



SGX368244M

36-Port 10/100/1G/10G
Managed Switch

User's Manual
v1.00

© 2022
VERSITRON, Inc.
83 Albe Drive / Suite C
Newark, DE 19702
www.versitron.com

Copyright © VERSITRON, Inc. All rights reserved. All brand and product names are trademarks or registered trademarks of their respective companies.

PROPRIETARY DATA

All data in this manual is proprietary and may not be disclosed, used or duplicated, for procurement or manufacturing purposes, without prior written permission by **VERSITRON**.

VERSITRON LIFETIME WARRANTY

All VERSITRON products are covered by a **Lifetime Warranty** against defects in materials and workmanship. This coverage is applicable to the original purchaser and is not transferable.

We repair, or at our option, replace parts/products that, during normal usage and operation, are proven to be defective during the time you own the products, provided that said products and parts are still manufactured and/or available. Such repair/replacement is subsequent to receipt of your product at our facility and our diagnostic evaluation and review of the unit. Advance replacements are not provided as part of the warranty coverage.

This warranty does not cover damage to products caused by misuse, mishandling, power surges, accident, improper installation, neglect, alteration, improper maintenance, or other causes which are not normal and customary applications of the products and for which they were not intended. No other warranty is expressed or implied, and VERSITRON is not liable for direct, indirect, incidental or consequential damages or losses.

In the unlikely event a warranty issue should arise, simply contact us at 302-894-0699 or 1-800-537-2296 or via email at fiberlink@versitron.com to obtain a Return Material Authorization (RMA) number, along with instructions for returning your product.

About This Manual

Copyright

Copyright © 2022 VERSITRON, Inc. All rights reserved.

The products and programs described in this manual are licensed products of VERSITRON, Inc. This manual contains proprietary information protected by copyright, and this manual and all accompanying hardware, software and documentation are copyrighted. No parts of this manual may be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of VERSITRON, Inc.

Purpose

This manual gives specific information on how to operate and use the management functions of the SGX368244M.

Audience

The Manual is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

Warranty

See the VERSITRON, Inc. warranty statement.

Disclaimer

VERSITRON, Inc. does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. VERSITRON, Inc. disclaims liability for any inaccuracies or omissions that may have occurred. Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of VERSITRON, Inc.. VERSITRON, Inc. assumes no responsibility for any inaccuracies that may be contained in this User's Manual. VERSITRON, Inc. makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and /or to the products described in this User's Manual, at any time without notice.

TABLE OF CONTENTS

1. Introduction	5
1.1 Overview.....	5
1.2 Web Management Login.....	5
1.3 Web-based User Interface	6
1.4 Main Menu.....	6
2. Network Management.....	7
2.1 IP Configuration.....	7
2.2 SNTP Configuration.....	8
2.3 SNMP Configuration.....	8
2.3.1 SNMP System Configuration	9
2.3.2 SNMP Trap Configuration	9
2.4 System Log Configuration.....	10
3. Port Configure.....	11
3.1 Port Configuration	11
3.2 Link Aggregation.....	12
3.2.1 Static Aggregation.....	12
3.2.2 LACP Aggregation	13
3.3 Port Mirroring	14
3.4 Thermal Protection Configuration.....	16
4. PoE Configuration (if applicable).....	17
4.1 PoE Setting	17
4.2 PoE Status	18
5. Advanced Configure.....	19
5.1 VLAN.....	19
5.2 Port Isolation	22
5.2.1 Port Group	22
5.2.2 Port Isolation.....	23
5.3 STP	23
5.3.1 STP Bridge Settings	23
5.3.2 STP Bridge Port.....	24

5.4 MAC Address Table	26
5.5 IGMP Snooping.....	27
5.5.1 Basic Configuration.....	27
5.5.2 IGMP Snooping VLAN Configuration	28
5.6 ERPS	29
5.7 LLDP	31
5.8 Loop Protection.....	32
6. QoS Configure	33
6.1 QoS Port Classification	33
6.2 Port Policing	34
6.3 Storm Control Configuration	35
7. Security Configure.....	36
7.1 Password.....	36
7.2 802.1X	36
7.3 DHCP Snooping.....	38
7.3.1 DHCP Overview	38
7.3.2 About DHCP Snooping.....	38
7.3.3 DHCP Snooping Configure	39
7.4 IP&MAC Source Guard	40
7.4.1 Port Configuration	40
7.4.2 Static Table.....	41
7.5 ARP Inspection	42
7.5.1 Port Configuration	42
7.5.2 VLAN Configuration	43
7.5.3 Static Table.....	44
7.6 ACL	45
7.6.1 ACL Ports Configure.....	45
7.6.2 Rate Limiter Configuration	47
7.6.3 Access Control List Configuration	47
8. Diagnostics.....	48
8.1 Ping Test	48
8.2 Cable Diagnostics.....	49
8.3 CPU Load.....	49

9. Maintenance.....	50
9.1 Restart Device.....	50
9.2 Factory Defaults.....	50
9.3 Firmware Upgrade.....	51
9.4 Firmware Select.....	51
9.5 Firmware Select.....	52
9.5.1 Download Configuration File.....	52
9.5.2 Upload Configuration File.....	53
9.5.3 Activate Configuration	53
9.5.4 Delete Configuration File.....	54

1. Introduction

1.1 Overview

Thank you for purchasing the SGX368244M managed switch. The software functions can be managed, configured, and monitored via the embedded Web-based (HTML) interface. Using a standard browser, you can manage the switch at any remote site in the network.

1.2 Web Management Login

Open a web browser on your PC and input the switch's default IP address of 192.168.2.1.

When the login window appears, please enter the default username: **admin**, and password: **system**. Then click OK to login.



Figure1-1 Login Window

1.3 Web-based User Interface

After entering the username and password, the main screen appears as follows in Figure1-2.

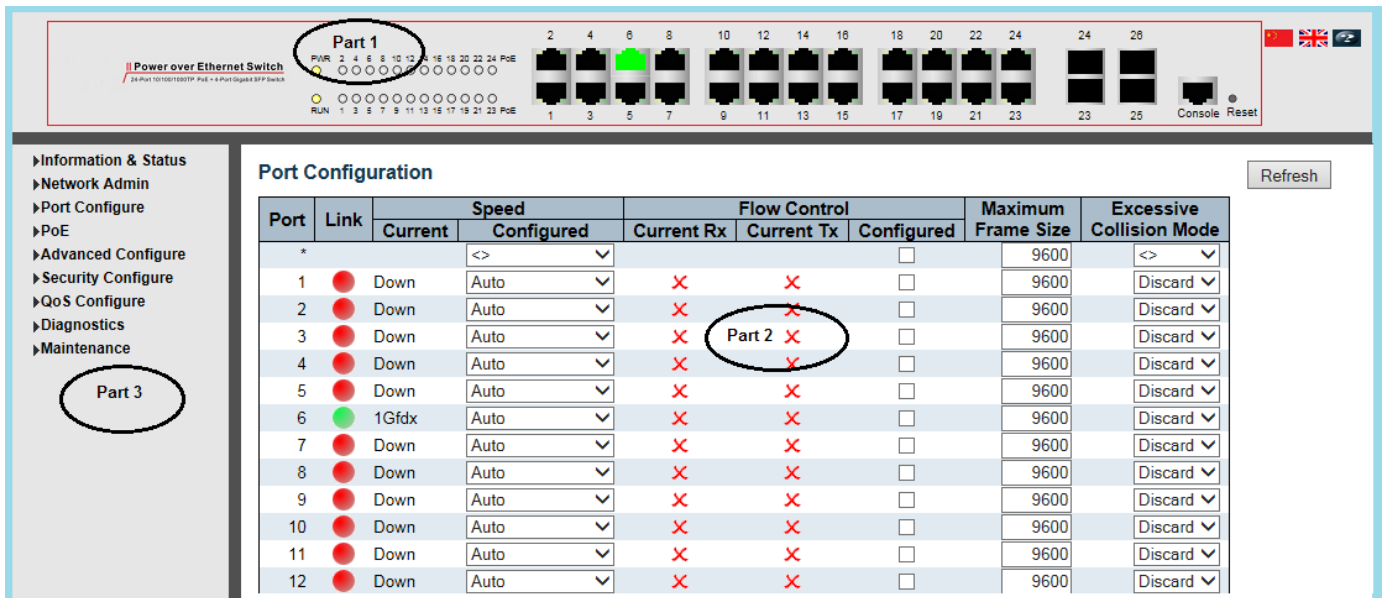


Figure1-2 Web management Main Page interface

This Main Page interface includes mainly 3 parts. Here is description:

Part	Description
Part 1	Panel display; Port indicators, including PoE (if applicable) and Link working status; Language selection button; Help document
Part 2	Main Screen, showing configuration details
Part 3	The Main Menu, lets you access all the commands and statistics

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

: 100Mbps linked ;
 : 1000Mbps linked ;
 : No link

1.4 Main Menu

Using the onboard Web agent, you can define system parameters, manage and control the switch and all of its ports, or monitor network conditions. Via the Web-Management, the administrator can set up the switch by selecting the functions from those listed in the Main Menu. Following is short description:

- Information & Status** - Users can check switch information and working status under this menu.
- Network Admin** - Users can check and configure related features of network under this menu.
- Port Configure** - Users can check and configure specification of ports under this menu.
- PoE** - Users can check and configure related features of Power-over-Ethernet (PoE) under this menu. (if applicable)
- Advanced Configure** - Users can check and configure L2 advanced features under this menu.
- Security Configure** - Users can check and configure security features of the switch under this menu.
- Qos Configure** - Users can check and configure Qos features of the switch under this menu.

