). Hosts within a VLAN can communicate directly with each other. But users on different VLAN groups can not communicate directly with each other. In essence the VLAN limits the broadcast packets within that VLAN. Since it blocks traffic between VLAN groups, it improves network security.

Select "Advanced Configure">"VLANs"to see 802.1Q VLAN configuration screen as following:



Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

Figure 5-1 802.1Q VLAN Configuration Screen

Object	Description
Allowed VLANs	This displays the created VLAN IDs. It is 1 by default. If you want to create new VLAN, just add the VLAN ID here. By default, VLAN 1 is pre-configured.
Ether type for Custom S-ports	This field specifies the ether type/TPID (specified in hexadecimal) used for Custom S- ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.
Mode	The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied.
	Access: Access ports are normally used to connect to end stations. Access ports have the following characteristics: Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1 Accepts untagged and C-tagged frames Discards all frames that are not classified to the Access VLAN On egress all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged

	Trunk: Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics: By default, a trunk port is member of all VLANs (1-4094) The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs Frames classified to a VLAN that the port is not a member of are discarded By default, all frames except frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress **Hybrid:** Hybrid ports resemble trunk ports in many ways, but add additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities: Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S- custom-tag aware Ingress filtering can be controlled Ingress acceptance of frames and configuration of egress tagging can be configured independently
Port VLAN	Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4094, default being 1. On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0). On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN. The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.
Port Type	Ports in hybrid mode allow the network manager to change the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required. **Unaware:** On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress. **C-Port:** On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag. **S-Port:** On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.

	Custom-Port: On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.
Port Type Continued	Ports in hybrid mode allow the network manager to change the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required. **Unaware:** On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress. **C-Port:** On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag. **S-Port:** On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag. **S-Custom-Port:** On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.
Ingress Filter	Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.
Ingress Acceptance	Hybrid ports allow for changing the type of frames that are accepted on ingress. **Tagged and Untagged** Both tagged and untagged frames are accepted. **Tagged Only** Only tagged frames are accepted on ingress. Untagged frames are discarded. **Untagged Only** Only untagged frames are accepted on ingress. Tagged frames are discarded.

Egress Tagging	**NB**: Ports in Trunk and Hybrid mode may control the tagging of frames on egress. **Untag Port VLAN** Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag. **Tag All** All frames, whether classified to the Port VLAN or not, are transmitted with a tag. **Untag All** All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.
Allowed VLANs	Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to **1-4094**. The field may be left empty, which means that the port will not become member of any VLANs.
orbidden VLANs	A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field. By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Click "Save" to store and active settings.

5.2. Port Isolation

Port isolation is for limiting data between ports. It is similar to VLAN, but its more rigid.

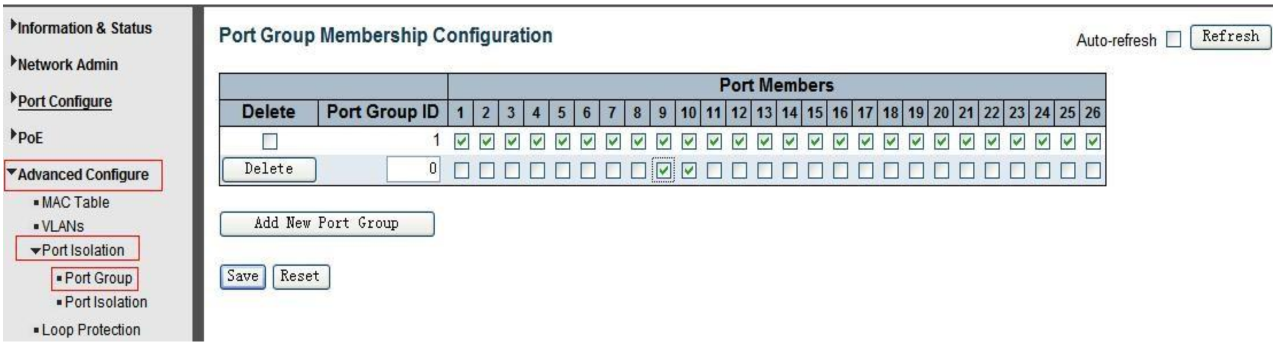
After Selecting "Advanced Configure">"Port Isolation">"Port Isolation", then the port isolation screen will appear allowing you to configure port isolation.

5.2.1. Port Groups

This switch support port groups. Members of port groups can forward data to each other.

Note: a port can belong to multiple port groups. Data can be forwarded among any port that belong to one port group.

After Selecting "Advanced Configure">"Port Isolation">"Port Group", then the following screen will appear allowing port group configuration.



Port Group Membership Configuration

		Port Members																									
Delete	Port Group ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Delete	0	□	□	□	□	□	□	□	□	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

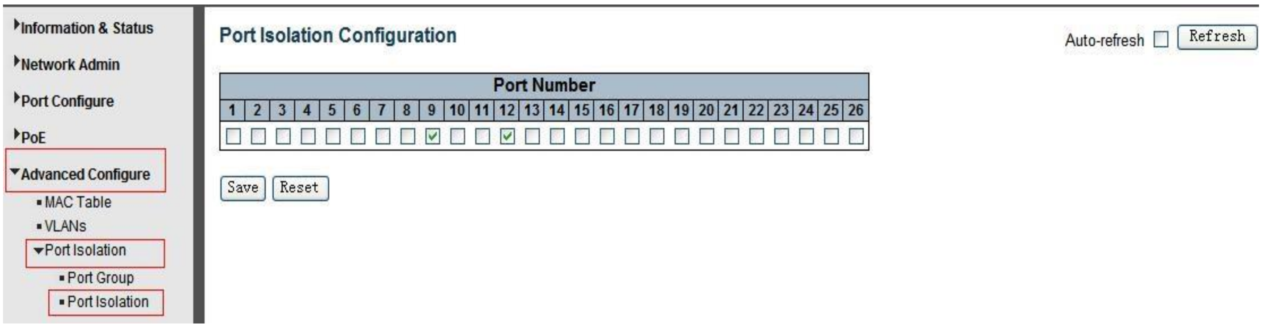
Figure 5-2-1 Port Group Configuration Screen

Object	Description
Port Members	Check the corresponding box to set them as one port group

Click "Add New Port Group" to create a new port group, "Delete" to remove corresponding port group, and "Save" to store and active settings.

5.2.2. Port Isolation

After Selecting "Advanced Configure">"Port Isolation">"Port Isolation", then the following screen will appear allowing you to configure port isolation.



Port Isolation Configuration

Port Number																									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
□	□	□	□	□	□	□	□	☑	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Figure 5-2-2. Port Isolation Configuration Screen Configuration object and description is:

Object	Description
Port number	Check box to set corresponding port as port isolation, so that they cannot forward data

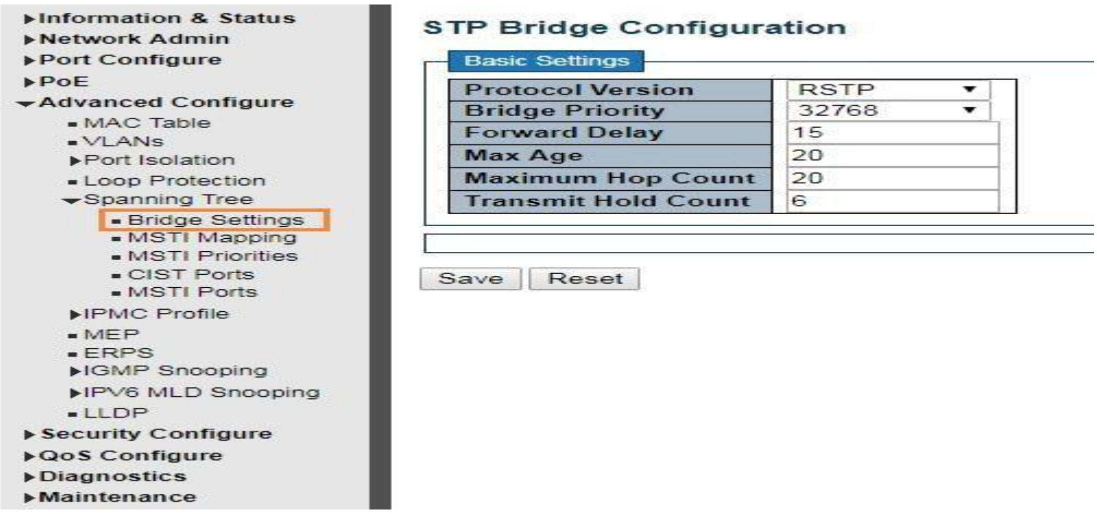
Click "Save" to store and active settings.

5.3. STP

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This is a standard which allows the switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

5.3.1. STP Bridge Settings

This page allows you to configure port STP settings. After Selecting "Advanced Configure">"Spanning Tree">"Bridge Settings", the following screen will appear.



STP Bridge Configuration

Basic Settings

Protocol Version	RSTP
Bridge Priority	32768
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Figure 5.3.1 Spanning Tree Configuration Screen

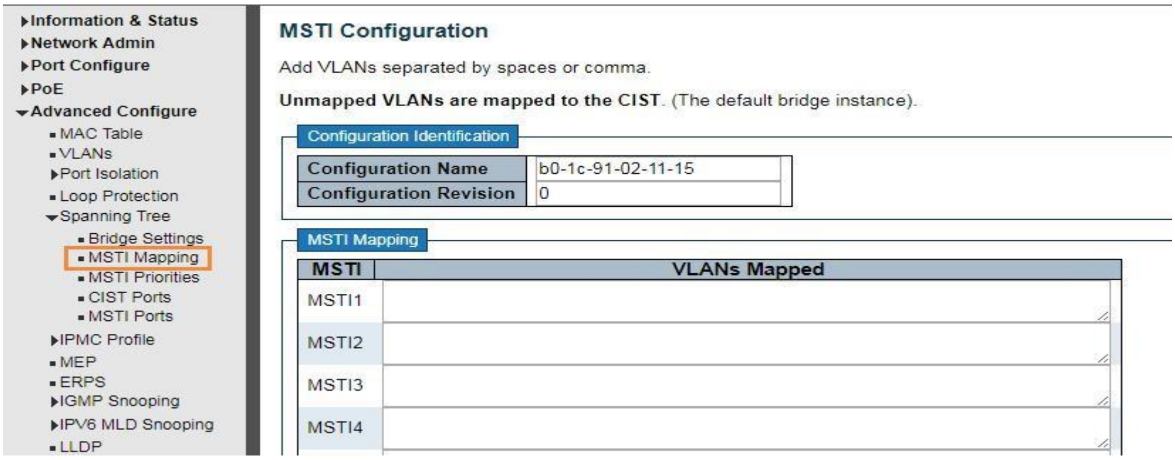
Object	Description
Protocol Version	Click drop-down menu to select STP protocol version, including: STP - Spanning Tree Protocol (IEEE802.1D); RSTP - Rapid Spanning Tree Protocol (IEEE802.1w)
Bridge Priority	Controls the bridge priority. The lower the value the higher the priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*.
Forward Delay (4-30)	Forward Delay setting range is from 4 to 30 seconds. Default value is 15 seconds.
Max Age (6-40)	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. Default value is 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. Valid values are in the range 6 to 40 hops.
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. Default value is 6 .

Click “save” to store and activate the setting

5.3.2. MSTI Mapping

Users can set the switches MSTI mapping, select “Advanced Configure”> “Spanning Tree” > “MSTI Mapping”.

Figure 5-3-2 MSTI Mapping Setting



MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	b0-1c-91-02-11-15
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	

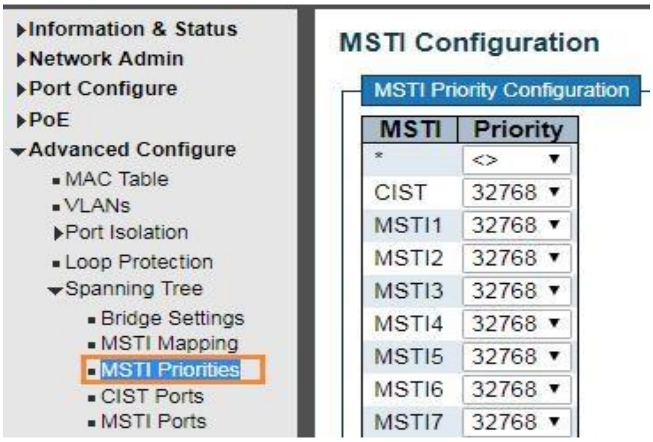
Object	Instruction
Configuration Name	Set domain name of MSTI
Configuration Revision	Set Configuration Revision
MSTI Mapping	Input the VLAN that need mapping

Click “Save” to enable your settings.

Note: Please set the same value for configuration name and configuration revision of all switches in the looped network when set MSTP

5.3.3. MSTI Priorities

Users can set MSTI priorities, click “advanced configure”>“Spanning Tree”>“MSTI Priorities”



MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
*	<> ▾
CIST	32768 ▾
MSTI1	32768 ▾
MSTI2	32768 ▾
MSTI3	32768 ▾
MSTI4	32768 ▾
MSTI5	32768 ▾
MSTI6	32768 ▾
MSTI7	32768 ▾

Figure 5.3.3. MSTI Priorities

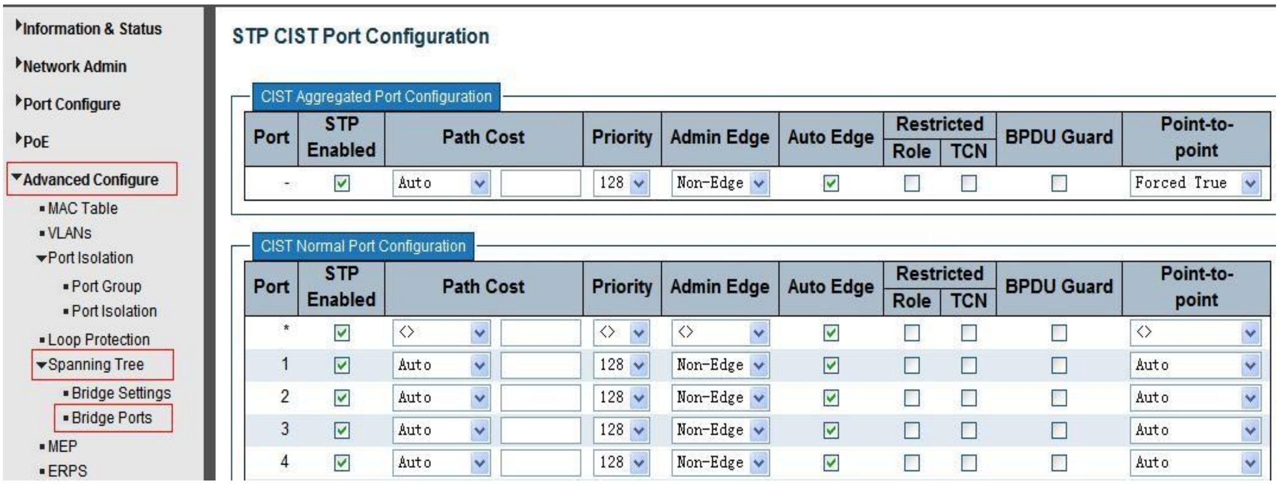
Object	Instruction
MSTI Priorities	Set the priority, value ranges : 0-61440

Set the priority, value ranges : 0-61440 Click “Save” to enable your settings.

Note: The priority value must be in multiples of 4094, at the range of 0-61440

5.3.4. STP Bridge Port

After selecting "Advanced Configure">"Spanning Tree">"Bridge Ports", the following screen will appear.



STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
-	☑	Auto		128	Non-Edge	☑	□	□	□	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	☑	<>		<>	<>	☑	□	□	□	<>
1	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
2	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
3	☑	Auto		128	Non-Edge	☑	□	□	□	Auto
4	☑	Auto		128	Non-Edge	☑	□	□	□	Auto

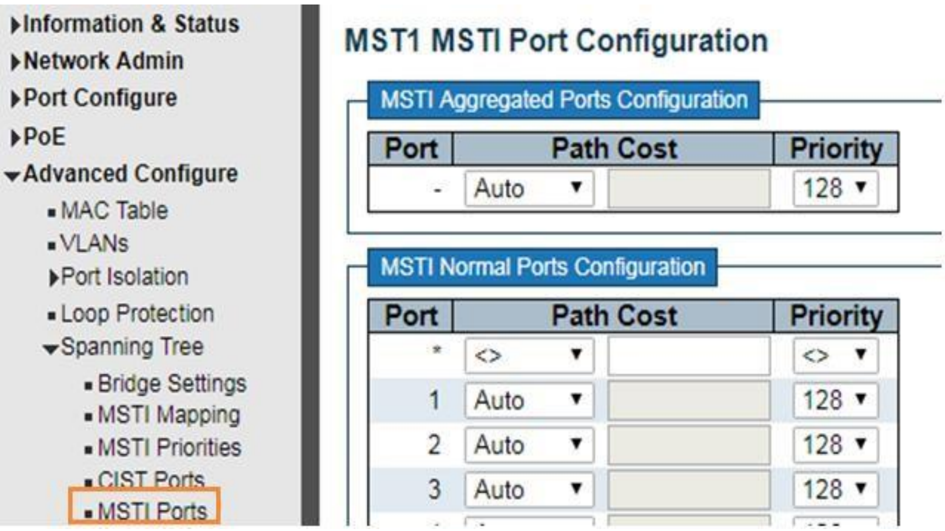
Figure 5.3.4 STP Configuration Screen

Object	Description
STP Enabled	Check to enable STP function.
Path Cost(0=Auto)	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
Auto Edge	Check box to set corresponding port as Auto Edge.
Restricted Role	Check box to set corresponding port as Restricted Role
Restricted TCN	Check box to set corresponding port as Restricted TCN
BPDU Guide	Check box to enable BPDU Guide. So when port receives BPDU reception, it will turn to Disable(Shut Down) status.
Point-to-point	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.(This applies to physical ports only. Aggregations are always forced Point 2 Point.

