



Vi35136

GUI User Guide

36 - Ports L2+/L3 Lite Managed GbE Switch

Release A1

About This Manual

Copyright

Copyright ©2022Vigtron, Inc. All rights reserved.

The products and programs described in this user's manual are licensed products of Vigtron, Inc.

This user's manual contains proprietary information protected by copyright, and this user's manual and all accompanying hardware, software and documentation are copyrighted. No parts of this user's manual may be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable form by any means electronic or mechanical. This also includes 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 Vigtron, Inc.

Purpose

This GUI user guide gives specific information on how to operate and use the management functions of the VI35136 via HTTP/HTTPS web browser

Audience

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 Hypertext Transfer Protocol (HTTP).

Conventions

Conventions The following conventions are used throughout this manual to show information.



NOTE: Emphasizes important information or calls your attention to related features or instructions.



WARNING: Alerts you to a potential hazard that could cause personal injury.



CAUTION: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warranty

Warranty See the Customer Support/Warranty booklet included with the product. A copy of the specific warranty terms applicable to Vigtron's products and replacement parts can be obtained from

Vigtron's Sales and Service Office or an authorized dealer.

Disclaimer

Vigitron 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. Vigitron 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 Vigitron. Vigitron assumes no responsibility for any inaccuracies that may be contained in this user's manual. Vigitron makes no commitment to update or keep current the information in this user's manual, and reserves the rights to make improvements to this user's manual and/or to the products described in this user's manual, at any time without notice.

FCC Caution

To assure continued compliance (example-use only shielded interface cables when connection to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This is a Class B device. In a domestic environment, this product may cause radio interference. In which case, the user may be required to take adequate measures.

CE Mark Warning

Overview

In this User Guide, it will not only tell you how to install and connect your network system but configure and monitor the Vi35136 through the web by (RJ-45) serial interface and Ethernet ports step-by-step. Many explanations in detail of hardware and software functions are shown as well as the examples of the operation for web-based interface.

The Vi35136 are the next generation Industrial L2+ managed GbE switch from Manufacture, is a portfolio of affordable managed switches that provides a reliable infrastructure for your business network. These switches deliver more intelligent features you need to improve the availability of your critical business applications, protect your sensitive information, and optimize your network bandwidth to deliver information and applications more effectively. It provides the ideal combination of affordability and capabilities for entry level networking includes small business or enterprise application and helps you create a more efficient, better-connected workforce.

Vi35136 L2+/L3 Lite Managed GbE Switch provide 36 ports in a single device; the specification is highlighted as follows:

- L2+ features provide better manageability, security, QoS, and performance.
- Support IPv4/IPv6 dual stack management
- Support SSH/SSL secured management
- Support SNMP v1/v2c/v3
- Support RMON groups 1,2,3,9
- Support sFlow
- Support IGMP v1/v2/v3 Snooping
- Support MLD v1/v2 Snooping
- Support RADIUS and TACACS+ authentication
- Support IP Source Guard
- Support DHCP Relay (Option 82)
- Support DHCP Snooping
- Support ACL and QCL for traffic filtering
- Support 802.1d(STP), 802.1w(RSTP) and 802.1s(MSTP)
- Support LACP and static link aggregation
- Support Q-in-Q double tag VLAN
- Support GVRP dynamic VLAN

Contents

Copyright	2
Purpose	2
Audience	2
Conventions	2
Warranty	2
ABOUT THIS MANUAL	2
Disclaimer	3
FCC Caution	3
CE Mark Warning	3
Overview	4
INTRODUCTION	4
USER GUIDE OVERVIEW	12
Overview	12
Front View of the Switch	12
Rear View of the Switch	12
LED Descriptions	12
System LED	12
Mode LEDs	12
Port Status LEDs	12
Reset Button	14
INSTALLING THE SWITCH	15
Package Contents	15

Mounting the Switch in a 19-inch Rack	15
Connecting the AC Power Cord	16
Insert Real panel drawing	16
Installing SFP+ Modules	16
INITIAL CONFIGURATION OF SWITCH	18
Initial Switch Configuration Using Web Browsers	18
Mounting the Switch on Desk or Shelf	18
The initial switch configuration procedure is as follows:	18
Insert Log in Screen	19
TROUBLESHOOTING	20
WARNING	20
MISE EN GARDE	20
SECTION 1: INTRODUCTION	21
1. Overview	21
1.1 Web Management	21
1.2 Web-Based user Interface	21
SECTION 2: INFORMATION & STATUS	24
2. Information & Status	24
2.1 System Information	24
2.2 IP Status	24
2.3 Syslog	25
2.4 Detailed Syslog	25
2.5 Mac Table	26
2.6 VLANS	26
2.6.1 Membership	26
2.6.1 VLANs Ports	27

2.7 Ports	27
2.7.1 Traffic Overview	27
2.7.2 Detailed Statistics	27
2.8 LACP	28
2.8.1 System Status	28
2.8.2 Port Status	28
2.8.3 Port Statistics	28
2.9 Thermal Protection	29
2.10 Green Ethernet	29
2.11 LLDP	30
2.11.1 Neighbors	30
2.11.2 Port Statistics	30
2.12 Loop Protection	31
2.13 Spanning Tree	31
2.13.1 Bridge Status	31
2.13.2 Port Status	31
2.13.3 Port Status	32
2.14 IGMP Snooping	32
2.14.1 IGMP Status	32
2.14.2 Group Information	33
2.14.3 IPv4 SFM	33
2.15 MLD Snooping	33
2.15.1 MLD Status	33
2.15.2 MLD Group Information	33
2.15.3 MLD IPv6 SFM	35
2.16 DHCP	35
2.16.1 Server	35
2.16.2 Snooping Table	36
2.16.3 Relay Statistics	37
2.16.4 Detailed Statistics	37
2.17 Security	38
2.17.1 Post Security	38
2.17.2 Access Management Statistics	39
2.17.3 802.1x	39
2.17.4 ACL Status	40
2.17.5 AAA	41
2.18 QOS	42
2.18.1 QOS Statistics	42
2.18.2 QOS Status	42

SECTION 3: NETWORK MANAGEMENT- SET UP AND OPERATIONS	43
3. Network Management	43
3.1 IP Configuration	43
3.2 IP Status	44
3.2.1 DHCP Server	44
3.2.2 DHCP Server> Server Excluded Configuration	45
3.2.3 DHCP Server> Server Pool Configuration	45
3.3 NTP Configuration	45
3.3.1 NTP Address assignment	46
3.3.2 Time reference confirmation and offset	46
3.3.3 Setting Time Zone as NTP Source	46
3.4 SNMP Configuration	47
3.4.1 SNMP System Configuration	47
3.4.2 SNMP Trap Configuration	48
3.4.3 SNMP Community Configuration	48
3.4.4 SNMP user	49
3.4.5 SNMP Groups Configuration	49
3.4.6 SNMP Views Configuration	49
3.4.7 SNMP Access Configuration	50
3.5 System Log Configuration	51
SECTION 4: PORT CONFIGURE	52
4.1 Port Configuration	52
4.2 Link Aggregation	53
4.2.1 Static Aggregation	53
4.2.2 LACP Aggregation	54
4.3 Port Mirroring	55
4.4 Thermal Protection Configuration	56
4.5 Green Ethernet	57
4.6 DDM	57
4.7 DDMI	58
SECTION 5: ADVANCED CONFIGURE	59
5. Advanced Configure	59

5.1 MAC Address Table	59
5.2 VLAN	60
5.3 Voice VLAN	63
5.4 GVRP	64
5.5 Port Isolation	66
5.5.1 Port Group	66
5.5.2 Port Isolation	66
5.6 Loop Protection	67
5.7 STP- Spanning Tree	68
5.7.1 Bridge Setting	68
5.7.2 MSTI Mapping	69
5.7.3 MSTI Priorities	70
5.7.4 CIST Ports	71
5.7.5 MSTI Ports	75
5.8 IPMC Profile	77
5.8.1 Profile Table	77
5.8.2 Address Entry	78
5.9 MEP	79
5.10 ERPS	79
5.11 IGMP Snooping	82
5.11.1 Basic Configuration	82
5.11.2 IGMP Snooping VLAN Configuration	83
5.11.3 IGMP Snooping Port Filtering Profile	84
5.12 IPV6 MLD Snooping	85
5.12.1 Basic Configuration	85
5.12.2 VLAC Configuration	87
5.12.3 Port Filtering Profile	90
5.13 LLDP	91
6. Security Configure	93
6.1 User configuration	93
6.2 Privilege Levels configuration	93
6.3 SSH configuration	94
6.4 HTTPS configuration	95

6.5 Ports Security Limit configuration	97
6.6 Access Management configuration	95
6.7 802.1X configuration	97
6.8 ACL configuration	98
6.8.1 ACL Ports Configure	99
6.8.2 Rate Limiter Configuration	100
6.8.3 Access Control List Configuration	100
6.9 DHCP	101
6.9.1 DHCP Snooping Configure	102
6.9.2 Snooping Table	103
6.9.3 DHCP Relay	108
6.9.4 DHCP Relay Statistics	110
6.9.5 DHCP Detailed Statistics	112
6.10 IP&MAC Source Guard	113
6.10.1 Port Configuration	113
6.10.2 Static Table	114
6.10.2 Dynamic Table	115
6.11 ARP Inspection	116
6.11.1 Port Configuration	116
6.11.2 VLAN Configuration	118
6.11.3 Static Table	119
6.11.4 Dynamic Table	120
6.12 AAA	121
6.12 RADIUS	122
6.12.2 TACACS+	125
SECTION 7: QOS CONFIGURE	127
7. QoS Configure	127
7.1 QoS Port Classification	127
7.2 Port Policing	129
7.3 Queue Policing	130
7.4 Port Scheduler	131
7.5 Port Shaping	133
7.6 Port Tag Remarking	135

7.7 Port DSCP	136
7.8 DSCP-based QoS	138
7.9 DHCP Translation	139
7.10 DSCP Classification	140
7.11 Control List	141
7.11 QCL Status	145
7.12 Storm Policing Configuration	145
SECTION 8: DIAGNOSTICS	147
8. Diagnostics	147
8.1 Ping Test	147
8.2 Cable Diagnostics	148
8.2 CPU Load	150
SECTION 9: MAINTENANCE	151
9. Maintenance	151
9.1 Restart Device	151
9.2 Factory Defaults	151
9.3 Firmware Upgrade	152
9.4 Firmware Select	152
9.5 Configuration	153
9.5.1 Download Configuration File	153
9.5.2 Upload	153
9.5.3 Activate Configuration	154
9.5.4 Delete Configuration File	154
9.5.5 Glossary	155
9.5.6 Appendix	166

User Guide Overview

Overview

This user guide describes how to install, configure, and troubleshoot the Vi30128, 36 Ports L2+ Managed GbE Switch.

By reading this user guide, users can perform the following tasks:

- To check the switch status by reading the LED behavior
- To reset the switch or to restore the switch to factory defaults
- To install the switch
- To use a Web browser to initially configure the switch
- To troubleshoot the switch

Front View of the Switch



Figure 1: Front panel of the switch

Rear View of the Switch

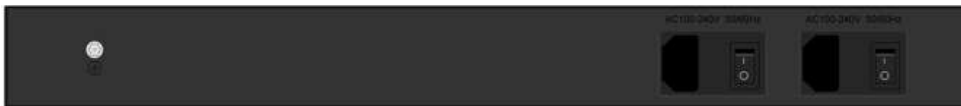


Figure 2: Rear panel of the switch

LED Descriptions

The LEDs on the front panel provide users with switch status checking and monitoring. There are three types of LEDs as follows:

System LED

Indicates if the switch is powered up correctly or not, or, indicates if there is a system alarm triggered for troubleshooting.

Mode LEDs

Indicates the mode of all ports on the switch. Users sequentially switch among the two different modes (Link/Activity/Speed mode)

Port Status LEDs

Indicates the current status of each port. Users can check these LEDs to understand the port status.

The following table details the functions and descriptions of various LED indicators:

Table 1: System LED

LED	Color	State	Description
System	Green	ON	The system is started.
		OFF	The system is not working.
		Blink	The system of switch is working normally.

Table 2: POWER LEDs

LED	Color	State	Description
Power	Green	ON	The power is working.
		OFF	The power is not working.

Table 3: RJ45 LEDs

LED	Color	State	Description
1000M Link/Act	Green	Blink	The Port Status LEDs are displaying link status, network activity.
		ON	The Port Status LEDs are link status, no data transmission
		OFF	The Port Status LEDs are link status, No Link
10/100M Link/Act	Yellow	Blink	The Port Status LEDs are displaying link status, network activity.
		ON	The Port Status LEDs are link status, no data transmission
		OFF	The Port Status LEDs are link status, No Link

Table 4: SFP LEDs

LED	Color	State	Description
All speed Link/Act	Green	Blink	The Port Status LEDs are displaying link status, network activity.
		ON	The Port Status LEDs are link status, no data transmission
		OFF	The Port Status LEDs are link status, No Link

Reset Button

By pressing the Mode/Reset Button for certain period of time, users can perform the following tasks.

- Change Port Status LED Mode
 - To read the port status correctly in the two different modes (Link/Act/Speed mode).
- Reset the Switch
 - To reboot and get the switch back to the previous configuration settings saved.
- Restore the Switch to Factory Defaults
 - To restore the original factory default settings back to the switch.

NOTE:



According to the table below, users can easily judge which task is being performed by reading the LED behaviors while pressing the Reset button. Once the LED behaviors are correctly displayed, users may just release the button.

Table 5: Reset Button Description

Task to be Performed	Time Period of Pressing Button	SYS LED Behavior	Port Status LED Behavior
Reset the Switch	Long press 5 seconds	Blink quickly and then off	Blink quickly and then off
Reset the Switch	Long press 5 seconds	Blink quickly And then off	Blink quickly and then off

Installing the Switch

Package Contents

- The Switch
- AC Power Cord
- (Must select power supply cord as Type SVT or SPT-2, Min. 18 AWG. Min. 1.5 m, max. 4.5m (14.76 ft) long. One end terminates with NEMA 5-15P, min. 125 Vac, the other end with and appliance coupler.)
- Four Adhesive Rubber Feet
- Installation Guide
- Mounting kit



NOTE: The switch is an indoor device. If you need to use it to connect outdoor devices such as outdoor IP cameras, then you need to install an arrester on the cable between outdoor device and the switch.

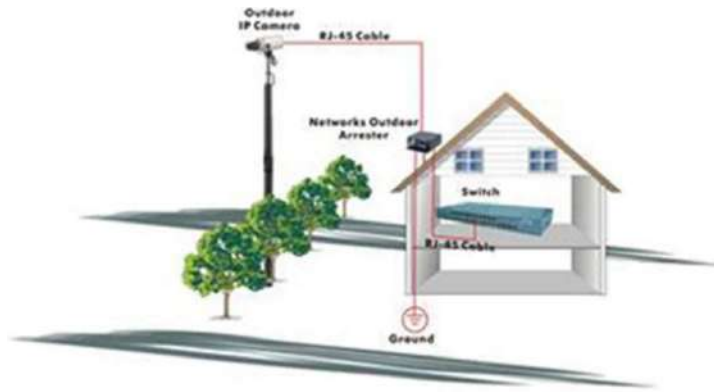


Figure: Addition an arrester between outdoor device and this switch

Mounting the Switch in a 19-inch Rack

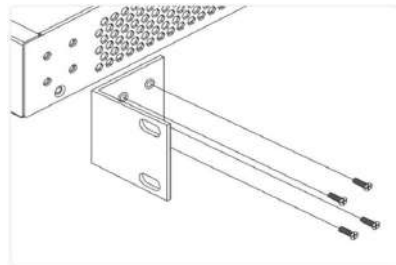
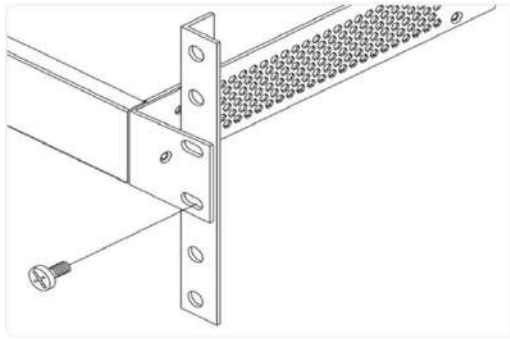


Figure 3: Attaching Brackets to the Switch

Step 1: Attach the mounting brackets to both sides of the chassis. Insert screws and tighten with a screwdriver to secure the brackets.

Step 2: Place the switch on a rack shelf in the rack. Push it in until the oval holes in the brackets align with the mounting holes in the rack posts.



Step 3: Attach the brackets to the posts. Insert screws and tighten them.

Figure 4: Attaching Brackets to the Rack Post

Connecting the AC Power Cord

Step 1: Connect the AC power cord to the AC power receptacle of switch.

Step 2: Connect the other end of the AC power cord to the AC power outlet.

Step 3: Check the SYS LED. If it is ON, the power connection is correct.

Insert Real panel drawing

The Vi35126 has two separate AC connect, if both are active, they will serve as back up to each other. If one fails the other will maintain the switch functions. If both are used, they should be connected to separate power sources



Figure 6: Connecting AC power cord

Installing SFP+ Modules

You can install or remove a mini-GBIC SFP+ module from an SFP+ port without having to power off the switch.

Step 1: Insert the module into the SFP+ port.

Step 2: Press firmly to ensure that the module seats into the connector.

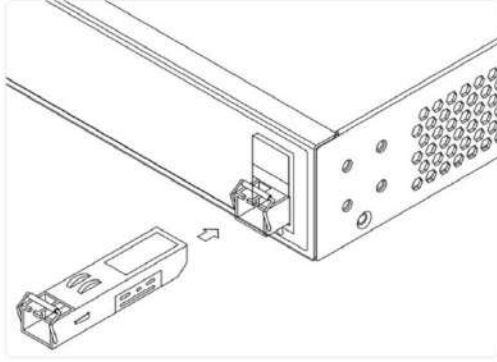


Figure 7: Installing an SFP+ Module into an SFP+ Port



NOTE: The SFP+ ports should use UL Listed Optional Transceiver product, Rated 3.3Vdc, Laser Class 1.

Initial Configuration of Switch

Initial Switch Configuration Using Web Browsers

After powering up the switch for the first time, you can perform the initial switch configuration using a web browser. For managing other switch features, please refer to the Web interface user guide for details.

To begin with the initial configuration stage, you need to reconfigure your PC's IP address and subnet mask so as to make sure the PC can communicate with the switch. After changing PC's IP address (for example, 192.168.0.250), then you can access the Web interface of the switch using the switch's default IP address as shown below.



NOTE:

The factory default IP address of the switch is 192.168.0.1

The factory default Subnet Mask of switch is 255.255.255.0

Mounting the Switch on Desk or Shelf

Step 1: Verify that the workbench is sturdy and reliably grounded.

Step 2: Attach the four adhesive rubber feet to the bottom of the switch.

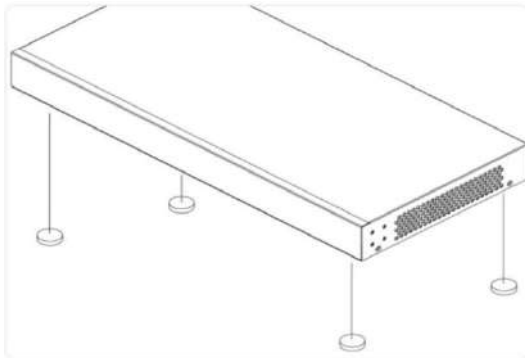


Figure 5: Attaching the Rubber Feet

1. Power up the PC that you will use for the initial configuration. Please make sure the PC has the Ethernet RJ45 connector to be connected to the switch via standard Ethernet LAN cable.
2. Reconfigure the PC's IP address and Subnet Mask as below, so that it can communicate with the switch. The method to change the PC's IP address, for example, for a PC running Windows® 7/8.x/10, is as follows:

Step 1: Type "network and sharing" into the Search Box in the Start Menu

Step 2: Select Network and Sharing Center

Step 3: Clicking on Change adapter settings on the left of PC screen

The initial switch configuration procedure is as



NOTE: Users can also skip step 1 to 3, by pressing WinKey+R and type "ncpa.cpl" command to get to step 4 directly.

Step 4: Right-clicking on your local adapter and select Properties

Step 5: In the Local Area Connection Properties window highlight Internet Protocol Version 4 (TCP/IPv4), then clicking the Properties button.



NOTE: Be sure to record all your PC's current IP settings to be able to restore them later.

Step 6: Select the radio button Use the following IP address and enter in the IP for the PC (e.g. any IP address not in use, and in between 192.168.0.2 and 192.168.0.254), Subnet mask (e.g. 255.255.255.0), and Default gateway that corresponds with your network setup. Then enter your Preferred and Alternate DNS server addresses.

Step 7: Clicking OK to change the PC's IP address.

3. Power up the switch to be initially configured, and wait until it has finished its start-up processes.
4. Connect the PC to any port on the switch using a standard Ethernet cable, and check the port LED on the switch to make sure the link status of the PC's is OK.
5. Run your Web browser on the PC, enter the factory default IP address, so as to access the switch's Web interface.

If your PC is configured correctly, you will see the login page of the switch as shown by Figure 9 below.

Insert Log in
Screen

Figure 9: Web Interface Login Page

If you do not see the above login page, please perform the following steps:

- Refresh the web page.
 - Check to see if there is an IP conflict issue.
 - Clean browser cookies and temporary internet files.
 - Check your PC settings again and repeat step 2.
6. Enter the factory default username and password in login page. Clicking "Login" to log into the switch.



NOTE: The factory default Username of the switch is **admin**.

The factory default Password of the switch is **admin**.

Troubleshooting

The following table provides information for users to easily troubleshoot problems by taking actions based on the suggested solutions within.

Symptoms	Possible Causes	Suggested Solutions
SYSTEM LED is Off	The switch is not receiving power.	<ol style="list-style-type: none"> 1. Check if correct power cord is connected firmly to the switch and to the AC outlet socket. 2. Perform power cycling the switch by unplugging and plugging the power cord back into the switch. 3. If the LED is still off, try to plug power cord into different AC outlet socket to make sure correct AC source is supplied.
Port Status LED is Off in the Link/Act/Speed Mode	The port cannot establish a link	<ol style="list-style-type: none"> 1. Check if the cable connector plug is firmly inserted and locked into the port at both the switch and the connected device. 2. Make sure the connected device is up and running correctly. 3. If the symptom still exists, try different cable or different port, in order to identify if it is related to the cable or specific port. 4. Check if the port is disabled in the configuration settings via WEB user interface. 5. WEB user interface.
Port Status LED is Off	The port is not supplying power	<ol style="list-style-type: none"> 1. Check if the cable connector plug is firmly inserted and locked into the port at both the switch and the connected device. 2. Make sure the correct Ethernet cables are used. 3. If the symptom still exists, try different cable or different port, in order to identify if it is related to the cable or specific port. 4. Check if the port is disabled in the configuration settings via WEB user interface.