2. Network Management

2.1 IP Configuration

Note: The default IP address of switch is 192.168.2.1. The default subnet mask is 255.255.255.0 (24)

Click "Network Admin" > "IP", the screen will show as:

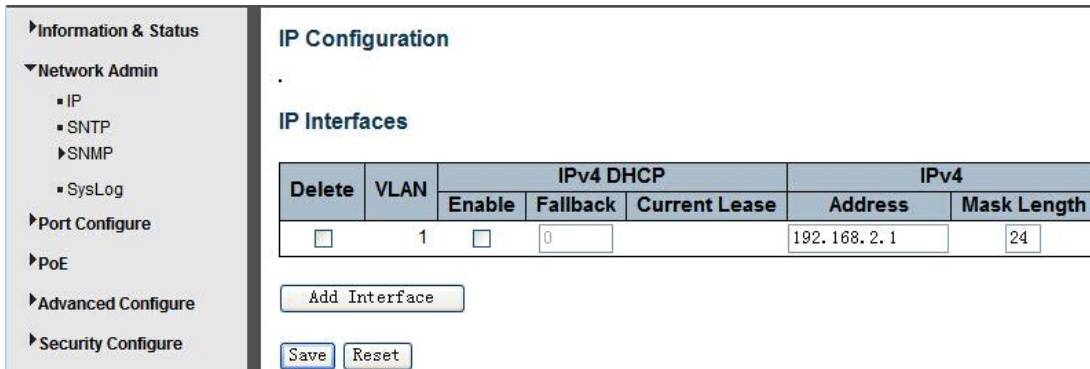


Figure 2-1 IP Configuration Screen

Following is description detail about IP configuration:

Name	Description
VLAN	VLAN for access and management of switch
IPv4 DHCP	<ul style="list-style-type: none">If enable, it means that VLAN port start IPv4 DHCP client, to dynamically get IPv4 addresses of 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	<ul style="list-style-type: none">Address: static IPv4 address entered by user.Mask Length: static IPv4 subnet mask entered by user.

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

Note: The switch has only VLAN1 by default. If the user needs to use another VLAN for switch management, please first add a VLAN in the VLAN module, and add the relevant port to the VLAN.

2.2 SNTP Configuration

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

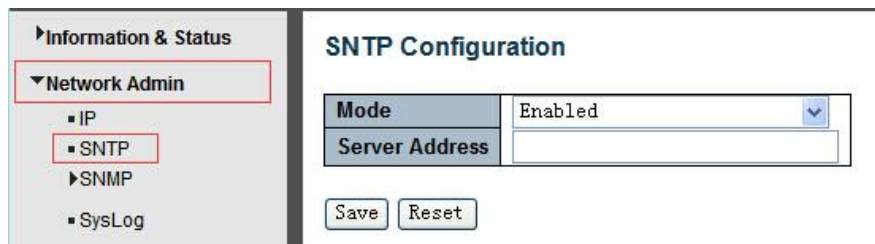


Figure 2-2 SNTP Setting Screen

Configuration object and description is:

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

After configuration is set, please click "Save" to save the settings.

2.3 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 switch supports SNMPv1, v2c. Different versions of SNMP provide different security levels for management stations and network devices.

In SNMP's v1 and v2c, it uses the "Community String" for user authentication. That string is similar to password function. The SNMP application of remote user and SNMP of the switch must use the same community string. SNMP packets of any unauthorized sites will be ignored (discarded).

"Community String" by default for switch's SNMPv1 and v2c access management is:

1. `public` – allow authentication management station to read MIB objects.
2. `private` – allow authentication management station to read, write and edit MIB objects.

Trap

Used by the agent 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, switch create trap information and send then to receiver or network admin. 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 switch uses the standard MIB-II information management module. So, MIB object value can be read by any SNMP web-managed software.

2.3.1 SNMP System Configuration

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

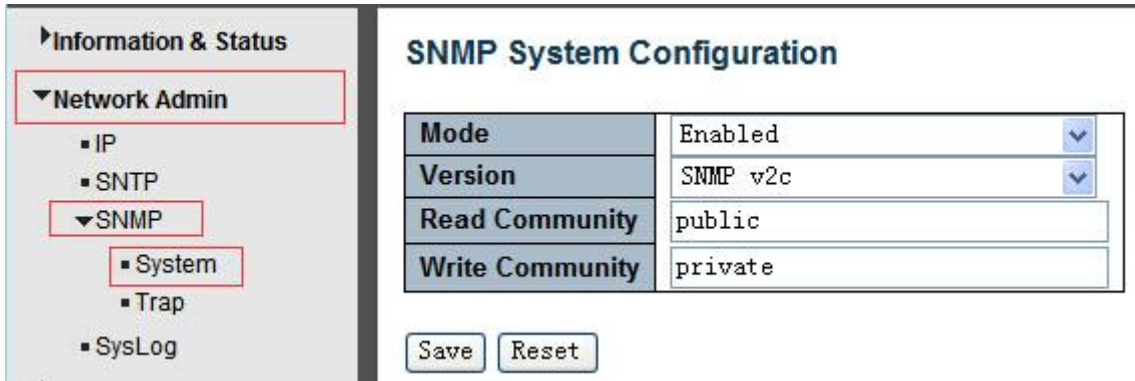


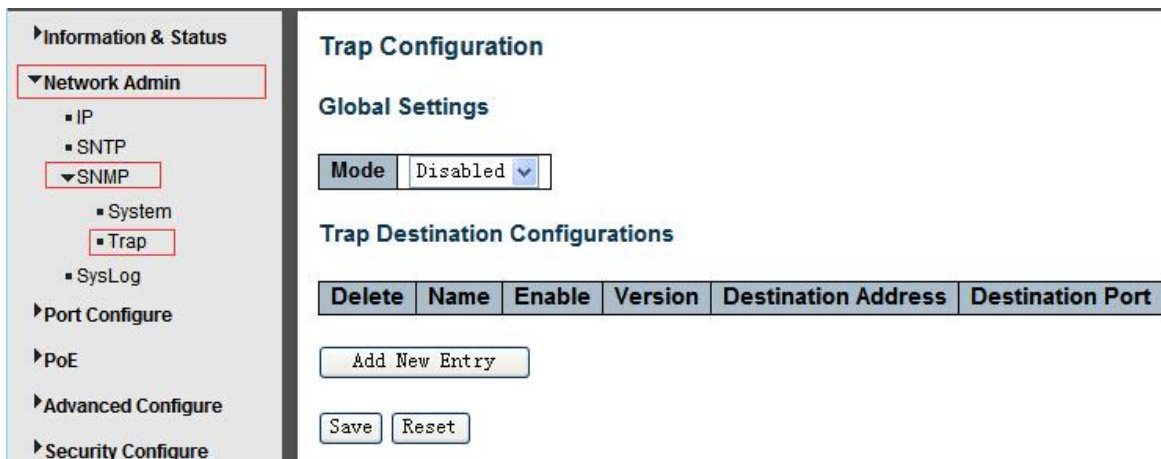
Figure 2-3 SNMP System Setting Screen

Configuration object and description is:

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.

2.3.2 SNMP Trap Configuration

Users can enable or disable SNMP Trap function and set configuration. Click "Network Admin" > "SNMP" > "Trap", then the screen will show as:



2.4 System Log Configuration

Users can configure the switch's system log, via the following screen After Clicking "Network Admin" > "Syslog"

The screenshot shows the 'System Log Configuration' interface. On the left, a navigation menu includes 'Information & Status', 'Network Admin' (expanded), 'IP', 'SNTP', 'SNMP', 'SysLog' (selected), and 'Port Configure'. The main configuration area has the following settings:

Field	Value
Server Mode	Disabled
Server Address	192.168.2.100
Syslog Level	Info

Buttons for 'Save' and 'Reset' are located below the configuration fields.

Figure 2-4 System Log Configuration Screen

Configuration object and description is:

Object	Description
Server Mode	Enabled or Disable SNMP System Log function. If "Enable" is selected, switch will send System Log to defined 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 Configure

3.1 Port Configuration

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

Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
		Current	Configured	Current Rx	Current Tx	Configured		
*			<>			<input type="checkbox"/>	9600	<>
1	● Down		Auto	X	X	<input type="checkbox"/>	9600	Discard
2	● 100fdx		Auto	X	X	<input type="checkbox"/>	9600	Discard
3	● Down		Auto	X	X	<input type="checkbox"/>	9600	Discard

Figure 3-1 Port Configure Screen

Configuration object and description is:

Object	Description
Link	Red color means Link Down, green color means Link 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 are 10M HDX, 10M FDX, 100M HDX, 100M FDX, 1000M FDX, 1000-X.
Flow Control	It is a flow control mechanism for a variety of port configurations. Full-duplex ports use 802.3x flow control, half-duplex ports use backpressure 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 is to support Jumbo frames.

Click "Save" to store and activate settings.

3.2 Link Aggregation

Users can set up multiple links among multiple switches. Link Aggregation, is a method that tie some physical ports together as one logical port, to enlarge bandwidth. This switch supports up to 13 groups of Link Aggregation, with 2 to 8 port as one group.

Note: If any port in the link aggregation group is disconnected, data packet sent to the disconnected port will share load with another connected port in this aggregation group.

3.2.1 Static Aggregation

Users can configure static aggregation of switch's ports. After Clicking the menu "Port Configure" > "Aggregation" > "Static", the following window will appear for making static aggregation settings.

- ▶ Information & Status
- ▶ Network Admin
- ▼ Port Configure
 - Ports
 - ▼ Aggregation
 - Static
 - LACP
 - Mirroring
 - Thermal Protection
 - Green Ethernet
- ▶ PoE
- ▶ Advanced Configure
- ▶ Security Configure
- ▶ QoS Configure
- ▶ Diagnostics
- ▶ Maintenance

Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	<input checked="" type="checkbox"/>
Destination MAC Address	<input checked="" type="checkbox"/>
IP Address	<input checked="" type="checkbox"/>
TCP/UDP Port Number	<input checked="" type="checkbox"/>

Aggregation Group Configuration

Group ID	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
Normal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 3-2 Port Static Aggregation Configuration Screen

Configuration object and description is:

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 activate settings.

Note: The switch 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 standardized 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 dynamic aggregation group for switches. After Clicking "Port Configure" > "Aggregation" > "LACP", users can set the LACP configuration in following screen.

Port	LACP Enabled	Key	Role	Timeout	Prio
*	<input type="checkbox"/>	<> ▼	<> ▼	<> ▼	32768
1	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
2	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
3	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
4	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768
5	<input type="checkbox"/>	Auto ▼	Active ▼	Fast ▼	32768

Figure 3-3 LACP Configuration Screen

Configuration object and description is:

Object	Description
LACP	Enable or disable LACP function of that port.
Key	The Key value incurred by the port, range 1-65535. The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
Role	The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).
Timeout	The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.
Prio	The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Click "Save" to store and activate settings.

3.3 Port Mirroring

Configure Port Mirroring on this page. This function provides monitoring of network traffic that forwards 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". The following screen will appear as:

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 3-4 Mirror Configuration Screen

Configuration object and description is:

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 and activate settings.

Note: You cannot set fast speed port(s) mirror to a low speed port. For example, there is problem if you try to mirror 100Mbps port(s) to a 10 Mbps port. So the destination port should have equal or higher speed compared to source port. The source port and destination port should not be same one.

3.4 Thermal Protection Configuration

Thermal protection is for detecting and protecting the switch. When the switch's detected port temperature is higher than the defined temperature, the system will disable the port, to protect the switch itself.