Click "Save" to store and active settings.

5.3.5. MSTI Ports

Users can set MSTI ports, select “ Advanced Configure”>“Spanning Tree”>“MSTI Ports”



MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost		Priority
-	Auto		128

MSTI Normal Ports Configuration

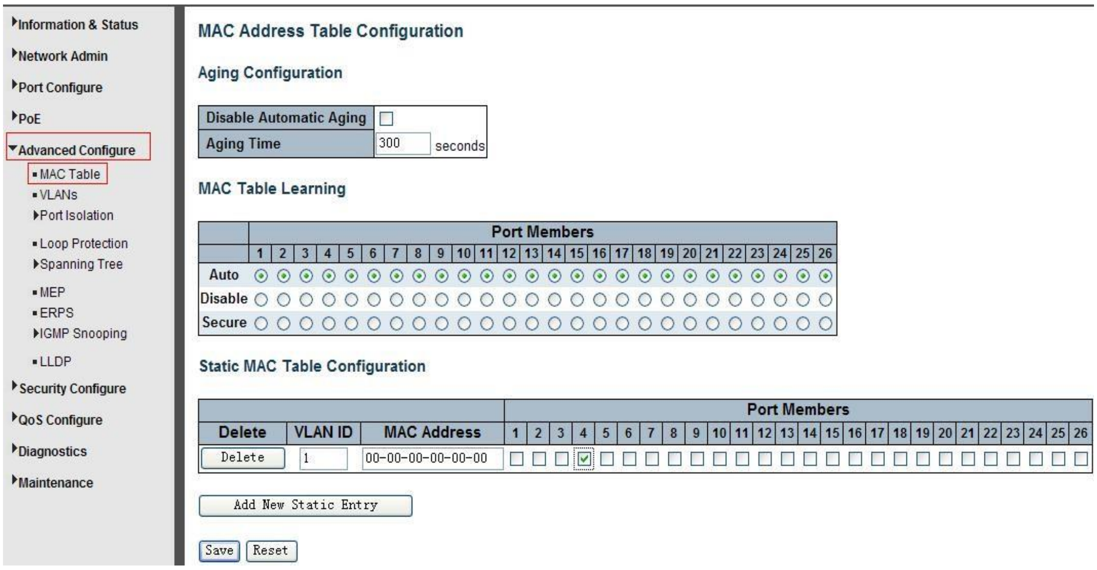
Port	Path Cost		Priority
*	<>		<>
1	Auto		128
2	Auto		128
3	Auto		128

Figure 5-3-5 MSTI Ports Setting

Object	Instruction
Path Cost	Used to define a metric, representing the associated overhead of forwarding packets to a specified port list. The port overhead can be automatically set or set to a metric value. The default value is 0 (automatic).The lower the number, the more likely it is to select the port to forward the packet. Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	When the port's path overhead is the same, the priority is used to decide the forwarding state of the port.

5.4. MAC Address Table

This page allows you to configure the Mac address table settings. After selecting "Advanced Configure">"Mac Table" , the following screen will appear.



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

MAC Table Learning

	Port Members																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Auto	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Static MAC Table Configuration

			Port Members																									
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Delete	1	00-00-00-00-00-00	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Figure 5-4 MAC Address Table

Object	Description
Disable Automatic Aging	If the box is checked, then the automatic aging function is disabled.
Aging Time	The time after which a learned entry is discarded . Range: 10-1000000 seconds; Default: 300 seconds.
IAC Table Learning	This switch supports 3 types for MAC Table Learning Auto: port will auto learn Mac address. Disable: port will NOT learn MAC address. Secure: port only forward data of configured static MAC address.
atic MAC Table Configuration	The static entries in the MAC table are shown in this table. Click "Add New Static Entry" to create a new record.

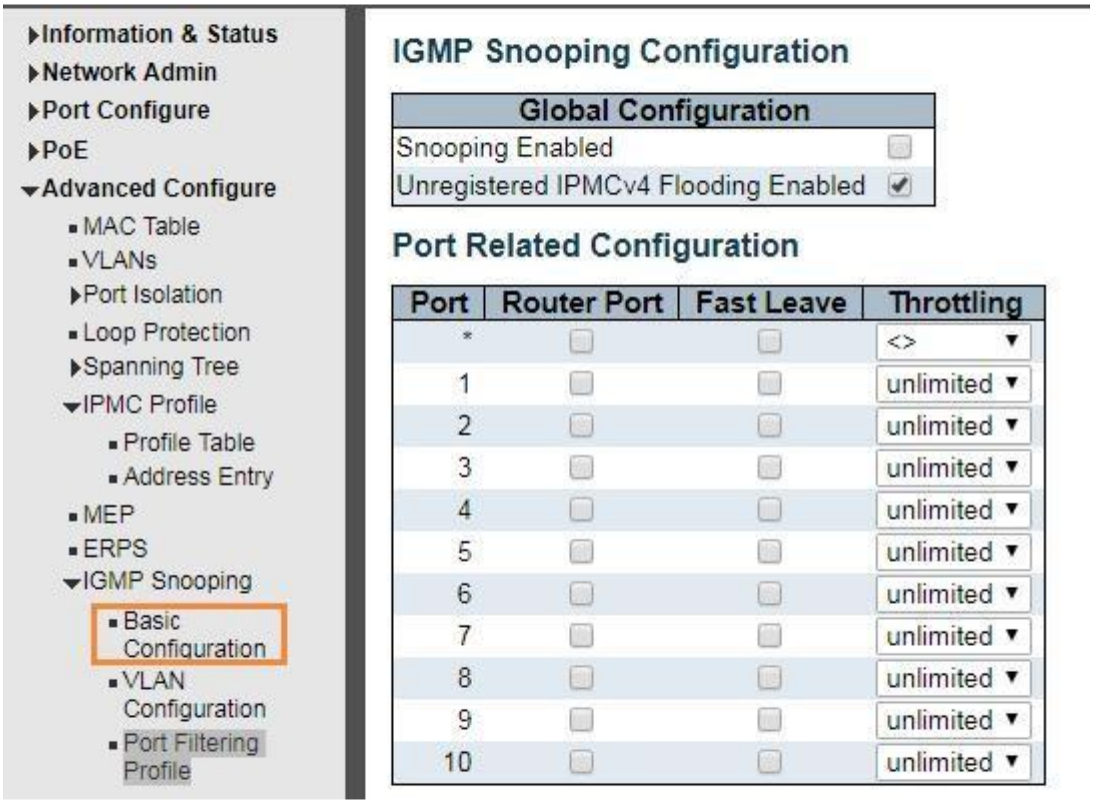
Click "Save" to store and active settings.

5.5. IGMP Snooping

The Internet Group Management Protocol (IGMP) lets host and routers share information about multicast groups memberships. IGMP snooping is a feature on the switch that monitors the exchange of IGMP messages and copies them to the CPU for feature processing. The overall purpose of IGMP Snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

5.5.1. Basic Configuration

After Clicking "Advanced Configure">"IGMP Snooping">"Basic Configuration", the following screen will appear.



IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	□
Unregistered IPMCv4 Flooding Enabled	☑

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	□	□	<> ▼
1	□	□	unlimited ▼
2	□	□	unlimited ▼
3	□	□	unlimited ▼
4	□	□	unlimited ▼
5	□	□	unlimited ▼
6	□	□	unlimited ▼
7	□	□	unlimited ▼
8	□	□	unlimited ▼
9	□	□	unlimited ▼
10	□	□	unlimited ▼

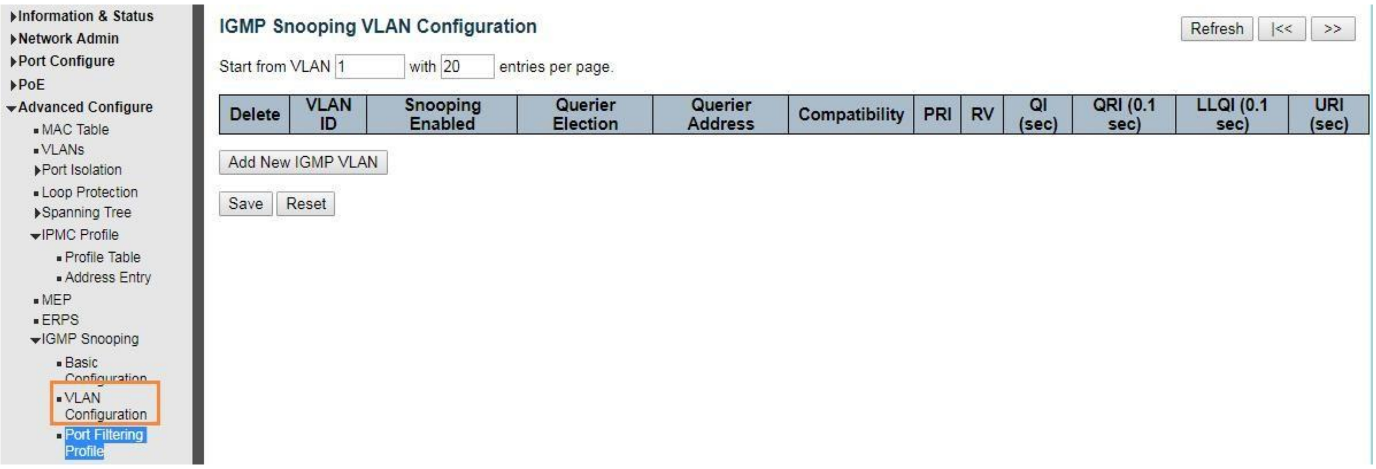
Figure 5-5-1 IGMP Snooping Basic Configuration object and description

Object	Description
Snooping Enabled	Enable or disable the IGMP snooping. The default value is "Disabled". Enable: check the box; Disable: do not check the box.
Unregistered IPMCv4 Flooding Enabled	Check the box to enable unregistered IPMCv4 Flooding
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Fast leave performs deleting MAC forward entry immediately upon receiving message for group de-registration

Click "Save" to store and active settings.

5.5.2. IGMP Snooping VLAN Configuration

After selecting "Advanced Configure">"IGMP Snooping">"VLAN Configuration", the following screen will appear.



IGMP Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)

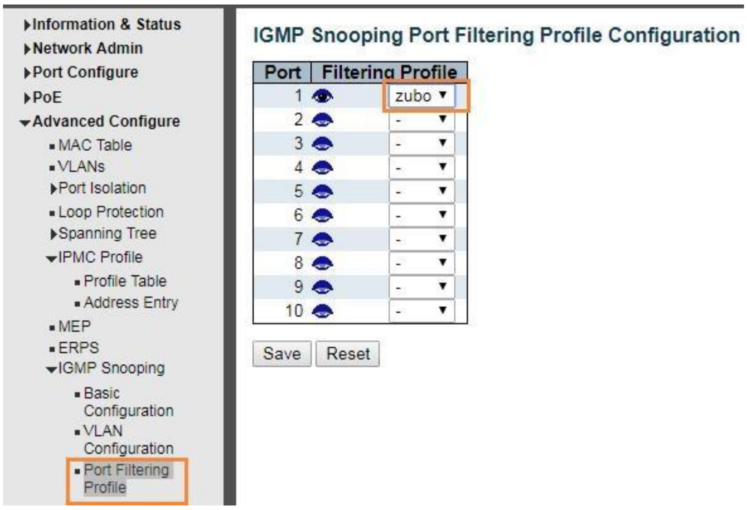
Figure 5-5-2 IGMP Snooping VLAN Configuration

Object	Description
Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier Election	Enable this to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
Querier Address	Define the IPv4 address as a source address used in IP header for IGMP Querier election. When the Querier address is not set, the system uses the IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, the system uses the first available IPv4 management address. Otherwise, the system uses a pre-defined value. By default, this value will be 192.0.2.1.

Click "Save" to store and active settings.

5.5.3. Port Filtering Profile

To Set Port filtering profile, select “Advanced Configure”>“IGMP Snooping”>“Port Filtering Profile”



IGMP Snooping Port Filtering Profile Configuration

Port	Filtering Profile
1	zubo
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-

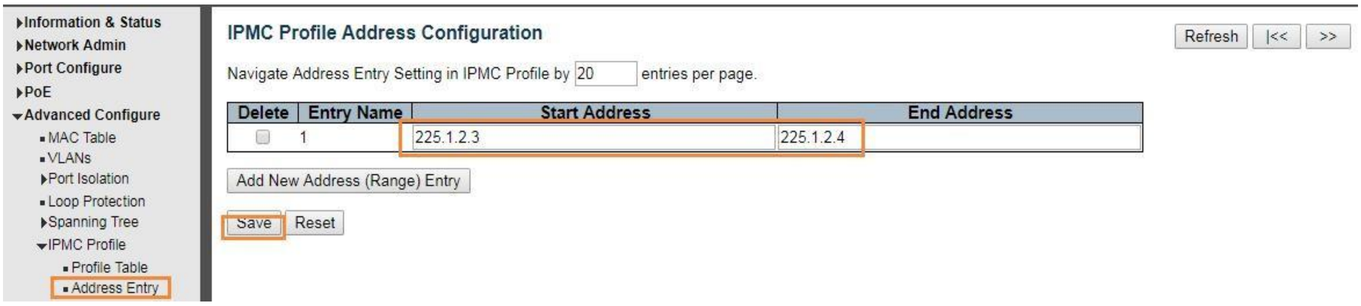
Figure 5-5-3 Port Filtering Profile Setting

Object	Instruction
VLAN ID	
Enable Snooping	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier（Querier Election）	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
Querier（Querier Address）	Define the IPv4 address as the source address used in IP header for IGMP Querier election. When the Querier address is not set, the switch uses the IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, the switch uses the first available IPv4 management address. Otherwise, the switch uses a pre-defined value. By default, this value will be 192.0.2.1.

Click “Save” to enable your setting.

5.6. IPMC Profile

Users can set the multicast filter list, Click “Advanced Configure” > “IPMC Profile” > “Address Entry”



IPMC Profile Address Configuration

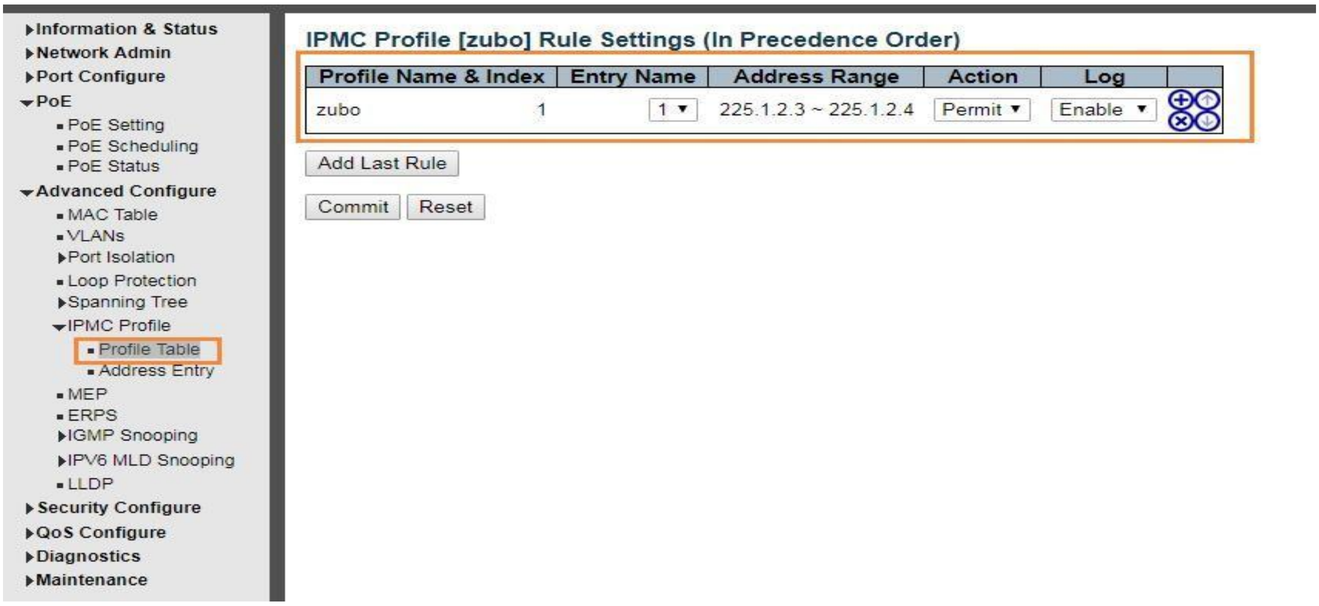
Navigate Address Entry Setting in IPMC Profile by 20 entries per page.