Table 5: Troubleshooting Table

WARNING

- Self-demolition on Product is strictly prohibited. Damage caused by self-demolition will be charged for repair fees.
- The switch is an indoor device; if it will be used in an outdoor environment or connects with some outdoor device, then it must use a lightning arrester to protect the switch.
- Before installation, please make sure input power supply and product specifications are compatible with each other.
- To reduce the risk of electric shock, please disconnect all AC or DC power cord and RPS cables to remove power from the unit completely.
- Before importing/exporting configuration, please make sure the firmware version is always the same.
- After the firmware upgrade, the switch will remove the configuration automatically to the latest firmware version.

MISE EN

- Il est strictement interdit de démonter le produit par vous-même. Si le dommage causé par le démontage est volontaire, des frais de réparation vous seront facturés.
- L'interrupteur est une unité intérieure; s'il doit être utilisé à l'extérieur ou relié à certaines unités extérieures, vous devez utiliser un parafoudre pour le protéger.

- Avant l'installation, veuillez vous assurer de la compatibilité de la puissance d'entrée et des spécifications du produit.
- Afin de réduire le risque de choc électrique, veuillez couper l'alimentation électrique de l'équipement et de toutes les lignes électriques de courant alternatif ou de courant continu et des câbles redondants du système d'alimentation.
- Avant d'importer/exporter la configuration, assurez-vous que la version du micrologiciel est toujours la même.
- Après la mise à niveau du micrologiciel, le commutateur supprime automatiquement la configuration de la dernière version du micrologiciel.

Section 1: Introduction

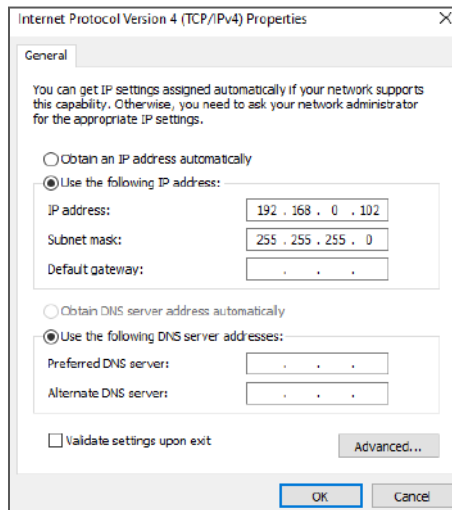
1. Overview

Thank you for purchasing our Managed Switch series, whose all-software function can be managed, configured and monitored via embedded Web-based (HTML) interface. By a standard browser, you can manage switch at any remote site in the network.

Browser as a universal access tool, uses the HTTP protocol to communicate with switch directly.

Open installed web browser on your PC, input the switch's IP address like <http://xxx.xxx.xxx.xxx>, then open that URL to login web management.

1.1 Web Management



Prior to accessing the switch, make certain your computer is set to operate on the same network as the switch.

It is recommended that regardless of the browser you are using access the switch using the private or incognito modes depending on the browser.

Note: IP address of switch is 192.168.0.1 by default. So please input <http://192.168.0.1> into browser.

When the login window appears, please enter the default username "admin" with password "admin". Then clicking OK to login

1.2 Web-Based user Interface

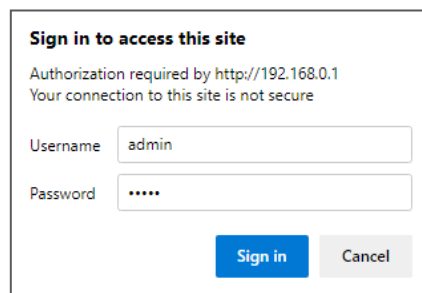


Figure1-1 Login Window

Default User Name: **admin**

Default Password: **admin**

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

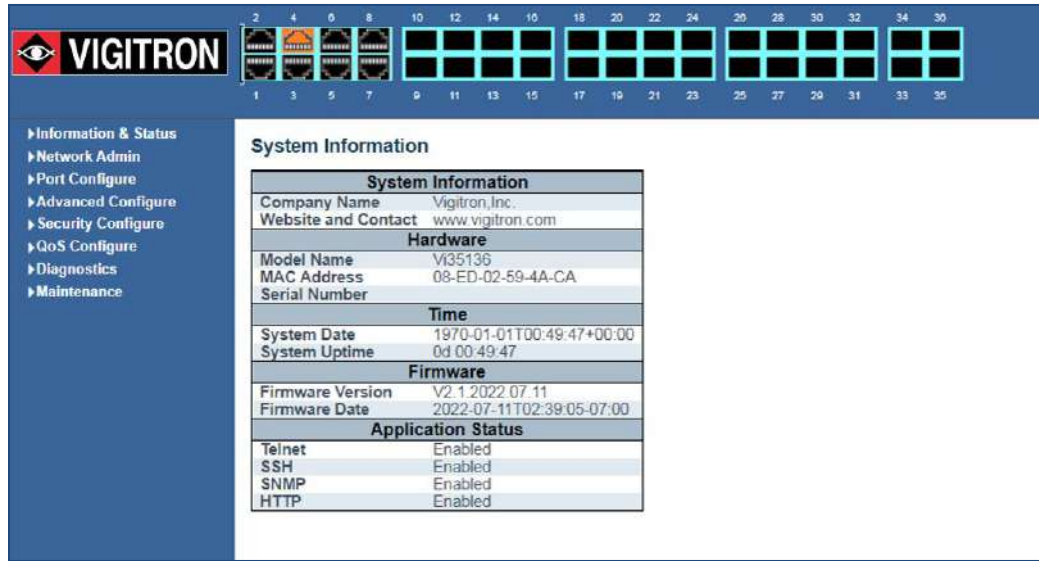


Figure1-2 Web Management Main Page

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

Part	Description
Status	Company Logo; Working Indicators; Port Indicators, including link working status; Help document;
Menu	Let's you access all the commands and statistics.
Information	Shows configuration details.

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



10/100M linked; : 1000M linked; :No link; link;

Using the onboard Web agent, you can define system parameters, manage and control the Managed Switch, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can set up the managed Switch by selecting the functions 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.

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.

Section 2: Information & Status

2. Information & Status

This section shows the basic information of the switch and status of functions/features setting. Clients can go to different sections to check detailed guidance to make the function work.

After clicking "Information & Status" > "System Information", following screen will appear as:

2.1 System Information

Figure 2-1 System Information Screen

2.2 IP Status

After clicking "Information & Status" > "IP Status", following screen will appear as:

Clients can go to Section "Network Admin" > "IP Configuration" to do the detailed management.

IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	82-22-06-27-4a-01	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.1/24	
VLAN1	IPv6	fe80::8022:6ff:fe27:4a01/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

ARP Table

IP Address	Link Address
192.168.0.119	VLAN1:04-0e-3c-16-61-e5
fe80::8022:6ff:fe27:4a01	VLAN1:82-22-06-27-4a-01

Figure 2-2 System Information Screen

2.3 Syslog

After clicking "Information & Status" > "System Information", following screen will appear as:

Clients can go to Section "Network Admin" > "System Log Configuration" to do the detailed management.

System Log Information

Level: Clear Level:

The total number of entries is 4 for the given level.

Start from ID with entries per page.

ID	Level	Time	Message
1	Informational	1970-01-01T00:00:03+00:00	SYS-BOOTING: Switch just made a cold boot.
2	Notice	1970-01-01T00:00:03+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
3	Notice	1970-01-01T00:00:10+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/4, changed state to up.
4	Notice	1970-01-01T00:00:15+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.

Figure 2-3 Syslog Screen

2.4 Detailed Syslog

After clicking "Information & Status" > "Detailed Syslog", following screen will appear as:

Clients can go to Section "Network Admin" > "System Log Configuration" to do the detailed management.

Detailed System Log Information

ID:

Message

Level	Informational
Time	1970-01-01T00:00:03+00:00
Message	SYS-BOOTING: Switch just made a cold boot.

Figure 2-4 Detailed Syslog Screen

2.6.1 VLANs
Ports

VLAN Port Status for Combined users							
Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VL	
1	C-Port	✓	All	1	Untag	PVID	
2	C-Port	✓	All	1	Untag	PVID	
3	C-Port	✓	All	1	Untag	PVID	
4	C-Port	✓	All	1	Untag	PVID	
5	C-Port	✓	All	1	Untag	PVID	
6	C-Port	✓	All	1	Untag	PVID	
7	C-Port	✓	All	1	Untag	PVID	
8	C-Port	✓	All	1	Untag	PVID	
9	C-Port	✓	All	1	Untag	PVID	
10	C-Port	✓	All	1	Untag	PVID	
11	C-Port	✓	All	1	Untag	PVID	
12	C-Port	✓	All	1	Untag	PVID	
13	C-Port	✓	All	1	Untag	PVID	
14	C-Port	✓	All	1	Untag	PVID	
15	C-Port	✓	All	1	Untag	PVID	
16	C-Port	✓	All	1	Untag	PVID	

Figure 2-6-1 Vlan Ports Screen

After clicking "Information & Status" > "Ports", following screen will appear as:

2.7 Ports

Clients can go to Section "Port Configure" > "Port Configuration" to do the detailed management.

2.7.1 Traffic
Overview

Port	Description	Packets		Bytes		Errors	
		Received	Transmitted	Received	Transmitted	Received	Transmitted
1		0	0	0	0	0	0
2		0	0	0	0	0	0
3		0	0	0	0	0	0
4		54561	5476	5602055	3239836	0	0
5		0	0	0	0	0	0
6		0	0	0	0	0	0
7		0	0	0	0	0	0
8		0	0	0	0	0	0
9		0	0	0	0	0	0
10		0	0	0	0	0	0
11		0	0	0	0	0	0
12		0	0	0	0	0	0
13		0	0	0	0	0	0
14		0	0	0	0	0	0
15		0	0	0	0	0	0
16		0	0	0	0	0	0
17		0	0	0	0	0	0
18		0	0	0	0	0	0
19		0	0	0	0	0	0
20		0	0	0	0	0	0
21		0	0	0	0	0	0

Figure 2-7-1 Ports-Traffic Overview Screen

2.7.2 Detailed

Detailed Port Statistics Port 1			
Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527-Bytes	0	Tx 1527-Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0

Figure 2-7-2 Ports-Detailed Statistics Screen

2.8 LACP

After clicking "Information & Status" > "LACP", following screen will appear as:

Clients can go to Section "Port Configure" > "Link Aggregation" > "LACP Aggregation" to do the detailed management.

2.8.1 System Status

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
No ports enabled or no existing partners					

Figure 2-8-2 LACP Port Status Screen

2.8.2 Port Status

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

Figure 2-8-2 LACP Port Status Screen

2.8.3 Port Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0

Figure 2-8-3 LACP Port Statistics Screen

2.9 Thermal Protection

After clicking "Information & Status" > "LACP", following screen will appear as:

Clients can go to Section "Port Configure" > "Thermal Protection Configuration" to do the detailed management.

Port	Temperature	Port status
1	68 °C	Port link operating normally
2	68 °C	Port link operating normally
3	68 °C	Port link operating normally
4	68 °C	Port link operating normally
5	68 °C	Port link operating normally
6	68 °C	Port link operating normally
7	68 °C	Port link operating normally
8	63 °C	Port link operating normally
9	63 °C	Port link operating normally
10	63 °C	Port link operating normally
11	63 °C	Port link operating normally

Figure 2-9 Thermal Protection Screen

2.10 Green Ethernet

After clicking "Information & Status" > "Green Ethernet", following screen will appear as:

Clients can go to Section "Port Configure" > "Green Ethernet" to do the detailed management.

Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE In power save	ActiPhy Savings	PerfectReach
1	●	✓	✗	✗	✗	✗	✗
2	●	✓	✗	✗	✗	✗	✗
3	●	✓	✗	✗	✗	✗	✗
4	●	✓	✗	✓	✗	✗	✗
5	●	✓	✗	✗	✗	✗	✗
6	●	✓	✗	✗	✗	✗	✗
7	●	✓	✗	✗	✗	✗	✗
8	●	✓	✗	✗	✗	✗	✗
9	●	✗	✗	✗	✗	✗	✗
10	●	✗	✗	✗	✗	✗	✗
11	●	✗	✗	✗	✗	✗	✗
12	●	✗	✗	✗	✗	✗	✗
13	●	✗	✗	✗	✗	✗	✗

Figure 2-10 Green Ethernet Screen

2.11 LLDP

After clicking "Information & Status" > "LLDP", following screen will appear as:

Clients can go to followed Section "Advanced Configure" > "LLDP" to do the detailed management.

The screenshot shows the "LLDP Neighbor Information" page. On the left is a navigation menu with "LLDP" expanded to show "Neighbors" and "Port Statistics". The main content area is titled "LLDP Remote Device Summary" and contains a table with the following columns: Local Interface, Chassis ID, Port ID, Port Description, System Name, System Capabilities, and Management Address. The table is currently empty, displaying "No neighbor information found".

2.11.1 Neighbors

Devices in your network with LLDP Discovery ability will be displayed

The screenshot shows the "LLDP Neighbor Information" page with discovered neighbors. The table has the following data:

Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
GigabitEthernet 1/2	08-ED-02-59-4A-EE	4	GigabitEthernet 1/4	Vi35128	Bridge(+)	192.168.0.1 (IPv4)
GigabitEthernet 1/4	08-ED-02-59-4A-EE	2	GigabitEthernet 1/2	Vi35128	Bridge(+)	192.168.0.1 (IPv4)
10GigabitEthernet 1/3	08-ED-02-50-10-C0	28	10GigabitEthernet 1/4	Vi30128	Bridge(+)	192.168.0.15 (IPv4)

Figure 2-11-1 LLDP-Neighbors Screen

2.11.2 Port Statistics

The screenshot shows the "LLDP Global Counters" and "LLDP Statistics Local Counters" screens. The "Global Counters" section includes a checkbox for "Clear global counters" (checked) and a timestamp "Neighbor entries were last changed 1970-01-01T00:00:00+00:00 (4942 secs. ago)". Below are statistics for neighbors: Total Neighbors Entries Added (0), Total Neighbors Entries Deleted (0), Total Neighbors Entries Dropped (0), and Total Neighbors Entries Aged Out (0).

The "LLDP Statistics Local Counters" section shows a table with the following data:

Local Interface	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded
GigabitEthernet 1/1	0	0	0	0	0
GigabitEthernet 1/2	0	0	0	0	0
GigabitEthernet 1/3	0	0	0	0	0
GigabitEthernet 1/4	165	0	0	0	0
GigabitEthernet 1/5	0	0	0	0	0
GigabitEthernet 1/6	0	0	0	0	0

Figure 2-11-2 LLDP-Ports Statistics Screen

2.12 Loop Protection

After clicking "Information & Status" > "Loop Protection", following screen will appear as:

Clients can go to Section "Advanced Configure" > "Loop Protection" to do the detailed management.

Loop Protection Status

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

Figure 2-12 Loop Protection Screen

2.13 Spanning Tree

After clicking "Information & Status" > "Loop Protection", following screen will appear as:

Clients can go to Section "Advanced Configure" > "STP" to do the detailed management.

STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768 08-ED-02-59-4A-EE	32768 08-ED-02-50-10-C0	35	2000	Steady	0d 00:49:25

Figure 2-13-1 Spanning Tree Bridge Status Screen

2.13.1 Bridge Status

STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	DesignatedPort	Forwarding	0d 01:23:19
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	Disabled	Discarding	-
11	Disabled	Discarding	-
12	Disabled	Discarding	-
13	Disabled	Discarding	-
14	Disabled	Discarding	-
15	Disabled	Discarding	-
16	Disabled	Discarding	-
17	Disabled	Discarding	-
18	Disabled	Discarding	-
19	Disabled	Discarding	-
20	Disabled	Discarding	-
21	Disabled	Discarding	-
22	Disabled	Discarding	-
23	Disabled	Discarding	-

Figure 2-13-2 Spanning Tree Port Status Screen

2.13.2 Port Status

2.13.3 Port Status

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
4	0	2513	0	0	0	0	0	0	0	0

Figure 2-13-3 Spanning Tree Port Statistics Screen

After clicking "Information & Status" > "IGMP Snooping", following screen will appear as: Clients can go to Section "Advanced Configure" > "IGMP Snooping" to do the detailed management.

2.14 IGMP Snooping

2.14.1 IGMP Status

VLAN ID	Querier Version	Host Version	Querier Status	Traffic

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-

Figure 2-14-1 IGMP Snooping Status Screen

2.14.2 Group Information

Information & Status

- System Information
- IP Status
- SysLog
- Detailed SysLog
- MAC Table
- VLANs
- Ports
- LACP
- Thermal Protection
- Green Ethernet
- LLDP
- Loop Protection
- Spanning Tree
- IGMP Snooping**
 - Status
 - Groups Information**
 - IPv4 SFM Information
- MLD Snooping
- DHCP
- Security
- QoS

IGMP Snooping Group Information

Start from VLAN and group address

VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
No more entries																	

Figure 2-14-2 IGMP Snooping Group Information Screen

2.14.3 IPv4 SFM

Information & Status

- System Information
- IP Status
- SysLog
- Detailed SysLog
- MAC Table
- VLANs
- Ports
- LACP
- Thermal Protection
- Green Ethernet
- LLDP
- Loop Protection
- Spanning Tree
- IGMP Snooping**
 - Status
 - Groups Information
 - IPv4 SFM Information**
- MLD Snooping
- DHCP
- Security
- QoS

IGMP SFM Information

Start from VLAN and Group

VLAN ID	Group	Port	Mode	Source Address
No more entries				

Figure 2-14-3 IGMP Snooping IPv4 SFM Information Screen

2.15 MLD Snooping

After clicking "Information & Status" > "MLD Snooping", following screen will appear as:

2.15.1 MLD Status

Clients can go to Section "Advanced Configure" > "IPv6 MLD Snooping" to do the detailed management.

MLD Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-

Figure 2-15-1 MLD Snooping Status Screen

MLD Snooping Group Information

Start from VLAN and group address

VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
<i>No more entries</i>																	

Figure 2-15-2 MLD Snooping Groups Information Screen

2.15.3 MLD IPv6
SFM

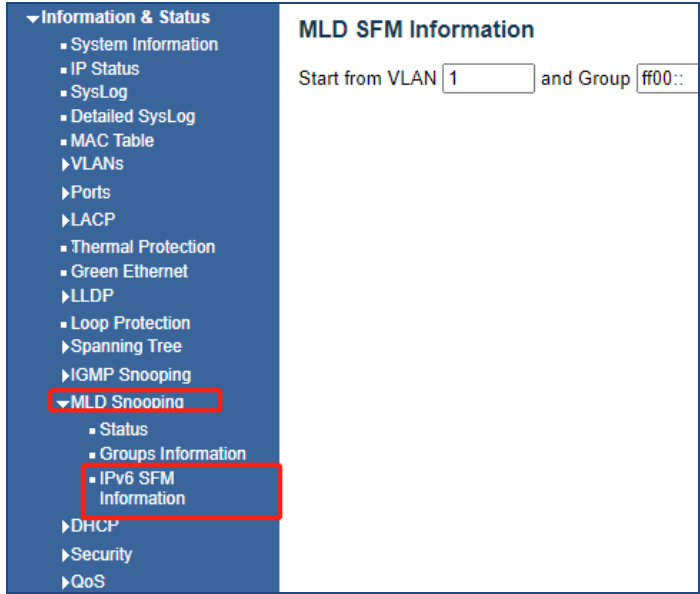


Figure 2-15-3 MLD Snooping IPv6 SFM Information Screen

2.16 DHCP
2.16.1 Server

After clicking "Information & Status" > "DHCP", following screen will appear as:
Clients can go to Section "DHCP" to do the detailed management.

2.16.1-1 Statistics

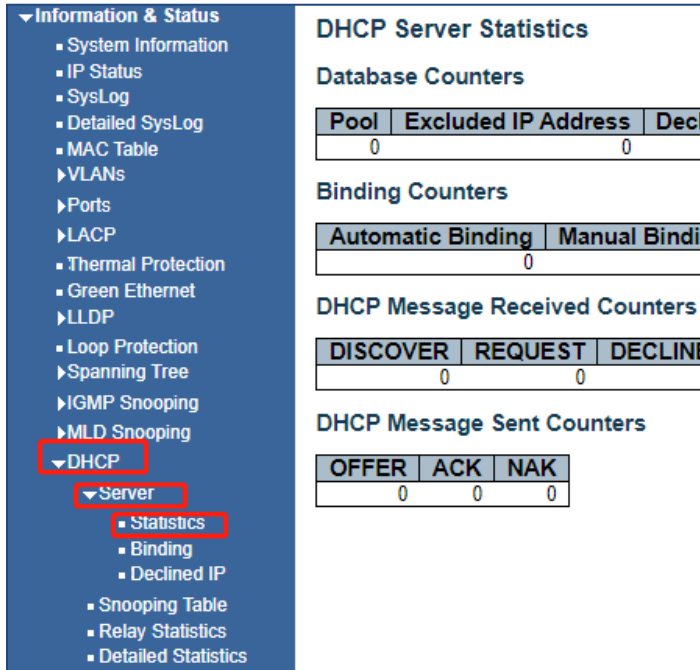
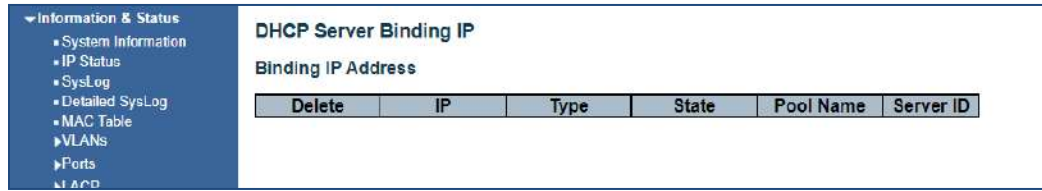


Figure 2-16-1 DHCP Server Statistics Screen

2.16.1-2 Binding

Information & Status>DHCP>Server>Binding

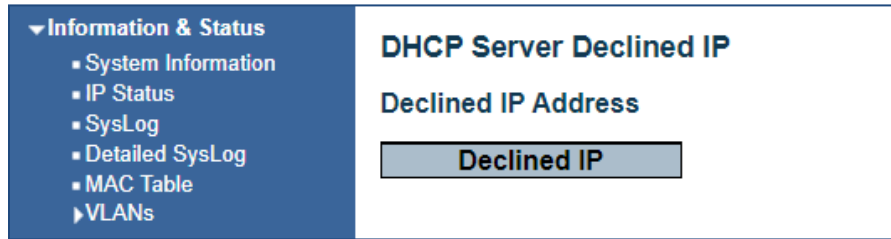


Figure

2-16-2 DHCP Server Binding

2.16.1-3 Declined IP

This screen displays the IP addresses that are connected to the DHCP server



Information & Status>DHCP>Server>Declined IP

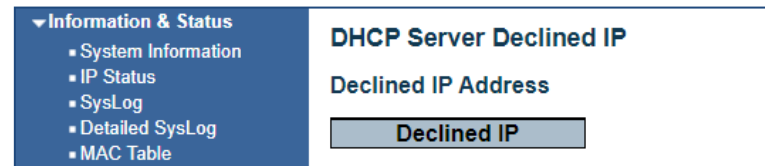


Figure 2-16-3 DHCP Server Declined IP

2.16.2 Snooping Table

This screen displays IP address that cannot or did not join as a DHCP address

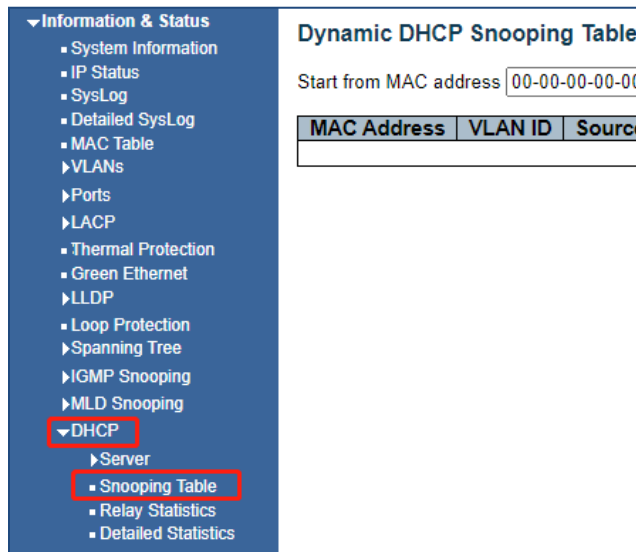


Figure 2-16-2 DHCP Server Binding Screen

2.16.3 Relay Statistics

The screenshot shows the DHCP Relay Statistics screen. On the left is a navigation menu with 'DHCP' expanded to show 'Relay Statistics'. The main content area is titled 'DHCP Relay Statistics' and contains two summary tables.