After Clicking "Port Configure" > "Thermal Protection", the following screen will appear as:

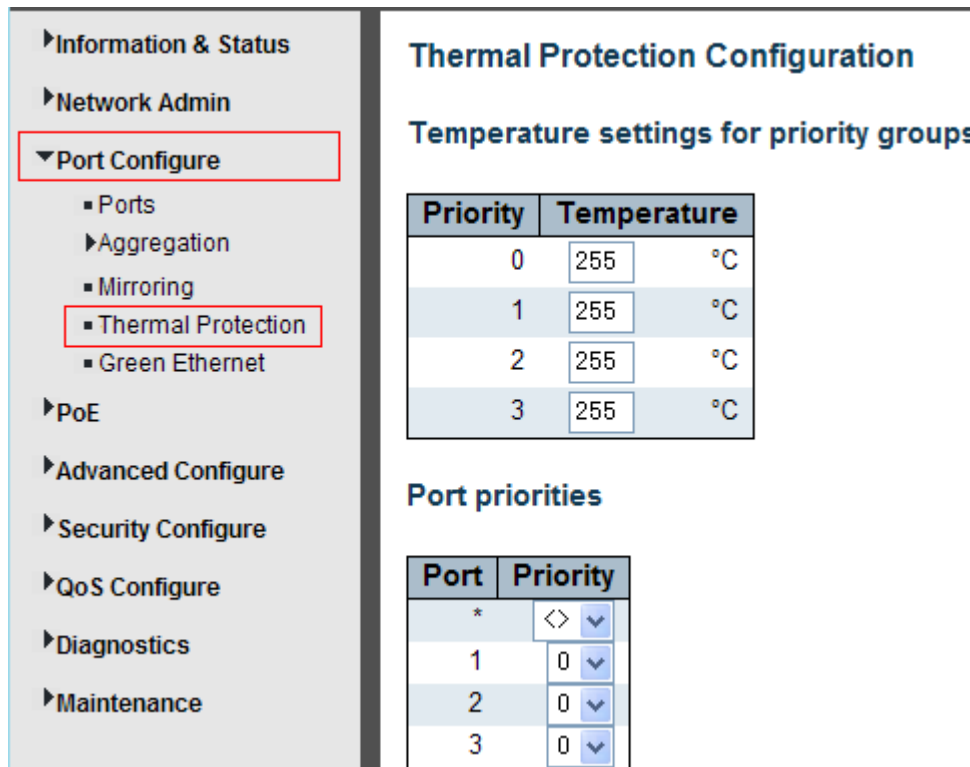


Figure 3-5 Thermal Protection Configuration Screen

Configuration object and description is:

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

Click "Save" to store and activate settings.

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

4. PoE Configuration

4.1 PoE Setting (if applicable to your switch model)

After Clicking "PoE"> "PoE Setting", the user can change PoE settings in the following screen:

Port	PoE Mode	Priority	Maximum Power [W]	Description
*	<>	<>	9	
1	PoE	High	9	
2	PoE+	Critical	9	
3	Disabled	Low	9	

Figure 4-1 PoE Setting Screen

Configuration object and description is:

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 customize by the user.
Power Management Mode	This switch supports 2 modes for Power Management. 1. 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. 2. 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, and 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 activate settings.

4.2 PoE Status

Users can check the PoE status of all ports, After Clicking "PoE"> "PoE Status".

Local Port	Description	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
2		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
3		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
4		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
5		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
6		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
7		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
8		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
9		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
10		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
11		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled

Figure 4-2 PoE Status Screen

5. Advanced Configure

5.1 VLAN

VLAN (Virtual Local Area Network) logically divide one LAN (Local Area Network) into a plurality of subsets, and each subset will form their own broadcast area network. In short, VLAN is a communication technology that logically divides one physical LAN into multiple broadcast area networks (multiple VLAN). Hosts within a VLAN can communicate directly. But VLAN groups can not directly communicate with each other. So it will limit the broadcast packets within a VLAN. Since it cannot directly access between VLAN groups, thus it improves network security.

Click "Advanced Configure"> "VLANs" to see 802.1Q VLAN configuration screen as follows:

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
2	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	

Figure 5-1 802.1Q VLAN Configuration Screen

Configuration object and description is:

Object	Description
Allowed VLANs	Here displays created VLAN ID. It is 1 by default. If you want to create new VLAN, just need to add VLAN ID here.
Ethertype for Custom S-ports	This field specifies the ethertype/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	<p>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.</p> <p>Access: Access ports are normally used to connect to end stations. Access ports have the following characteristics:</p> <ul style="list-style-type: none"> 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

	<ul style="list-style-type: none"> On egress all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged <p>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:</p> <ul style="list-style-type: none"> 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 but 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 <p>Hybrid: Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:</p> <ul style="list-style-type: none"> 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	<p>Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4094, default being 1.</p> <p>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).</p> <p>On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.</p> <p>The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.</p>
Port Type	<p>Ports in hybrid mode allow for changing 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.</p> <p>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.</p> <p>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.</p> <p>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.</p>

	<p><u>S-Custom-Port:</u> 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.</p>
Ingress Filter	<p>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.</p>
Ingress Acceptance	<p>Hybrid ports allow for changing the type of frames that are accepted on ingress.</p> <p><u>Tagged and Untagged</u> Both tagged and untagged frames are accepted.</p> <p><u>Tagged Only</u> Only tagged frames are accepted on ingress. Untagged frames are discarded.</p> <p><u>Untagged Only</u> Only untagged frames are accepted on ingress. Tagged frames are discarded.</p>
Egress Tagging	<p>Ports in Trunk and Hybrid mode may control the tagging of frames on egress.</p> <p><u>Untag Port VLAN</u> Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.</p> <p><u>Tag All</u> All frames, whether classified to the Port VLAN or not, are transmitted with a tag.</p> <p><u>Untag All</u> 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.</p>
Allowed VLANs	<p>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.</p>
Forbidden VLANs	<p>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.</p>

Click "Save" to store and activate settings.

5.2 Port Isolation

Port isolation is for limiting data between ports. It is similar to VLAN, but stricter.

5.2.1 Port Group

This switch supports port groups. Members of a port group can forward data.

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

After Clicking "Advanced Configure" > "Port Isolation" > "Port Group", the following screen will appear for making port group configuration changes.

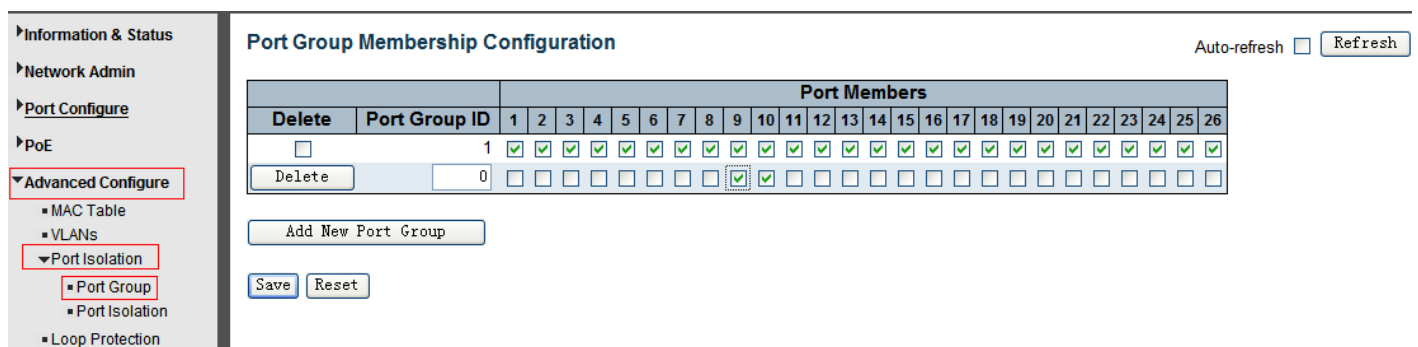


Figure 5-2 Port Group Configuration Screen

Configuration object and description is:

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 a corresponding port group, and "Save" to store and activate settings.

5.2.2 Port Isolation

After Clicking "Advanced Configure" > "Port Isolation" > "Port Isolation", the following screen will appear for making port isolation configuration changes.

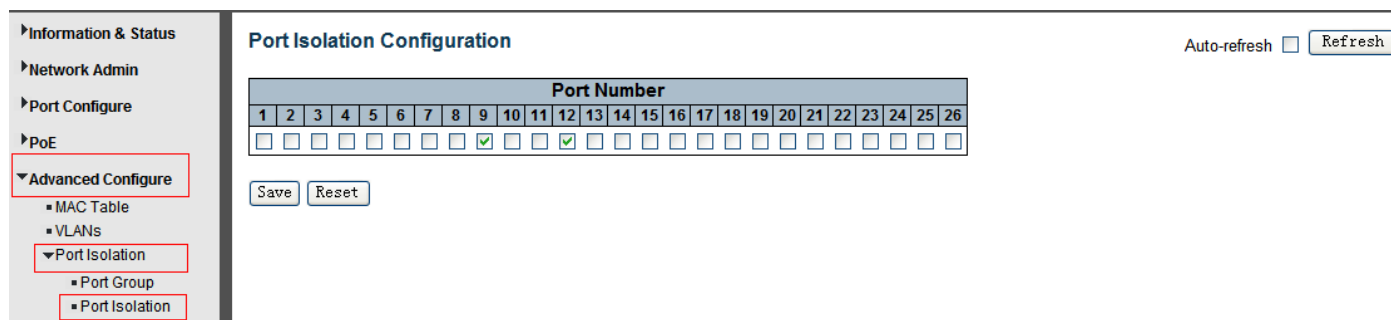


Figure 5-3 Port Isolation Configuration Screen

Configuration object and description is:

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

Click "Save" to store and activate 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 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 Clicking "Advanced Configure" > "Spanning Tree" > "Bridge Settings", the following screen will appear.