Delete	Entry Name	Start Address	End Address
□	1	225.1.2.3	225.1.2.4

Object	Instruction
Entry Name	Input the name of the group to be filtered
Start Address	Input the start group address
End Address	Input the end group address

Click “Save” to enable your setting.

To Bind the filter multicast list, click “Advanced Configure”>“IPMC Profile”>“ Profile Table



IPMC Profile [zubo] Rule Settings (In Precedence Order)

Profile Name & Index	Entry Name	Address Range	Action	Log
zubo 1	1	225.1.2.3 ~ 225.1.2.4	Permit	Enable

Figure 5-6 IGMP Snooping Setting

Object	**Instruction**
Entry Name	Choose created Address Entry by dropping down the menu.
Action	Choose Deny / Permit
Log	Enable / Disable

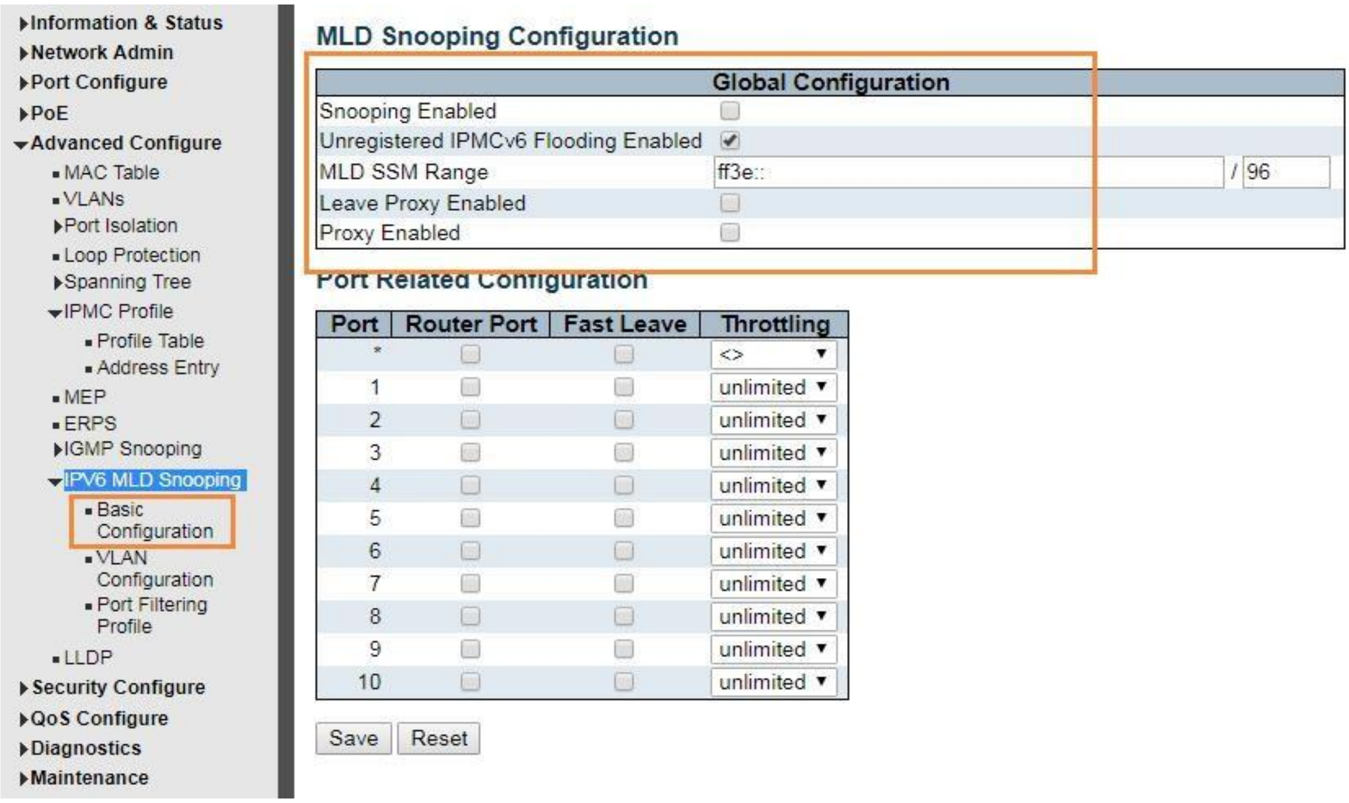
5.7. IPV6 MLD Snooping

IPV6 MLD Snooping is a multicast management and control mechanism working at Layer 2 in the Ethernet switch

When IPV6 MLD Snooping is enabled, the switch receives the IPV6 MLD messages by listening on each interface, to exchange interface and multicast group address mapping relationships, the mapping relationship allows the switch to forward the multicast data flow.

5.7.1. Basic Configuration

Click “Advanced Configure”>“IPv6 MLD Snooping”>“Basic Configuration”, to check the configuration information for IPv6 MLD Snooping.



MLD Snooping Configuration

Global Configuration		
Snooping Enabled	□	
Unregistered IPMCv6 Flooding Enabled	☑	
MLD SSM Range	ff3e::	/ 96
Leave Proxy Enabled	□	
Proxy Enabled	□	

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	□	□	<>
1	□	□	unlimited
2	□	□	unlimited
3	□	□	unlimited
4	□	□	unlimited
5	□	□	unlimited
6	□	□	unlimited
7	□	□	unlimited
8	□	□	unlimited
9	□	□	unlimited
10	□	□	unlimited

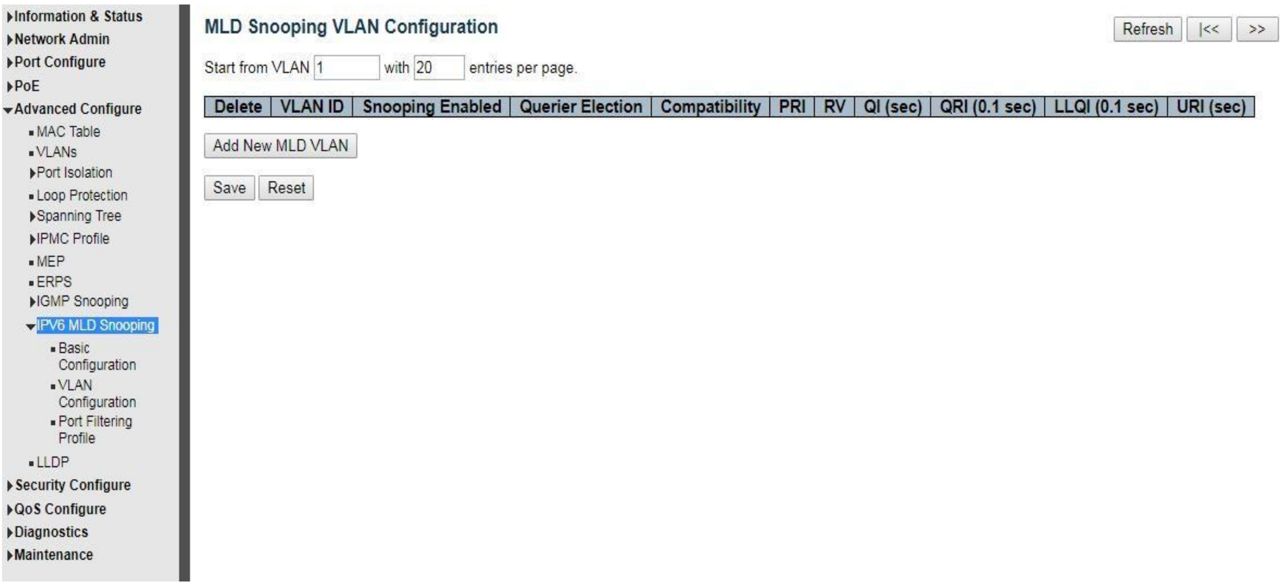
Figure 5-7-1 IGMP Snooping Basic Setting

Object	Instruction
Snooping Enable	Enable/ Disable IGMP Snooping
Unregistered IPMCv6 Flooding Enable	
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast leave	Fast leave Performs deleting MAC forward entry immediately upon receiving message for group de-registration

Click “Save” to enable your setting.

5.7.2. VLAN Configuration

Select “Advanced Configure”>“IPv6 MLD Snooping”>“VLAN Configuration”, to check the configuration information of IPv6 MLD Snooping.



MLD Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)

Figure 5-7-2 IPV6 MLD Snooping Setting

Object	Instruction
VLAN ID	Select the VLAN ID
Snooping Enable	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier（Querier Election）	Enable to join MLD Querier election in the VLAN. Disable to act as an MLD Non-Querier.

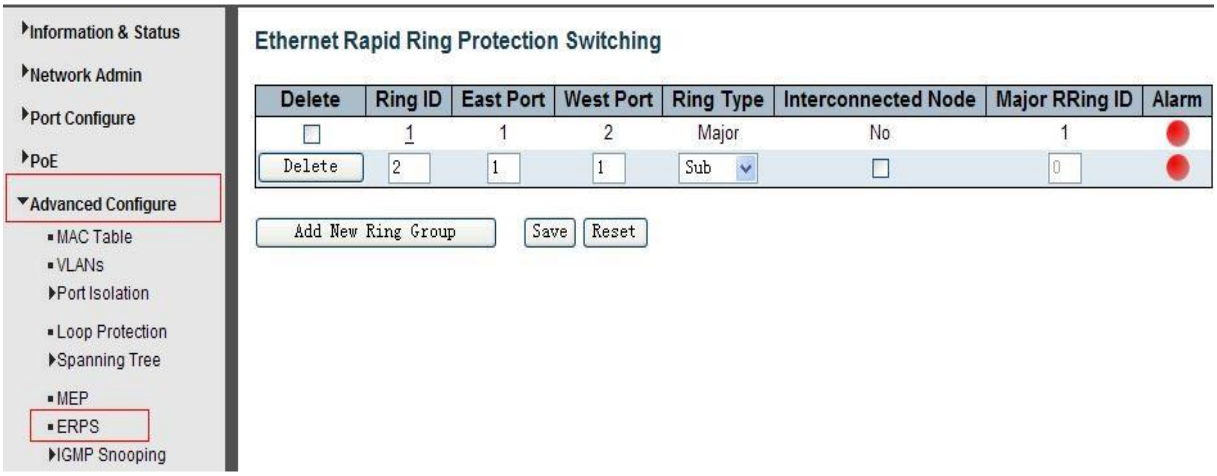
Click “Save” to enable your setting.

5.8. ERPS

ERPS (Ethernet Ring Protection Switching), integrates the OAM function and the APS protocol. If the ring network is interrupted (ie a failure somewhere) , the fault recovery time should be less than 50ms to bring the network back to normal operation. ITU-T G.8032 is the first industry standard for ERPS.

Note: Before enabling ERPS, STP on the ring port should be disabled.

Clicking "Advanced Configure">"ERPS " , the following screen will appear.



Ethernet Rapid Ring Protection Switching

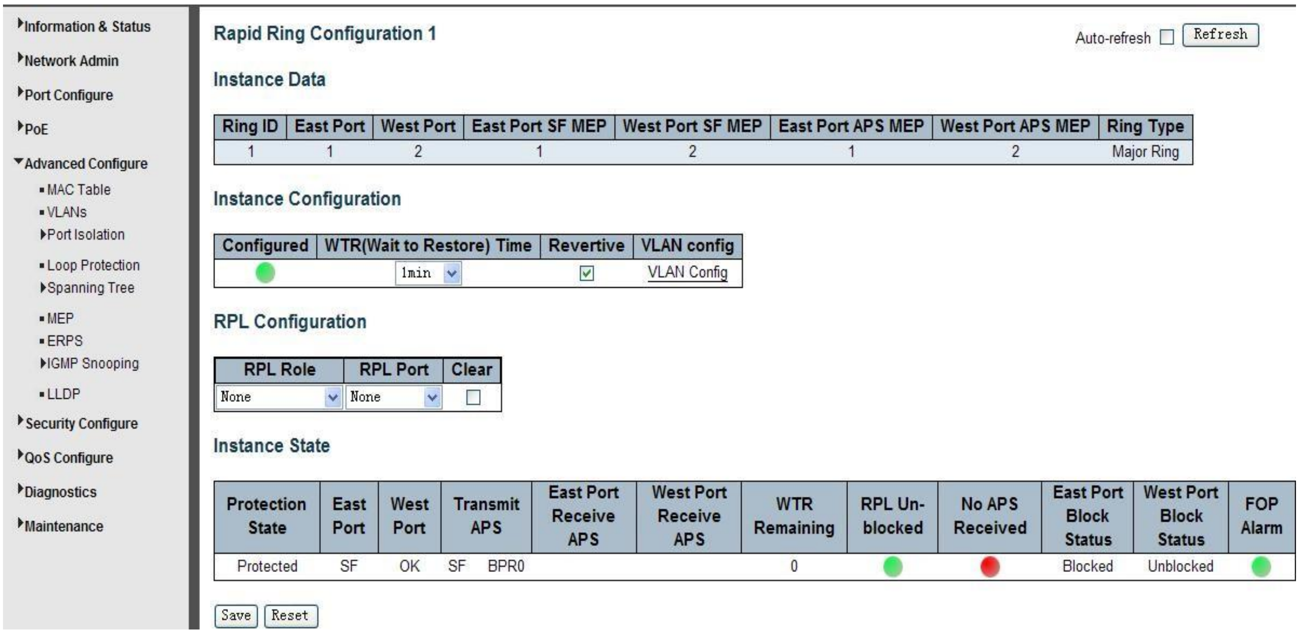
Delete	Ring ID	East Port	West Port	Ring Type	Interconnected Node	Major RRing ID	Alarm
□	1	1	2	Major	No	1	●
Delete	2	1	1	Sub	□	0	●

Figure 5-8-1 EPRS Configuration Screen

Object	Description
Ring ID	ERPS Ring ID
East Port	Number of the port which participate in this Ring.
West Port	Number of the other port which participate in this Ring.
Ring Type	Available selection: "Major Ring" or "Sub Ring". Only in case of Multi Ring application, "Sub Ring" need to be configured. **Default Ring Type**: "Major Ring". Only set this if there is multi ring application.
Interconnected Node	In Multi Ring application, Interconnected Node is the node that connect 2 or more rings.
Major Ring ID	In Single Ring application, Major Ring ID is same as Ring ID. In Multi Ring application, Sub Ring has to be type as Major Ring ID.
R-APS VLAN(1-4094)	Define VLAN for R - APS VLAN .

Select"Add New Ring Group "to create a new ERPS ring application. Select "Save" to store and active settings.

After clicking the number under "Ring ID", the switch will go to the page for Ring Configuration as shown in the following screen:



Rapid Ring Configuration 1

Instance Data

Ring ID	East Port	West Port	East Port SF MEP	West Port SF MEP	East Port APS MEP	West Port APS MEP	Ring Type
1	1	2	1	2	1	2	Major Ring

Instance Configuration

Configured	WTR(Wait to Restore) Time	Revertive	VLAN config
●	1min	☑	VLAN Config

RPL Configuration

RPL Role	RPL Port	Clear
None	None	□

Instance State

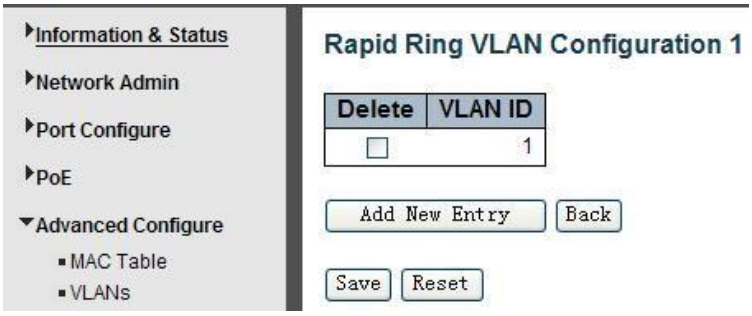
Protection State	East Port	West Port	Transmit APS	East Port Receive APS	West Port Receive APS	WTR Remaining	RPL Un-blocked	No APS Received	East Port Block Status	West Port Block Status	FOP Alarm
Protected	SF	OK	SF BPR0			0	🟢	🔴	Blocked	Unblocked	🟢

Figure 5-8-2 EPRS Ring Configuration

Object	Description
WTR (Wait to Restore) Time(1-12)	Click drop-down menu to select WTR time for R-APS. Available selection: 1-12min Default: 1 min
Revertive	Check to enable Revertive status of R-APS.
VLAN config	After selecting "VLAN config ", Rapid Ring VLAN Configuration page appears
RPLRole	Click drop-down menu to select "None", "RPL Owner", or "RPL Neighbour" role.
RPL Port	Click drop-down menu to select "None", "East Port", or "West Port".