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Mis Agent Opti
0	0	0	0

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option
0	0	0	0

Figure 2-16-3 DHCP Relay Statistics Screen

2.16.4 Detailed Statistics

The screenshot shows the DHCP Detailed Statistics Port 1 screen. On the left is a navigation menu with 'DHCP' expanded to show 'Detailed Statistics'. The main content area is titled 'DHCP Detailed Statistics Port 1' and contains a table with a 'Combined' view selector.

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

Figure 2-16-4 DHCP Detailed Statistics Screen

2.17 Security

2.17.1 Post Security

2.17.1-1 Switch

After clicking "Information & Status" > "Security" > Port Security, the following screen will appear. Clients can go to Section "Security Configure" to do the detailed management.

Port Security Switch Status

User Module Legend

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

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	---	Disabled	-	-
2	---	Disabled	-	-
3	---	Disabled	-	-
4	---	Disabled	-	-
5	---	Disabled	-	-
6	---	Disabled	-	-
7	---	Disabled	-	-
8	---	Disabled	-	-
9	---	Disabled	-	-
10	---	Disabled	-	-
11	---	Disabled	-	-
12	---	Disabled	-	-
13	---	Disabled	-	-
14	---	Disabled	-	-
15	---	Disabled	-	-
16	---	Disabled	-	-
17	---	Disabled	-	-
18	---	Disabled	-	-
19	---	Disabled	-	-

Figure 2-17-1 Security - Port Security - Switch Screen

2.17.1-2 Port

Port Security Port Status Port 1

MAC Address	VLAN ID	State	Time of
No MAC addresses attached			

Figure 2-17-1-2 Security - Port Security - Port Screen

2.17.2 Access Management Statistics

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

Figure 2-17-2 Security - Port Security - Access Screen

2.17.3 802.1x
2.17.3-1 Switch

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	
5	Force Authorized	Globally Disabled			-	
6	Force Authorized	Globally Disabled			-	
7	Force Authorized	Globally Disabled			-	
8	Force Authorized	Globally Disabled			-	
9	Force Authorized	Globally Disabled			-	
10	Force Authorized	Globally Disabled			-	
11	Force Authorized	Globally Disabled			-	
12	Force Authorized	Globally Disabled			-	
13	Force Authorized	Globally Disabled			-	
14	Force Authorized	Globally Disabled			-	
15	Force Authorized	Globally Disabled			-	
16	Force Authorized	Globally Disabled			-	
17	Force Authorized	Globally Disabled			-	

Figure 2-17-3 Security - 802.1X - Switch Screen

2.17.3-2 Port

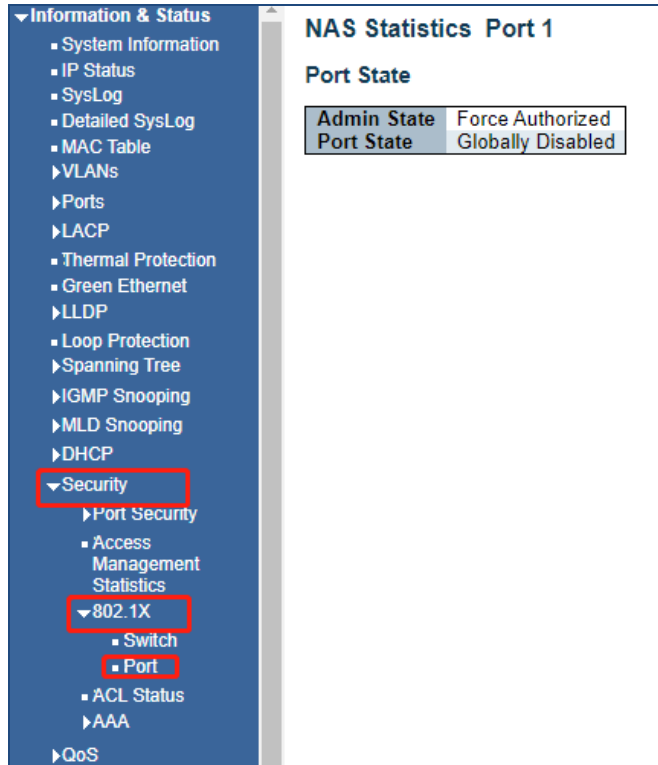


Figure 2-17-3-2 Security - 802.1X - Port Screen

2.17.4 ACL Status

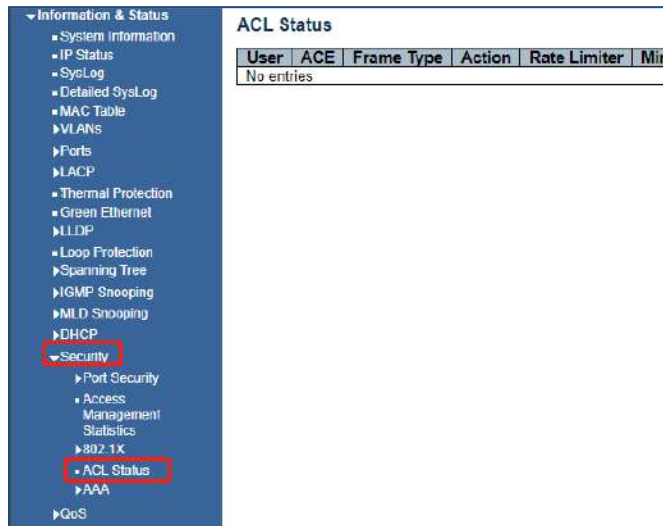


Figure 2-17-6 Security - ACL Status Screen

2.17.5 AAA

2.17.5-1 RADIUS Overview
Overview

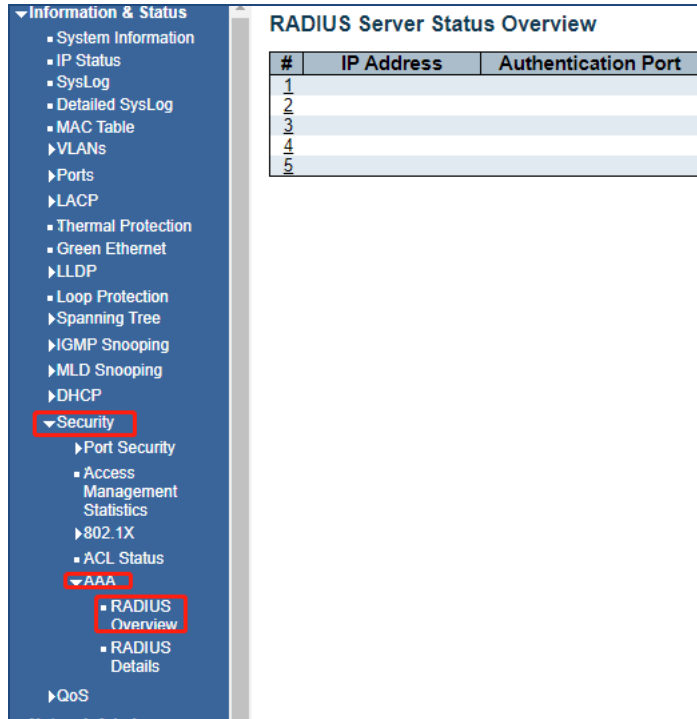


Figure 2-17-7 Security - AAA - RADIUS Overview Screen

2.17.5-2 RADIUS
Details

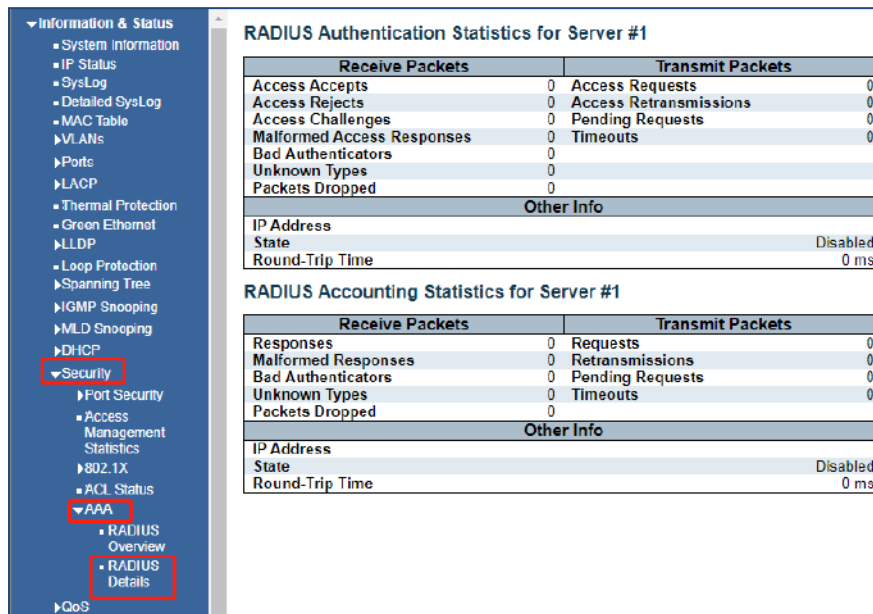


Figure 2-17-8 Security - AAA - RADIUS Details Screen

2.18 QOS

2.18.1 QOS Statistics

After clicking "Information & Status" > "Security", following screen will appear as:
 Clients can go to Section "QOS" Configure" to do the detailed management.

Queuing Counters																
Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	93884	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9737
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 2-18-1 QOS Statistics Screen

2.18.2 QOS Status

QoS Control List Status																
User	QCE	Port	Frame Type	Action												
				CoS	DPL	DSCP	PCP	DE								
No entries																

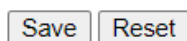
Figure 2-18-2 QOS Status Screen

Section 3: Network Management- Set up and Operations

3. Network Management

Important note:

After entering an operation, in order to save the setting, select the "Save" button. After programming if you want to change a setting select the Reset button and re-enter your required programming



The following menus are the found in the Network Admin Section

3.1 IP Configuration

Note: IP address of switch is 192.168.0.1 by default, and the default subnet mask is 255.255.255.0(24)

Clicking "Network Admin" > "IP Config", screen will show as:

Figure 3-1 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.

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

3.2 IP Status

3.2 IP Status

Clicking "Network Admin" > "IP Status ", screen will show as:

The IP links connected to the switch will be displayed

- ▼ Information & Status
 - System Information
 - IP Status
 - SysLog
 - Detailed SysLog
 - MAC Table
 - ▶ VLANs
 - ▶ Ports
 - ▶ LACP
 - Thermal Protection
 - Green Ethernet
 - ▶ LLDP
 - Loop Protection
 - ▶ Spanning Tree
 - ▶ IGMP Snooping
 - ▶ MLD Snooping
 - ▶ DHCP
 - ▶ Security
 - ▶ QoS
- ▼ Network Admin
 - IP Config

IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	08-ed-02-59-4a-ee	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.1/24	
VLAN1	IPv6	fe80::aed:2ff:fe59:4aee/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

ARP Table

IP Address	Link Address
192.168.0.102	VLAN1:bc-14-ef-ee-91-df
fe80::aed:2ff:fe59:4aee	VLAN1:08-ed-02-59-4a-ee

DHCP Server>Mode Configuration

3.2.1 DHCP

- ▼ Information & Status
 - System Information
 - IP Status
 - SysLog
 - Detailed SysLog
 - MAC Table
 - ▶ VLANs
 - ▶ Ports
 - ▶ LACP
 - Thermal Protection
 - Green Ethernet
 - ▶ LLDP
 - Loop Protection
 - ▶ Spanning Tree
 - ▶ IGMP Snooping
 - ▶ MLD Snooping
 - ▶ DHCP
 - ▶ Security

DHCP Server Mode Configuration

Global Mode

Mode: ▼

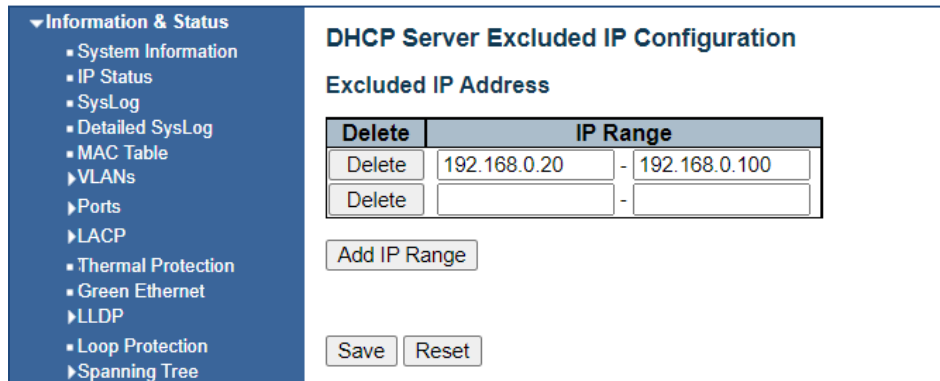
VLAN Mode

Delete	VLAN Range	Mode
<input type="button" value="Delete"/>	<input type="text" value="1"/> - <input type="text" value="5"/>	<input type="text" value="Enabled"/> ▼
<input type="button" value="Delete"/>	<input type="text"/> - <input type="text"/>	<input type="text" value="Enabled"/> ▼

Enable the mode and enter the VLAN range that will have access to DHCP servers.

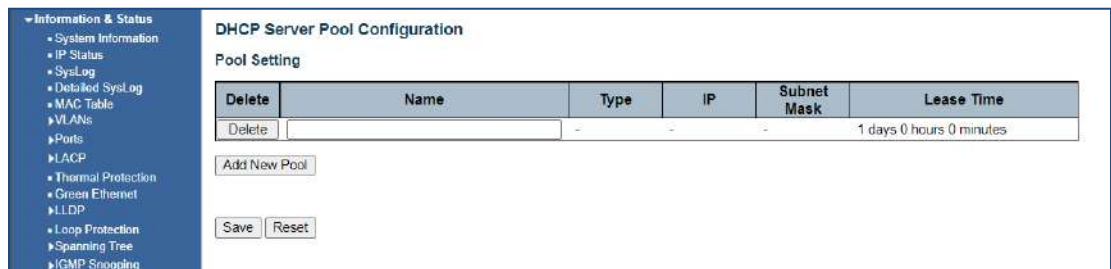
3.2.2 DHCP Server Excluded IP Configuration

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



Enter the IP ranges for devices that will be connected to the DHCP Server

3.2.3 DHCP Server Pool Configuration



This section will define a group of IP address that will be allowed DHCP participation

3.3 NTP Configuration

NTP (Network Time Protocol) is a protocol used to synchronize the time of each computer in the network. Its purpose is to synchronize the clock of the computer to the world coordinates UTC, its accuracy can reach 0.1 ms in the LAN and 1-50 MS in most places on the Internet.

Clicking "Network Admin" > "NTP", screen will show as:

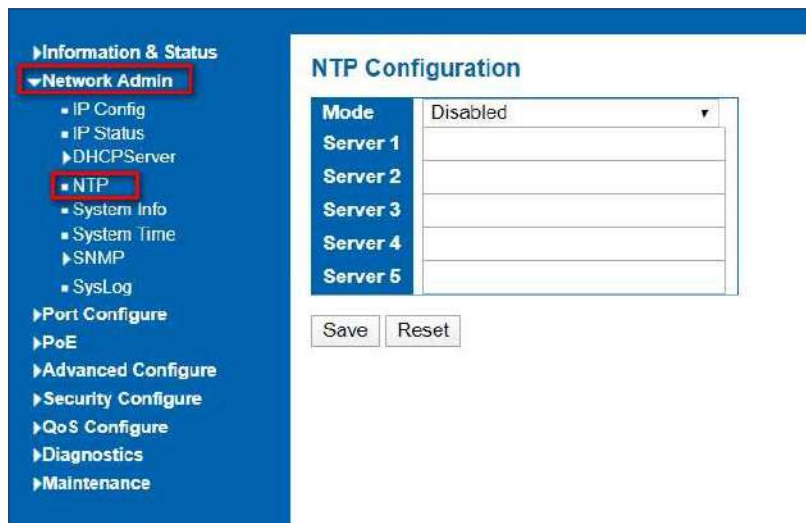


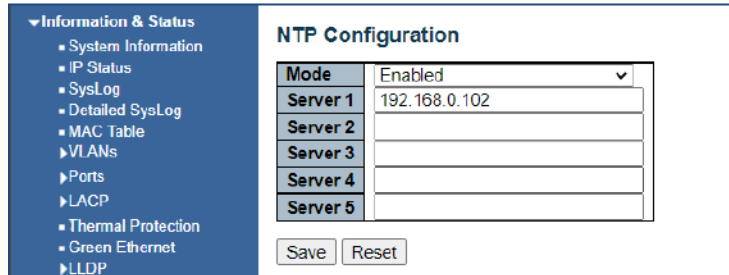
Figure 3-3 NTP Configuration Screen

3.3.1 NTP Address assignment

Clicking "Save" to save settings.

Client can use time zone configuration to set system time zone offset (minutes), and Client can synchronize PC Web browser time to the switch local time as well.

Clicking "Network Admin" > "System Time", screen will show as:



3.3.2 Time reference confirmation and offset

Time and date are referenced from any connected device in the system that provides time and date Use the drop-down menu to confirm the correct date format

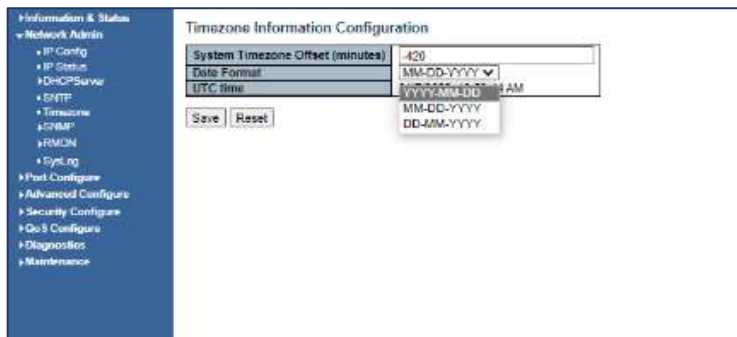


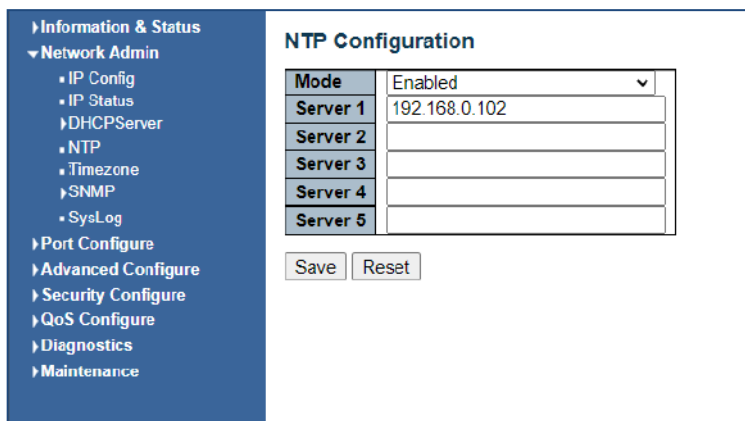
Figure 3-3.2 Time zone Configuration Screen

Clicking "Save" to save settings.

The time zone setting will show the time and date as connect to a network source. This source can be independent of an NTP source.

3.3.3 Setting Time Zone as NTP Source

If the NTP source is the address of the system computer all timing from the switch be referenced to that time and date.



3.4 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 switch support SNMPv1, v2c. Different versions of SNMP provides different security level 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. 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:

- private – allow authentication management station to read, write and edit MIB object

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. Switch uses standard MIB-II information management module. So, MIB object value can be read by any SNMP web-managed software.

We can provide ALL the MIBs file including private MIBs to client if requested.

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

3.4.1 SNMP System

SNMP System Configuration	
Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e50171000001

Configuration object and description is:

Object	Description
Mode	Enabled or Disable SNMP function
Version	Clicking 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.