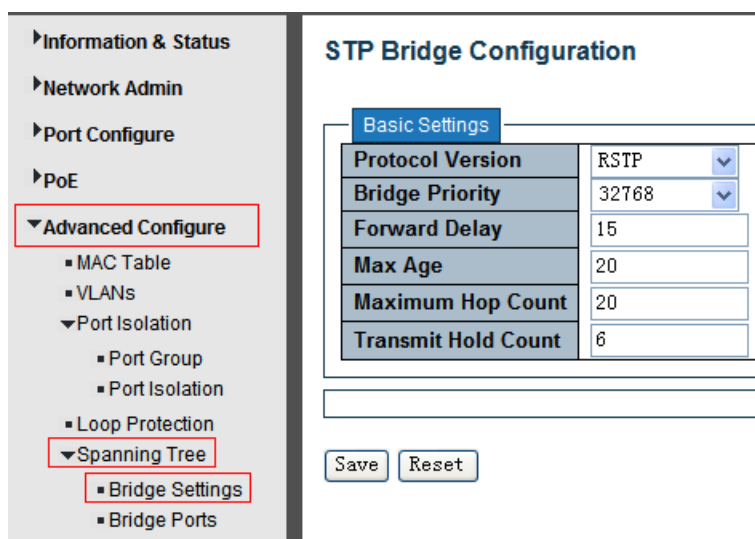


Figure 5-4 Spanning Tree Configuration Screen

Configuration object and description is:

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. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a <i>Bridge Identifier</i> .
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 settings.

5.3.2 STP Bridge Port

After Clicking "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		
-	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
						Role	TCN		
*	<input checked="" type="checkbox"/>	<>	<>	<>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Figure 5-5 STP Configuration Screen

Configuration object and description is:

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 favor 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 Point2Point.

Click "Save" to store and activate settings.

5.4 MAC Address Table

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

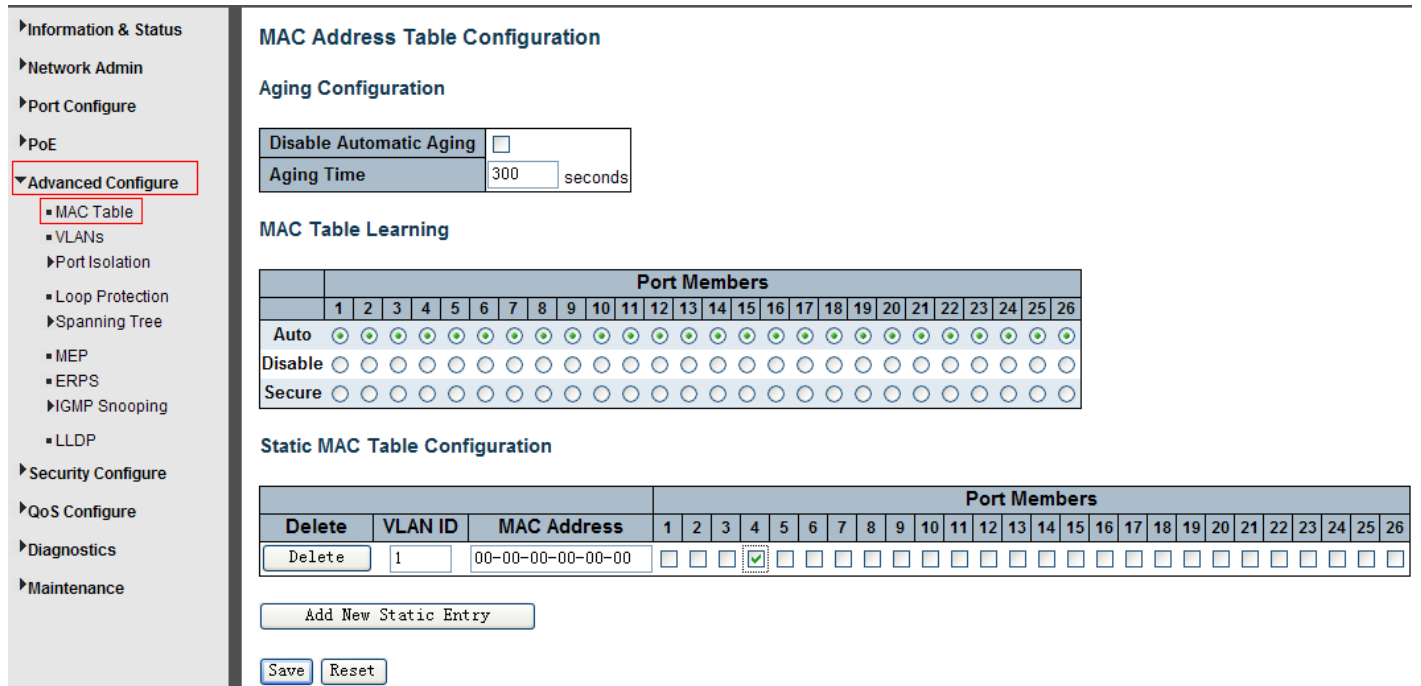


Figure 5-6 MAC Address Table Configuration Screen

Configuration object and description is:

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.
MAC Table Learning	This switch supports 3 types for MAC Table Learning 1. Auto: port will auto learn Mac address. 2. Disable: port will NOT learn MAC address. 3. Secure: port only forward data of configured static MAC address.
Static 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 activate settings.

5.5 IGMP Snooping

Internet Group Management Protocol (IGMP) lets host and routers share information about multicast groups memberships. IGMP snooping is a switch feature 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.

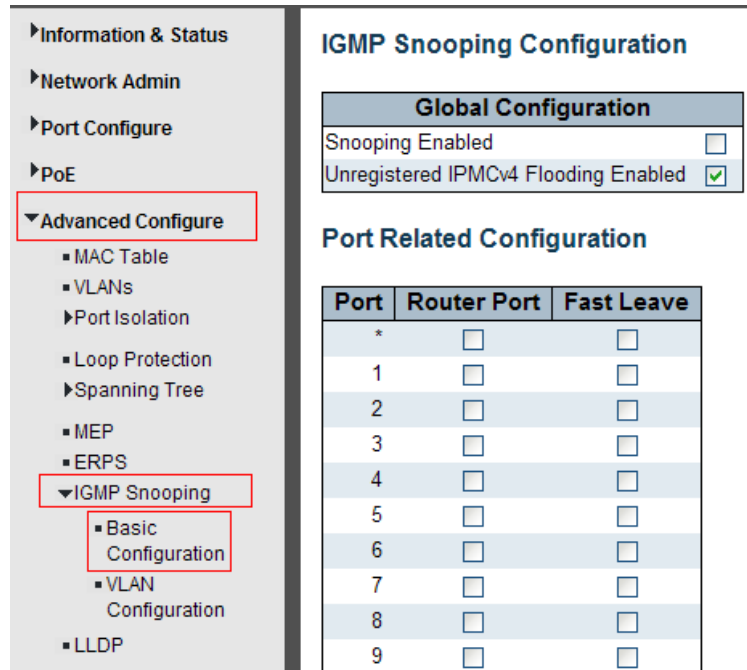


Figure 5-7 IGMP Snooping Basic Configuration

Configuration object and description is:

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 activate settings.

5.5.2 IGMP Snooping VLAN Configuration

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

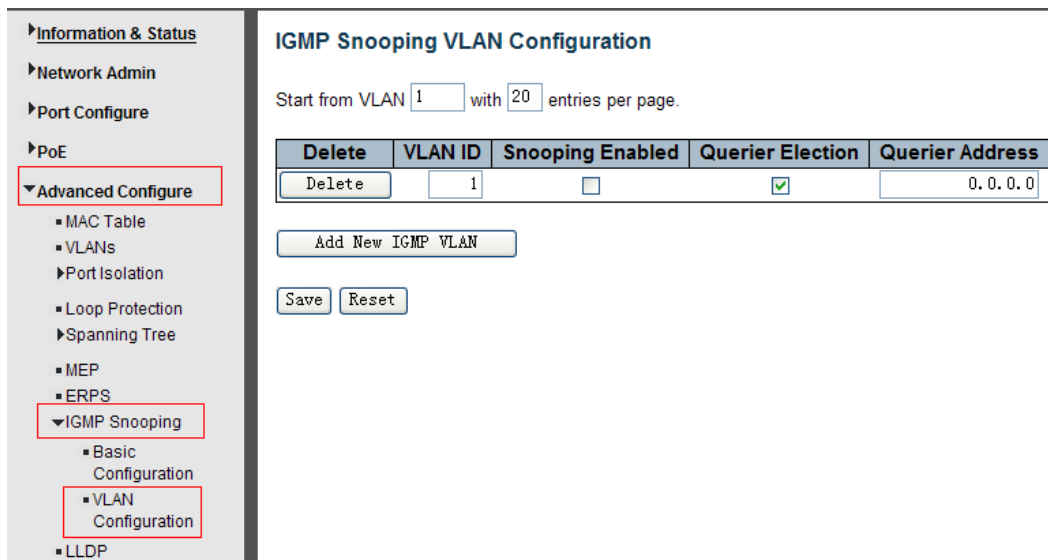


Figure 5-7 IGMP Snooping VLAN Configuration

Configuration object and description is:

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

Click "Save" to store and activate settings.

5.6 ERPS

ERPS (Ethernet Ring Protection Switching), it integrates the OAM function and the APS protocol. If the ring network was interrupted accidentally, the fault recovery times could be less than 50ms to quickly bring the network back to normal operation. ITU-T G.8032 is the first industry standard for ERPS.

Note: Before enable ERPS, STP of ring port should be disabled.

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

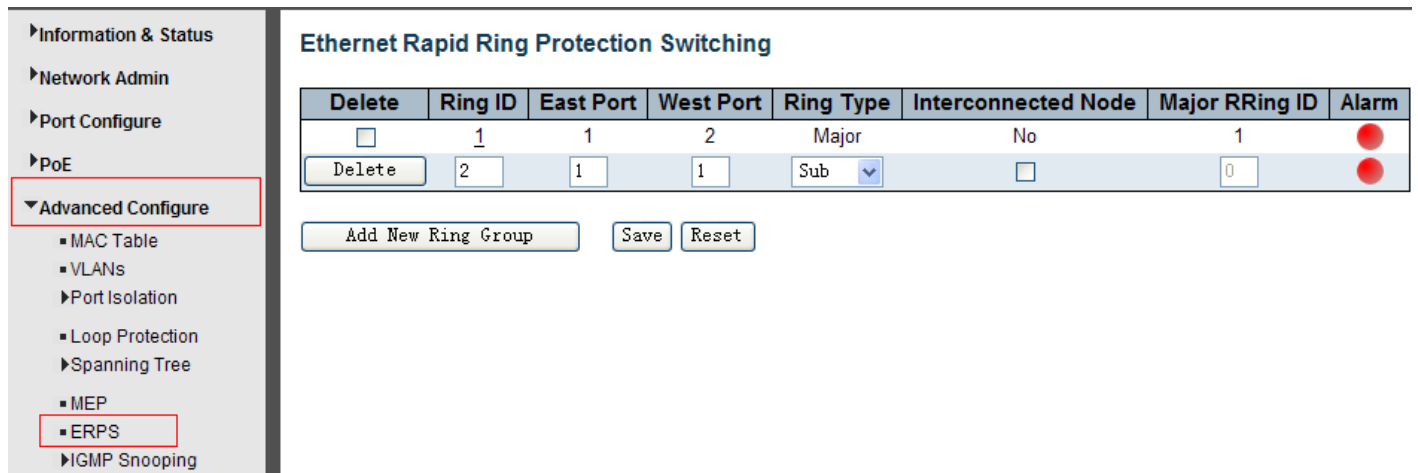


Figure 5-8 EPRS Configuration

Configuration object and description is:

Object	Description
Ring ID	ERPS Ring ID
East Port	Number of the port which participate in this Ring protection.
West Port	Number of the other port which participate in this Ring protection.
Ring Type	Available selection: "Major Ring" or "Sub Ring". Only in case of Multi Ring application, "Sub Ring" is required to configure. Default Ring Type: "Major Ring". Only if there is multi ring application, it is required to set.
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 the same type as Major Ring ID.
R-APS VLAN(1-4094)	Define VLAN for R - APS VLAN.