Click "Save" to store and active settings.

After clicking the " VLAN config ", the switch will go the page displaying the ‘Rapid Ring ‘VLAN Configuration as shown below:



Rapid Ring VLAN Configuration 1

Delete	VLAN ID
□	1

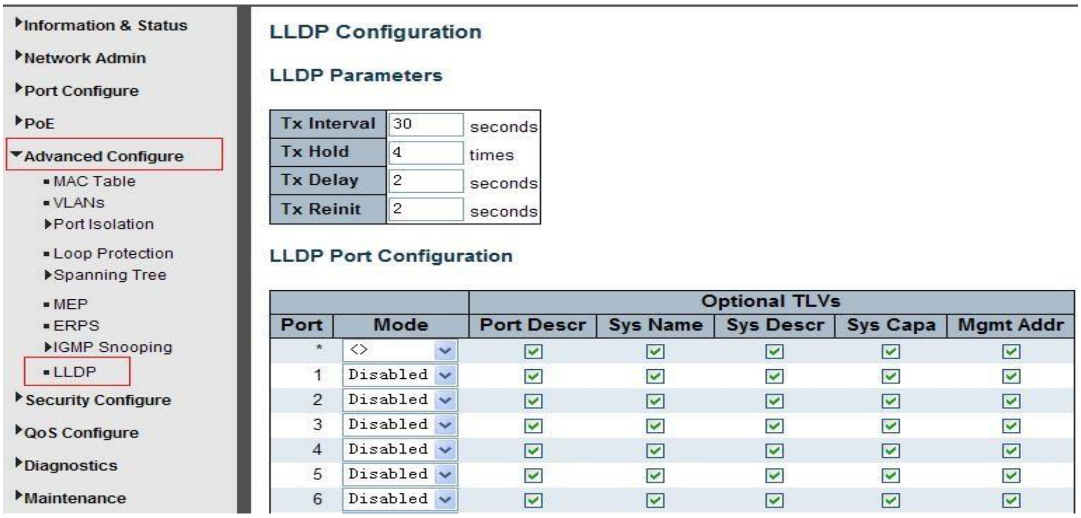
Figure 5-8-3 Rapid Ring VLAN Configuration

Click "Add New Entry" to create a new entry. Click "Save" to store and active settings.

5.9. LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighbouring devices on the local broadcast domain. LLDP and is a Layer 2 protocol that uses periodic broadcasts to advertise information about devices. Advertised information is represented in a Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighbouring network nodes it discovers.

After selecting "Advanced Configure">"LLDP" , the following screen will appear.



LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

LLDP Port Configuration

		Optional TLVs				
Port	Mode	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☑	☑	☑	☑	☑
1	Disabled	☑	☑	☑	☑	☑
2	Disabled	☑	☑	☑	☑	☑
3	Disabled	☑	☑	☑	☑	☑
4	Disabled	☑	☑	☑	☑	☑
5	Disabled	☑	☑	☑	☑	☑
6	Disabled	☑	☑	☑	☑	☑

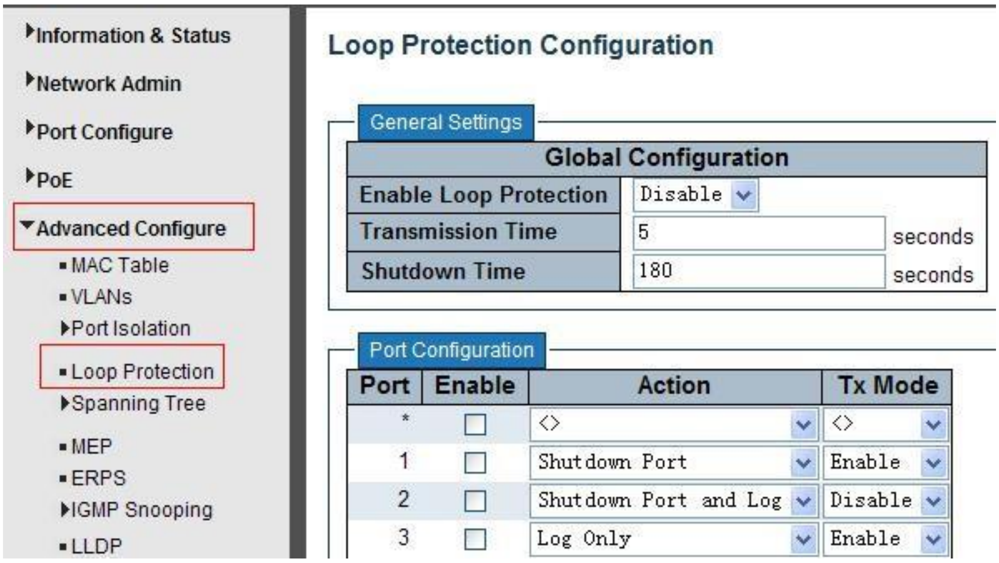
Figure 5-9 LLDP Configuration Screen

Object	Description
LLDP Parameters	This option allows the user to inspect and configure the current LLDP port settings: ➢ Tx Interval: Transmission Interval Time ➢ Tx Hold: Hold time Multiplier ➢ Tx Delay: Transmit Delay Time ➢ Tx Remit: Transmit Remit Time
Mode	Selects LLDP messages transmit and receive modes for LLDP Protocol Data Units. Options are Tx only, Rx only, Enabled, and Disabled.
Optional TLVs	Configures the information included in the TLV field of advertised messages. When the following option is checked, corresponding information will be includedin LLDP information transmitted. ➢ Port Descr: Port Description ➢ Sys Name: System Name ➢ Sys Descr: System Description ➢ Sys Capa: System Capability ➢ Mgmt Addr: Management Address

Click "Save" to store and active settings.

5.10. Loop Protection

Loop protection is designed to avoid broadcast loops. After selecting “Advanced Configure">"Loop Protection" , the following screen will appear.



Loop Protection Configuration

General Settings

Global Configuration		
Enable Loop Protection	Disable	
Transmission Time	5	seconds
Shutdown Time	180	seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	□	<>	<>
1	□	Shutdown Port	Enable
2	□	Shutdown Port and Log	Disable
3	□	Log Only	Enable

Figure 5-10 Loop Protection Configuration Screen

Object	Description
Global Configuration	Enable Loop Protection: click drop-down menu to disable or enable Loop Protection; Transmission Time: enter a number to set Loop Protection Interval Time; Shutdown Time: enter a number to set port Shutdown Time.
Enable	Check to enable corresponding port loop protection.
Action	Action take when the port detected loop. There are 3 types of action for users to select, Shutdown port, Shutdown port and Log, Log Only.
Tx Mode	To enable or disable Tx.

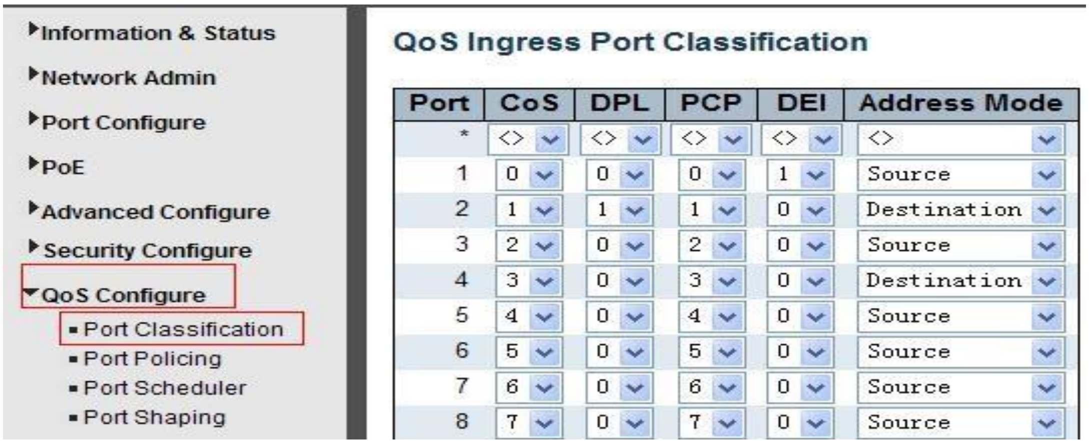
Click "Save" to store and active settings.

6. QoS Configure

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic. This function can not only reserve bandwidth, but also limit other traffic that is less important.

6.1. QoS Port Classification

After Selecting "QoS Configure">"Port Classification" , the following screen will appear.



QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Address Mode
*	<>	<>	<>	<>	<>
1	0	0	0	1	Source
2	1	1	1	0	Destination
3	2	0	2	0	Source
4	3	0	3	0	Destination
5	4	0	4	0	Source
6	5	0	5	0	Source
7	6	0	6	0	Source
8	7	0	7	0	Source

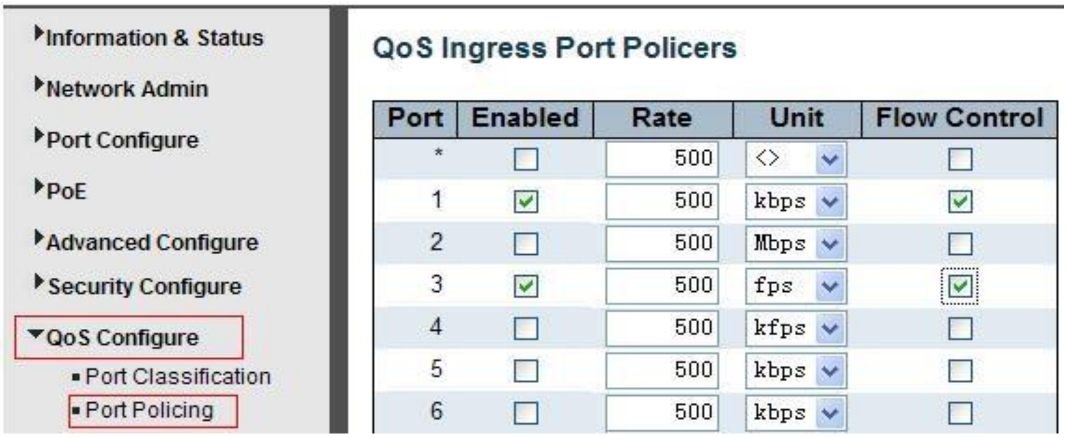
Figure 6-1 Port Classification Configuration Screen Configuration

ct	Description
CoS	Controls the default class of service, ranging from 0 (lowest) to 7 (highest). All Frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority The classified CoS can be overruled by a QCL entry. If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.
DPL	Controls the default drop precedence level. All frames are classified to a drop precedence level. The classified DPL can be overruled by a QCL entry.
PCP (Priority Code Point)	Controls the default PCP value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.
DEI	Controls the default DEI value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.
Address Mode	The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are: Source: Enable SMAC/SIP matching. Destination: Enable DMAC/DIP matching.

Click "Save" to store and active settings.

6.2. Port Policing

After selecting "QoS Configure">"Port Policing" , the following screen will appear.



QoS Ingress Port Policers

Port	Enabled	Rate	Unit	Flow Control
*	□	500	<>	□
1	☑	500	kbps	☑
2	□	500	Mbps	□
3	☑	500	fps	☑
4	□	500	kfps	□
5	□	500	kbps	□
6	□	500	kbps	□

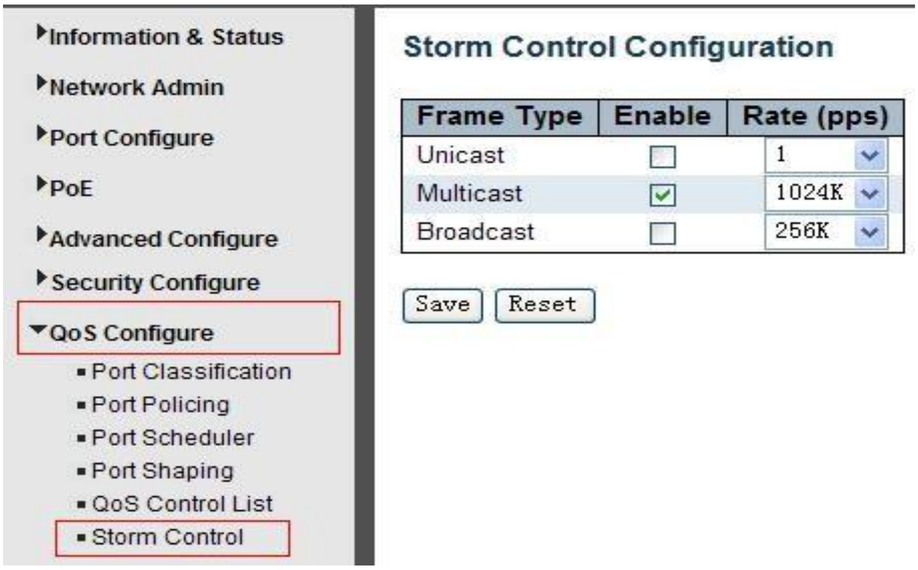
Figure 6-2 Port Policing Configuration Screen

Object	Description
Enabled	Check the box to enable Port Policing.
Rate	Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps".
Unit	Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".
Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Click "Save" to store and active settings.

6.3. Storm Control Configuration

After Selecting "QoS Configure">"Storm Control" , the following screen will appear.



Storm Control Configuration

Frame Type	Enable	Rate (pps)
Unicast	☐	1
Multicast	☑	1024K
Broadcast	☐	256K

Figure 6-3Port Policing Configuration Screen

Object	Description
Frame Type	This switch supports 3 kinds of Frame: Unicast, Unknown Multicast, Broadcast.
Enable	Tick the box to enable Storm Control.
Rate(pps)	The rate unit is packets per second (pps). Valid values are:1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K..

Click "Save" to store and active settings.

7. Configuring Security

7.1. Password

To change the system login password of the switch, please click "Security Configure">"Password".

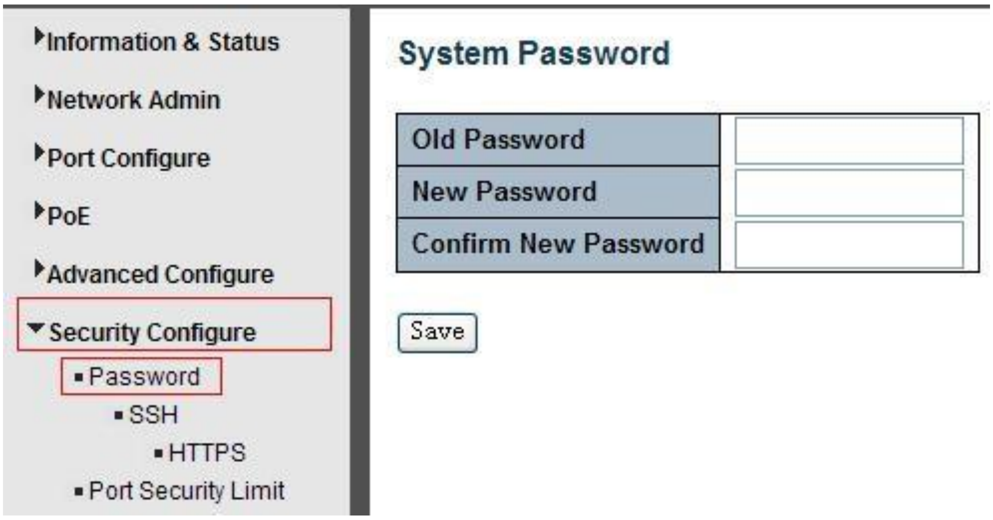


Figure 7-1 System Password Configuration Screen Click "Save" to store and active settings.

7.2. 802.1X

In 802.1X, the 'user' is called the' supplicant', the switch is the 'authenticator,' and the RADIUS server is the 'authentication' server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets.

RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

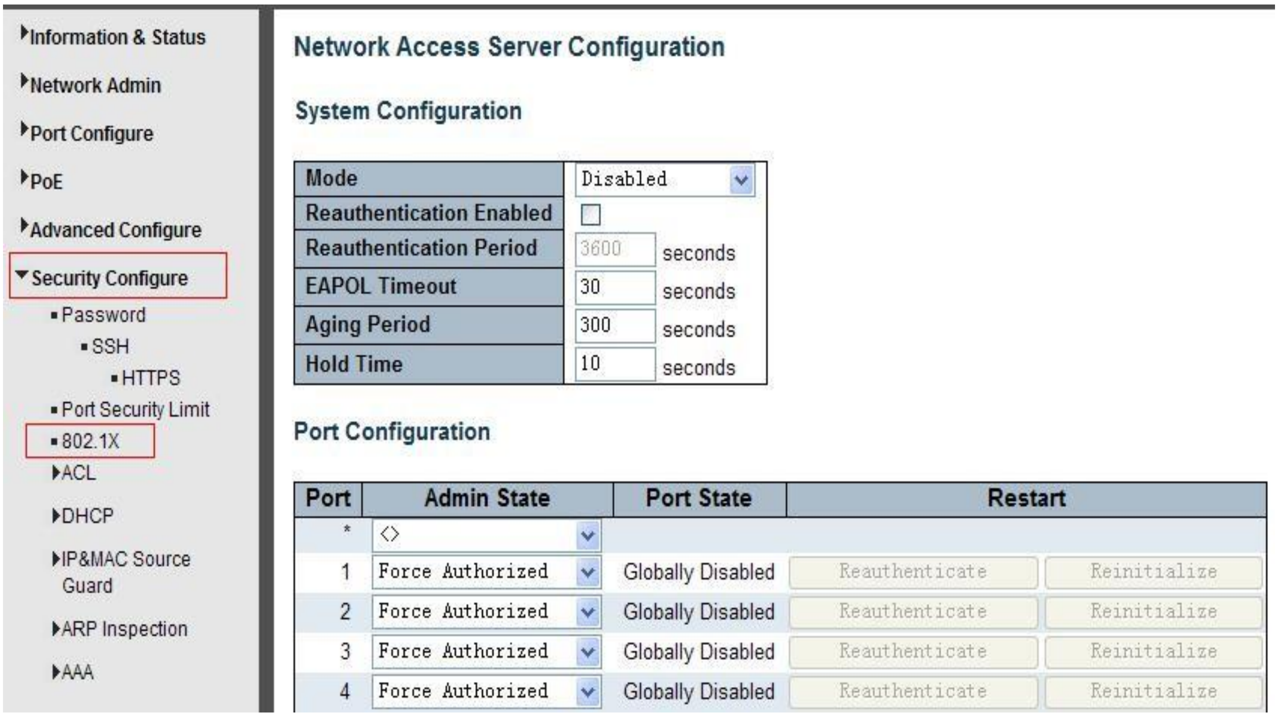
When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorised clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port. The Case Communications Layer 3 switch supports 802.1X port-based authentication

After selecting "Security Configure">"802.1X", the following screen will appear.

Figure 7-2 802.1X Configuration Screen



Network Access Server Configuration

System Configuration

Mode	Disabled
Reauthentication Enabled	□
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds

Port Configuration

Port	Admin State	Port State	Restart	
*	<>			
1	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	Globally Disabled	Reauthenticate	Reinitialize

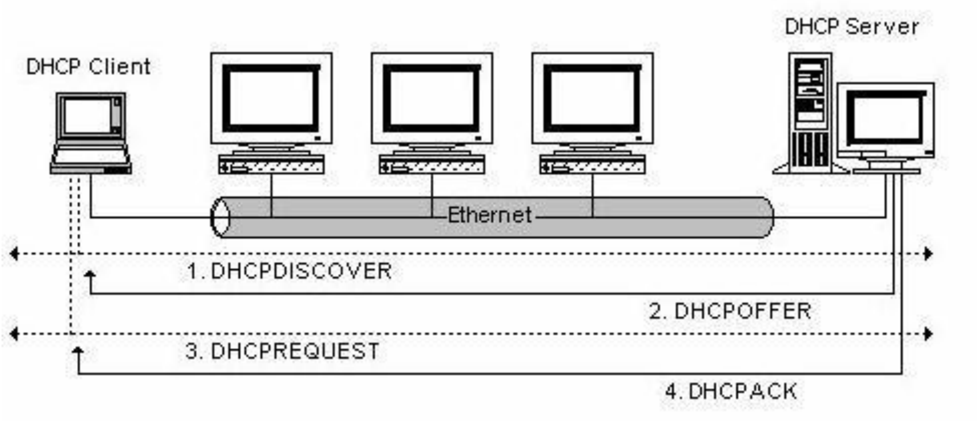
Object	Description
System Configuration	Here, a user can enable or disable 802.1X or Re-authentication, as well as set the Re- authentication Period / EAPOL Timeout / Aging Period / Hold Time
Port Configuration	Click the drop-down menu to select an Admin State. Available options: Force Authorized, Force Unauthorised, 802.1X, Mac-based Auth.
Reauthentication	After the user goes online, the device saves user authentication information. After re-authentication is enabled for 802.1X authentication users, the device sends the saved authentication information of the online user to the authentication server for re-authentication. If the user's authentication information does not change on the authentication server, the user is kept online. If the authentication information has been changed, the user is forced to go offline, and then re-authenticated according to the changed authentication information.
Re-Initialise	This will force a re-initialisation.

Click "Save" to store and active settings.

7.3. DHCP Snooping

7.3.1. DHCP Overview

The DHCP protocol is used to dynamically allocate reusable network resources, such as IP address to devices connecting to the network. A typical process of DHCP to obtain an IP address is explained below.



DHCP Client sends DHCP DISCOVER message to the DHCP Server, if the Client does not receive a response from the server within a period of time, it will resend a DHCP DISCOVER message.

After receiving the DHCP DISCOVER message, the DHCP Server will assign resources (IP address for example) to the client, and then send a DHCP OFFER message to DHCP Client.

After receiving the DHCP OFFER message, the DHCP Client sends a DHCP REQUEST to ask for a server lease, and notifies the other servers that it has accepted this server to assign addresses.

After receiving a DHCP REQUEST, the server will verify whether resource can be allocated. If OK, it will send a DHCP ACK message; If not OK, it will send a DHCP NAK message. After receiving the DHCP ACK message, it will start using the source (ie IP Address) which the server has assigned it. If it received a DHCP NAK, the Client will resend a DHCP DISCOVER message.

7.3.2. About DHCP Snooping

The addresses assigned to DHCP clients on insecure ports can be carefully controlled using the dynamic bindings registered within DHCP Snooping. DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.

Command Usage

Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or firewall **When DHCP snooping** is enabled globally and enabled on a VLAN interface, DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped

Table entries are only learned from trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.

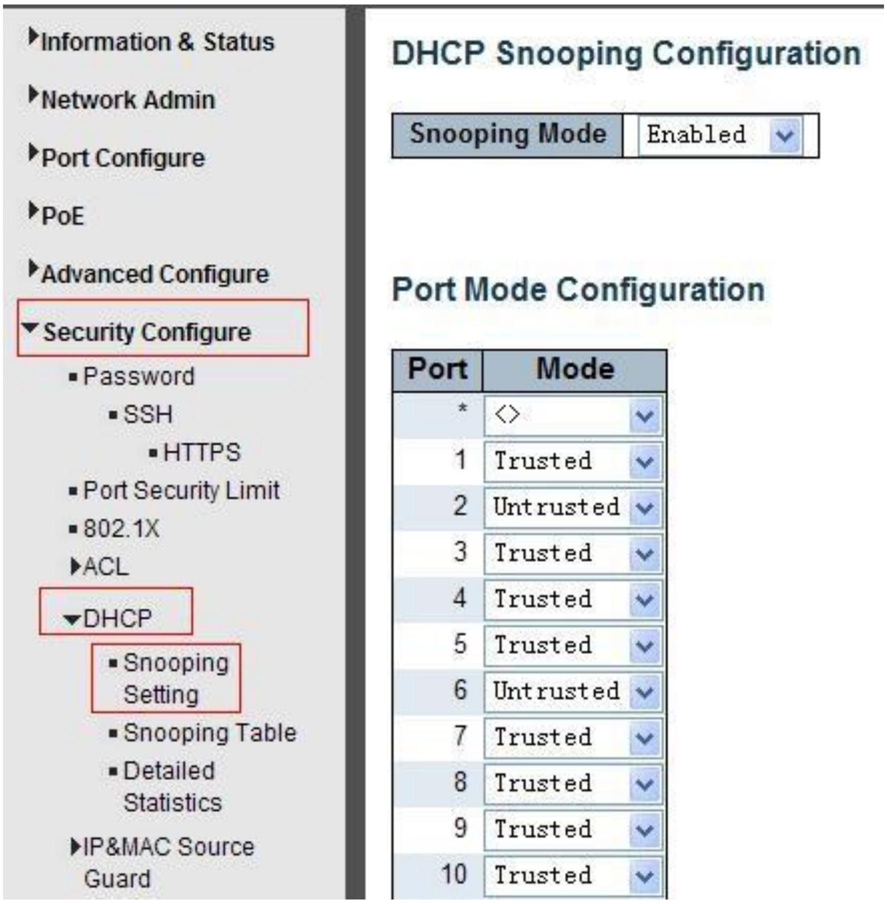
When DHCP snooping is enabled, DHCP messages entering an untrusted interface are

filtered based upon dynamic entries learned via DHCP snooping.
If a DHCP packet from a client passes the filtering criteria, it will only be forwarded to trusted ports in the same VLAN

If a DHCP packet is from the server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.
If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

7.3.3. Configuring DHCP Snooping

After clicking "Security Configure">"DHCP ">"Snooping Setting", the following screen will appear.



DHCP Snooping Configuration

Snooping Mode: Enabled

Port Mode Configuration

Port	Mode
*	<>
1	Trusted
2	Untrusted
3	Trusted
4	Trusted
5	Trusted
6	Untrusted
7	Trusted
8	Trusted
9	Trusted
10	Trusted

Figure 7-3 DHCP Snooping Configuration Screen

Object	Description
DHCP Snooping Mode	Click the drop-down menu to enable or disable DHCP Snooping
Port Mode	Indicates the DHCP snooping port mode. Possible port modes are: **Trusted**: Configures the port as trusted source of the DHCP messages. **Untrusted**: Configures the port as untrusted source of the DHCP messages.

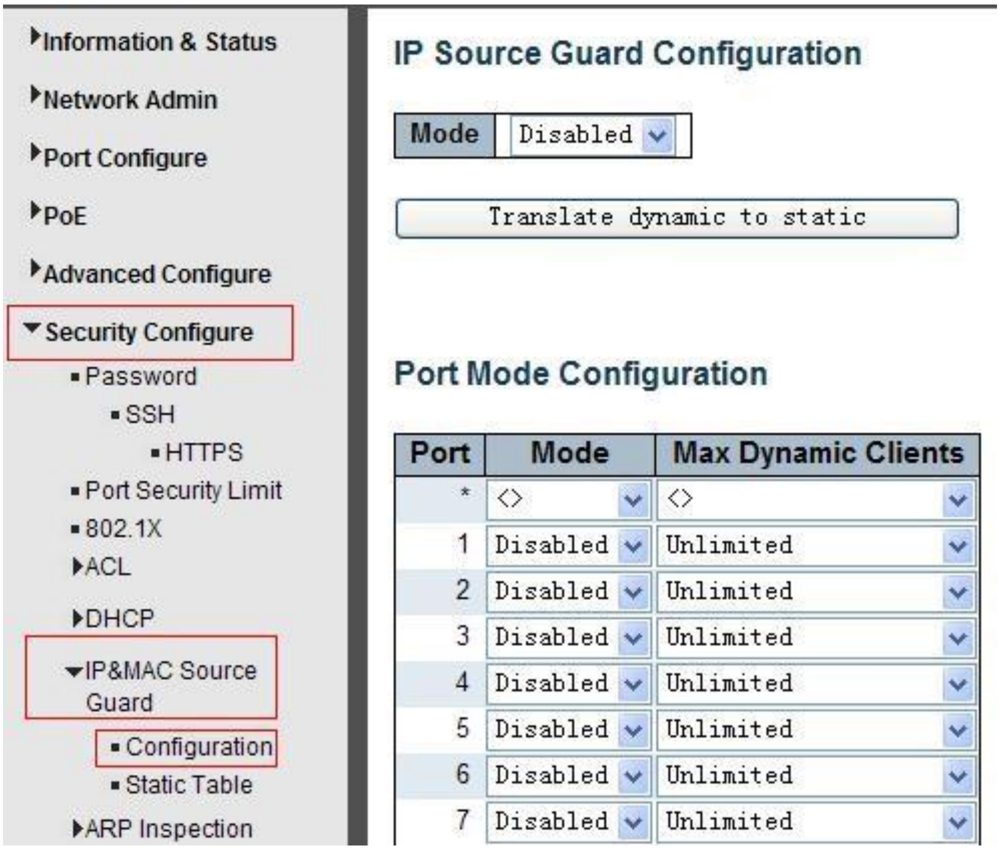
Click "Save" to store and active settings.

7.4. IP&MAC Source Guard

IP&MAC Source Guard is a secure feature used to restrict IP traffic on DHCP untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

7.4.1. Port Configuration

In this page, user can make IP&MAC Source Guard Port Configuration. After clicking "Security Configure">"IP & MAC Source Guard">"Configuration", the following screen will appear.



IP Source Guard Configuration

Mode: Disabled

Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	<>	<>
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited

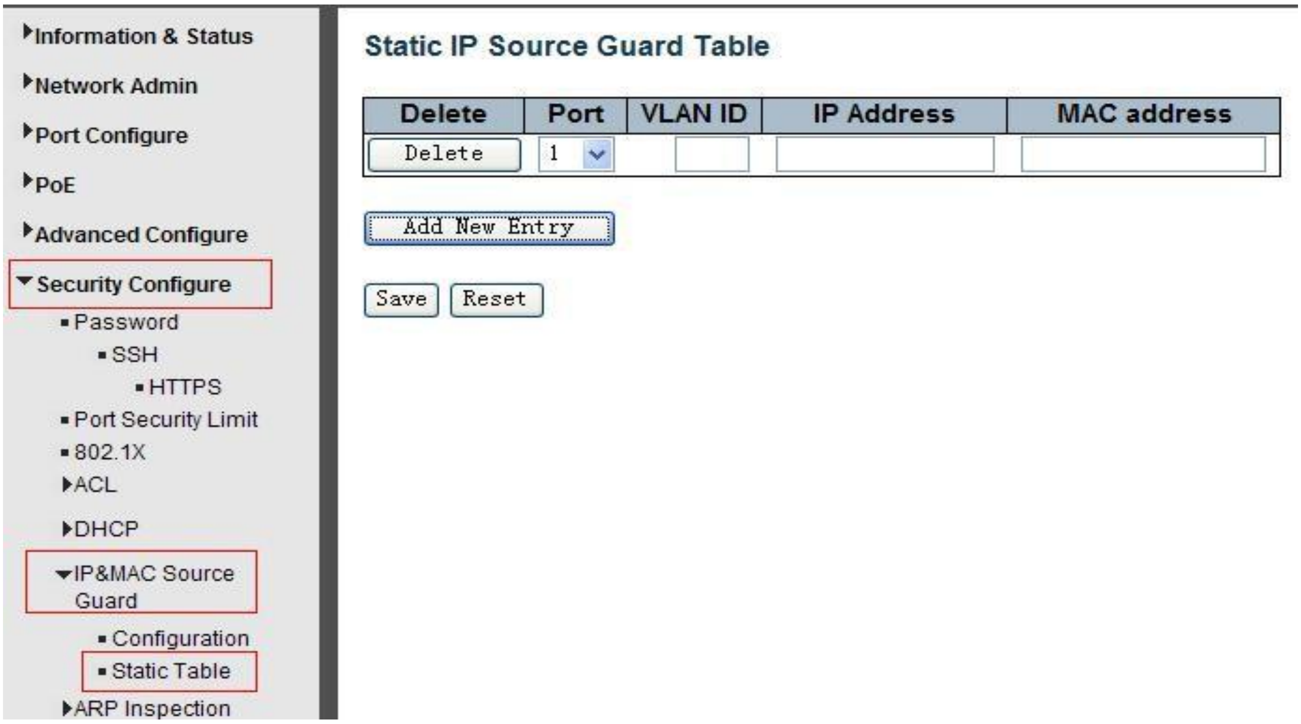
Figure 7-4 IP&MAC Guard- Port

Object	Description
Global Mode	Click the drop-down menu to enable or disable Global IP&MAC Source Guard function
Port Mode	Click the drop-down menu to enable or disable the IP&MAC Source Guard function for corresponding port.
Max Dynamic Clients	Click the drop-down menu to select Max Dynamic Clients. Available options: Unlimited, 0, 1, 2.

Click "Save" to store and active settings.

7.4.2. Static Table

In this page, a network manager can manually set a Static Table based on an IP&MAC address to control the port. After clicking on "Security Configure">"IP&MAC Source Guard">"Static Table", the following screen will appear.



Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address
Delete	1			

Figure 7-4-2 Static Table Configuration Screen

Object	**Description**
Port	Click the drop-down menu to select which port should be fixed.
VLAN	Type VLAN ID that should be fixed to
IP Address	Type IP Address that should be fixed to
MAC Address	Type Mac Address that should be fixed to

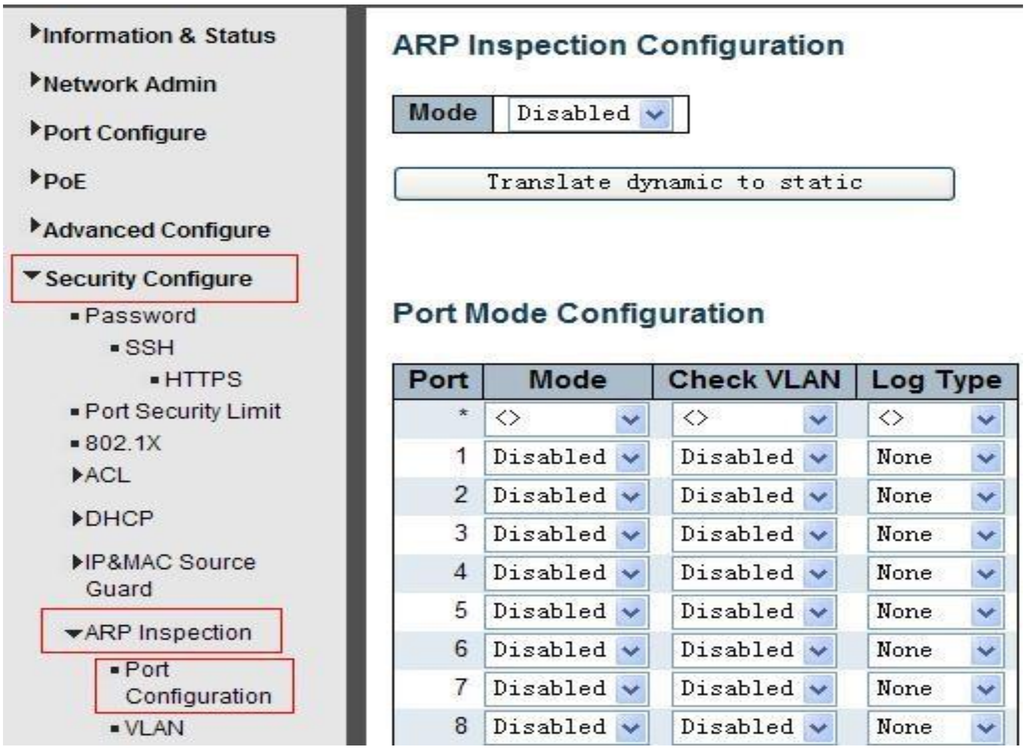
Click "Add New Entry" button to create a new record. Click "Save" to store and active settings.

7.5. ARP Inspection

Dynamic ARP Inspection (DAI) is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through but, a Dynamic ARP prevents the untrusted ARP packets based on the DHCP Snooping Database. This page provides ARP Inspection related configuration.

7.5.1. Port Configuration

User can make port configuration changes on this page. After clicking "Security Configure">"ARP Inspection">"Port Configuration", the following screen will appear.



ARP Inspection Configuration

Mode: Disabled

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
*	<>	<>	<>
1	Disabled	Disabled	None
2	Disabled	Disabled	None
3	Disabled	Disabled	None
4	Disabled	Disabled	None
5	Disabled	Disabled	None
6	Disabled	Disabled	None
7	Disabled	Disabled	None
8	Disabled	Disabled	None

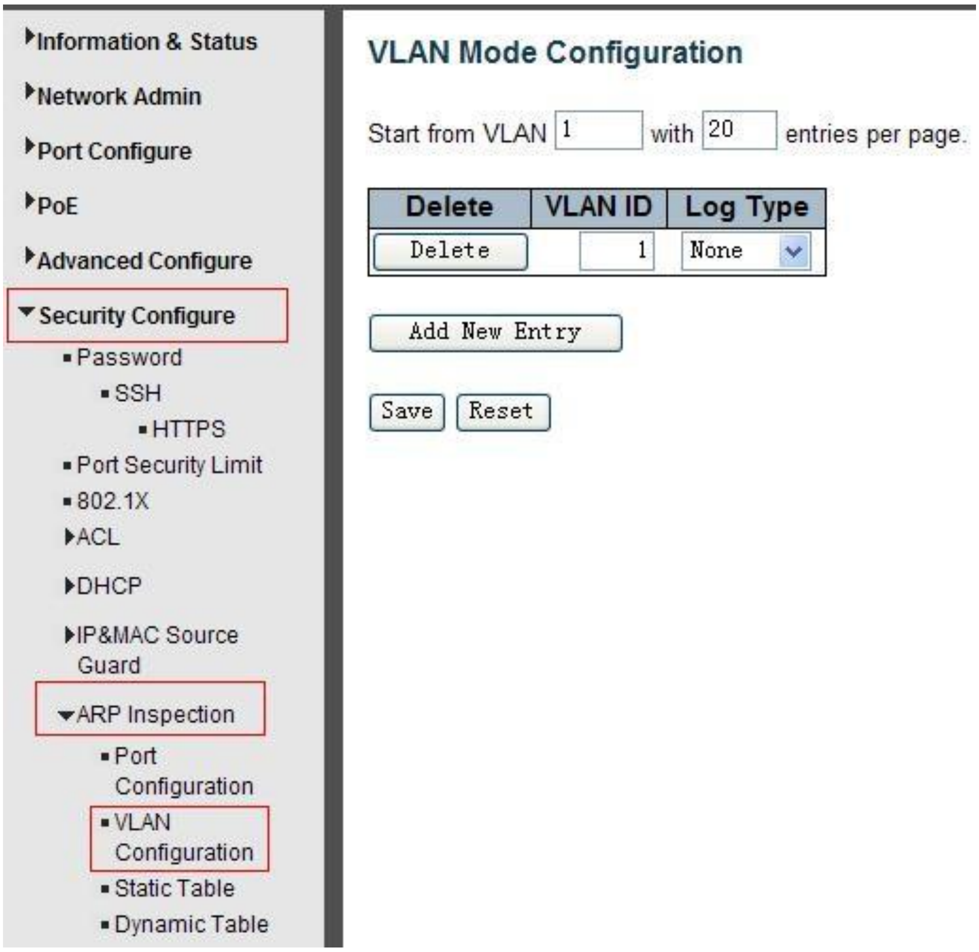
Figure 7-5-1 ARP Inspection Port Configuration Screen

Object	Description
Global Mode	Click on the drop-down menu to enable or disable Global ARP Inspection
Port Mode	Click on the drop-down menu to enable or disable port-based ARP Inspection
Check VLAN	If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are: Enabled: Enable check VLAN operation. Disabled: Disable check VLAN operation.
Log Type	Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types: None: Log nothing. Deny: Log denied entries. Permit: Log permitted entries. ALL: Log all entries.

Click "Save" to store and active settings.

7.5.2. VLAN Configuration

After clicking on "Security Configure">"ARP Inspection">"VLAN Configuration", the following screen will appear.



VLAN Mode Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Log Type
Delete	1	None

Figure 7-5-2 ARP Inspection VLAN Configuration Screen

Object	Description
VLAN ID	Indicates the ID of this particular VLAN
Log Type	Click drop-down menu to enable or disable port-based ARP Inspection. Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting. Possible types are: None: Log nothing. Deny: Log denied entries. Permit: Log permitted entries. ALL: Log all entries.

Click "Add New Entry" button to create a new record of VLAN configuration. Click **"Save" to store and active settings.**

7.5.3. Static Table

The Network Manager can manually configure the ARP Inspection Static Table to control a port. After clicking on "Security Configure">"ARP Inspection">"Static Table", the following screen will appear.

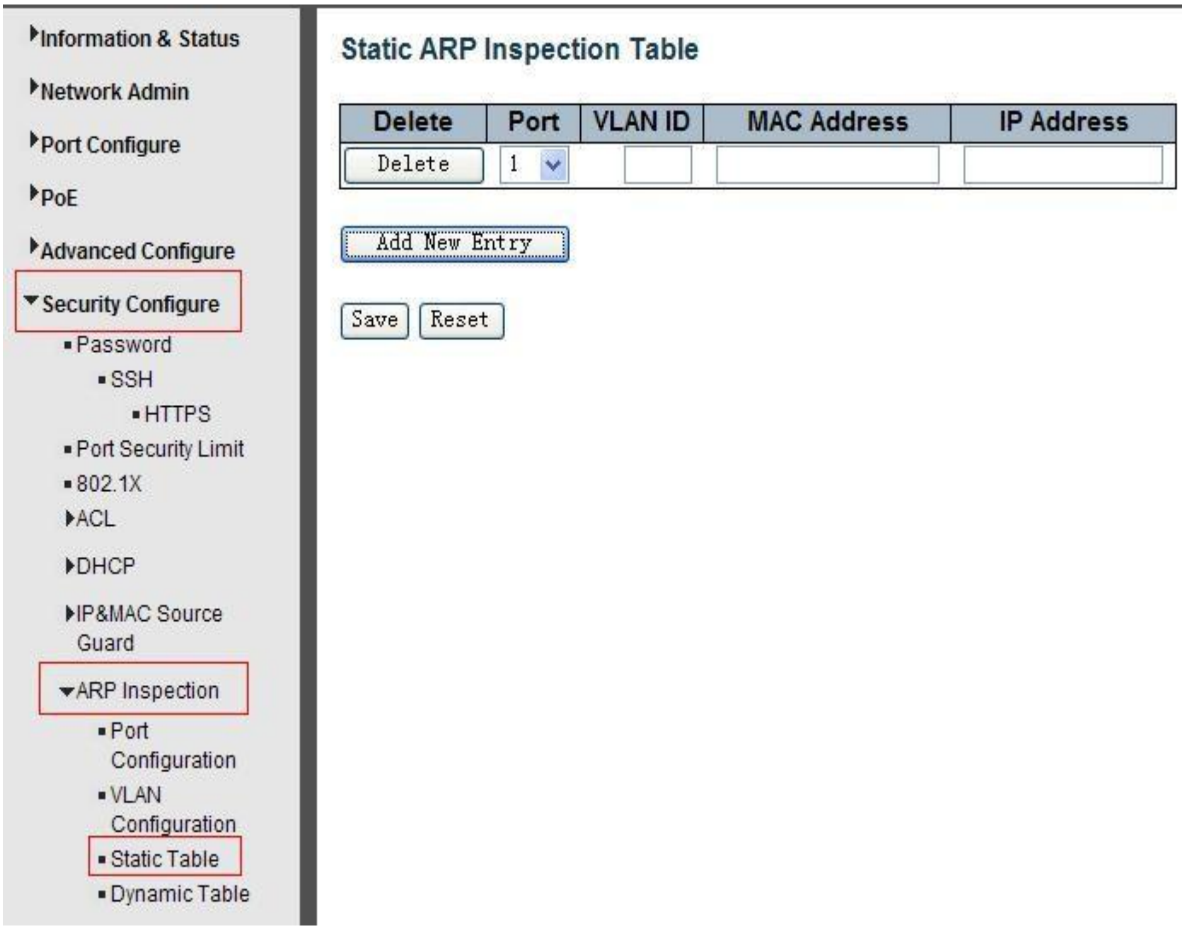


Figure 7-5-3 Static Table Configuration Screen

Object	Description
Port	Click drop-down menu to select which port should be fixed.
VLAN	Type VLAN ID that should be fixed to
IP Address	Type IP Address that should be fixed to
MAC Address	Type Mac Address that should be fixed to

Click "Add New Entry" button to create a new record.

Click "Save" to store and active settings.

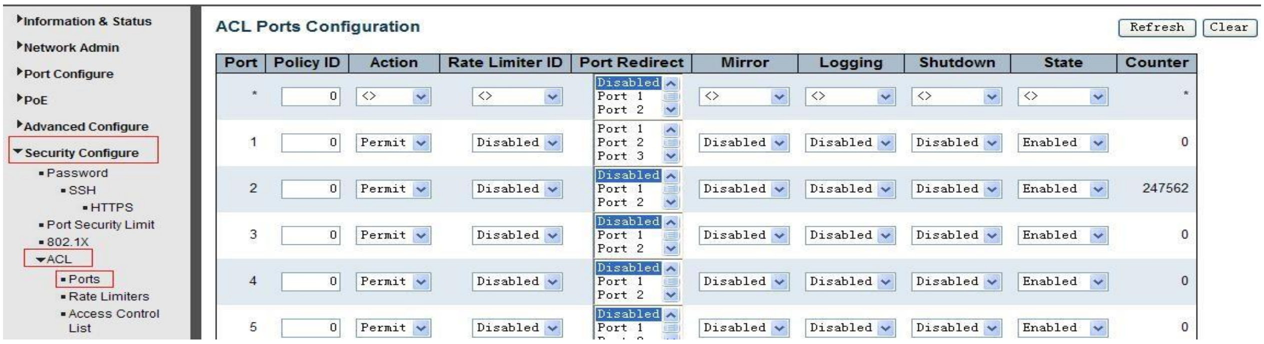
7.6. ACL

ACL is an acronym for **Access Control List**. It is the list table of ACEs (Devices Allowed to Connect to the network) , containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritised for the various situations. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and are similar to firewalls.

7.6.1. ACL Ports Configuration

After clicking "Security Configure">"ACL">"Ports", following screen will appear.



ACL Ports Configuration

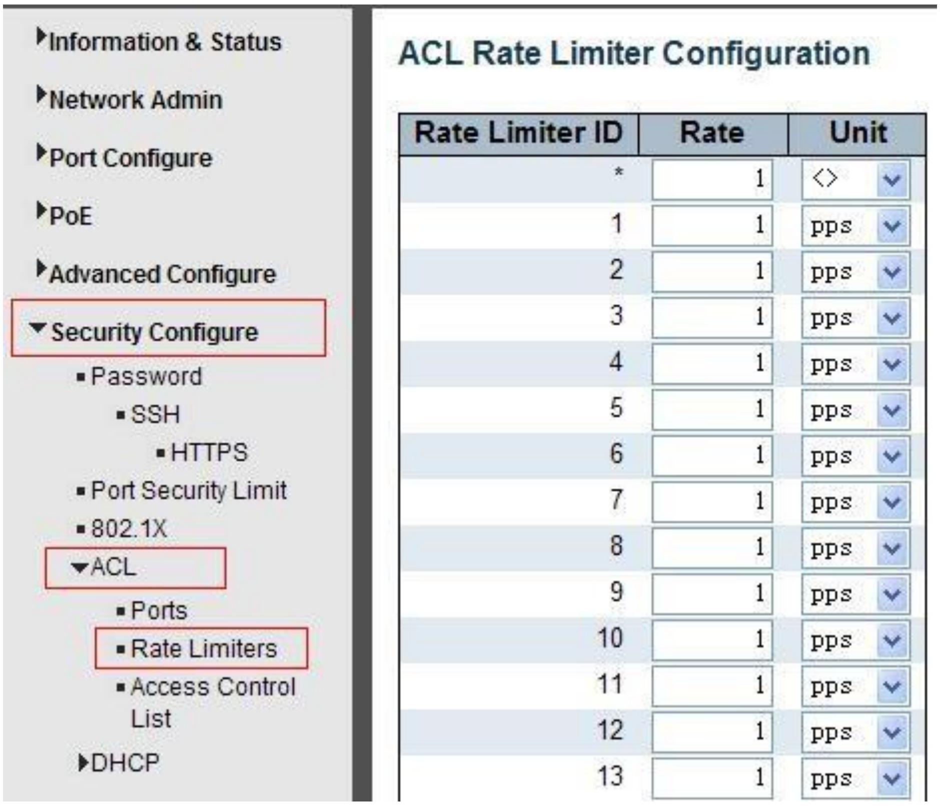
Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Port 1 Port 2 Port 3	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	247562
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled Port 1	Disabled	Disabled	Disabled	Enabled	0

Figure 7-6-1 ACL Ports

Object	Description
Action	There are 2 available options: Permit: that specific port allows data going through. Deny: that specific port forbid data going through.
Rate Limiter ID	Port’s fixed Rate Limiter ID, please go to Rate Limiter Configuration for more details.
Port Redirect	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".
Mirror	Specify the mirror operation of this port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled".
Logging	Enabled or Disabled Log
Shut Down	Specify the port shut down operation of this port. The allowed values are: Enabled: If a frame is received on the port, the port will be disabled. Disabled: Port shut down is disabled. The default value is "Disabled". Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).
State	Specify the port state of this port. The allowed values are: Enabled: To reopen ports by changing the volatile port configuration of the ACL user module. Disabled: To close ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled".
Counter	Counts the number of frames that match this rule.

7.6.2. Rate Limiter Configuration

The Network Manager can make ACL Rate limiter configuration in this page. After click "Security Configure">"ACL">"Rate Limiter", the following screen will appear.



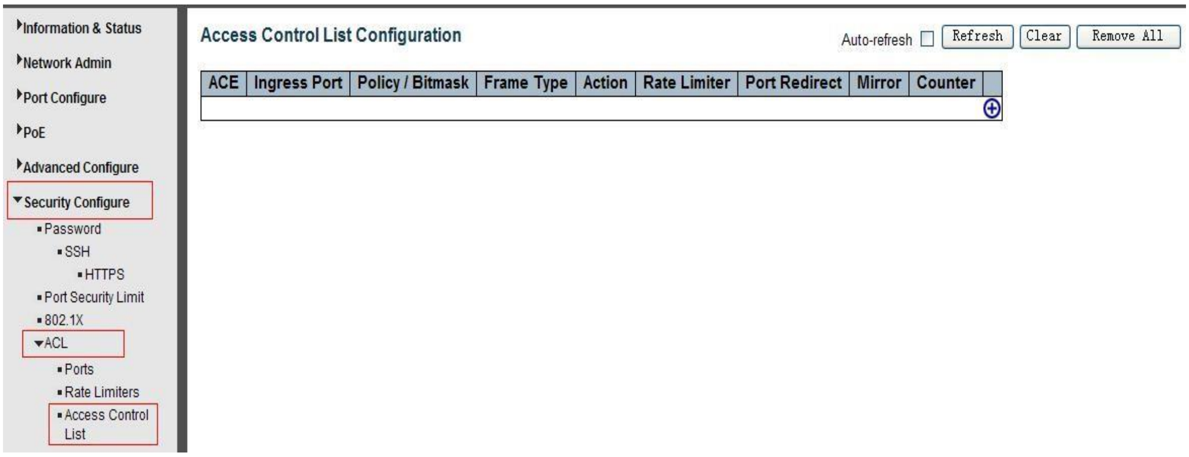
ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	1	<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps

Figure 7-6-2 ACL Rate Limiters Configuration Screen Click "Save" to store and active settings.