3.4.2 SNMP Trap Configuration

User can enable or disable SNMP Trap function and set configuration. Clicking "Network Admin" > "SNMP" > "Trap", then this screen will show as:

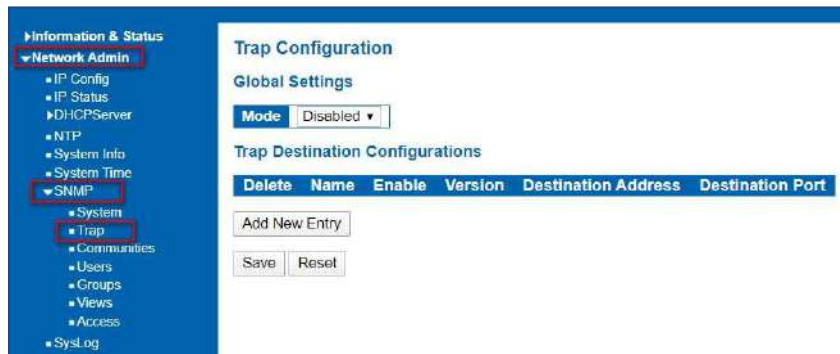


Figure 3-4.2 SNMP Trap Configuration Screen

3.4.3 SNMP Community Configuration

Users can set SNMPv3 Community function. Clicking "Network Admin" > "SNMP" > "Communities", then this screen will show as:

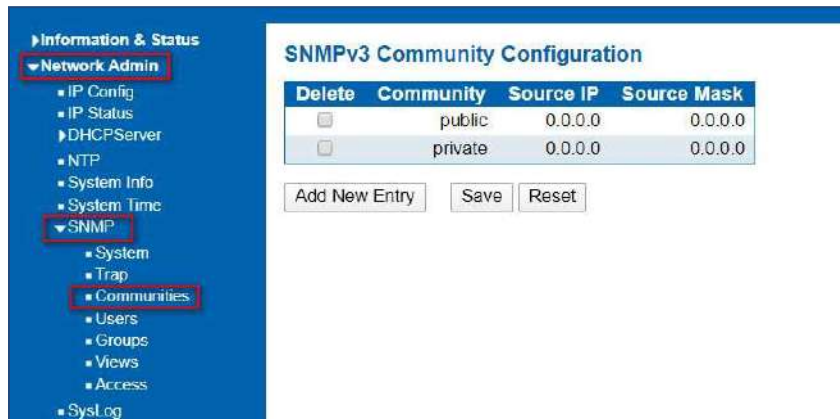


Figure 3-4.3 SNMP Communities Configuration Screen

3.4.4 SNMP user

Users can set SNMPv3 User function. Clicking "Network Admin" > "SNMP" > "User", then this screen will show as:



Figure 3-4.4 SNMP User Configuration Screen

3.4.5 SNMP Groups Configuration

Users can set SNMPv3 Group function. Clicking "Network Admin" > "SNMP" > "Groups", then this screen will show as:

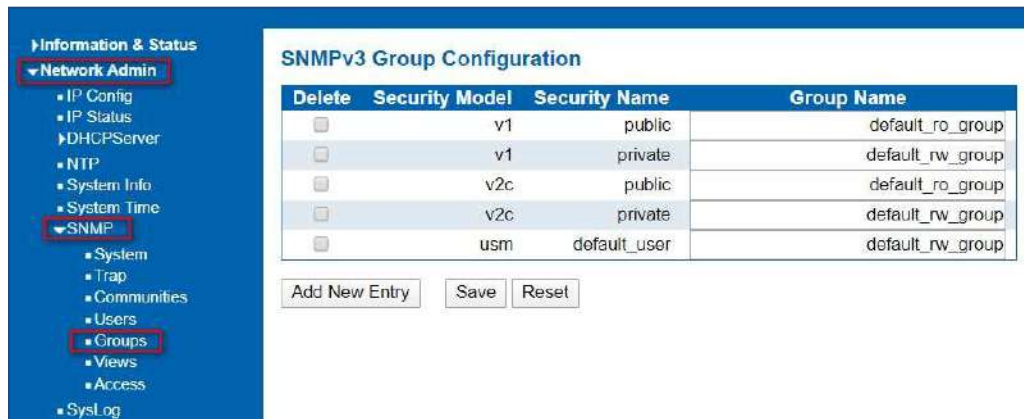


Figure 3-4.5 SNMP Group Configuration Screen

3.4.6 SNMP Views Configuration

Users can set SNMPv3 Group function. Clicking "Network Admin" > "SNMP" > "Views", then this screen will show as:



Figure 3-4.6 SNMP View Configuration Screen

3.4.7 SNMP Access Configuration

Users can set SNMPv3 Group function. Clicking "Network Admin" > "SNMP" > "Access", then this screen will show as:

The screenshot displays the 'SNMPv3 Access Configuration' interface. On the left, a navigation menu is visible with 'Network Admin' expanded to 'SNMP', and 'Access' selected. The main area contains a table with the following data:

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view ▼	None ▼
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view ▼	default_view ▼

Below the table, there are three buttons: 'Add New Entry', 'Save', and 'Reset'.

Figure 3-4.7 SNMP Access Configuration Screen

3.5 System Log Configuration

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

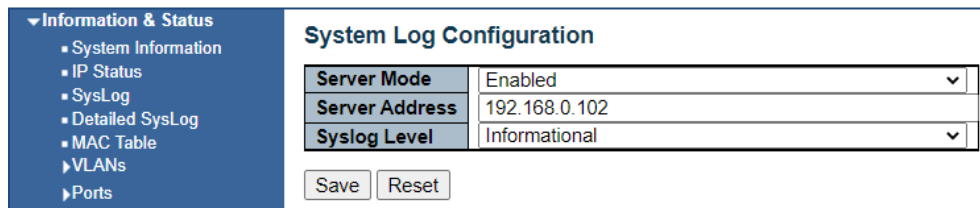


Figure 3-5 System Log Configuration Screen

Configuration object and description is:

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

Section 4: Port Configure

4.1 Port Configuration

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

Port	Description	Link	Current	Speed Configured	Adv Duplex Fdx	Hdx	Adv speed 10M	100M	1G	Flow Control Enable	Curr Rx	Curr Tx	Maximum Frame Size
1		Down	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600
2		Up	Up	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600
3		Down	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600
4		Down	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600
5		Down	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600
6		Down	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600
7		Down	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600
8		Down	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600
9		Down	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600
10		Down	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600
11		Down	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600
12		Down	Down	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9600

Figure 4-1 System Log Configuration 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.

Clicking "Save" to store and active settings.

4.2 Link Aggregation

Users can set up multiple links among multiple switches. Link Aggregation, is a method that tie some physical ports together as one logic port, to enlarge bandwidth. This switch supports up to 6 groups Link Aggregation, 2 to 8 ports as one group.

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

In this page, user can configure static aggregation of switch's ports. After clicking the menu "Port Configure" > "Aggregation" > "Static", following window will appear for making static aggregation settings.

4.2.1 Static Aggregation

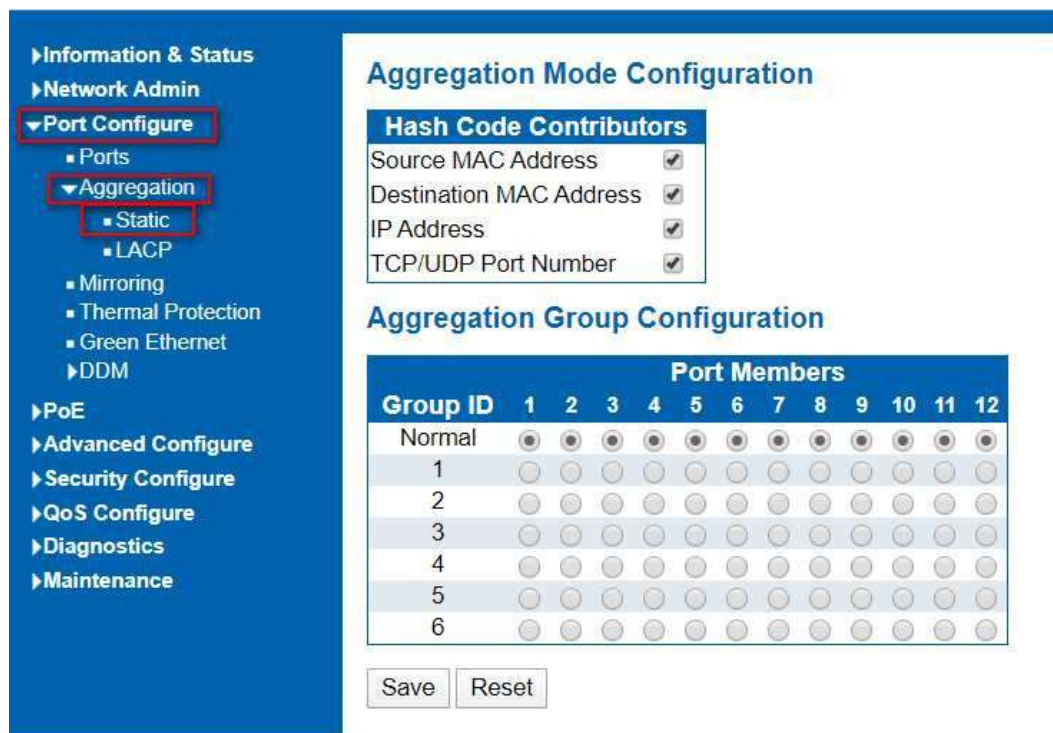


Figure 4-2.1 Port Static Aggregation Configuration Screen

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 sample switch supports up to 6 groups Link Aggregation, 2 to 8 port as one group.

Clicking "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.

4.2.2 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 LACP configuration in following screen.



Figure 4-2.2 LACP Configuration Screen

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.

Clicking "Save" to store and active settings.

4.3 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 clicking "Port Configure" > "Mirroring". Then following screen will appear as:

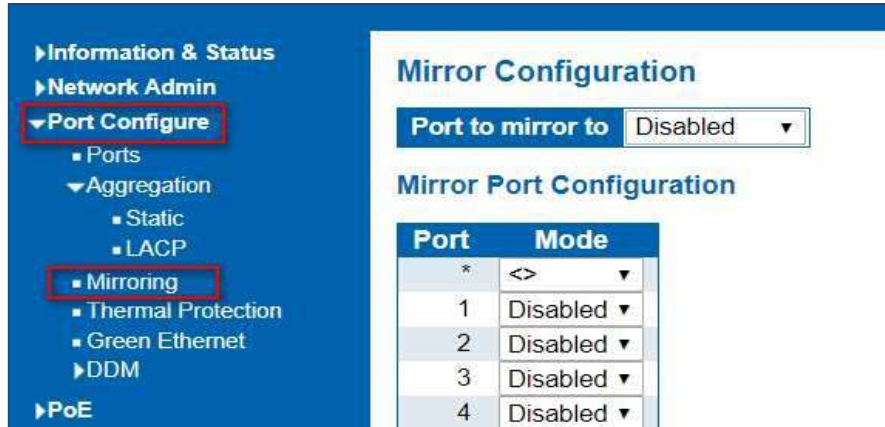


Figure 4-3 Mirroring Configuration Screen

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	<p>Select source port mirror mode.</p> <p>Rx only Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.</p> <p>Tx only Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.</p> <p>Disabled Neither frames transmitted nor frames received are mirrored.</p> <p>Enabled Frames received and frames transmitted are mirrored on the mirror port.</p> <p>Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror mirror port Tx frames. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.</p>

Clicking "Save" to store and active 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, destination port should have equal or higher speed comparing to source port. Besides, source port and destination port should not be same one.

4.4 Thermal Protection Configuration

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

The highest programmable setting is 115C

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

Thermal Protection Configuration

Temperature settings for groups

Group	Temperature	
0	80	°C
1	80	°C
2	0	°C
3	0	°C

Port groups

Port	Group
*	<>
1	Disabled
2	Disabled

Figure 4-4 Mirroring 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.

Clicking "Save" to store and active settings.

Note: By default, all ports of switch are belonging to Priority Group 0, with protected temperature 115-degree C.

4.5 Green Ethernet

After clicking "Port Configure" > "Green Ethernet", following screen will appear as:

Port Power Savings Configuration

Optimize EEE for: Latency

Port Configuration

Port	ActiPHY	PerfectReach	EEE	EEE Urgent Queues									
				1	2	3	4	5	6	7	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"/>
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"/>
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"/>
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"/>
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"/>
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"/>
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"/>
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"/>
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"/>
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"/>
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"/>

Figure 4-5 Green Ethernet Configuration Screen

After clicking "Port Configure" > "DDM(DDMI)", following screen will appear as:

4.6 DDM

DDMI Configuration

Mode: Enabled

Save Reset

Figure 4-6.1 DDM (DDMI) Configuration Screen

Information & Status		DDMI Overview					
Port	Vendor	Part Number	Serial Number	Revision	Data Code	Transceiver	
9	-	-	-	-	-	-	
10	-	-	-	-	-	-	
11	-	-	-	-	-	-	
12	-	-	-	-	-	-	
13	-	-	-	-	-	-	
14	-	-	-	-	-	-	
15	-	-	-	-	-	-	
16	Vigtron	V101310sm-H	CIB210105280	A □□	2021-01-05	1000BASE_LX	
17	-	-	-	-	-	-	
18	-	-	-	-	-	-	
19	-	-	-	-	-	-	
20	-	-	-	-	-	-	
21	-	-	-	-	-	-	
22	-	-	-	-	-	-	
23	-	-	-	-	-	-	
24	-	-	-	-	-	-	
25	-	-	-	-	-	-	
26	-	-	-	-	-	-	
27	-	-	-	-	-	-	
28	-	-	-	-	-	-	
29	-	-	-	-	-	-	
30	-	-	-	-	-	-	
31	-	-	-	-	-	-	
32	-	-	-	-	-	-	
33	-	-	-	-	-	-	
34	-	-	-	-	-	-	
35	Vigtron, Inc.	V11310G10SM	8201014013	□□	2020-10-20	10G	
36	-	-	-	-	-	-	

Figure 4-6.2 DDM Overview Screen

4.7 DDMI

DDMI Transceiver and Information Screen

Information & Status		Transceiver Information	
Vendor	Vigtron	Part Number	V101310sm-H
Part Number	V101310sm-H	Serial Number	CIB210105280
Serial Number	CIB210105280	Revision	
Revision		Data Code	2021-01-05
Data Code	2021-01-05	Transceiver	1000BASE_LX
Transceiver	1000BASE_LX		

DDMI Information		Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	31.575			90.000	85.000	-40.000	-45.000
Voltage(V)	3.3150			3.6000	3.5000	3.1000	3.0000
Tx Bias(mA)	16.872			90.000	85.000	3.000	2.000
Tx Power(mW)	0.2541			0.6310	0.5012	0.1258	0.1000
Rx Power(mW)	0.7225			1.0000	0.7943	0.0040	0.0032

Figure 4-6.3 DDM Detailed Screen

Section 5: Advanced Configure

5. Advanced Configure

5.1 MAC Address Table

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

Figure 6-1 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 <ol style="list-style-type: none"> 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. Clicking "Add New Static Entry" to create a new record.

Clicking "Save" to store and active settings

5.2 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 divide one physical LAN into multiple broadcast area network (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.

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



Figure 6-2 802.1Q 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	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.

	<p>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.</p> <p>Grayed out fields show the value that the port will get when the mode is applied.</p> <p>Access:</p> <p>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 ➤ On egress all frames classified to the Access VLAN are transmitted untagged. ➤ Other (dynamically added VLANs) are transmitted tagged <p>Trunk:</p> <p>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:</p> <p>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 untagged 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:</p> <p>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:</p> <p>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:</p> <p>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>S-Custom-Port:</p> <p>On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ether type 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.</p> <p>If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.</p> <p>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>Tagged and Untagged</p> <p>Both tagged and untagged frames are accepted.</p> <p>Tagged Only</p> <p>Only tagged frames are accepted on ingress. Untagged frames are discarded.</p> <p>Untagged Only</p> <p>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>Untagged Port VLAN</p> <p>Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.</p> <p>Tag All</p> <p>All frames, whether classified to the Port VLAN or not, are transmitted with a tag.</p> <p>Untagged All</p> <p>All frames, whether classified to the Port VLAN or not, are transmitted without a tag.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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>

Clicking "Save" to store and active settings.

After clicking "Advanced Configure" > "Voice Vlan", following screen will appear as:

5.3 Voice VLAN

Voice VLAN Configuration

Mode	Disabled
VLAN ID	1000
Aging Time	86400 seconds
Traffic Class	7 (High)

Port Configuration

Port	Mode	Security	Discovery Protocol
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI

Figure 5-3.1 Voice Vlan configuration screen

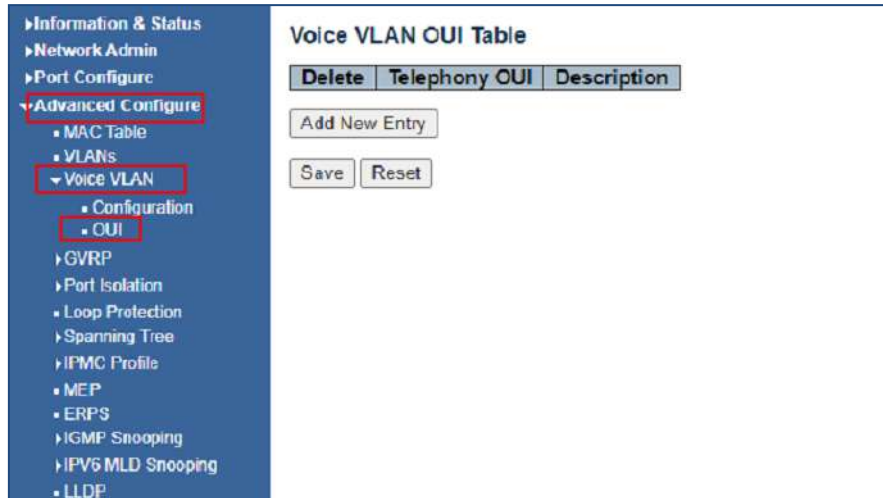


Figure 5-3.2 Voice Plan OUI screen

5.4 GVRP

Adjacent Virtual Local Area Network (VLAN)-aware devices can exchange VLAN information with each other with the use of the Generic VLAN Registration Protocol (GVRP). GVRP is based on the Generic Attribute Registration Protocol (GARP) and propagates VLAN information throughout a bridged network. When GVRP is activated, it transmits and receives GARP Packet Data Units (GPDUs). This allows you to configure a VLAN on one switch and then propagate its information across the network, instead of the previously required creation of the VLAN on each switch in the network.

Clicking "Advanced Configure"> "GVRP" to see the configuration screen as following:

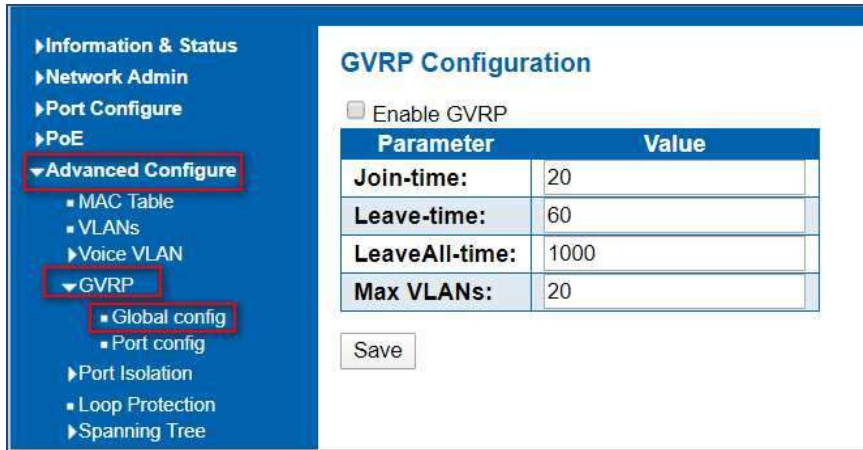


Figure 5.4.1 GVRP configuration screen

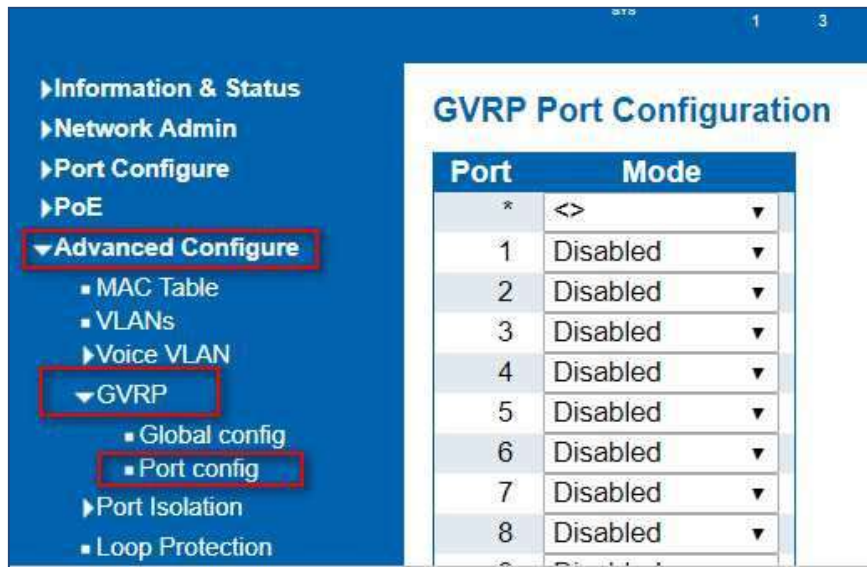


Figure 5.4.2 GVRP configuration screen

5.5 Port Isolation

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

This switch support port groups. Members of port group can forward data.

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

5.5.1 Port Group

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

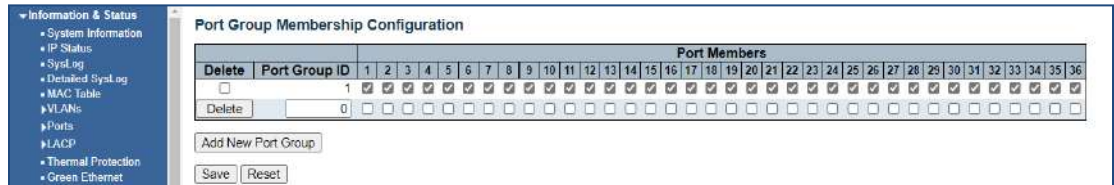


Figure 5-5.1 Port Group Configuration Screen

Configuration object and description is:

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

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

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

5.5.2 Port Isolation

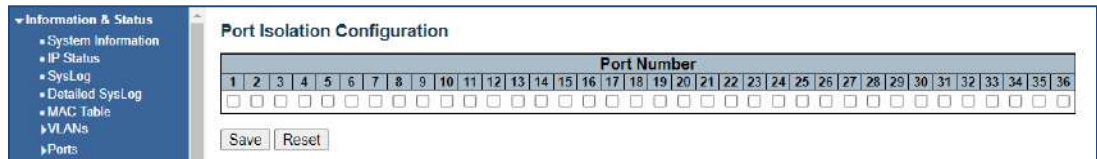


Figure 5-5.2 Port Isolation Configuration Screen

Configuration object and description is:

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

Clicking "Save" to store and active settings.

5.6 Loop Protection

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

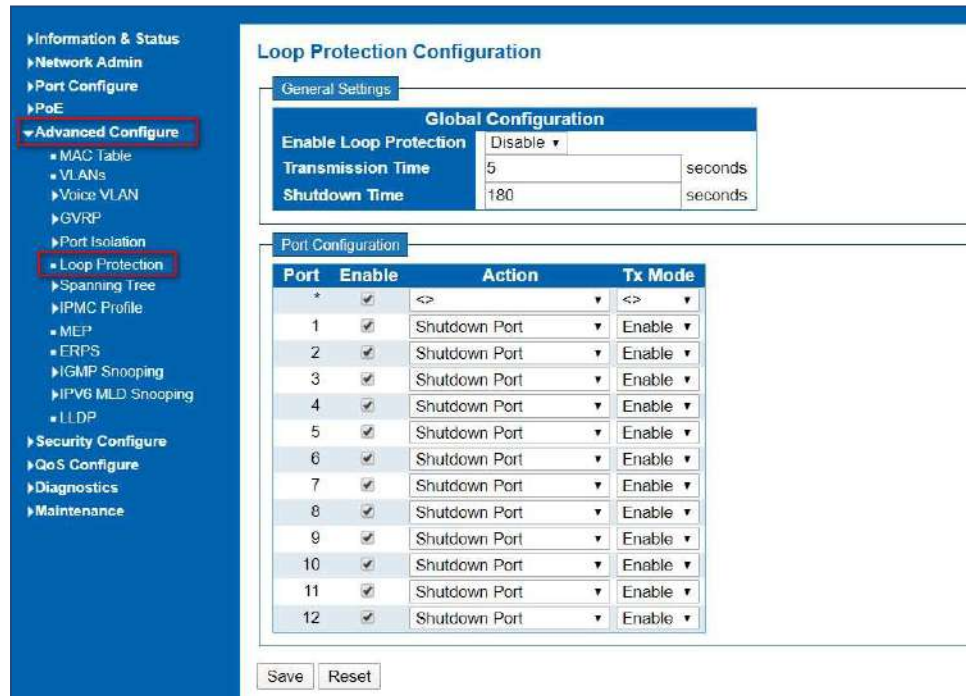


Figure 5.6 Loop Protection Configuration Screen

Configuration object and description is:

Object	Description
Global Configuration	Enable Loop Protection: clicking 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 takes 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.