Click "Add New Ring Group" to create a new ERPS ring application.

Click "Save" to store and activate settings.

After Clicking the number under "Ring ID", it will go to the page for Ring Configuration as on the following screen:

Figure 5-9 EPRS Ring Configuration

Configuration object and description is:

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 Clicking " <u>VLAN config</u> ", it will go the page of Rapid Ring VLAN Configuration.
RPL Role	Click drop-down menu to select "None", "RPL Owner", or "RPL Neighbor" role.
RPL Port	Click drop-down menu to select "None", "East Port", or "West Port".

Click "Save" to store and activate settings.

After Clicking " VLAN config ", it will go the page of Rapid Ring VLAN Configuration as on the following screen:

Figure 5-10 Rapid Ring VLAN Configuration

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

5.7 LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in 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 neighboring network nodes it discovers.

After Clicking "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

Port	Mode	Optional TLVs				
		Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	Disabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Disabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Disabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Disabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Disabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Disabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 5-10 LLDP Configuration Screen

Configuration object and description is:

Object	Description
LLDP Parameters	Here allows the user to inspect and configure the current LLDP port settings: <ul style="list-style-type: none"> ➤ Tx Interval: Transmission Interval Time ➤ Tx Hold: Hold time Multiplier ➤ Tx Delay: Transmit Delay Time ➤ Tx Remit: Transmit Remit Time
Mode	Select LLDP messages transmit and receive modes for LLDP Protocol Data Units. Options are Tx only, Rx only, Enabled, and Disabled.
Optional TLVs	To configure the information included in the TLV field of advertised messages. When followed option is checked, corresponding information will be included in LLDP information transmitted. <ul style="list-style-type: none"> ➤ 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 activate settings.

5.8 Loop Protection

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

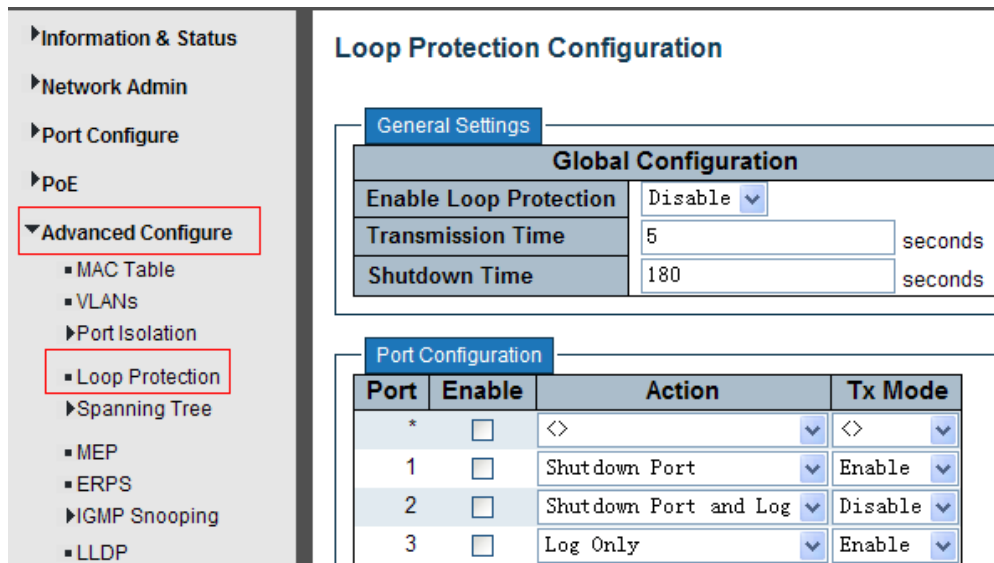


Figure 5-11 Loop Protection Configuration Screen

Configuration object and description is:

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 activate 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 not so important.

6.1 QoS Port Classification

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

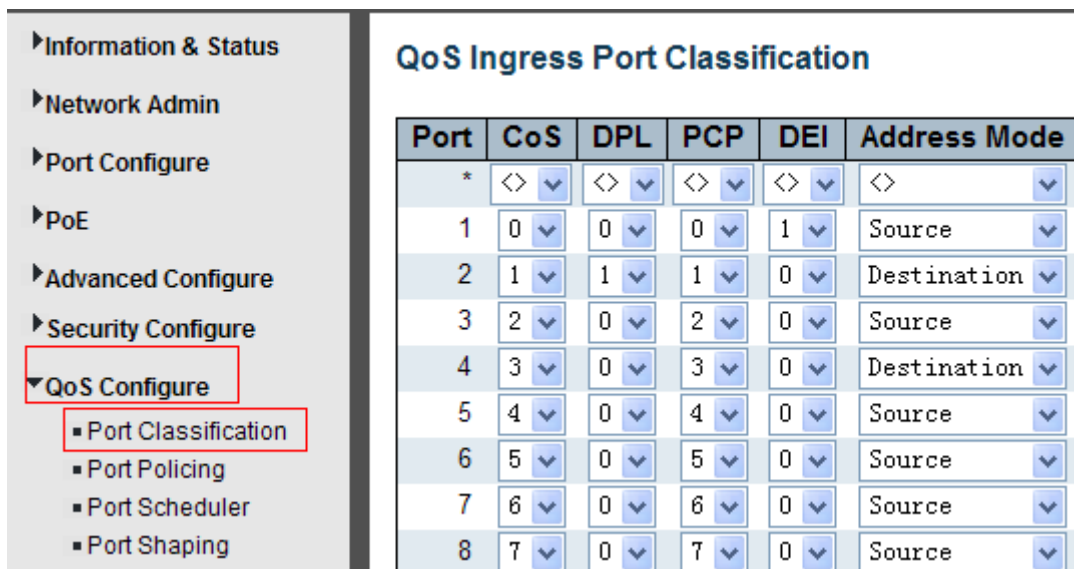


Figure 6-1 Port Classification Configuration Screen

Configuration object and description is:

Object	Description
CoS	<p>Controls the default class of service, ranging from 0 (lowest) to 7 (highest).</p> <p>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</p> <p>The classified CoS can be overruled by a QCL entry.</p> <p>Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.</p>
DPL	<p>Controls the default drop precedence level.</p> <p>All frames are classified to a drop precedence level.</p> <p>The classified DPL can be overruled by a QCL entry.</p>
PCP	<p>Controls the default PCP value.</p> <p>All frames are classified to a PCP value.</p> <p>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.</p>

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 activate settings.

6.2 Port Policing

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

Port	Enabled	Rate	Unit	Flow Control
*	<input type="checkbox"/>	500	<>	<input type="checkbox"/>
1	<input checked="" type="checkbox"/>	500	kbps	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	500	Mbps	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	500	fps	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>	500	kfps	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>

Figure 6-2 Port Policing Configuration Screen

Configuration object and description is:

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 activate settings.

6.3 Storm Control Configuration

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

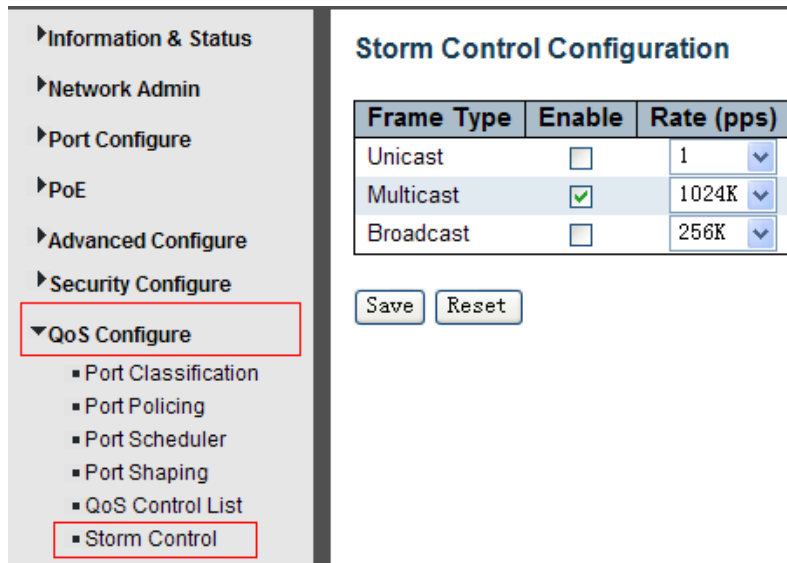


Figure 6-3 Port Policing Configuration Screen

Configuration object and description is:

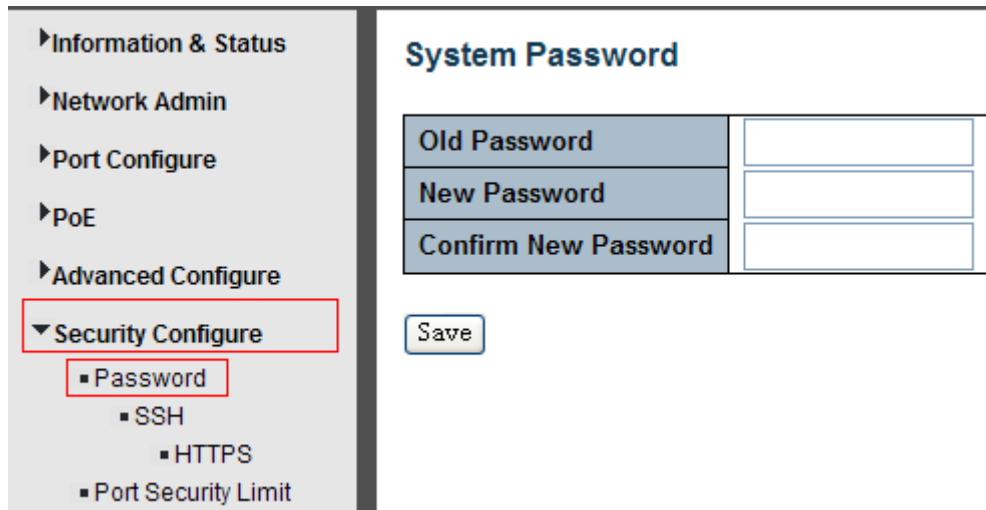
Object	Description
Frame Type	This switch supports 3 kinds of Frame Type: Unicast, Unknown Multicast, Broadcast.
Enable	Check the box to enable Storm Control.
Rate (pps)	The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K,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

Click "Save" to store and activate settings.