7.6.3. Access Control List Configuration

The Network Manager can make an Access Control List from this page . After clicking "Security Configure">"ACL">"Access Control List", the following screen will appear.



Access Control List Configuration

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
									⊕

Figure 7-6-3 Access Control List Configuration Screen Click the ⊕ button, to go to the Access Control List, and edit it.

7.7. IP Routing

In order to configure the switches IP Routing tables its necessary to enter the CLI (Command Line Interface) mode. See CLI Manual section 4.9 for more details or follow the CLI Commands below.

Router Configuration

Router Configuration Command:
ip routing interface vlan ip address ip route show ip interface brief - **show ip route**

7.7.1 ip routing

Command Description

ip routing [Enable the function]
no ip routing [Disable the function]

Parameter - N/A
Default - Host-only mode
Command Mode - Global Configuration Mode
Example to enable ip routing
Switch (config)#ip routing

7.7.2 interface vlan

Command Description - interface vlan<vlan_id>

Command	Command Parameters
vlan_id	Vlan port ID ranges: vlan1-vlan4094。

Command Mode - vlan_id Vlan port ID ranges: vlan1-vlan4094

Default - N/A

Command Mode - Global Configuration Mode, use command mode which also allows access to - vlan Port Configuration Mode

Example
Below command for VLAN1 Port Configuration Mode: switch(config)# interface vlan1
switch(config-if-vlan)#

7.7.3 ip address

Command Description
ip address <address><netmask> -]To add an address on a port]
no ip address – [To delete an IP address on a port]

Parameter	Parameter Command
Address	Vlan IP address
Netmask	subnet mask

Default -VLAN 1
Command Mode - VLAN Port Configuration Mode
Example for setting IP of VLAN 2

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip address 192.168.1.1 255.255.255.0
```

7.7.4 ip route

Command Description

ip route <v_ipv4_addr><v_ipv4_netmask><v_ipv4_gw><v_nhop_vlanid> [To add a static route]

no ip route [Delete a static route]

Parameter

Parameter	Parameter Command Mode
v_ipv4_addr	IP
v_ipv4_netmask	Subnet mask
v_ipv4_gw	Gateway
v_nhop_vlanid	next VLAN

Default - N/A

Command Mode - Global Configuration Mode

Example to set a static route

switch(config)# ip route 192.168.3.0 255.255.255.0 192.168.100.100 2

7.7.5 show ip interface

Command Description

show ip interface brief – To check the IP address of a port

Parameter - N/A

Default - N/A

Command Mode - Privilege mode

Example for checking IP Address of a port