Clicking "Save" to store and active settings.

5.7 STP- Spanning Tree

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.

5.7.1 Bridge Setting

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

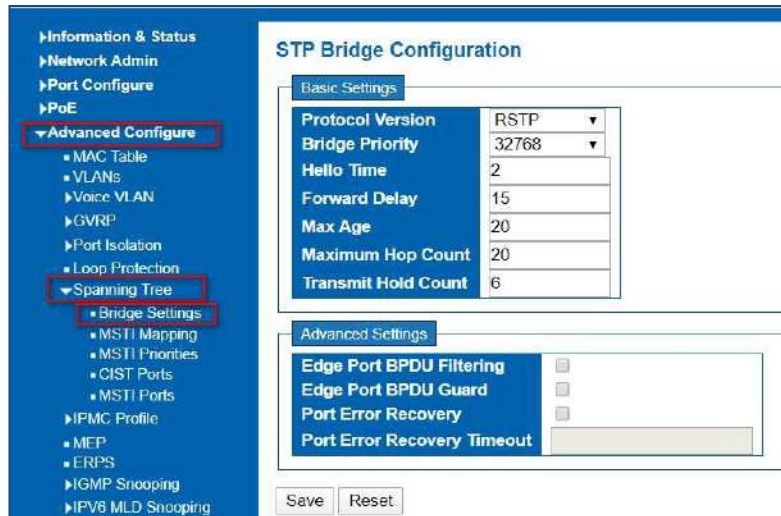


Figure 5.7.1 Spanning Tree Configuration Screen

Configuration object and description is:

Object	Description
Protocol Version	Clicking drop-down menu to select STP protocol version, including: STP - Spanning Tree Protocol (IEEE802.1D); RSTP - Rapid Spanning Tree Protocol (IEEE802.1w)
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.

5.7.2 MSTI Mapping

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well. The MSTI Configuration screen in Figure 5-6-2-1 appears.

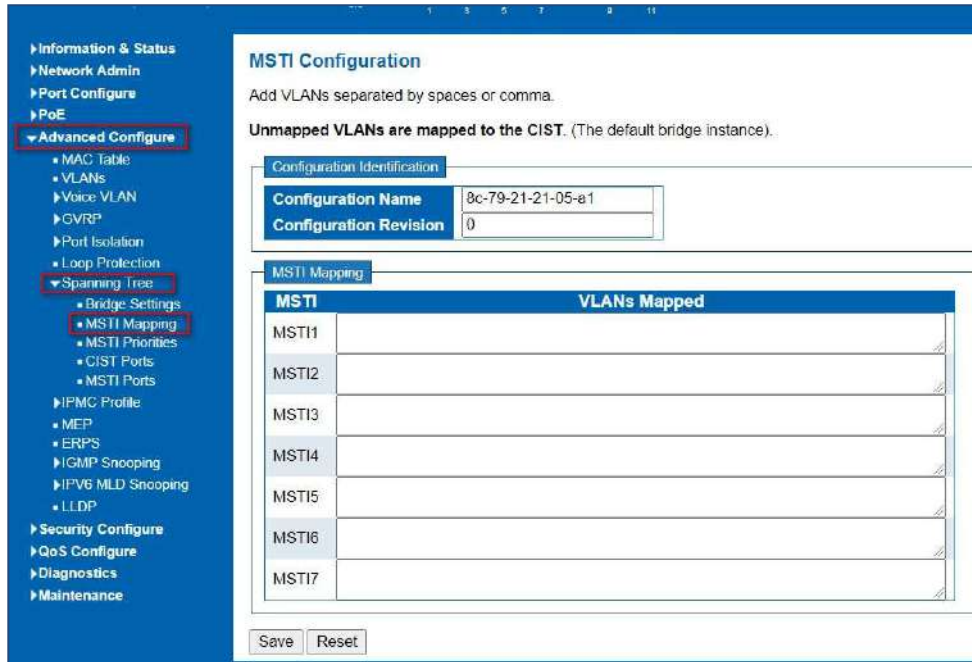


Figure 5.7.2 MSTI Configuration Page Screenshot The page includes the following fields:

Configuration Identification

Object	Description
Configuration Name	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to- MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is at most 32 characters.
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

Object	Description
MSTI	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
VLANs Mapped	The list of VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e., not having any VLANs mapped to it.)

Buttons

: Clicking to apply changes

: Clicking to undo any changes made locally and revert to previously saved values

5.7.3 MSTI Priorities

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well. The MSTI Priority screen in Figure6- 7-3-1 appears.

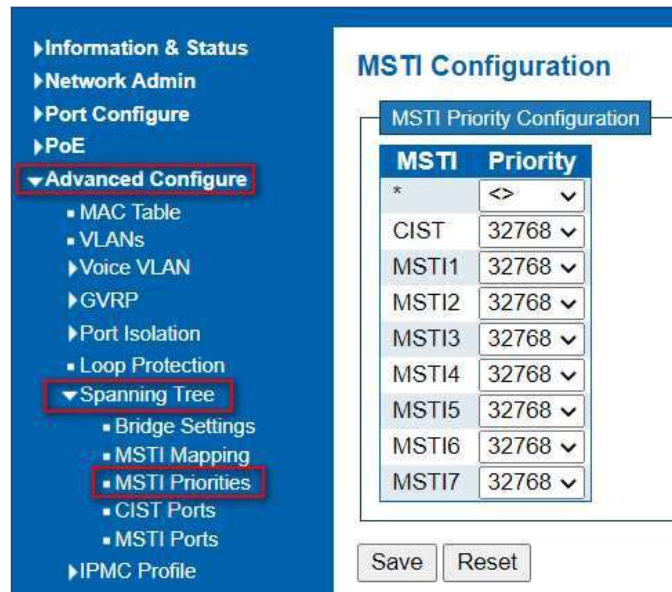
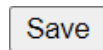


Figure 6-7.3 MSTI Priority Page Screenshot

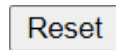
The page includes the following fields:

Object	Description
MSTI	The bridge instances. The CIST is the default instance, which is always active.
Priority	Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Buttons



: Clicking to apply changes



: Clicking to undo any changes made locally and revert to previously saved

values

5.7.4 CIST Ports

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well. The CIST port Configuration screen in Figure appears.

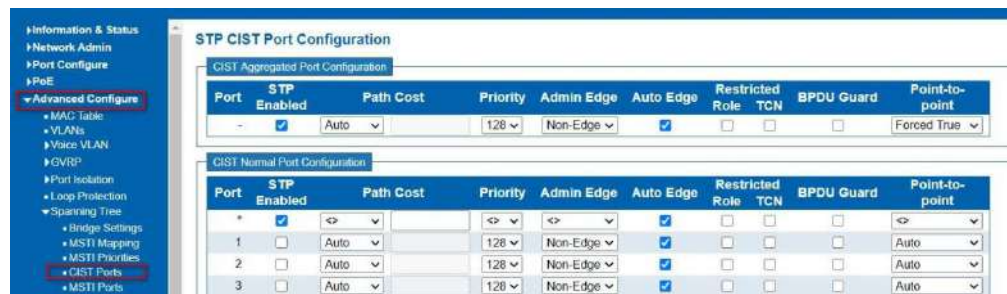


Figure 5.7.4 STP CIST Port Configuration Screenshot

Configuration object and description is:

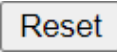
Object	Description
Port	The switch port number of the logical STP port
STP Enabled	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-

	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) Default: 128 Range: 0-240, in steps of 16
Admi Edge	Controls whether the operEdge flag should start as being set or cleared. (The initial operEdge state when a port is initialized).
Auto Edge	Controls whether the bridge should enable automatic edge deection on the bridge port. This allows operEdge to be derived from whether DPDU's are received on the port or not.
Restricted Role	If enabled, caused the port nor to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Altermatic Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard .
Restricted TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.
BPDU Guard	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
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. Transitions to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons



: Clicking to apply changes



: Clicking to undo any changes made locally and revert to previously saved

values

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 802.1w standard exceeds 65,535, the default is set to 65,535

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 5.7.4 Recommended STP Path Cost Range

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

Table 5.7.4 Recommended STP Path Costs

Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex	2,000,000
	Full Duplex	1,000,000
	Trunk	500,000
Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000
Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

Table 5.7.4 Default STP Path Costs

5.7.5 MSTI Ports

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well. A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are global. The MSTI Port Configuration screen in Figure 6-7-5- 1& Figure 6-7-5-2 appears.

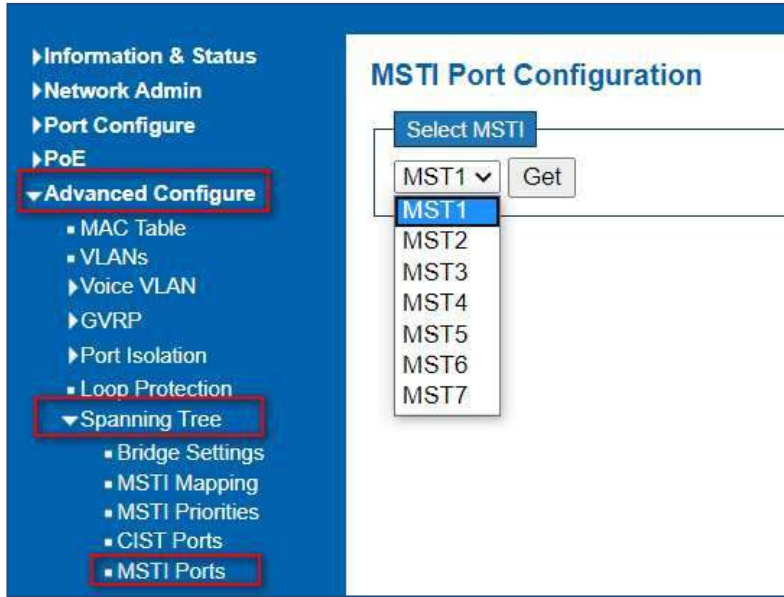


Figure 5-7.5 MSTI Port Configuration Page Screenshot

The page includes the following fields:

MSTI Port Configuration

Object	Description
Select MSTI	Select the bridge instance and set more detail configuration.

Figure 5.7.5 MST1 MSTI Port Configuration Page Screenshot

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
4	Auto	128
5	Auto	128

The page includes the following fields:

MSTx MSTI Port Configuration

Object	Description
Select MSTI	The switch port number of the corresponding STP CIST (and MSTI) port.
Path cost	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.

Buttons

: Clicking to set MSTx configuration

: Clicking to apply changes

: Clicking to undo any changes made locally and revert to previously saved values

5.8 IPMC Profile



5.8.1 Profile Table

This page provides IPMC Profile related configurations. The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each. The Profile Table screen in Figure 6-8-1 appears.



Figure 5-8.1 IPMC Profile Configuration Page

The page includes the following fields:

Object	Description
Global Profile Mode	Enable/Disable the Global IPMC Profile. System starts to do filtering based on profile settings only when the global profile mode is enabled.
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
Profile Name	The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.
Profile Description	Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.
Rule	When the profile is created, clicking the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons:  : List the rules associated with the designated profile.
	: Adjust the rules associated with the designated profile.

Buttons

Add New IPMC Profile : Clicking to add new IPMC profile. Specify the name and configure the new entry. Clicking "Save".

Save

: Clicking to apply changes

Reset

: Clicking to undo any changes made locally and revert to previously saved Value.

Address Entry

5.8.2 Address Entry

This page provides address range settings used in IPMC profile. The address entry is used to specify the address range that will be associated with IPMC Profile. It is allowed to create at maximum 128 address entries in the system. The Profile Table screen in Figure 5.8.2 appears

Figure 5-8.2 IPMC Profile Address Configuration Page

The page includes the following fields:

Object	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
Entry Name	The name used for indexing the address entry table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present
Start Address	The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.
End Address	The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

Buttons

Add New Address (Range) Entry

: Clicking to add new address range. Specify the name and configure the addresses. Clicking "Save".

Save

: Clicking to apply changes

Reset

: Clicking to undo any changes made locally and revert to previously saved

values

5.9 MEP

MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

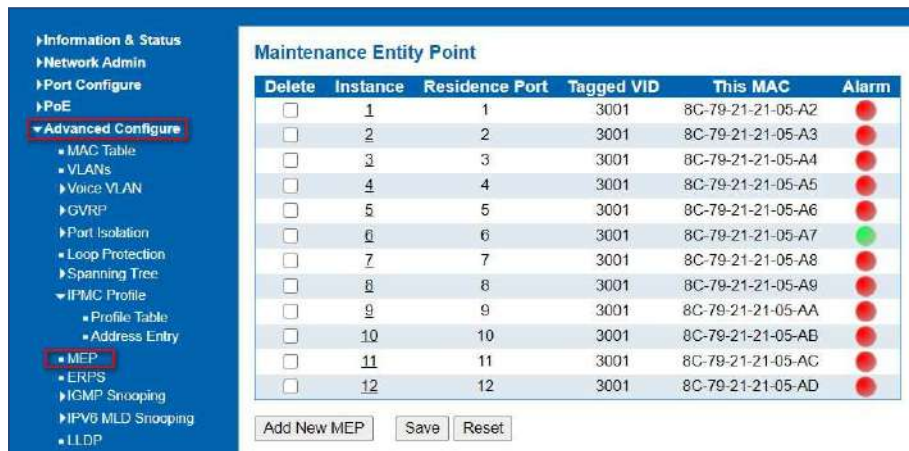


Figure 5-9 MEP Page

5.10 ERPS

ERPS (Ethernet Ring Protection Switching), it integrates OAM function and 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 ", following screen will appear.



Figure 5-10-1 ERPS Configuration Screen

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 type as Major Ring ID.
R-APS VLAN (1- 4094)	Define VLAN for R - APS VLAN.

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

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

Figure 5-10-2 ERPS Ring Configuration Screen

Configuration object and description is:

Rapid Ring Configuration 1 Auto-refresh Refresh

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: 1min Revertive VLAN config

RPL Configuration

RPL Role: None RPL Port: None Clear

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	SF	SF DNF BPR0			0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Blocked	Blocked	<input checked="" type="checkbox"/>

Save | Reset

Object	Description
WTR(Wait to Restore) Time(1-12)	Clicking 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 clickinged " VLAN config ", it will go the page of Rapid Ring VLAN Configuration.
RPL Role	Clicking drop-down menu to select "None", "RPL Owner", or "RPL Neighbor" role.
RPL Port	Clicking drop-down menu to select "None", "East Port", or "West Port".

Clicking "Save" to store and active settings.

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

Rapid Ring VLAN Configuration 1

Information & Status
 Network Admin
 Port Configure
 PoE
 Advanced Configure
 MAC Table
 VLANs
 Voice VLAN
 GVRP
 Port Isolation

Delete VLAN ID

Add New Entry | Back

Save | Reset

Figure 5-10-3 Rapid Ring VLAN Configuration Screen

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

5.11 IGMP Snooping

5.11.1 Basic Configuration

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.

Basic Configuration

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

IGMP Snooping Configuration			
Global Configuration			
Snooping Enabled	<input type="checkbox"/>		
Unregistered IPMCv4 Flooding Enabled	<input checked="" type="checkbox"/>		
IGMP SSM Range	232.0.0.0	/	8
Leave Proxy Enabled	<input type="checkbox"/>		
Proxy Enabled	<input type="checkbox"/>		
Port Related Configuration			
Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
12	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Save Reset

Figure 5-11-1 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

Clicking "Save" to store and active settings.

5.11.2 IGMP Snooping VLAN Configuration

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



Figure 5-11-2 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.

Clicking "Save" to store and active settings.

5.11.3 IGMP Snooping Port Filtering Profile

IGMP Snooping Port Filtering Profile

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

IGMP filtering enables you to assign a profile to a switch port that specifies

multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.

IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace". If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group. The IGMP Snooping Port Group Filtering Configuration screen in Figure 5-10-3 appears

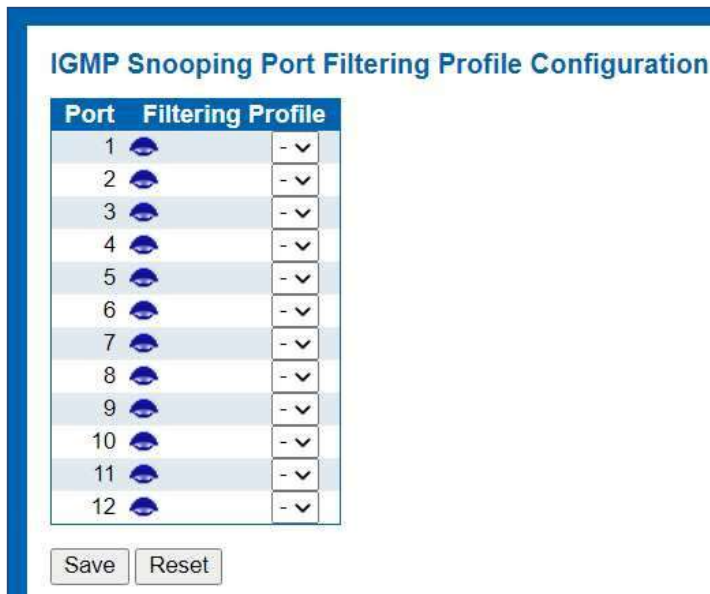


Figure 5-11-4: IGMP Snooping Port Filtering Profile Configuration Page Screenshot

Configuration object and description

Object	Description
Port	The logical port for the settings
Filtering Profile	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Buttons

Save

: Clicking to apply changes

Reset

: Clicking to undo any changes made locally and revert to previously saved values.

5.12 IPV6 MLD Snooping

This page provides MLD Snooping related configuration. The MLD Snooping Configuration screen in Figure 6-11-1 appears

5.12.1 Basic Configuration

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
*	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
12	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Save Reset

Figure 5-12-1: MLD Snooping Configuration Page Screenshot

Configuration object and description is:

Object	Description
Snooping Enabled	Enable the Global MLD Snooping
Unregistered IPMCv6 Flooding enabled	Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.
MLD SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
Leave Proxy Enable	Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enable	Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
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. The allowed selection is Auto, Fix, Fone, default compatibility value is Auto.
Fast Leave	Enable the fast leave on the port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

Save

: Clicking to apply changes

Reset

: Clicking to undo changes made locally and revert to previously saved values.

5.12.2 VLAC Configuration

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the

web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. The MLD Snooping VLAN Configuration screen in Figure5-12-2 appears.

MLD Snooping VLAN Configuration

Start from VLAN with 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)
Delete	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	MLD-Auto	0	2	125	100	10	1

Figure 6-12-2: IGMP Snooping VLAN Configuration Page Screenshot

Configuration object and description is:

Object	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
Vlan ID	The VLAN ID of the entry.
MLD Snooping Enable	Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.
Querier Election	Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.
Compatibility	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is MLD-Auto, Forced MLDv1, Forced MLDv2, default compatibility value is MLD-Auto.
PRI	(PRI) Priority of Interface. It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (Best effort) to 7 (highest), default interface priority value is 0
RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255, default robustness variable value is 2
QI	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.
QRI	Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).
LLQI (LMQI for IGMP)	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).
URI	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons



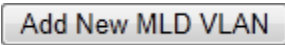
: Refreshes the displayed table starting from the "VLAN" input fields.



: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.



: Updates the table, starting with the entry after the last entry currently displayed.



: Clicking to add new MLD VLAN. Specify the VID and configure the new entry. Clicking "Save". The specific MLD VLAN starts working after the corresponding static VLAN is also created.



: Clicking to apply changes



: Clicking to undo any changes made locally and revert to previously saved values.

5.12.3 Port Filtering Profile

Port

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The MLD filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and MLD throttling limits the number of simultaneous multicast groups a port can join.

MLD filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. A MLD filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, MLD join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the MLD join report is forwarded as normal. If a requested multicast group is denied, the MLD join report is dropped.

MLD throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace". If the action is set to deny, any new MLD join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group. The MLD Snooping Port Group Filtering Configuration screen in Figure 5-12-3 appears

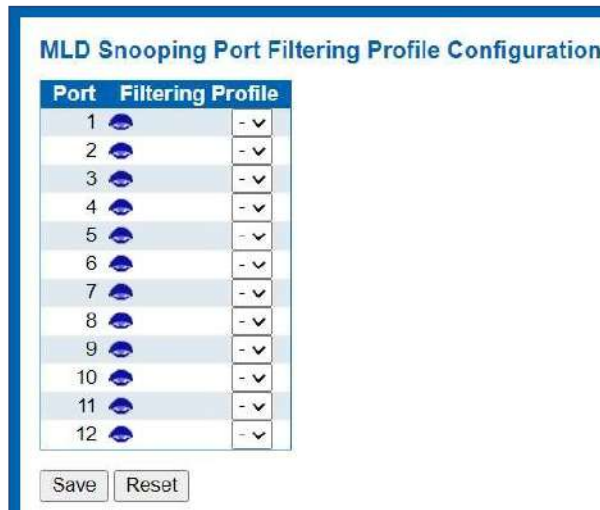


Figure 5-12-3: MLD Snooping Port Group Filtering Configuration Page Screenshot

Configuration object and description is:

Object	Description
Port	The logical port for the settings
Filtering Group	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button

Buttons



: Clicking to apply changes



: Clicking to undo any changes made locally and revert to previously saved values.

5.13 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", following screen will appear.

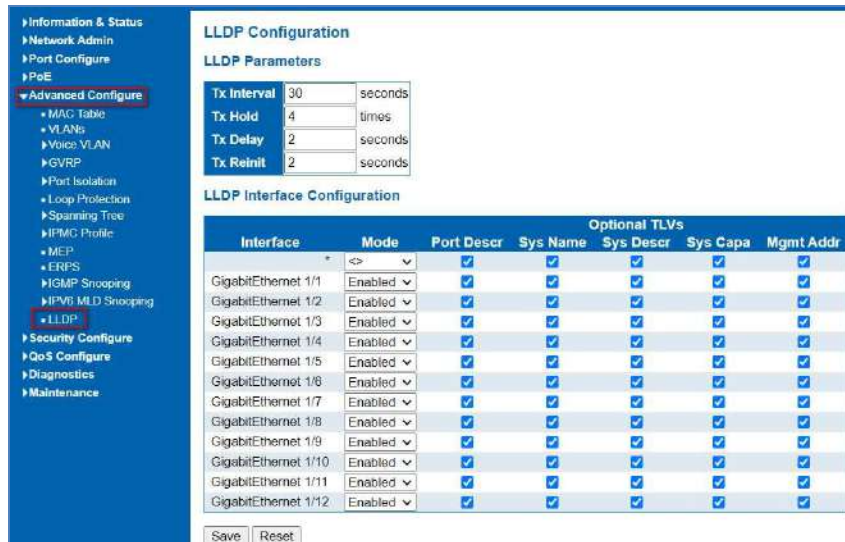


Figure 5-13 LLDP Configuration Screen

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 following 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

Clicking "Save" to store and active settings.