7. Security Configure

7.1 Password

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



System Password	
Old Password	<input type="text"/>
New Password	<input type="text"/>
Confirm New Password	<input type="text"/>

Figure 7-1 System Password Configuration Screen

Click "Save" to store and activate settings.

7.2 802.1X

In the 802.1X-world, 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 unauthorized 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.

This switch supports 802.1X port-based authentication. In this page, user can configure 802.1X. After Clicking "Security Configure" > "802.1X", the following screen will appear.

The screenshot shows the 'Network Access Server Configuration' page. On the left is a navigation menu with 'Security Configure' > '802.1X' selected. The main content area is divided into two sections:

System Configuration

Mode	Disabled
Reauthentication Enabled	<input type="checkbox"/>
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

Figure 7-2 802.1X Configuration Screen

Configuration object and description is:

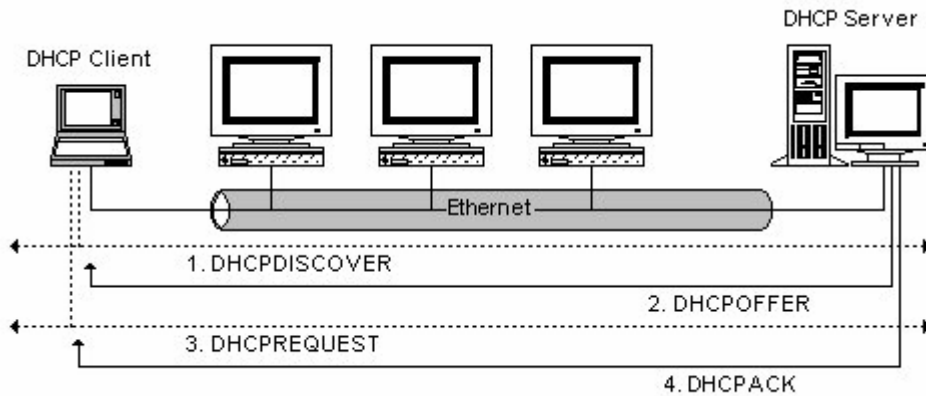
Object	Description
System Configuration	Here, user can enable or disable 802.1X or Reauthentication, as well as set Reauthentication Period / EAPOL Timeout / Aging Period / Hold Time
Port Configuration	Click drop-down menu to select an Admin State. Available options: Force Authorized, Force Unauthorized, 802.1X, Mac-based Auth.

Click "Save" to store and activate settings.

7.3 DHCP Snooping

7.3.1 DHCP Overview

DHCP protocol is widely used to dynamically allocate reusable network resources, such as IP address. A typical process of DHCP to obtain IP is as following:



DHCP Client sent DHCP DISCOVER message to DHCP Server, if Client did not receive respond from server within a period of time, it will resend DHCP DISCOVER message.

After received DHCP DISCOVER message, DHCP Server will assign sources (IP address for example) to client, and then send DHCP OFFER message to DHCP Client.

After received DHCP OFFER message, DHCP Client send DHCP REQUEST to ask for server lease, and notify the other servers that it has accepted this server to assign addresses.

After received DHCP REQUEST, server will verify whether resource can be allocated. If OK, it will send DHCP ACK message; If not OK, it will send DHCP NAK message. After received DHCP ACK message, start using the source which server assigned. If received DHCP NAK, DHCP Client will resend 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 with 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 for 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 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 DHCP Snooping Configure

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

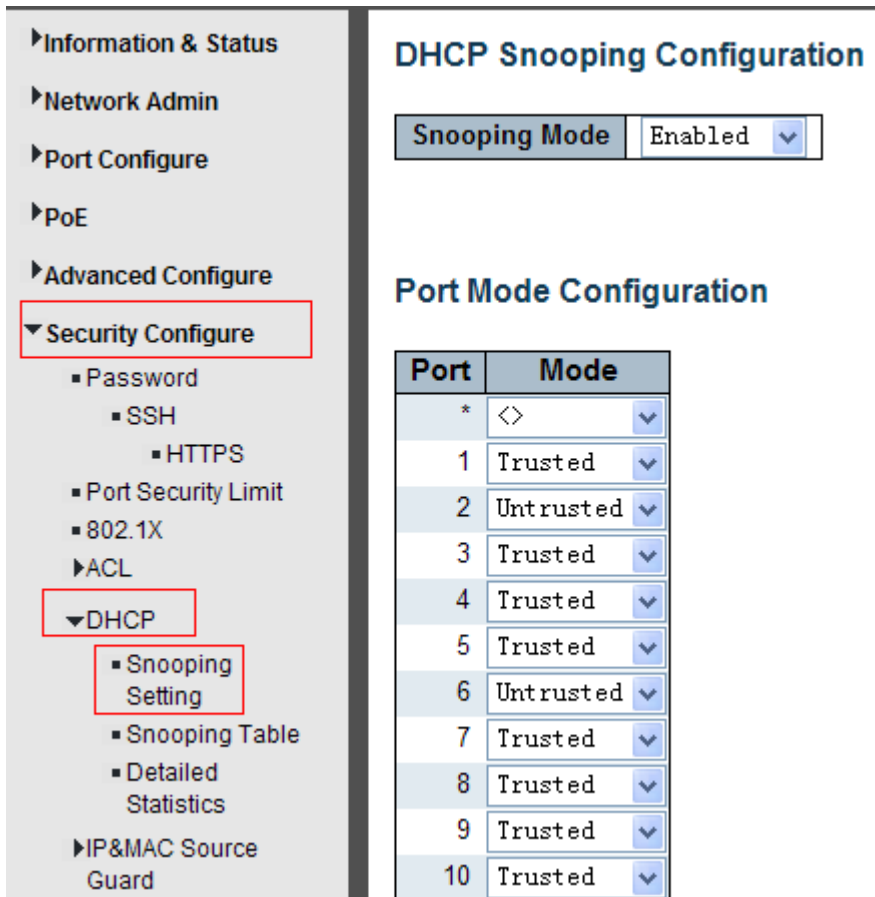


Figure 7-3 DHCP Snooping Configuration Screen

Configuration object and description is:

Object	Description
DHCP Snooping Mode	Click 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 activate settings.

7.4 IP&MAC Source Guard

IP&MAC Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on 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.

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 Configuration Screen

Configuration object and description is:

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

Click "Save" to store and activate settings.

7.4.2 Static Table

In this page, user can manually set Static Table of IP&MAC Guard to fulfill controlling function to port. After Clicking "Security Configure">"IP&MAC Source Guard" >"Static Table", the following screen will appear.

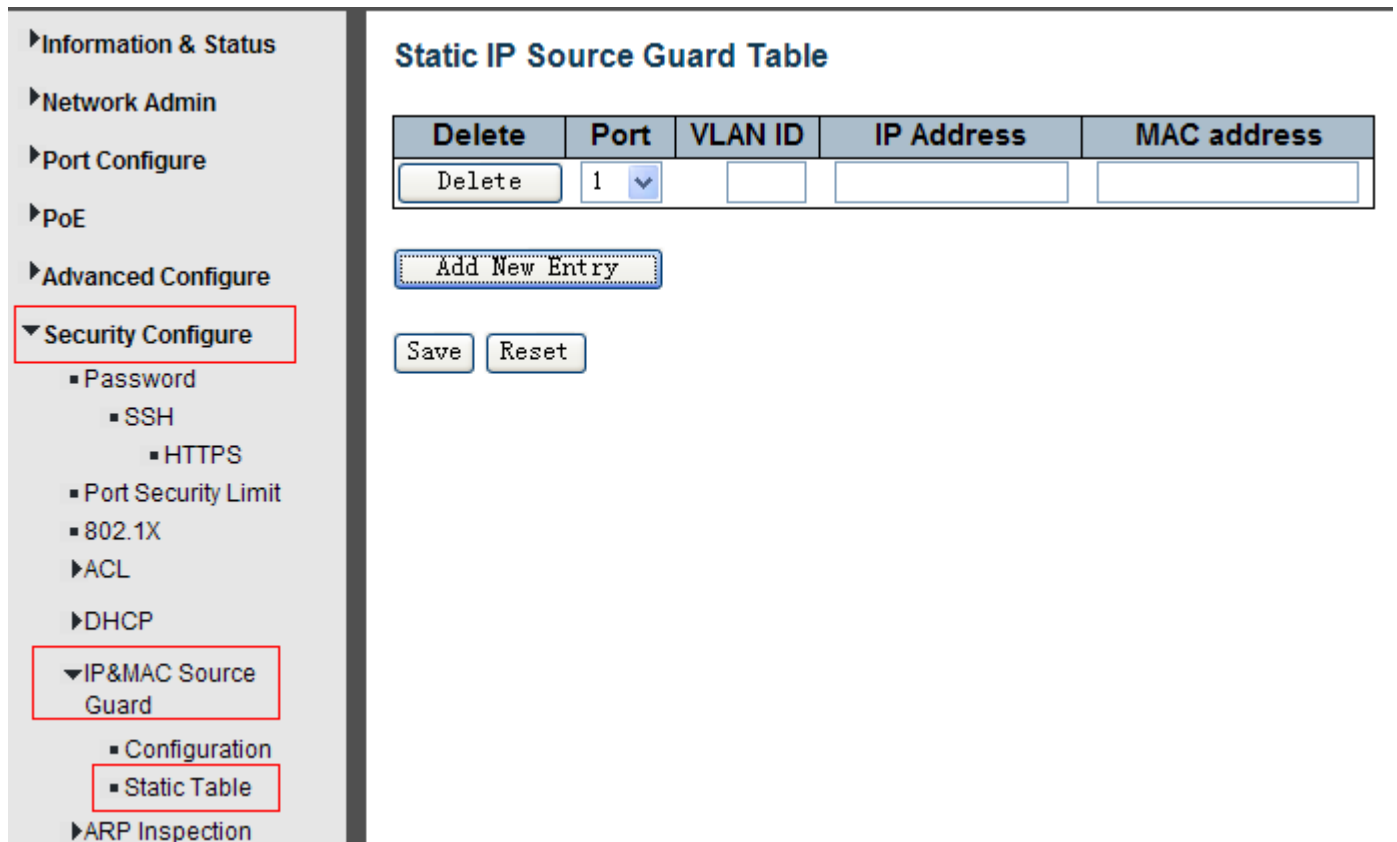


Figure 7-5 Static Table Configuration Screen

Configuration object and description is:

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 activate 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 DUT. 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 in this page. After Clicking "Security Configure">"ARP Inspection" >"Port Configuration", the following screen will appear.