```
Switch#show ip interface brief
```

7.7.6 show ip route

Command Description

show ip route [To check the static route]

Parameter - N/A

Default - N/A

Command Mode

Configure [Privilege mode]

Example for checking static route

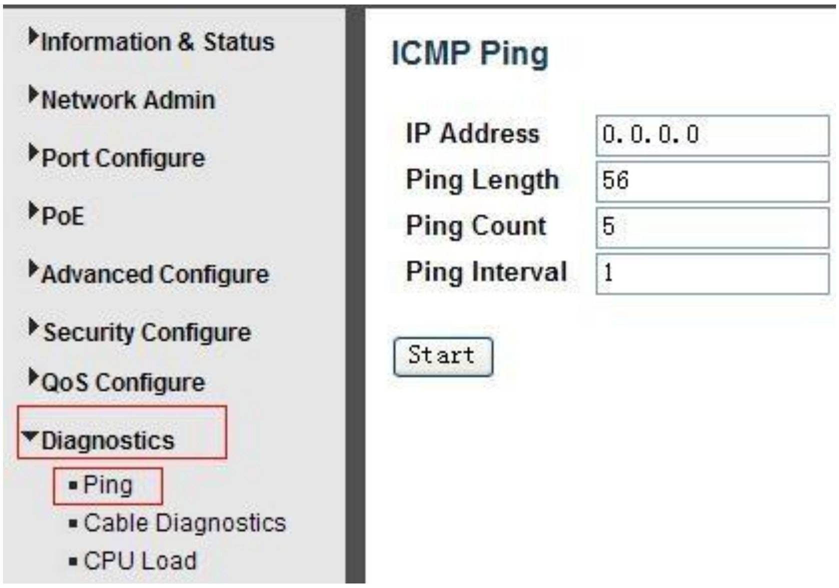
```
Switch#show ip route
```

8. Diagnostics

8.1. Ping Test

Ping is a program that can issue ICMP Echo packets to a defined IP address. The destination node should respond to the packets sent from the switch. Pings are used to troubleshoot IP connectivity issues.

After click "Diagnostics ">"Ping", followed screen appear.



ICMP Ping

IP Address: 0.0.0.0
Ping Length: 56
Ping Count: 5
Ping Interval: 1

Figure 8-1 Ping Test Screen

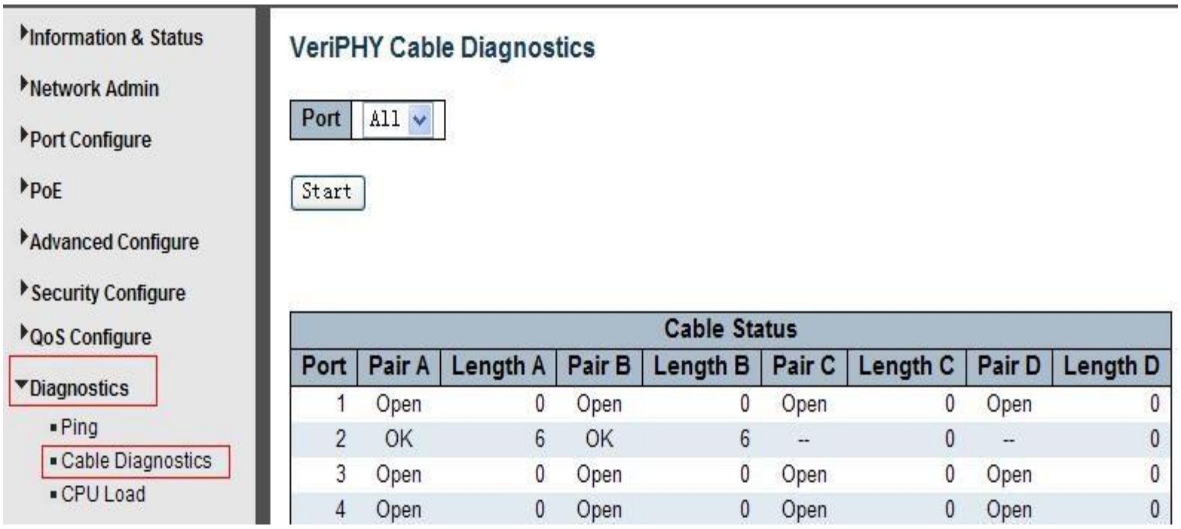
Object	Description
IP Address	estination IP Address that needed to Ping
Ping Length	a number between 1 and 1452. Default: 56
Ping Count	The times for inputting Ping IPv4 address or IPv6 address (Number of echo requests to send). User can input a number between 1 and 60.
Ping Interval	al time for Ping (Send interval for each ICMP packet)

Click "Start" button to start Ping testing.

8.2. Cable Diagnostics

The Cable Diagnostics performs tests on 10/100/1000BASE-T copper cables. These functions have the ability to identify the cable length and operating conditions, and to isolate a variety of common faults that can occur on the Cat5 twisted-pair cabling.

After selecting "Diagnostics ">"Cable Diagnostics", the following screen will appear.



VeriPHY Cable Diagnostics

Port: All

Cable Status

Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	Open	0	Open	0	Open	0	Open	0
2	OK	6	OK	6	--	0	--	0
3	Open	0	Open	0	Open	0	Open	0
4	Open	0	Open	0	Open	0	Open	0

Figure 8-2 Cable Diagnostics Screen Click "Start" button to start "Cable Diagnostics" testing

8.3. CPU Load

This page shows percent of CPU load. After click "Diagnostics">"CPU Load", followed screen will appear.

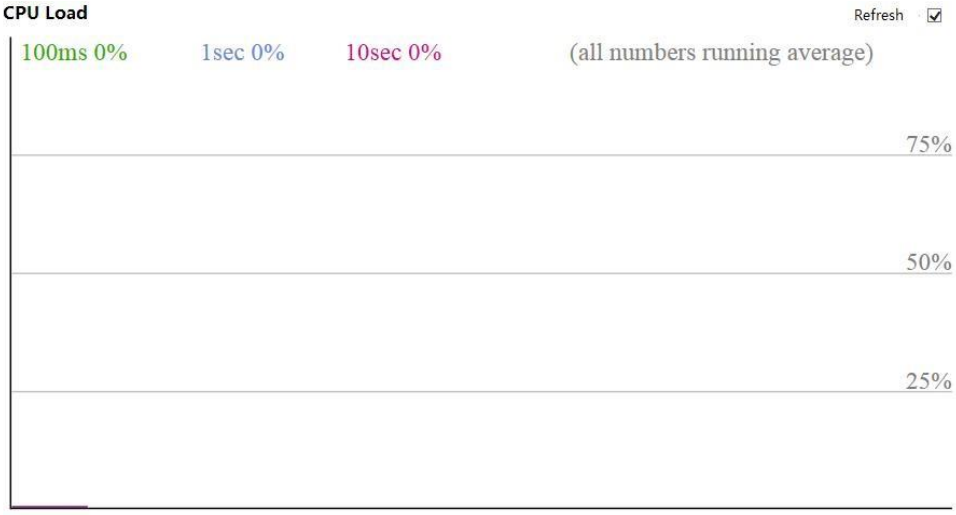
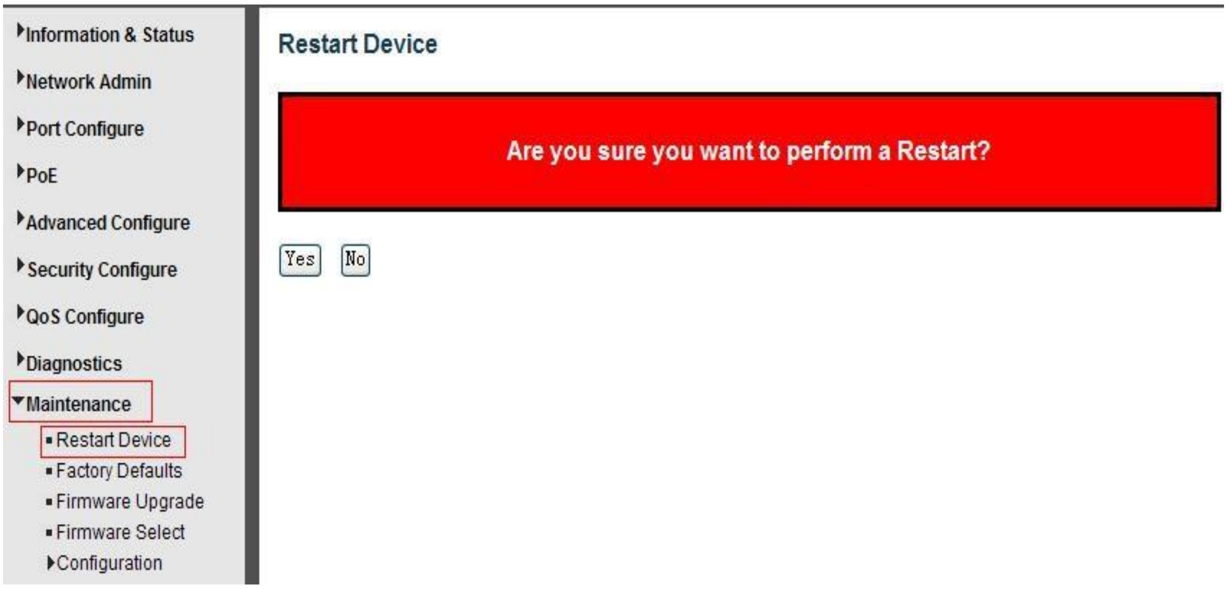


Figure 8-3 CPU Load Screen

9. Maintenance

9.1. Restart Device

This page is used to restart the switch. After clicking "Maintenance ">"Restart Device", the following screen will appear.



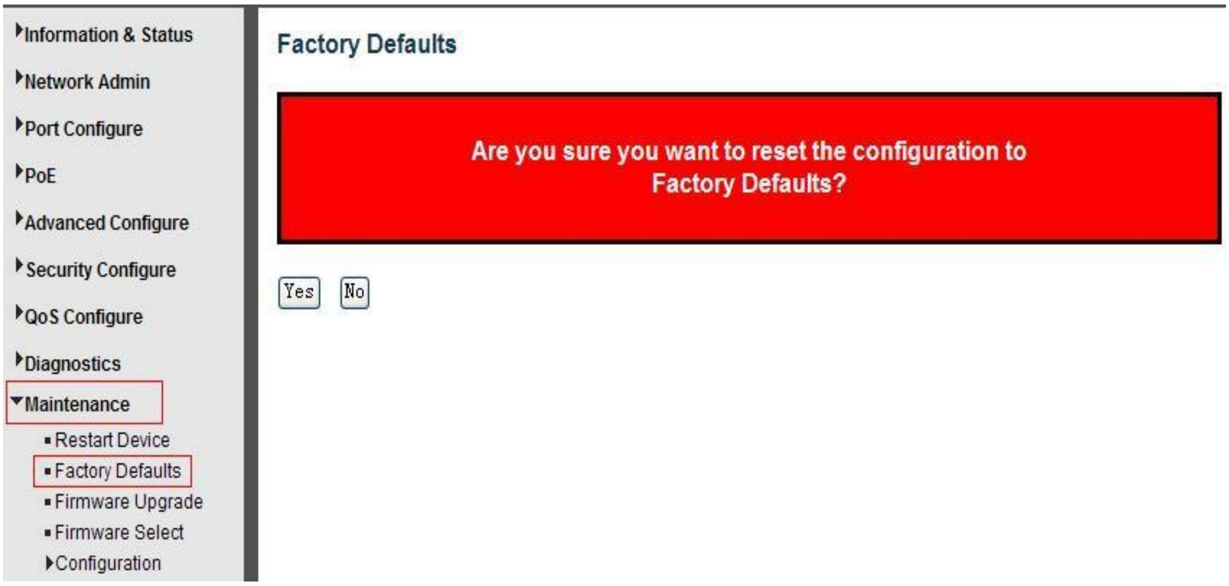
Restart Device

Are you sure you want to perform a Restart?

Please click "Yes" to restart the switch.

9.2. Factory Defaults

This page restores the switch back to its factory defaults. After clicking "Maintenance ">"Factory Defaults", the following screen will appear.



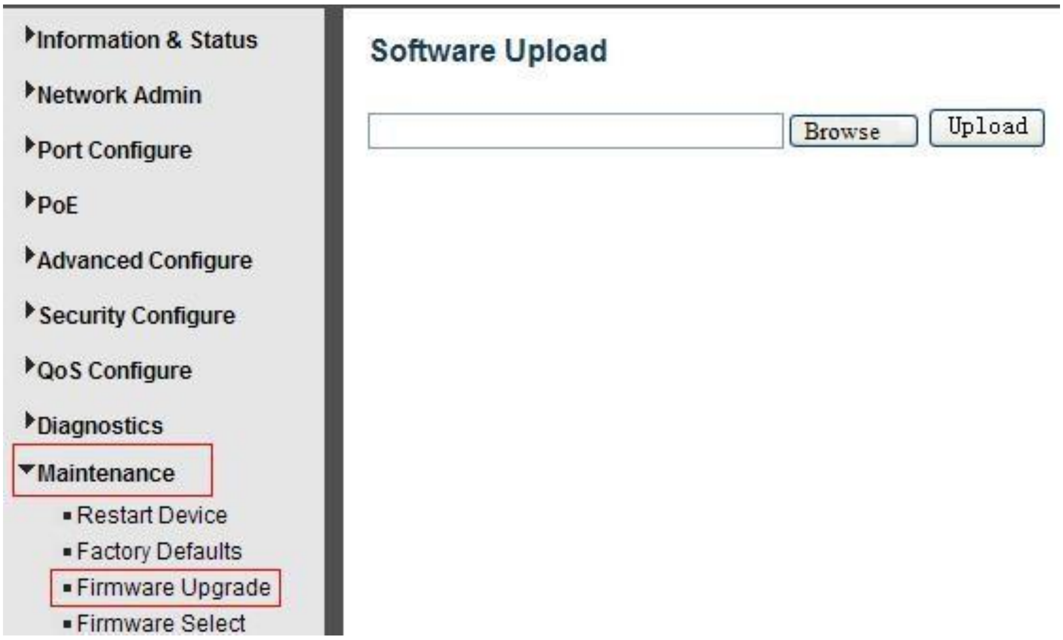
Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

Please click "Yes" to reset the configuration to Factory Defaults.

9.3. Firmware Upgrade

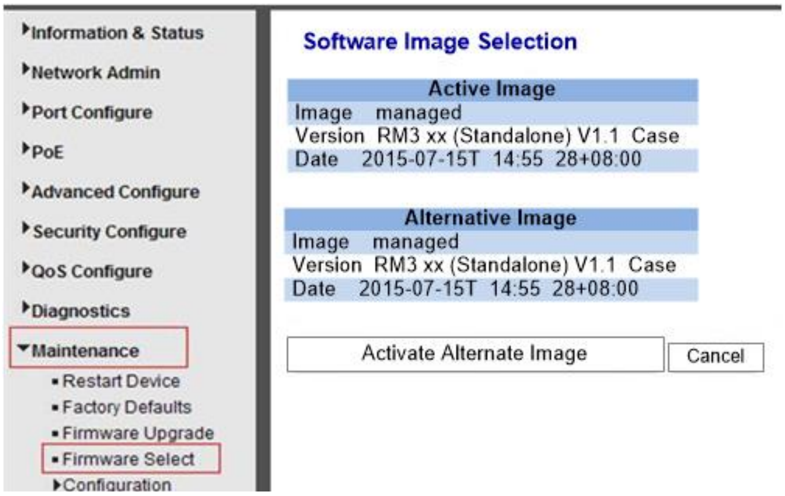
This page allows you to upgrade the system firmware. After clicking "Maintenance ">"Firmware Upgrade", followed screen will appear.



Please click "Browse" to select the firmware that needed to upgrade. And then click "Upload" to start upgrading.

9.4. Software Image Select

This page allows you to upgrade the system firmware. After clicking "Maintenance ">"Firmware Upgrade", followed screen will appear.



Software Image Selection

Active Image	
Image	managed
Version	RM3 xx (Standalone) V1.1 Case
Date	2015-07-15T 14:55 28+08:00

Alternative Image	
Image	managed
Version	RM3 xx (Standalone) V1.1 Case
Date	2015-07-15T 14:55 28+08:00

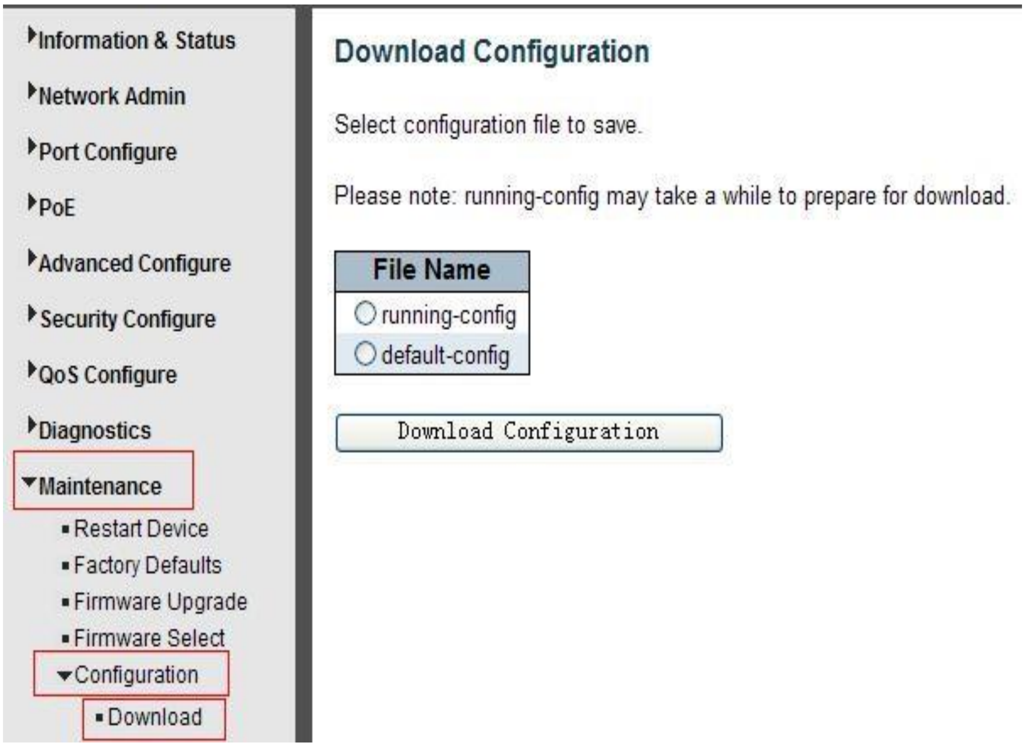
Please click ''Activate Alternate Image'' to select the firmware.

9.5. Firmware Select

In this page, user can download, upload, activated or delete configuration files.

9.5.1. Download Configuration File

After click "Maintenance ">"Download", followed screen will appear.



Download Configuration

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

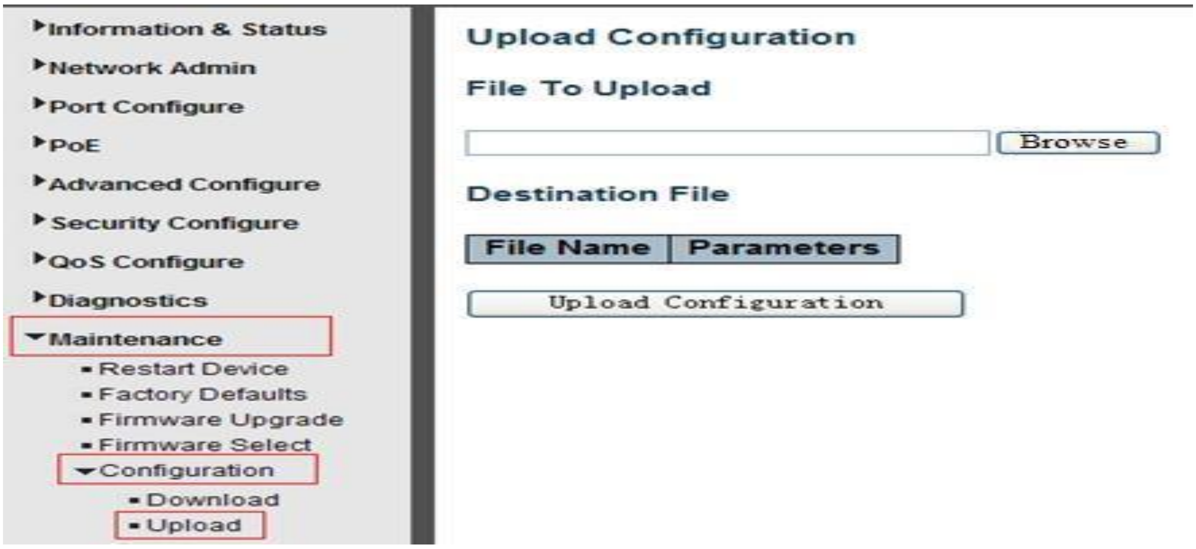
File Name
○ running-config
○ default-config

Download Configuration

Please choose a file and then click "Download Configuration" button to download.

9.5.2. Upload Configuration File

After clicking "Maintenance ">"Upload", the following screen will appear. Then user can upload Configuration File.



Upload Configuration

File To Upload

Browse

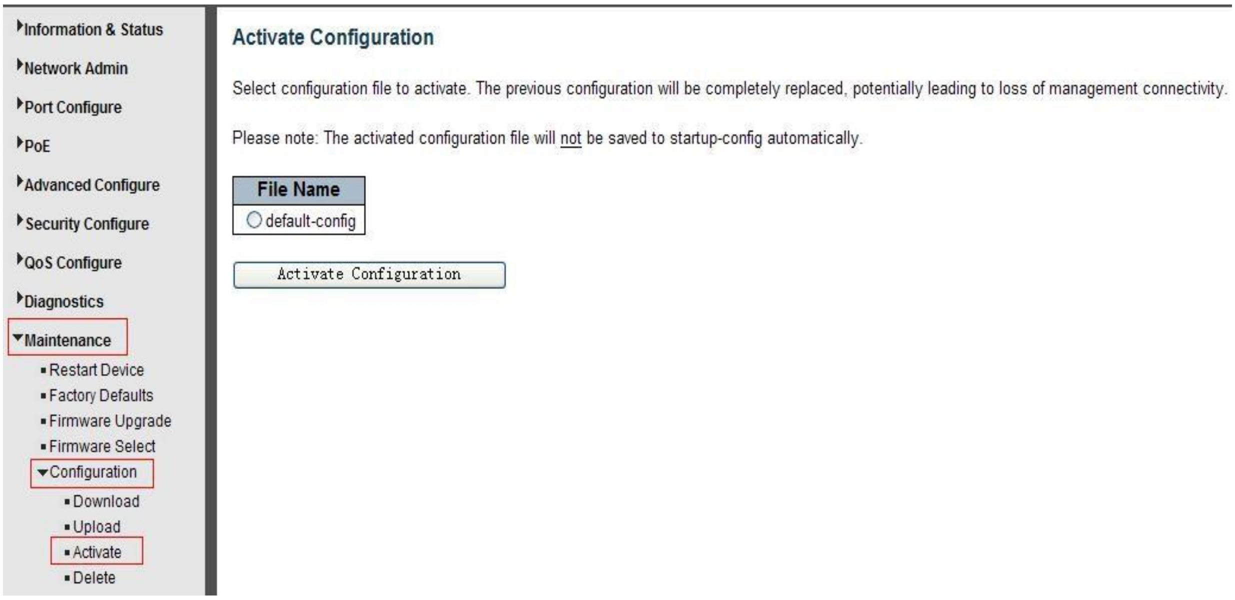
Destination File

File Name	Parameters

Upload Configuration

9.5.3. Activate Configuration

After click "Maintenance ">"Activate", followed screen will appear. Then user can activate Configuration File.



Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

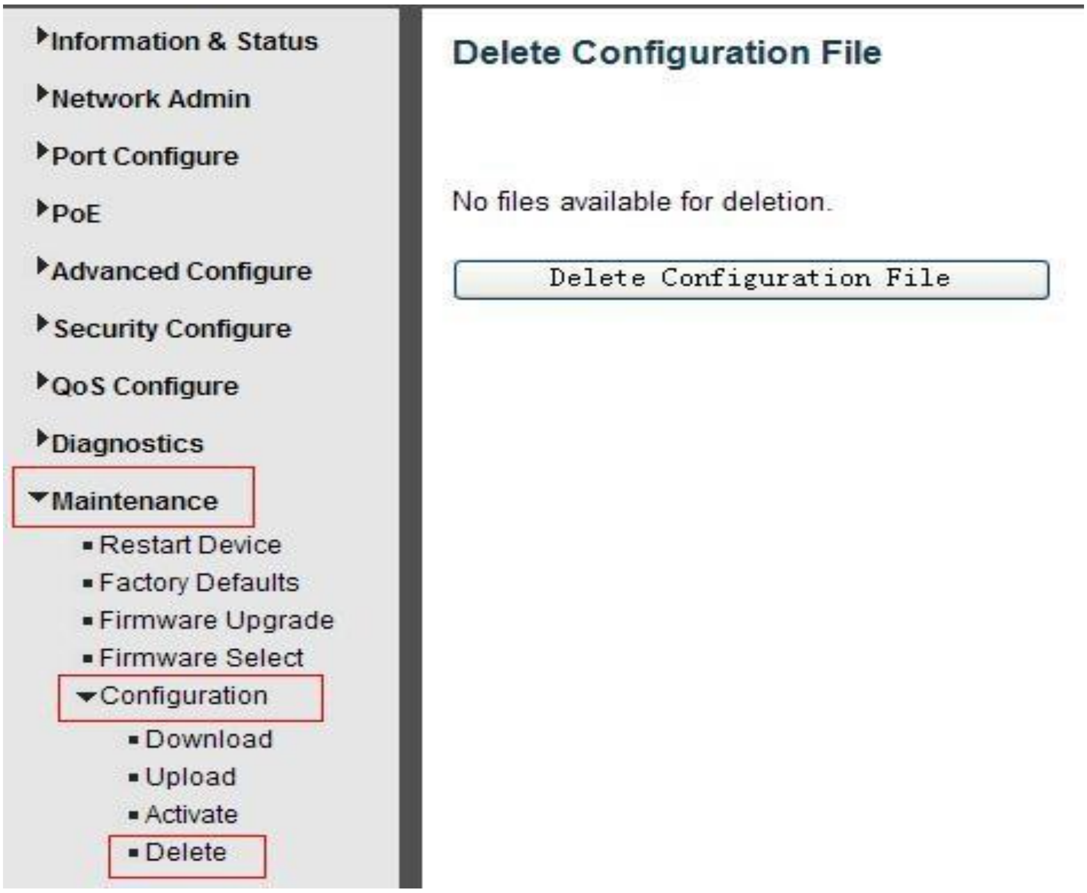
Please note: The activated configuration file will not be saved to startup-config automatically.

File Name
○ default-config

Activate Configuration

9.5.4. Delete Configuration File

After click "Maintenance ">"Delete", followed screen will appear. Then user can delete Configuration File.



Delete Configuration File

No files available for deletion.

Delete Configuration File

Appendices

Appendix 1　Terminology List

	Expression	Description
A	ARP（Address Resolution Protocol）	A protocol that converts an IP address to a physical address
	Auto-Negotiation	To automatically negotiate the working rate and duplex mode on both ends of the switch and other equipment
B	Broadcast Storm	Excessive broadcast frames are sent across the network via a single port. The response to forward information will stack up in the network, consume excessive network resources, or cause network timeouts
	Broadcasting	The forwarding of data to all nodes in the network
C	CoS（Class of Service）	The 802.1 p priority scheme. The CoS provides a way to add a priority label to the packet and divides the message into eight levels. Range of values: 0 ~ 7
D	DHCP（Dynamic Host Configuration Protocol）	The IP address, subnet mask, gateway and other information are distributed dynamically in the network
	DSCP（DiffServe Code Point）	In a six-bit domain encapsulated in the IP header, the message can be divided into 64 levels. Value range: 0 ~ 63
E	Ethernet	Ethernet USES a total line or star topology and supports a transmission rate of 10Mbps.The new version, called fast Ethernet, can be up to 100Mbps.
F	Flow Control	Flow control enables low-speed equipment to communicate with high speed devices. This kind of flow control is the way to suspend the bag through high speed port to match the speed of the high-speed port and the speed of the low- speed port
	Frame	A packet containing the header and tail information required for the physical medium layer.
	Full-Duplex	Using the IEEE802.3 x standard, you can simultaneously receive and send data operations in both directions at one time
H	Half-Duplex	Using the Backpressure standard, you can only receive or send a data operation in one direction at a time
I	IGMP （Internet Group Management Protocol）	The mechanism of establishing and maintaining the relationship between the host and three-layer multicast equipment is provided
	IEEE 802.1p	
	IEEE 802.1q	
Q	QoS（Quality of Service）	A technique used to solve problems such as network latency and congestion
T	Trunking	A group of ports is bundled together to form an aggregate group to increase the bandwidth and enhance the reliability of the connection
	ToS（Type of Service）	In an 8-bit domain encapsulated in the IP header, a message representing different priority characteristics is represented
U	UDP（User Datagram Protocol）	An unconnected, unreliable transport layer protocol
	UTP(Unshielded Twisted Pair)	There is no shielding media outside the double strand

Appendix 2 FAQ

1. Why do the web pages not display correctly sometimes?

A: Before accessing the switch with the WEB Browser, remove the cache and Cookies on the Browser. Otherwise, it may cause the pages to be displayed incorrectly.

2. Forgetting your Password?

A. If you forget your password you can initialise the switch restoring it to the factory settings. Press the button for 10s.The initial user name should be “root” and password “case” or on some models "admin" and password "system".

3. Can we configure by both the web browser and CLI?

A : Yes, both the web browser and CLI can be used ti configure the switch..

4. Unable to increase the bandwidth after configuring Trunking?

A: Please check if the information for setting port Trunking, is the same between ports for example it must include rate, duplex mode and VLAN etc..

5. How to deal with the problem of partial ports of switch?

A: If some ports are blocked on the switch, it may be a network cable fault, a network card failure or a switch port failure, users can test by following steps:

Test the failure:

1. The connection between the computer and switch ports remains unchanged - replace the network cables.
2. The network cable and switch port remains unchanged - change the computer;
3. The network cable and computer remain unchanged - replace the switch ports.
4. If you confirm that the problem is caused by a switch port failure, please contact your local Case Communications partner for maintenance.

6. What order do the port self-adaptive status detection operate in?

A: Port of state testing was conducted in the following order: 1000Mbps full-duplex, 100Mbps full-duplex, 100Mbps half-duplex, 10Mbps full-duplex, 10 Mbps half-duplex. And automatically connect with maximum speed.

Case Communications

www.casecomms.com

support@case.uk.com

Unit12E
Norths Estate
Old Oxford Road
Piddington
High Wycombe
Bucks HP14 3BE
Great Britain
+44 (0) 1494 880 240