Section 6: Security Configure

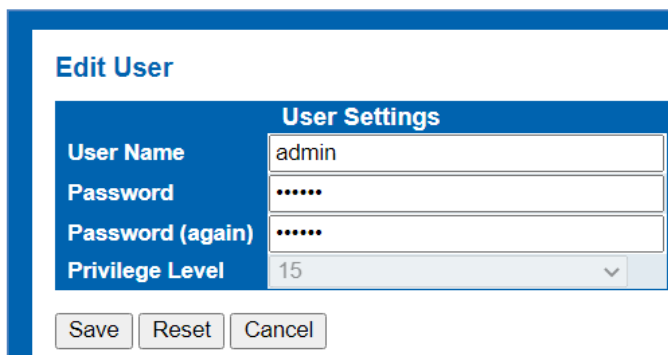
6. Security Configure

6.1 User configuration

Users can add user to manage the switch, please clicking "Security Configure">" Users">" Add New User"



Figure 6.1 Users Configuration Screen



Clicking "Save" to store and active settings.

Note: Privilege Level 15 is the highest management authority.

This page provides an overview of the privilege levels. After setup is completed, please press the "Apply" button to take effect. Please login web interface with new user name and password and the screen in Figure 6-2-1 appears. please clicking "Security Configure">" Privilege Levels".

6.2 Privilege Levels

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
DDMI	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
Diagnostics	5	10	5	10
EPS	5	10	5	10
ERPS	5	10	5	10
ETH_LINK_OAM	5	10	5	10
EVC	5	10	5	10
Green_Ethernet	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10

Figure 6-2Privilege Configuration Screen

The page includes the following fields:

Object	Description
Group Name	<p>The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contain more than one. The following description defines these privilege level groups in details:</p> <p>System: Contact, Name, Location, Timezone, Log</p> <ul style="list-style-type: none"> ➤ Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP source guard. ➤ IP: Everything except 'ping'. ➤ Port: Everything except 'VeriPHY'. ➤ Diagnostics: 'ping' and 'VeriPHY'. ➤ Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance. ➤ Debug: Only present in CLI.
Privilege Level	Status/statistics read-write (e.g. for clearing of statistics).

Buttons



: Clicking to apply changes



: Clicking to undo any changes made locally and revert to previously saved values.

6.3 SSH configuration

Configure SSH on this page. This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

Users can enable or disable the SSH configuration, please clicking "Security Configure">"SSH".

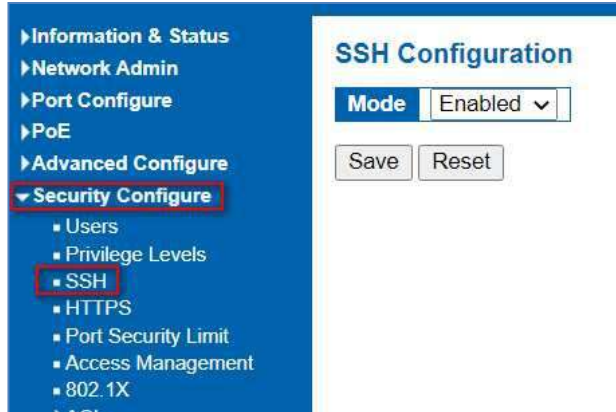


Figure 7-3 SSH Configuration Screen

The page includes the following fields:

Object	Description
Mode	<p>Indicates the SSH mode operation. Possible modes are:</p> <ul style="list-style-type: none"> ➤ Enabled: Enable SSH mode operation. ➤ Disabled: Disable SSH mode operation.

Buttons



: Clicking to apply changes



: Clicking to undo any changes made locally and revert to previously saved values.

6.4 HTTPS configuration

Users can configure HTTPS function, please clicking "Security Configure">" HTTPS".



Figure 6.5 HTTPS Configuration Screen

The page includes the following fields:

Object	Description
Mode	<p>Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are:</p> <ul style="list-style-type: none"> ➤ Enabled: Enable HTTPS mode operation. ➤ Disabled: Disable HTTPS mode operation.
Automatic Redirect	<p>Indicates the HTTPS redirect mode operation. It only significant if HTTPS mode "Enabled" is selected. Automatically redirects web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled or redirects web browser to an HTTP connection when both are disabled. Possible modes are:</p> <ul style="list-style-type: none"> ➤ Enabled: Enable HTTPS redirect mode operation. ➤ Disabled: Disable HTTPS redirect mode operation.
Certificate Maintain	<p>The operation of certificate maintenance. Possible operations are: None: No operation. Delete: Delete the current certificate. Upload: Upload a certificate PEM file. Possible methods are: Web Browser or URL. Generate: Generate a new self-signed RSA certificate.</p>
Certificate Pass Phrase	<p>Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.</p>
Certificate Upload	<p>Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem</p> <p>Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g., Firefox v37 and Chrome v39.</p> <p>Possible methods are: Web Browser: Upload a certificate via Web browser. URL: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is</p> <p><protocol>://[<username>[:<password>] @]< host>[:<port>][/<path>]/<file_name>.</p> <p>For example, tftp://10.10.10.10/new_image_path/new_image.dat, http://username:password@10.10.10.10:80/new_image_path/new_image.dat. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score (_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.</p>
Certificate Status	<p>Display the current status of certificate on the switch. Possible statuses are:</p> <p>Switch secure HTTP certificate is presented. Switch secure HTTP certificate is NOT presented. Switch secure HTTP certificate is generating</p>

Buttons

Save

: Clicking to apply changes

Reset

: Clicking to undo any changes made locally and revert to previously saved values.

Refresh

6.5 Ports Security Limit configuration

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

Port Security Limit Control Configuration

System Configuration

Mode: Disabled
Aging Enabled:
Aging Period: 3600 seconds

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<>	4	<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9	Disabled	4	None	Disabled	Reopen
10	Disabled	4	None	Disabled	Reopen
11	Disabled	4	None	Disabled	Reopen
12	Disabled	4	None	Disabled	Reopen

Save Reset

Figure 6.5 IP&MAC Guard-Port Configuration Screen

Configuration object and description is:

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

Clicking "Save" to store and active settings.

6.6 Access Management configuration

Configure access management table on this page. The maximum entry number is 16. If the application's type matches any one of the access management entries, it will allow access to the switch.



The Access Management Configuration screen in Figure 6.6 appears.

Program the range of address that will be allowed access the communication methods

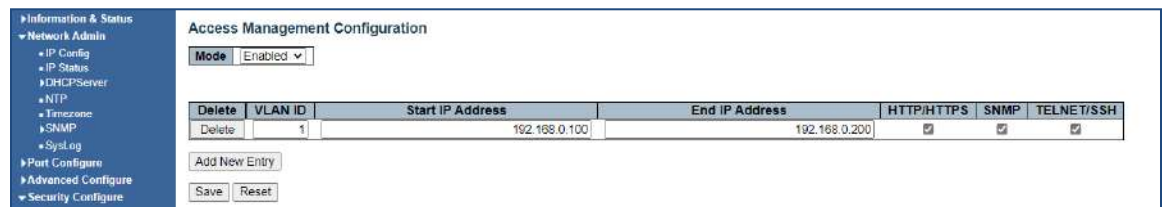


Figure 6-6-1: Access Management Configuration Overview Page Screenshot

The page includes the following fields:

Object	Description
Mode	Indicates the access management mode operation. Possible modes are: Enabled: Enable access management mode operation. Disabled: Disable access management mode operation.
Delete	Check to delete the entry. It will be deleted during the next apply
VLAN ID	Indicates the VLAN ID for the access management entry
Start IP address	Indicates the start IP address for the access management entry
End IP address	Indicates the end IP address for the access management entry
HTTP/HTTPS	Indicates the host can access the switch from HTTP/HTTPS interface that the host IP address matched the entry
SNMP	Indicates the host can access the switch from SNMP interface that the host IP address matched the entry
Telnet/SSH	Indicates the host can access the switch from TELNET/SSH interface that the host IP address matched the entry

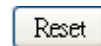
Buttons



: Clicking to add a new access management entry.



: Clicking to apply changes



: Clicking to undo any changes made locally and revert to previously saved valu

6.7 802.1X configuration

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", following screen will appear.

Network Access Server Configuration

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
RADIUS-Assigned QoS Enabled	<input type="checkbox"/>
RADIUS-Assigned VLAN Enabled	<input type="checkbox"/>
Guest VLAN Enabled	<input type="checkbox"/>
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	<input type="checkbox"/>

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
1	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
2	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
5	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize

Figure 6.7 802.1X 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	Clicking drop-down menu to select a Admin State. Available options: Force Authorized, Force Unauthorized, 802.1X, Mac-based Auth.

Clicking "Save" to store and active settings.

6.8 ACL configuration

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.

6.8.1 ACL Ports Configure

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



Figure 6-8-1 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.

Clicking "Save" to store and active settings.

6.8.2 Rate Limiter Configuration

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

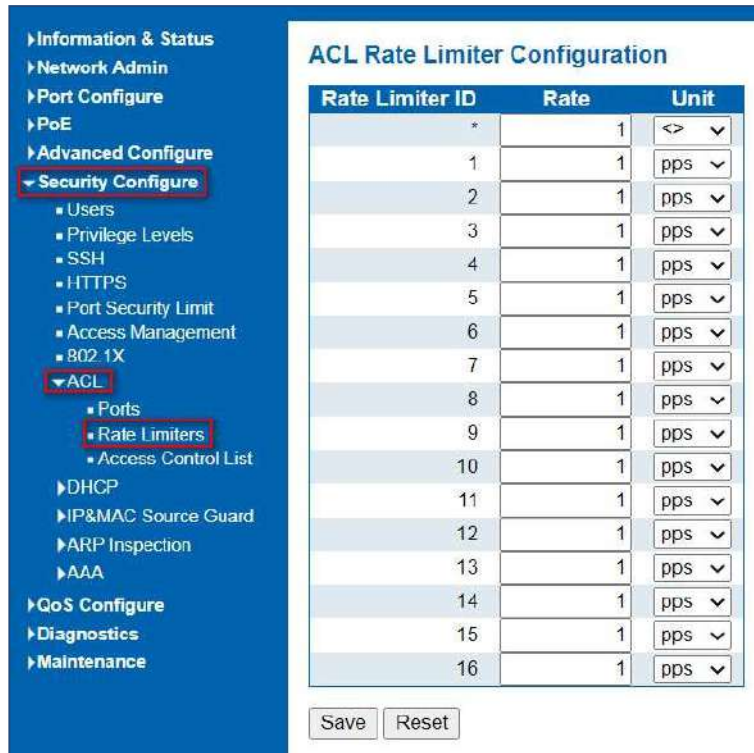


Figure 6-8-2 ACL Rate Limiters Configuration Screen


Clicking "Save" to store and active settings.

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

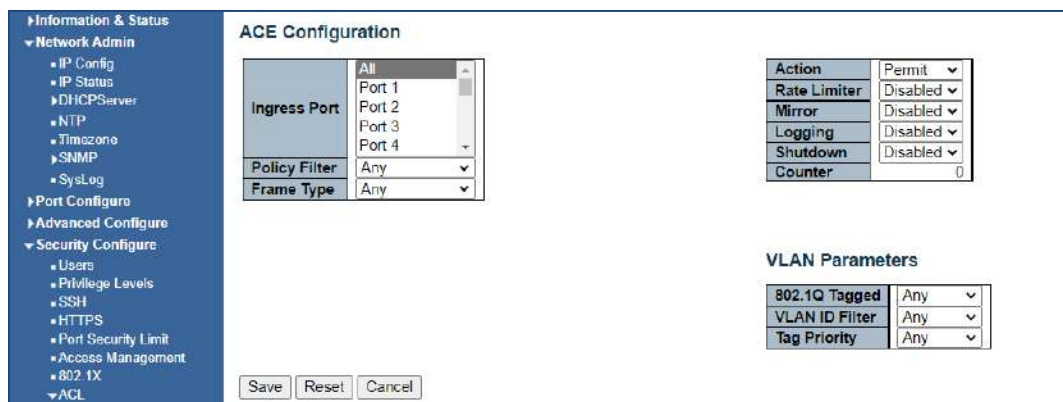
6.8.3 Access Control List Configuration



Figure 6-8-3 Access Control Limiters Configuration Screen

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

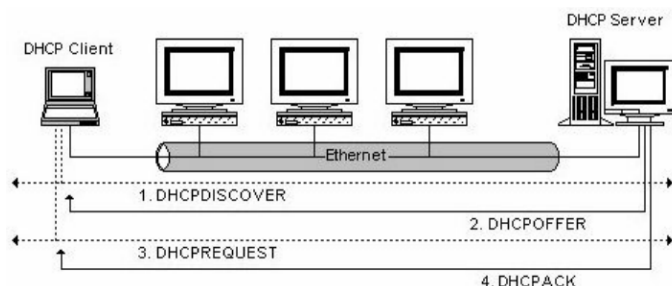
6.8.3.1 ACE Configuration



6.9 DHCP

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.

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 entrusted 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 entrusted 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 entrusted ports in the same VLAN.

If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

6.9.1 DHCP Snooping Configure

Snooping Setting

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

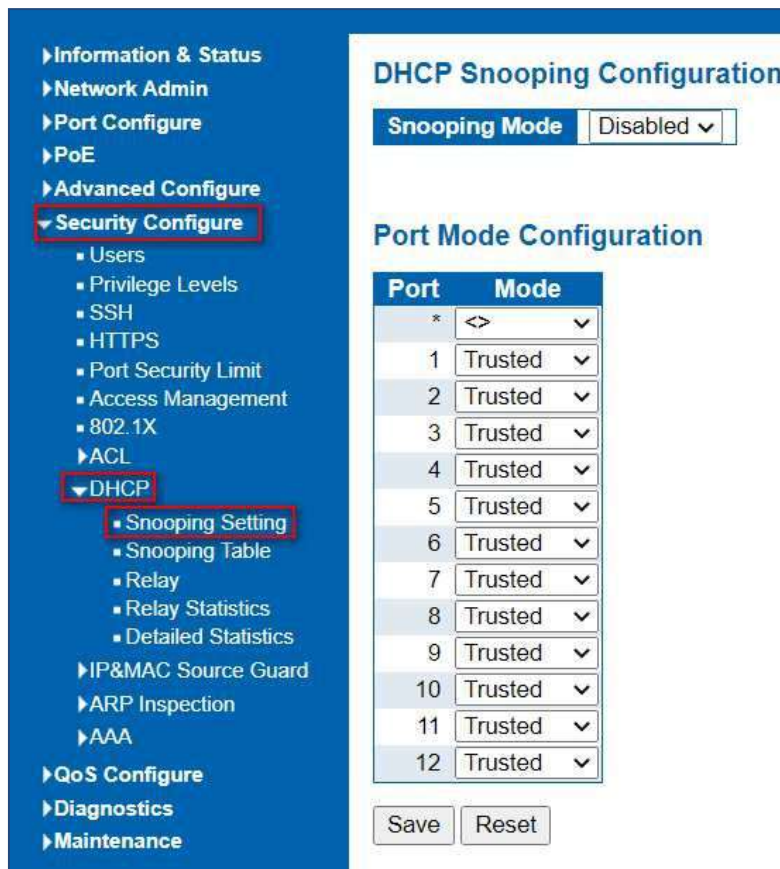


Figure 6-9-1 DHCP Snooping Configuration Screen

Configuration object and description is:

Object	Description
DHCP Snooping Mode	Clicking 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.

Clicking "Save" to store and active settings.

Snooping Table

6.9.2 Snooping Table

This page display the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page. The Dynamic DHCP Snooping Table screen in Figure 6-9-2 appears.

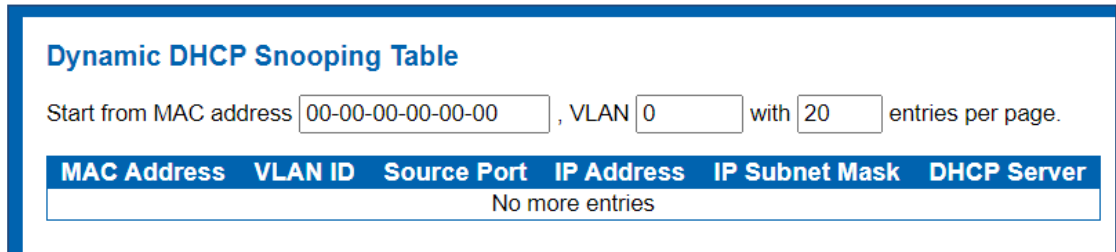


Figure 6-9-2: Dynamic DHCP Snooping Table Screen Page Screenshot

Configuration object and description is:

Object	Description
MAC Address	User MAC address of the entry
VLAN ID	VLAN-ID in which the DHCP traffic is permitted
Source port	Switch Port Number for which the entries are displayed
IP Address	User IP address of the entry
IP Subnet Mask	User IP subnet mask of the entry
DHCP Server Address	DHCP Server address of the entry

Buttons

Auto-refresh

: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Refreshes the displayed table starting from the input fields

: It will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table

: To start over

6.9.3 DHCP Relay

Configure DHCP Relay on this page. DHCP Relay is used to forward and transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically, the option works by setting two sub-options:

Circuit ID (option 1) Remote ID (option 2)

The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes representing the VLAN ID. The parameter of "module_id" is the third byte for the module ID. The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value equals the DHCP relay agent's MAC address. The DHCP Relay Configuration screen in Figure 6-9-3 appears.

DHCP Relay Configuration	
Relay Mode	Disabled
Relay Server	0.0.0.0
Relay Information Mode	Disabled
Relay Information Policy	Keep

Save Reset

Figure 6-9-3 DHCP Relay Configuration Page Screenshot

Configuration object and description is:

Object	Description
Relay mode	<p>Indicates the DHCP relay mode operation. Possible modes are:</p> <ul style="list-style-type: none"> ➤ Enabled: Enable DHCP relay mode operation. When enabling DHCP relay mode operation, the agent forwards and transfers DHCP messages between the clients and the server when they are not on the same subnet domain. And the DHCP broadcast message won't flood for security considered. ➤ Disabled: Disable DHCP relay mode operation
Relay Server	<p>Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and transfer DHCP messages between the clients and the server when they are not on the same subnet domain.</p>
Relay Information Mode	<p>Indicates the DHCP relay information mode option operation. Possible modes are:</p> <ul style="list-style-type: none"> ➤ Enabled: Enable DHCP relay information mode operation. When enabling DHCP relay information mode operation, the agent inserts specific information (option82) into a DHCP message when forwarding to DHCP server and removing it from a DHCP message when transferring to DHCP client. It only works under DHCP relay operation mode enabled. ➤ Disabled: Disable DHCP relay information mode operation
Relay Information Policy	<p>Indicates the DHCP relay information option policy. When enabling DHCP relay information mode operation, if agent receives a DHCP message that already contains relay agent information. It will enforce the policy. And it only works under DHCP relay information operation mode enabled.</p> <p>Possible policies are:</p> <ul style="list-style-type: none"> ➤ Replace: Replace the original relay information when receiving a DHCP message that already contains it. ➤ Keep: Keep the original relay information when receiving a DHCP message that already contains it. ➤ Drop: Drop the package when receiving a DHCP message that already contains relay information.

Buttons



: Clicking to apply changes



: Clicking to undo any changes made locally and revert to previously saved values.

6.9.4 DHCP Relay Statistics

This page provides statistics for DHCP relay. The DHCP Relay Statistics screen in Figure 6-9-4 appears.

DHCP Relay Statistics							
Server Statistics							
Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0
Client Statistics							
Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option	
0	0	0	0	0	0	0	0

Figure 7-9-3-4: DHCP Relay Statistics Page Screenshot

Configuration object and description is:

Server Statistics

Object	Description
Transmit to Server	The packets number that relayed from client to server.
Transmit Error	The packets number that erroneously sent packets to clients.
Receive from Server	The packets number that received packets from server.
Receive Missing Agent Option	The packets number that received packets without agent information options.
Receive Missing Circuit ID	The packets number that received packets whose the Circuit ID option was missing.
Receive Missing Remote ID	The packets number that received packets whose Remote ID option was missing.
Receive Bad Circuit ID	The packets number whose the Circuit ID option did not match known circuit ID.
Receive Bad Remote ID	The packets number whose the Remote ID option did not match known Remote ID.

Client Statistics

Object	Description
Transmit to Client	The packets number that relayed packets from server to client.
Transmit Error	The packets number that erroneously sent packets to servers.
Receive from Client	The packets number that received packets from server.
Receive Agent Option	The packets number that received packets with relay agent information option.
Replace Agent Option	The packets number that replaced received packets with relay agent information option.
Keep Agent Option	The packets number that kept received packets with relay agent information option.
Drop Agent Option	The packets number that dropped received packets with relay agent information option.
Transmit to Client	The packets number that relayed packets from server to client.

Buttons:

Auto-refresh

: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

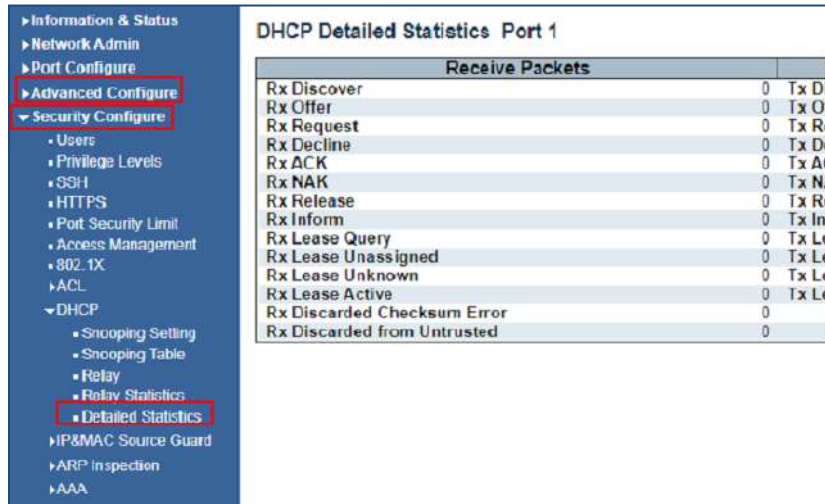
: Clicking to refresh the page immediately

: Clears all statistics.

6.9.5 DHCP Detailed Statistics

DHCP Detailed Statistics

After clicking "Advanced Configure" > "Security Configure" > "DHCP" > "Detailed Statistics" following screen will appear as:



The screenshot displays the DHCP Detailed Statistics for Port 1. The left sidebar shows a navigation menu with 'Advanced Configure' and 'Security Configure' highlighted. The main content area shows a table of statistics under the heading 'DHCP Detailed Statistics Port 1'. The table is titled 'Receive Packets' and lists various DHCP message types and their counts.