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 7-6 ARP Inspection Port Configuration Screen

Configuration object and description is:

Object	Description
Global Mode	Click drop-down menu to enable or disable Global ARP Inspection
Port Mode	Click 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 activate settings.

7.5.2 VLAN Configuration

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

VLAN Mode Configuration

Start from VLAN with entries per page.

Delete	VLAN ID	Log Type
<input type="button" value="Delete"/>	<input type="text" value="1"/>	None <input type="button" value="v"/>

Figure 7-8 ARP Inspection VLAN Configuration Screen

Configuration object and description is:

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 activate settings.

7.5.3 Static Table

User can manually configure ARP Inspection Static Table to control port. After Clicking "Security Configure">"ARP Inspection" >"Static Table", the following screen will appear.

The screenshot displays the configuration interface for the Static ARP Inspection Table. On the left, a navigation sidebar is visible with the following structure:

- Information & Status
- Network Admin
- Port Configure
- PoE
- Advanced Configure
 - Security Configure**
 - Password
 - SSH
 - HTTPS
 - Port Security Limit
 - 802.1X
 - ACL
 - DHCP
 - IP&MAC Source Guard
 - ARP Inspection**
 - Port Configuration
 - VLAN Configuration
 - Static Table**
 - Dynamic Table

The main configuration area is titled "Static ARP Inspection Table" and contains the following elements:

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1			

Below the table, there is an "Add New Entry" button and "Save" and "Reset" buttons.

Figure 7-9 Static Table Configuration Screen

Configuration object and description is:

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 activate settings.

7.6 ACL

ACL is an acronym for **Access Control List**. It is the list table of ACEs, 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 prioritized for the various situation. 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 in this context, they are similar to firewalls.

7.6.1 ACL Ports Configure

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

The screenshot displays the 'ACL Ports Configuration' interface. On the left is a navigation sidebar with the following structure:

- Information & Status
- Network Admin
- Port Configure
- PoE
- Advanced Configure
 - Security Configure (highlighted)
 - Password
 - SSH
 - HTTPS
 - Port Security Limit
 - 802.1X
 - ACL (highlighted)
 - Ports (highlighted)
 - Rate Limiters
 - Access Control List

The main content area is titled 'ACL Ports Configuration' and includes 'Refresh' and 'Clear' buttons. Below is a table with the following data:

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	Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	247562
3	0	Permit	Disabled	Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Port 1	Disabled	Disabled	Disabled	Enabled	0

Figure 7-10 ACL Ports Configuration Screen

Configuration object and description is:

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.

Click "Save" to store and activate settings.

7.6.2 Rate Limiter Configuration

User can make ACL Rate limiter configuration in this page. After Clicking "Security Configure">"ACL" >"Rate Limiter", the following screen will appear.

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 7-11 ACL Rate Limiters Configuration Screen

Click "Save" to store and activate settings.

7.6.3 Access Control List Configuration

User can make Access Control List Configuration in this page. After Clicking "Security Configure" > "ACL" > "Access Control List", the following screen will appear.

Figure 7-12 Access Control List Configuration Screen

Click button, to go to Access Control List, and edit it.

8. Diagnostics

8.1 Ping Test

Ping is a little program that can issue ICMP Echo packets to the IP address you defined. Destination node will respond to those packets sent from switch. So Ping test is to troubleshoot IP connectivity issues.

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

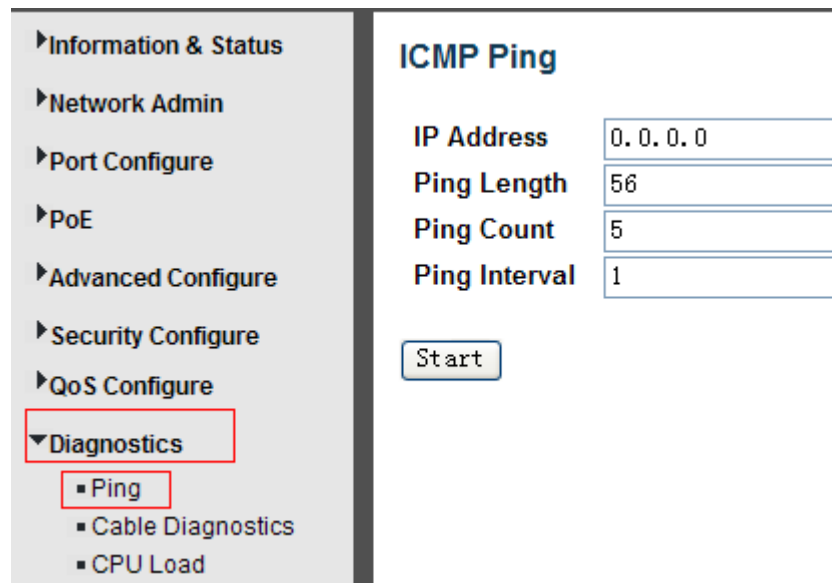


Figure 8-1 Ping Test Screen

Configuration object and description is:

Object	Description
IP Address	The destination IP Address that needed to Ping
Ping Length	Input 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	Interval 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 Clicking "Diagnostics ">"Cable Diagnostics", the following screen will appear.

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 the percentage of CPU load. After Clicking "Diagnostics">"CPU Load", the following screen will appear.

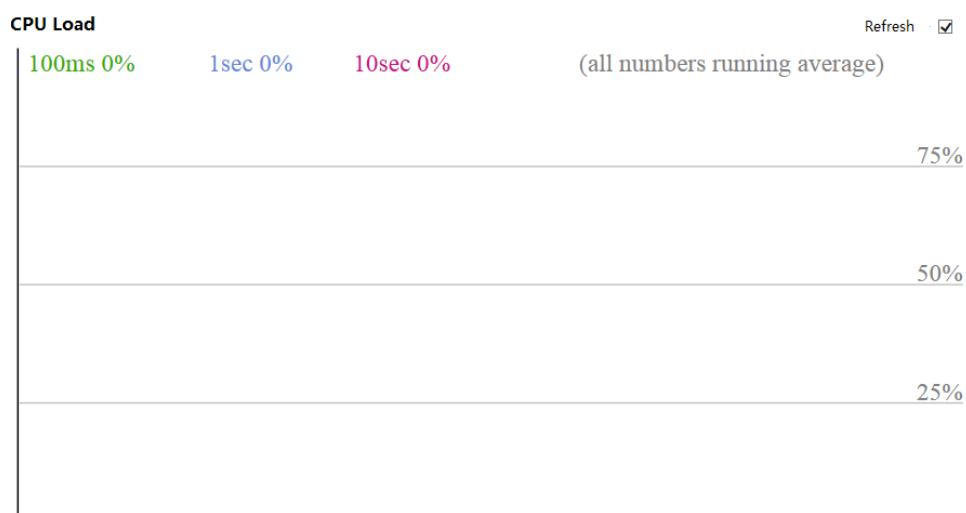
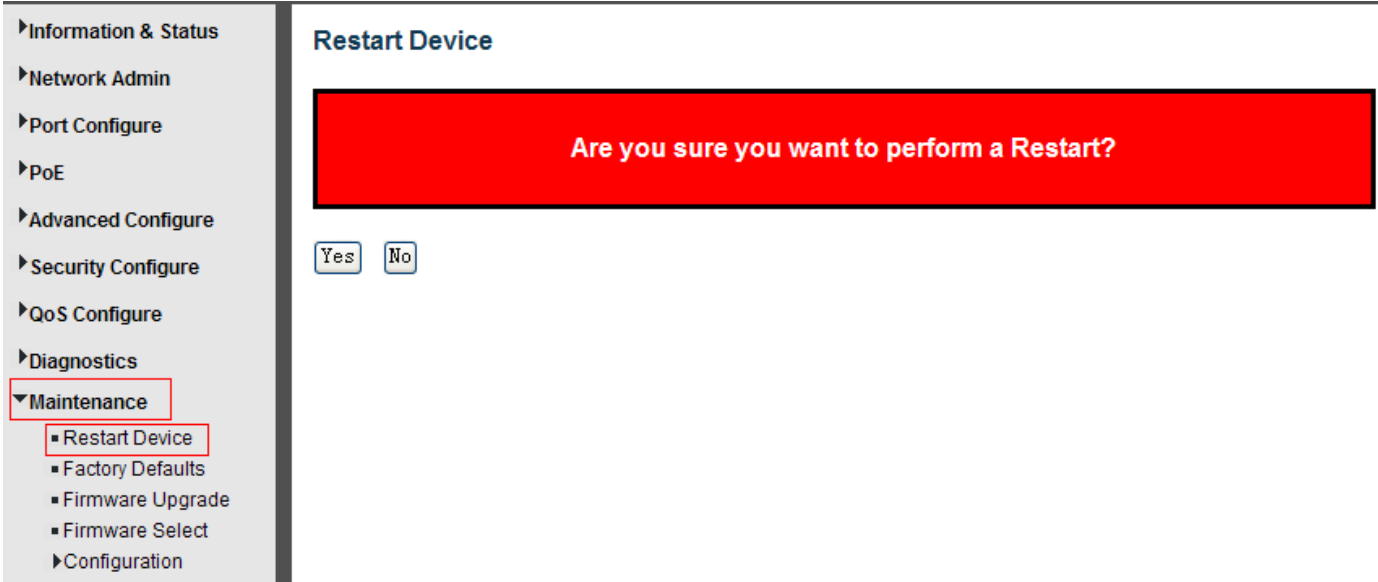