Receive Packets	
Rx Discover	0
Rx Offer	0
Rx Request	0
Rx Decline	0
Rx ACK	0
Rx NAK	0
Rx Release	0
Rx Inform	0
Rx Lease Query	0
Rx Lease Unassigned	0
Rx Lease Unknown	0
Rx Lease Active	0
Rx Discarded Checksum Error	0
Rx Discarded from Untrusted	0

Figure 7-9-3-5: DHCP Detailed Statistics Screenshot

6.10 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.

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

6.10.1 Port Configuration

IP Source Guard Configuration

Mode: Disabled

Translate dynamic to static

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
8	Disabled	Unlimited
9	Disabled	Unlimited
10	Disabled	Unlimited
11	Disabled	Unlimited
12	Disabled	Unlimited

Save Reset

Figure 6-10-1 IP&MAC Guard-Port Configuration Screen

Configuration object and description is:

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

Clicking "Save" to store and active settings.

6.10.2 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", following screen will appear.

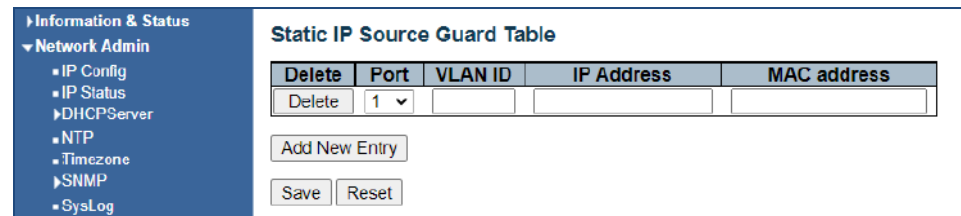


Figure 6-10.2 Static Table Configuration Screen

Configuration object and description is:

Object	Description
Port	Clicking 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

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

6.10.2 Dynamic Table

This page provides Static IP Source Guard Table. The Static IP Source Guard Table screen in Figure 6-10-3 appears.

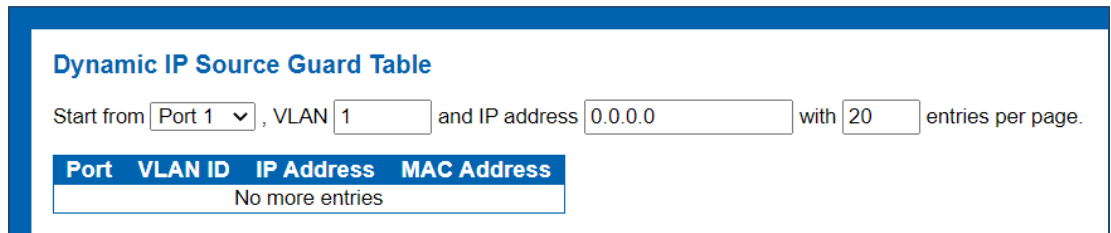


Figure 6-10-3: Static IP Source Guard Table Screen Page Screenshot

Configuration object and description is:

Object	Description
Port	Switch Port Number for which the entries are displayed.
VLAN ID	VLAN-ID in which the IP traffic is permitted.
IP Address	User IP address of the entry.
MAC Address	Source MAC address.

Buttons:

Auto-refresh

: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Refreshes the displayed table starting from the input fields

: Updates the table starting from the first entry in the Dynamic IP Source Guard Table.

: Updates the table, starting with the entry after the last entry currently displayed

6.11 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 untrust ARP packets based on the DHCP Snooping Database. This page provides ARP Inspection related configuration.

6.11.1 Port Configuration

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

ARP Inspection Configuration

Mode: Disabled

Translate dynamic to static

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
9	Disabled	Disabled	None
10	Disabled	Disabled	None
11	Disabled	Disabled	None
12	Disabled	Disabled	None

Save Reset

Figure 6-11-1 ARP Inspection Port Configuration Screen

Configuration object and description is:

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

Clicking "Save" to store and active settings.

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

6.11.2 VLAN Configuration

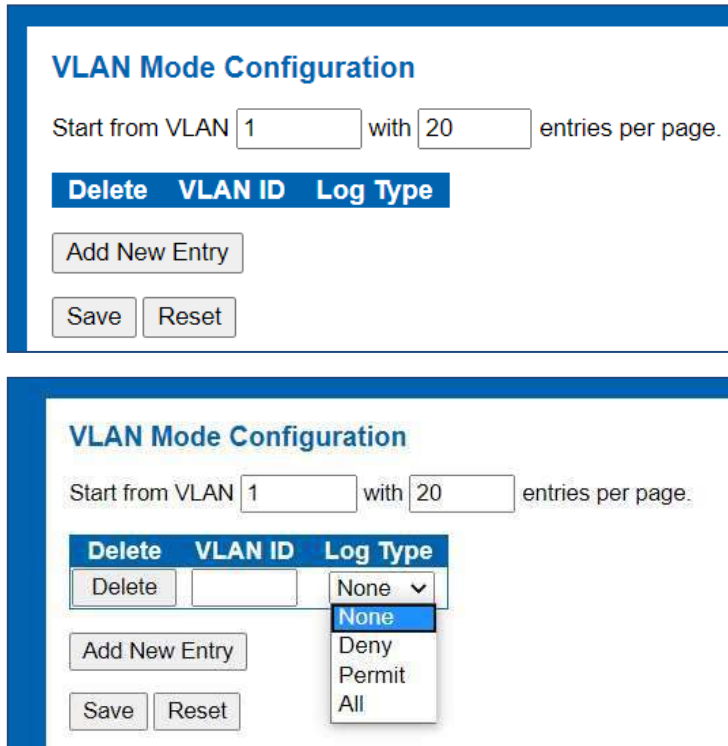


Figure 6-11-2/3 ARP Inspection VLAN Configuration Screen

Configuration object and description is:

Object	Description
VLAN ID	Indicates the ID of this particular VLAN
Log Type	Clicking 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.

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

6.11.3 Static Table

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

The figure shows two screenshots of the "Static ARP Inspection Table" configuration interface. The top screenshot displays the table header with columns: Delete, Port, VLAN ID, MAC Address, and IP Address. Below the header are buttons for "Add New Entry", "Save", and "Reset". The bottom screenshot shows the same interface but with a single entry in the table. The "Port" column for this entry has a dropdown menu with "1" selected. The other columns (VLAN ID, MAC Address, IP Address) are empty text boxes. The "Add New Entry", "Save", and "Reset" buttons are also present.

Figure 6-11-3 Static Table Configuration Screen

Configuration object and description is:

Object	Description
Port	Clicking 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

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

6.11.4 Dynamic Table

After clicking "Security Configure">"ARP Inspection" >"Dynamic Table", following screen will appear. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. The Dynamic ARP Inspection Table screen in Figure –11-4 appears.

Figure 6–11-4: Dynamic ARP Inspection Table Screenshot

Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per Page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a "Refresh" button clicking - assume the value of the first displayed entry, allowing for continuous refresh with the same start address

The ">>" will use the last entry of the currently displayed as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "|<<" button to start over. The page includes the following fields:

Configuration object and description is:

Object	Description
Port	The port number for which the status applies. Clicking the port number to see the status for this particular port.
VLAN ID	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
IP Address	The IP address of the entry.

Buttons:

Auto-refresh

: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh

: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields

|<<

: Updates the table starting from the first entry in the MAC Table, the entry with the lowest VLAN ID & MAC address.

|<<

: Updates the table, starting with the entry after the last entry currently displayed

6.12 AAA

This section is to control the access to the Managed Switch, including the user access and management control. The Authentication section contains links to the following main topics:

User Authentication

IEEE 802.1X Port-based Network Access Control MAC-based Authentication

Overview of 802.1X (Port-Based) Authentication

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.

Overview of MAC-based Authentication

Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using static entries into the MAC Table. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users, equipment whose MAC address is a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported. The 802.1X and MAC-Based Authentication configuration consists of two sections, a system- and a port-wide.

Overview of User Authentication

It is allowed to configure the Managed Switch to authenticate users logging into the system for management access using local or remote authentication methods, such as telnet and Web browser. This Managed Switch provides secure network management access using the following options:

- Remote Authentication Dial-in User Service (RADIUS)
- Terminal Access Controller Access Control System Plus (TACACS+)
- Local user name and Privilege Level control

RADIUS and TACACS+ are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS-aware devices on the network. An authentication server contains a database of multiple user name / password pairs with associated privilege levels for each user that requires management access to the Managed Switch.

6.12 RADIUS

This page allows you to configure the RADIUS Servers. The RADIUS Configuration screen in Figure 6-12-1 appears.

Global Configuration		
Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key	<input type="text"/>	
NAS-IP-Address	<input type="text"/>	
NAS-IPv6-Address	<input type="text"/>	
NAS-Identifier	<input type="text"/>	

Server Configuration						
Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
<input type="button" value="Add New Server"/>						
<input type="button" value="Save"/> <input type="button" value="Reset"/>						

Figure 6-12-1: RADIUS Server Configuration Page Screenshot

The page includes the following fields:

Global Configuration

These settings are common for all of the RADIUS Servers. Configuration object and description is:

Object	Description
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.
Retransmit	Retransmit is the number of times, in the range from 1 to 1000; a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit, it is considered to be dead.
Dead Time	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
Key	The secret key - up to 63 characters long - shared between the RADIUS server and the switch.
NAS-IP-Address	The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets.
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request. If this field is left blank, the IP address of the outgoing interface is used.
NAS-IPv6-Address	The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

Server Configuration

The table has one row for each RADIUS Server and a number of columns, which are:

Object	Description
Delete	To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.
Hostname	The IP address or hostname of the RADIUS server.
Auth Port	The UDP port to use on the RADIUS server for authentication.
Acct Port	The UDP port to use on the RADIUS server for accounting.
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
Retransmit	This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.
Key	This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

: Clicking to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported.

: Clicking to save changes

: Clicking to undo any changes made locally and revert to previously saved values.

6.12.2 TACACS+

This page allows you to configure the TACACS+ Servers. The TACACS+ Configuration screen in Figure 6-12-1 appears.

Figure 76-12-2: TACACS+ Server Configuration Page Screenshot

The page includes the following fields:

Global Configuration

These settings are common for all of the TACACS+ Servers.

Object	Description
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.
Dead Time	The Dead Time, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
Key	Specify to change the secret key or not. When "Yes" is selected for the option, you can change the secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration

The table has one row for each TACACS+ server and a number of columns, which are:

Object	Description
Delete	To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.
Hostname	The IP address or hostname of the TACACS+ server.
Port	The TCP port to use on the TACACS+ server for authentication.
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
Key	This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

: Clicking to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported

: Clicking to save changes

: Clicking to undo any changes made locally and revert to previously saved values.

Section 7: QoS Configure

7. 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 n can not only reserve bandwidth, but also limit other traffic that is not so important.

After Clicking "QoS Configure" > "Port Classification"

QoS Port Classification, following screen will appear.

7.1 QoS Port Classification

QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<> v	<> v	<> v	<> v		<input type="checkbox"/>	<> v
1	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>	Source v
2	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>	Source v
3	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>	Source v
4	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>	Source v
5	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>	Source v
6	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>	Source v
7	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>	Source v
8	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>	Source v
9	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>	Source v
10	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>	Source v
11	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>	Source v
12	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>	Source v

Save Reset

Figure 8-1 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	<p>Controls the default DEI value.</p> <p>All frames are classified to a DEI value.</p> <p>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.</p>
Address Mode	<p>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.</p> <p>Destination: Enable DMAC/DIP matching.</p>

Clicking "Save" to store and active settings.

7.2 Port Policing

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

Port	Enable	Rate	Unit	Flow Control
*	<input type="checkbox"/>	500	<> ▾	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
8	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
9	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
10	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
11	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>
12	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>

Save Reset

Figure 7-2 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	Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".

Clicking "Save" to store and active settings.

7.3 Queue Policing

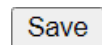
This page allows you to configure the Queue Policer settings for all switch ports. The Queue Policing screen in Figure 7-3 appears.

Port	Queue 0 Enable	Queue 1 Enable	Queue 2 Enable	Queue 3 Enable	Queue 4 Enable	Queue 5 Enable	Queue 6 Enable	Queue 7 Enable
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input 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"/>
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"/>
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"/>
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"/>
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"/>
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"/>
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"/>
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"/>
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"/>
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"/>
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"/>
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"/>

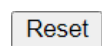
Figure 7-3: QoS Ingress Port Classification Page Screenshot The page includes the following fields:

Object	Description
Port	The port number for which the configuration below applies.
Enable (E)	Enable or disable the queue policer for this switch port.
Rate	Controls the rate for the queue policer. This value is restricted to 25-13128147 when "Unit" is kbps, and 1-13128 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer. This field is only shown if at least one of the queue policers are enabled.
Unit	Controls the unit of measure for the queue policer rate as kbps or Mbps. This field is only shown if at least one of the queue policers are enabled.

Buttons



: Clicking to apply changes



: Clicking to undo any changes made locally and revert to previously saved values.

7.4 Port Scheduler

The Port Scheduler and Shapers for a specific port are configured on this page. The QoS Egress Port Schedule and Shaper screen in Figure 7-4 4-1 appears.

- ▶ Information & Status
- ▶ Network Admin
- ▶ Port Configure
- ▶ PoE
- ▶ Advanced Configure
- ▶ Security Configure
- ▼ QoS Configure
 - Port Classification
 - Port Policing
 - Queue Policing
 - Port Scheduler
 - Port Shaping
 - Port Tag Remarking
 - Port DSCP
 - DSCP-Based QoS
 - DSCP Translation
 - DSCP Classification
 - QoS Control List
 - Storm Policing
- ▶ Diagnostics
- ▶ Maintenance

QoS Egress Port Schedulers

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

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority

Queue Shaper

Enable	Rate	Unit	Excess
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>

Port Shaper

Enable	Rate	Unit	Burst	Unit
<input type="checkbox"/>	500	kbps	12288	Byte

The diagram illustrates the data flow from individual queue shapers to a central scheduler and then to a port shaper. On the left, eight queue shapers labeled Q0 through Q7 are shown, each with a '5' in a circle and a '500 kbps' rate. Arrows from each queue shaper point to a central vertical oval labeled 'STRICT'. An arrow from the 'STRICT' scheduler points to a port shaper on the right, which has a '5' in a circle and is configured with a rate of 500 kbps, a burst of 12288, and a unit of Byte.

Figure 8-3/5: QoS Egress Port Schedule and Shapers Page Screenshot

The page includes the following fields:

Object	Description
Schedule Mode	Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.
Queue Shaper Enable	Controls whether the queue shaper is enabled for this queue on this switch port.
Queue Shaper Rate	Controls the rate for the queue shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps". The default value is 500.
Queue Shaper Unit	Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".
Queue Shaper Excess	Controls whether the queue is allowed to use excess bandwidth.
Queue Scheduler Weight	Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted". The default value is "17".
Queue Scheduler Percent	Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
Port Shaper Enable	Controls whether the port shaper is enabled for this switch port.
Port Shaper Rate	Controls the rate for the port shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps". The default value is 500.
Port Shaper Unit	Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

: Clicking to apply changes

: Clicking to undo any changes made locally and revert to previously saved values.

: Clicking to undo any changes made locally and return to the previous page

7.5 Port Shaping

Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports. The Port shaping screen in Figure 7-5 5-1 appears.

- ▶ Information & Status
- ▶ Network Admin
- ▶ Port Configure
- ▶ PoE
- ▶ Advanced Configure
- ▶ Security Configure
- ▼ QoS Configure
- Port Classification
- Port Policing
- Queue Policing
- Port Scheduler
- Port Shaping
- Port Tag Remarking
- Port DSCP
- DSCP-Based QoS
- DSCP Translation
- DSCP Classification
- QoS Control List
- Storm Policing
- ▶ Diagnostics
- ▶ Maintenance

QoS Egress Port Shapers

Port	Shapers							Port	
	Q0	Q1	Q2	Q3	Q4	Q5	Q6		Q7
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-

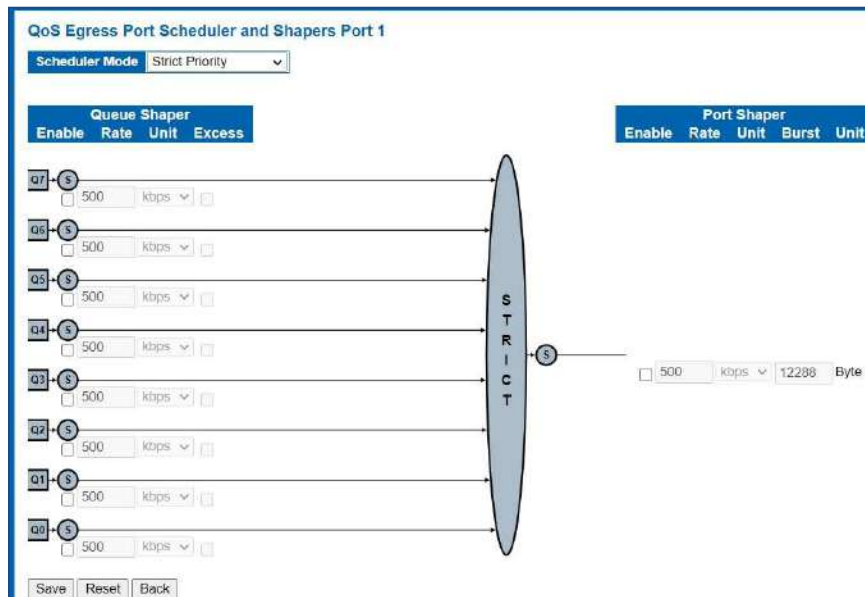


Figure 7.5-1: QoS Egress Port Schedule and Shapers Page Screenshot

The page includes the following fields:

Object	Description
Schedule Mode	Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.
Queue Shaper Enable	Controls whether the queue shaper is enabled for this queue on this switch port.
Queue Shaper Rate	Controls the rate for the queue shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1- 13200 when the "Unit" is "Mbps". The default value is 500.
Queue Shaper Unit	Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".
Queue Shaper Excess	Controls whether the queue is allowed to use excess bandwidth.
Queue Scheduler Weight	Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted". The default value is "17".
Queue Scheduler Percent	Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
Port Shaper Enable	Controls whether the port shaper is enabled for this switch port.
Port Shaper Rate	Controls the rate for the port shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1- 13200 when the "Unit" is "Mbps". The default value is 500.
Port Shaper Unit	Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

Save

: Clicking to apply changes

Reset

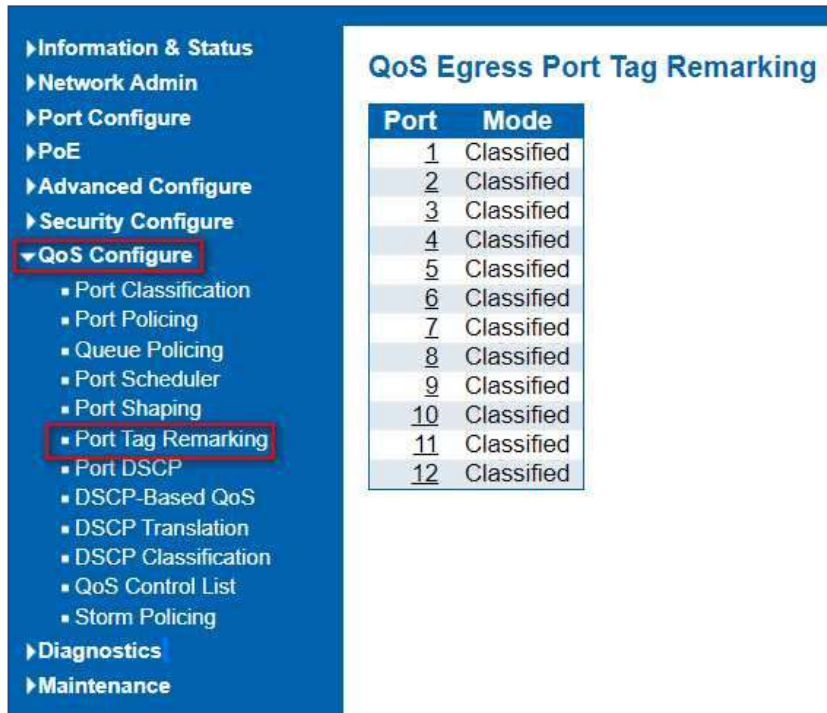
: Clicking to undo any changes made locally and revert to previously saved values.

Back

: Clicking to undo any changes made locally and return to the previous page

7.6 Port Tag Remarking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports. The Port tag remarking screen in Figure 7-6 appears.



Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified



QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode: Classified

Buttons: Save, Reset, Cancel

Figure 7-6 6-1 : Port Tag Remarking Page Screenshot

The page includes the following fields:

Object	Description
Port	The logical port for the settings contained in the same row. Clicking on the port number in order to configure tag remarking
Mode	<ul style="list-style-type: none"> ➤ Shows the tag remarking mode for this port. ➤ Classified: Use classified PCP/DEI values. ➤ Default: Use default PCP/DEI values. ➤ Mapped: Use mapped versions of CoS and DPL.

Buttons



: Clicking to apply changes



: Clicking to undo any changes made locally and revert to previously saved values.



: Clicking to undo any changes made locally and return to the previous page

7.7 Port DSCP

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports. The Port DSCP screen in Figure 7-10 appears.

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<>	<>
1	<input type="checkbox"/>	Disable	Disable
2	<input type="checkbox"/>	Disable	Disable
3	<input type="checkbox"/>	Disable	Disable
4	<input type="checkbox"/>	Disable	Disable
5	<input type="checkbox"/>	Disable	Disable
6	<input type="checkbox"/>	Disable	Disable
7	<input type="checkbox"/>	Disable	Disable
8	<input type="checkbox"/>	Disable	Disable
9	<input type="checkbox"/>	Disable	Disable
10	<input type="checkbox"/>	Disable	Disable
11	<input type="checkbox"/>	Disable	Disable
12	<input type="checkbox"/>	Disable	Disable

Figure 7-7 QoS Port DSCP Configuration Page Screenshot The page includes the following fields:

Object	Description
Port	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
Ingress	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: Translate Classify
Translate	To Enable the Ingress Translation, clicking the checkbox.
Classify	<ul style="list-style-type: none"> ➤ Classification for a port have 4 different values. ➤ Disable: No Ingress DSCP Classification. ➤ DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0. Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSP. ➤ All: Classify all DSCP.
Egress	Port Egress Rewriting can be one of - Disable: No Egress rewrite. Enable: Rewrite enable without remapped. Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table. Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.

Buttons

Save

: Clicking to apply changes

Reset

: Clicking to undo any changes made locally and revert to previously saved values.