Figure 8-3 CPU Load Screen

9. Maintenance

9.1 Restart Device

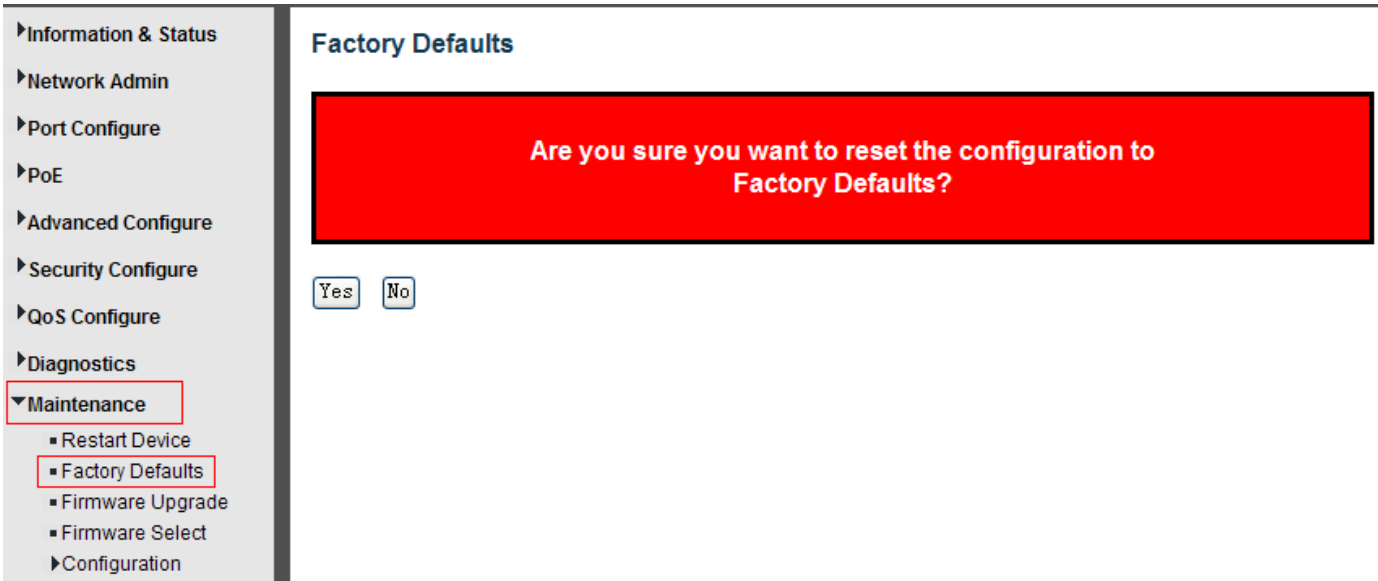
This page is for restarting switch. After Clicking "Maintenance ">"Restart Device", the following screen will appear.



Please click "Yes" to restart the switch.

9.2 Factory Defaults

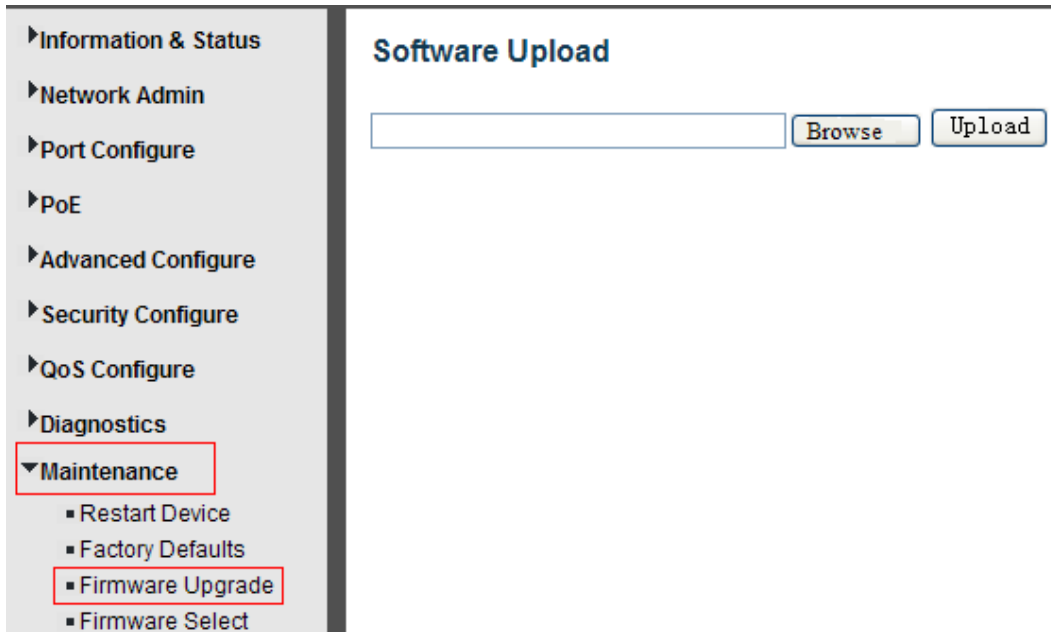
This page is for making all settings to factory defaults. After Clicking "Maintenance ">"Factory Defaults", the following screen will appear.



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

9.3 Firmware Upgrade

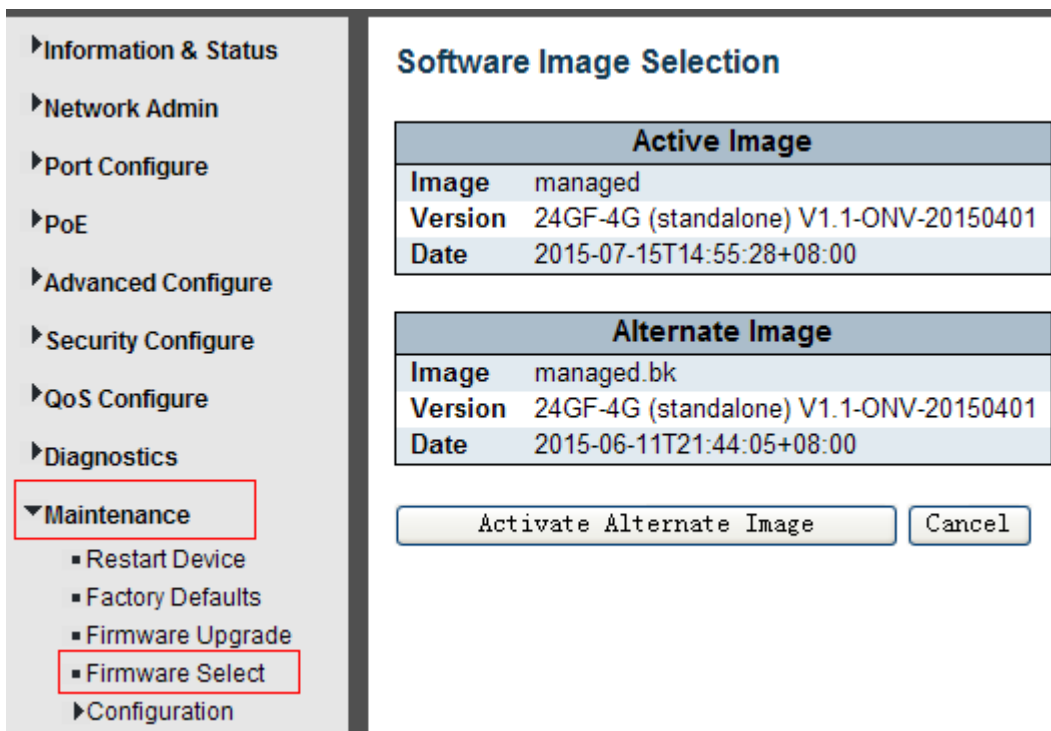
This page is for upgrading system firmware. After Clicking "Maintenance ">"Firmware Upgrade", the following screen will appear.



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

9.4 Firmware Select

This page is for upgrading system firmware. After Clicking "Maintenance ">"Firmware Upgrade", the following screen will appear.



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 Clicking "Maintenance ">"Download", the following screen will appear.

Information & Status

Network Admin

Port Configure

PoE

Advanced Configure

Security Configure

QoS Configure

Diagnostics

Maintenance

- Restart Device
- Factory Defaults
- Firmware Upgrade
- Firmware Select
- Configuration**

 - Download**

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.

The screenshot shows a web management interface with a left sidebar and a main content area. The sidebar contains a tree view of navigation options: Information & Status, Network Admin, Port Configure, PoE, Advanced Configure, Security Configure, QoS Configure, Diagnostics, Maintenance, and Configuration. The 'Maintenance' and 'Configuration' menus are expanded, with 'Upload' selected. The main content area is titled 'Upload Configuration' and includes a 'File To Upload' section with a text input field and a 'Browse' button. Below this is a 'Destination File' section with a table with two columns: 'File Name' and 'Parameters'. At the bottom of the main area is an 'Upload Configuration' button.

9.5.3 Activate Configuration

After Clicking "Maintenance ">"Activate", the following screen will appear. Then user can activate Configuration File.

The screenshot shows a web management interface with a left sidebar and a main content area. The sidebar contains a tree view of navigation options: Information & Status, Network Admin, Port Configure, PoE, Advanced Configure, Security Configure, QoS Configure, Diagnostics, Maintenance, and Configuration. The 'Maintenance' and 'Configuration' menus are expanded, with 'Activate' selected. The main content area is titled 'Activate Configuration' and includes a warning message: '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.' Below this is a 'File Name' section with a radio button and the text 'default-config'. At the bottom of the main area is an 'Activate Configuration' button.

9.5.4 Delete Configuration File

After Clicking "Maintenance ">"Delete", the following screen will appear. Then user can delete Configuration File.

The screenshot shows a web management interface with a left sidebar and a main content area. The sidebar contains a list of menu items: Information & Status, Network Admin, Port Configure, PoE, Advanced Configure, Security Configure, QoS Configure, Diagnostics, Maintenance, and Configuration. The 'Maintenance' and 'Configuration' items are highlighted with red boxes. The 'Configuration' item is expanded, showing sub-items: Download, Upload, Activate, and Delete. The 'Delete' item is also highlighted with a red box. The main content area is titled 'Delete Configuration File' and displays the message 'No files available for deletion.' Below this message is a button labeled 'Delete Configuration File'.

- ▶ Information & Status
- ▶ Network Admin
- ▶ Port Configure
- ▶ PoE
- ▶ Advanced Configure
- ▶ Security Configure
- ▶ QoS Configure
- ▶ Diagnostics
- ▼ Maintenance
 - Restart Device
 - Factory Defaults
 - Firmware Upgrade
 - Firmware Select
 - ▼ Configuration
 - Download
 - Upload
 - Activate
 - Delete

Delete Configuration File

No files available for deletion.

Delete Configuration File