7.8 DSCP-based QoS

This page allows you to configure the basic QoS DSCP-based QoS Ingress Classification settings for all switches. The DSCP-based QoS screen in Figure 7-8 appears

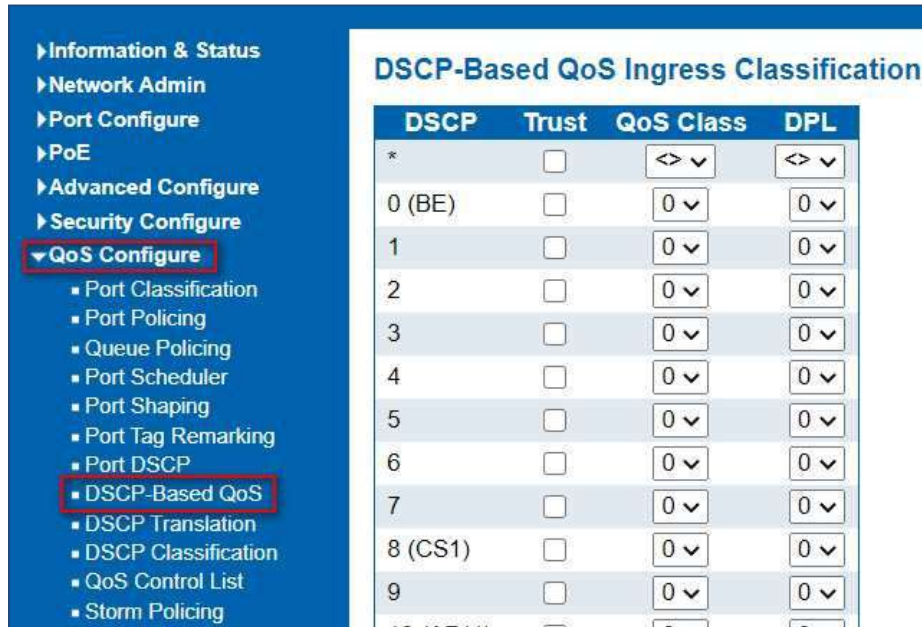


Figure 7-8: DSCP-based QoS Ingress Classification Page Screenshot

The page includes the following fields:

Object	Description
DSCP	Maximum number of supported DSCP values are 64.
Trust	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.
QoS Class	QoS Class value can be any of (0-7)
DPL	Drop Precedence Level (0-1)

Buttons

Save

: Clicking to apply changes

Reset

: Clicking to undo any changes made locally and revert to previously saved values.

7.9 DHCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress. The DSCP Translation screen in Figure 7.9 appears.

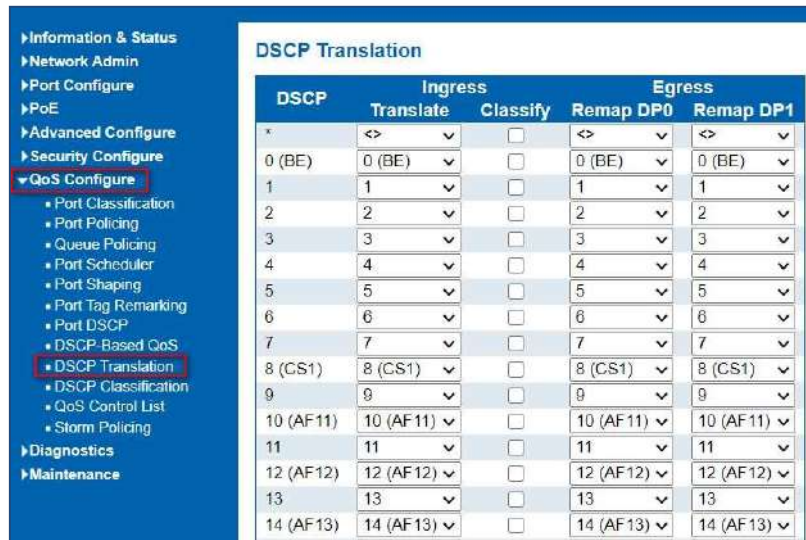


Figure 7.9: DSCP Translation Page Screenshot

The page includes the following fields:

Object	Description
DSCP	Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.
Ingress	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation – Translate - Classify
Translate	DSCP at Ingress side can be translated to any of (0-63) DSCP values.
Classify	Clicking to enable Classification at Ingress side.
Egress	There is following configurable parameter for Egress side - Remap
Remap DP	Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

Buttons

Save

: Clicking to apply changes

Reset

: Clicking to undo any changes made locally and revert to previously saved values.

7.10 DSCP Classification

This page allows you to map DSCP value to a QoS Class and DPL value. The DSCP Classification screen in Figure 8-13 appears.

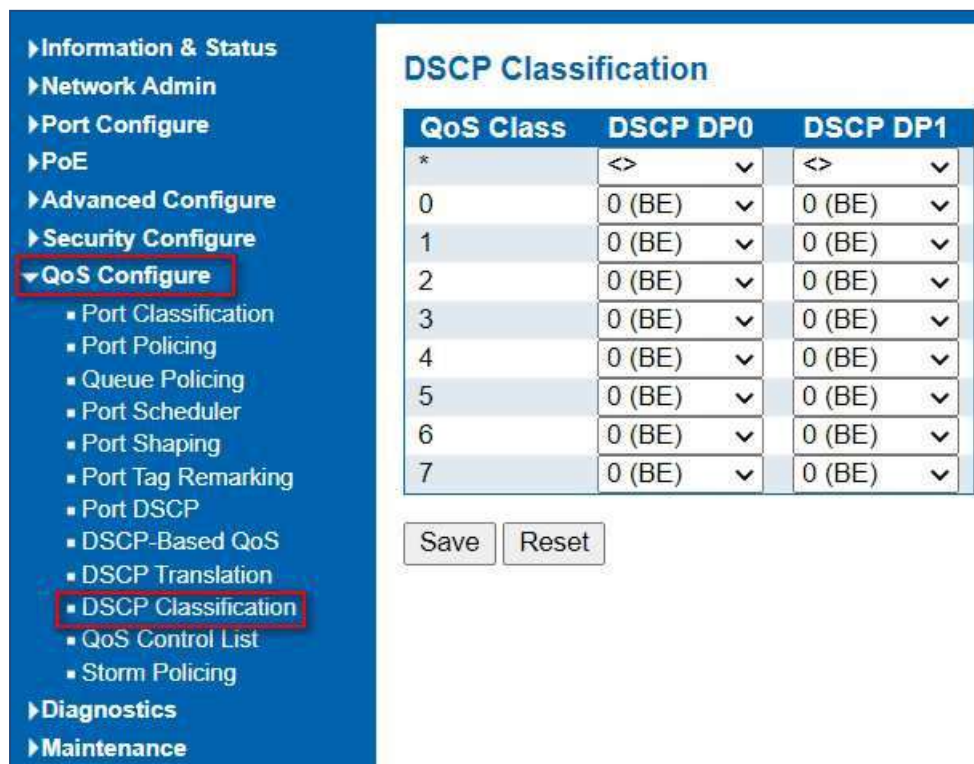


Figure 7.10: DSCP Classification Page Screenshot

The page includes the following fields:

Object	Description
QoS Class	Available QoS Class value ranges from 0 to 7. QoS Class (0-7) can be mapped to following parameters.
DPL	Actual Drop Precedence Level.
DSCP	Select DSCP value (0-63) from DSCP menu to map DSCP to corresponding QoS Class and DPL value

Buttons

Save

: Clicking to apply changes

Reset

: Clicking to undo any changes made locally and revert to previously saved values.

7.11 Control List

This page shows the QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch.

Clicking on the lowest plus sign to add a new QCE to the list. The QoS Control List screen in Figure 7-14 appears.

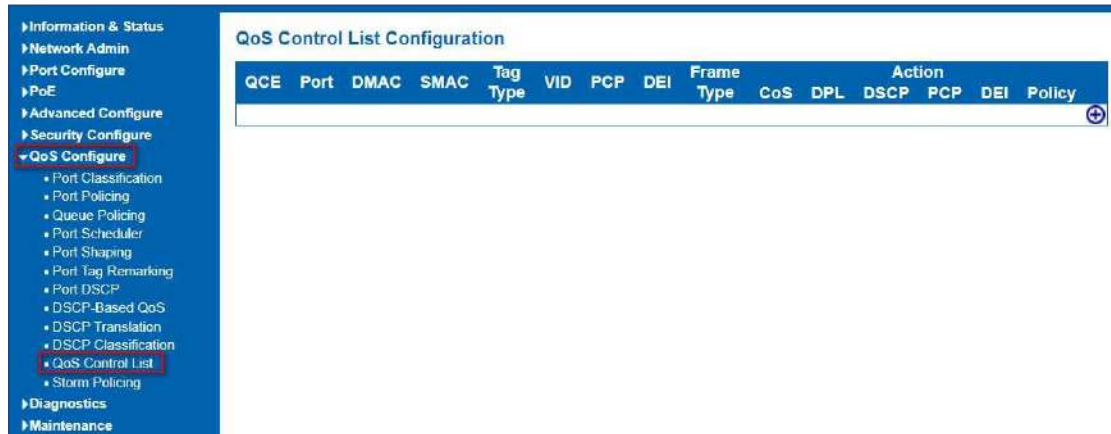








Figure 7.11: QoS Control List Configuration Page Screenshot

The page includes the following fields:

Object	Description
QCE#	Indicates the index of QCE.
Port	Indicates the list of ports configured with the QCE.
DMAC	Specify the type of Destination MAC addresses for incoming frame. Possible values are: <ul style="list-style-type: none"> ➤ Any: All types of Destination MAC addresses are allowed. ➤ Unicast: Only Unicast MAC addresses are allowed. ➤ Multicast: Only Multicast MAC addresses are allowed. ➤ Broadcast: Only Broadcast MAC addresses are allowed. The default value is 'Any'.
SMAC	Displays the OUI field of Source MAC address, i.e. first three octet (byte) of MAC address.
Tag Type	Indicates tag type. Possible values are: <ul style="list-style-type: none"> ➤ Any: Match tagged and untagged frames. ➤ Untagged: Match untagged frames. ➤ Tagged: Match tagged frames. The default value is 'Any'
VID	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'
PCP	Priority Code Point: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
DEI	Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'.

Frame Type	<p>Indicates the type of frame to look for incoming frames. Possible frame types are:</p> <ul style="list-style-type: none"> ➤ Any: The QCE will match all frame type. ➤ Ethernet: Only Ethernet frames (with Ether Type 0x600- 0xFFFF) are allowed. ➤ LLC: Only (LLC) frames are allowed. ➤ SNAP: Only (SNAP) frames are allowed. ➤ IPv4: The QCE will match only IPV4 frames. ➤ IPv6: The QCE will match only IPV6 frames.
Action	<p>Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.</p> <p>There are three action fields: Class, DPL and DSCP.</p> <ul style="list-style-type: none"> ➤ Class: Classified QoS class. ➤ DPL: Classified Drop Precedence Level. ➤ DSCP: Classified DSCP value.
Modification Buttons	<p>You can modify each QCE in the table using the following buttons:</p> <p>: Inserts a new QCE before the current row.</p> <p>: Edits the QCE.</p> <p>: Moves the QCE up the list.</p> <p>: Moves the QCE down the list.</p> <p>: Deletes the QCE.</p> <p>: The lowest plus sign adds a new entry at the bottom of the list of QCL.</p>

QoS Control Entry Configuration

QCE Configuration

Port Members											
1	2	3	4	5	6	7	8	9	10	11	12
<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"/>

Key Parameters

DMAC	Any
SMAC	Any
Tag	Any
VID	Any
PCP	Any
DEI	Any
Frame Type	Any

Action Parameters

CoS	0
DPL	Default
DSCP	Default
PCP	Default
DEI	Default
Policy	

Figure 7-11-14: QCE Configuration Page Screenshot

The page includes the following fields:

Object	Description
Port Members	Check the checkbox button in case you want to make any port member of the QCL entry. By default, all ports will be checked
Key Parameters	<p>Key configuration is described as below:</p> <ul style="list-style-type: none">➤ DMAC Type Destination MAC type: possible values are unicast(UC), multicast(MC), broadcast(BC) or 'Any'➤ SMAC Source MAC address: 24 MS bits (OUI) or 'Any'➤ Tag Value of Tag field can be 'Any', 'Untag' or 'Tag'➤ VID Valid value of VLAN ID can be any value in the range 1- 4095 or 'Any'; user can enter either a specific value or a range of VIDs➤ PCP Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'➤ DEI Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'➤ Frame Type Frame Type can have any of the following values<ul style="list-style-type: none">• Ethernet• LLC• SNAP• IPv4• IPv6• Note: all frame types are explained below.

Any	Allow all types of frames.
EtherType	Ethernet Type Valid Ethernet type can have value within 0x600- 0xFFFF or 'Any' but excluding 0x800(IPv4) and 0x86DD(IPv6), default value is 'Any'.
LLC	<ul style="list-style-type: none"> ➤ SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any' ➤ DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any' ➤ Control Address Valid Control Address can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'
SNAP	PID Valid PID(a.k.a Ethernet type) can have value within 0x00- 0xFFFF or 'Any', default value is 'Any'
IPv4	<p>Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'</p> <p>Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero</p> <p>DSCP Diffserv Code Point value(DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43</p> <p>IP Fragment IPv4 frame fragmented option: yes no any</p> <p>Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP</p> <p>Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP</p>
IPv6	<p>Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'</p> <p>Source IP IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits</p> <p>DSCP Diffserv Code Point value(DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43</p> <p>Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP</p> <p>Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP</p>
Action Parameters	<p>Class QoS class: (0-7) or 'Default'.</p> <p>DPL Valid Drop Precedence Level can be (0-3) or 'Default'. DSCP Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11- AF43) or 'Default'. 'Default' means that the default classified value is not modified by this QCE.</p>

Buttons

Save

: Clicking to apply changes

Reset

: Clicking to undo any changes made locally and revert to previously saved values.

Cancel

: Return to the previous page without saving the configuration change

7.11 QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

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

7.12 Storm Policing Configuration

Frame Type	Enable	Rate	Unit
Unicast	<input type="checkbox"/>	1	fps
Multicast	<input type="checkbox"/>	1	fps
Broadcast	<input type="checkbox"/>	1	fps

Save Reset

Port Storm Policer Configuration									
Port	Unicast Frames			Broadcast Frames			Unknown Frames		
	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit
*	<input type="checkbox"/>	500	<> ▾	<input type="checkbox"/>	500	<> ▾	<input type="checkbox"/>	500	<> ▾
1	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
2	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
3	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
4	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
5	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
6	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
7	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
8	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾
9	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	500	kbps ▾

Figure 7.12: Storm 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..

Clicking "Save" to store and active settings.

7.12 Weighted Random Early Detection Configuration

Weighted Random Early Detection Configuration						
Group	Queue	DPL	Enable	Min	Max	Max Unit
1	0	1	<input type="checkbox"/>	0	50	Drop Probability ▾
1	0	2	<input type="checkbox"/>	0	50	Drop Probability ▾
1	0	3	<input type="checkbox"/>	0	50	Drop Probability ▾
1	1	1	<input type="checkbox"/>	0	50	Drop Probability ▾
1	1	2	<input type="checkbox"/>	0	50	Drop Probability ▾
1	1	3	<input type="checkbox"/>	0	50	Drop Probability ▾
1	2	1	<input type="checkbox"/>	0	50	Drop Probability ▾
1	2	2	<input type="checkbox"/>	0	50	Drop Probability ▾
1	2	3	<input type="checkbox"/>	0	50	Drop Probability ▾
1	3	1	<input type="checkbox"/>	0	50	Drop Probability ▾
1	3	2	<input type="checkbox"/>	0	50	Drop Probability ▾
1	3	3	<input type="checkbox"/>	0	50	Drop Probability ▾

This operation defines the number of frames prior to be dropped to avoid traffic congestion. It measures the size of the queues and will drop frames when the queue is between the minimum and maximum threshold.

Section 8: Diagnostics

8. Diagnostics

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.

8.1 Ping Test

After clicking "Diagnostics ">"Ping", following screen appear.

Please note the packet size test is limited to 1452 bytes

The screenshot shows a network management interface with a left-hand navigation menu and a main configuration area. The navigation menu includes: Information & Status, Network Admin, Port Configure, PoE, Advanced Configure, Security Configure, QoS Configure, Diagnostics (expanded), and Maintenance. Under Diagnostics, there are sub-items: Ping (highlighted with a red box), Cable Diagnostics, and CPU Load. The main configuration area is titled "ICMP Ping" and contains the following fields: IP Address (0.0.0.0), Ping Length (56), Ping Count (5), and Ping Interval (1). A "Start" button is located below these fields.

The screenshot shows the "ICMP Ping Output" screen. It displays the following text: "PING server 192.168.0.1, 1452 bytes of data." followed by five lines of results: "1460 bytes from 192.168.0.1: icmp_seq=0, time=40ms", "1460 bytes from 192.168.0.1: icmp_seq=1, time=0ms", "1460 bytes from 192.168.0.1: icmp_seq=2, time=0ms", "1460 bytes from 192.168.0.1: icmp_seq=3, time=0ms", and "1460 bytes from 192.168.0.1: icmp_seq=4, time=0ms". The final line reads "Sent 5 packets, received 5 OK, 0 bad". A "New Ping" button is located at the bottom of the screen.

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)

Clicking "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", following screen will appear.

Note: Cable Diagnostics only apply to UTP (copper) connections and will be valid with connection at or under 328 feet (100m)

The screenshot displays the VeriPHY Cable Diagnostics interface. On the left, a navigation menu is visible with the following items: Information & Status, Network Admin, Port Configure, PoE, Advanced Configure, Security Configure, QoS Configure, Diagnostics (expanded), Ping, Cable Diagnostics (highlighted), GPU Load, and Maintenance. The main content area is titled 'VeriPHY Cable Diagnostics' and features a 'Port' dropdown menu set to 'All' and a 'Start' button. Below this is a table titled 'Cable Status' with the following columns: Port, Pair A, Length A, Pair B, Length B, Pair C, Length C, Pair D, and Length D. The table contains 8 rows of data, all showing dashes in the length columns.

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

VeriPHY Cable Diagnostics

Port: All ▾

Start

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	0	OK	0	OK	0	OK	0
3	Open	0	Open	0	Open	0	Open	0
4	OK	3	OK	3	OK	3	OK	3
5	Open	0	Open	0	Open	0	Open	0
6	Open	0	Open	0	Open	0	Open	0
7	Open	0	Open	0	Open	0	Open	0
8	Open	0	Open	0	Short	0	Short	0

Figure 8-2 Cable Diagnostics Screen

Configuration object and description is:

Object	Description
Port	The port where you are requesting Cable Diagnostics.
Description	Display per port description.
Cable Status	<p>Port: Port number.</p> <p>Pair: The status of the cable pair. OK - Correctly terminated pair Open - Open pair Short - Shorted pair</p> <p>Short A - Cross-pair short to pair A Short B - Cross-pair short to pair B Short C - Cross-pair short to pair C Short D - Cross-pair short to pair D</p> <p>Cross A - Abnormal cross-pair coupling with pair A Cross B - Abnormal cross-pair coupling with pair B Cross C - Abnormal cross-pair coupling with pair C Cross D - Abnormal cross-pair coupling with pair D</p> <p>Length: The length (in meters) of the cable pair. The resolution is 3 meters</p>

Clicking "Start" button to start "Cable Diagnostics" testing.

8.2 CPU Load

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

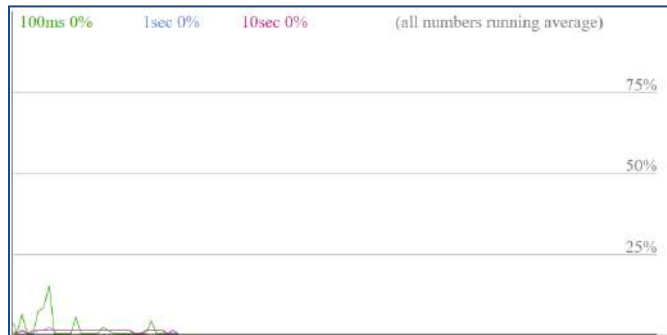


Figure 8-3 CPU Load Screen

This page displays the CPU load, using an SVG graph. The load is measured as average over the last 100ms, 1 sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well. In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support.

Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

9. Maintenance

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

9.1 Restart Device



Figure 9-1 Restart Device Screen

Please clicking "Yes" to restart the switch.

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

9.2 Factory Defaults



Figure 9-2 Factory Defaults Screen

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

9.3 Firmware Upgrade

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

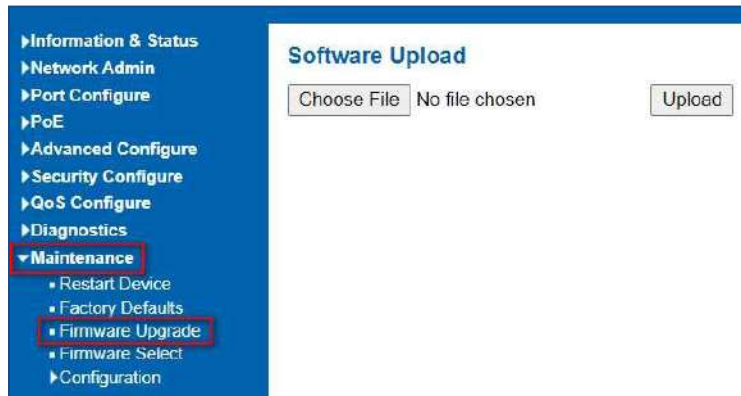


Figure 9-3 Firmware Upgrade Screen

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

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image. The web page displays two tables with information about the active and alternate firmware images. After clicking "Maintenance" > "Firmware Upgrade", following screen will appear.

9.4 Firmware Select

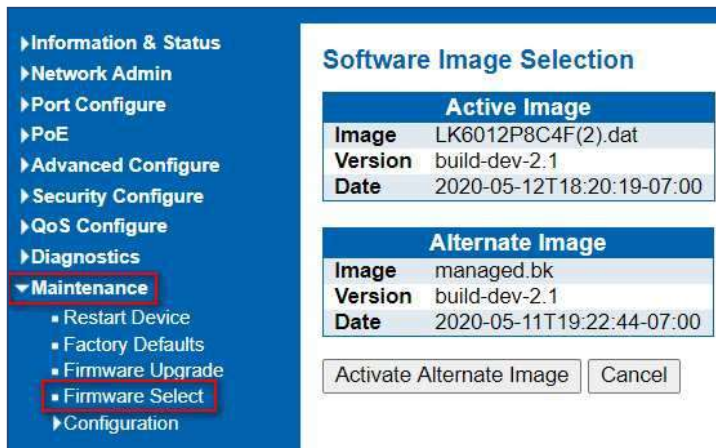
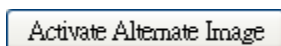


Figure 9-4 Firmware Select Screen

Configuration object and description is:

Object	Description
Image	The flash index name of the firmware image. The name of primary (preferred) image is image, the alternate image is named image.bk.
Version	The version of the firmware image.
Date	The date when the firmware was produced.

Buttons



9.5 Configuration

9.5.1 Download Configuration File

: Clicking to use the alternate image. This button may be disabled depending on system state. Configuration

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

After clicking "Maintenance ">"Download", following screen will appear.

Download Configuration

Select configuration file to save.

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

File Name
<input type="radio"/> running-config
<input type="radio"/> default-config
<input type="radio"/> startup-config

Download Configuration

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

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

Upload Configuration

File To Upload

Choose File No file chosen

Destination File

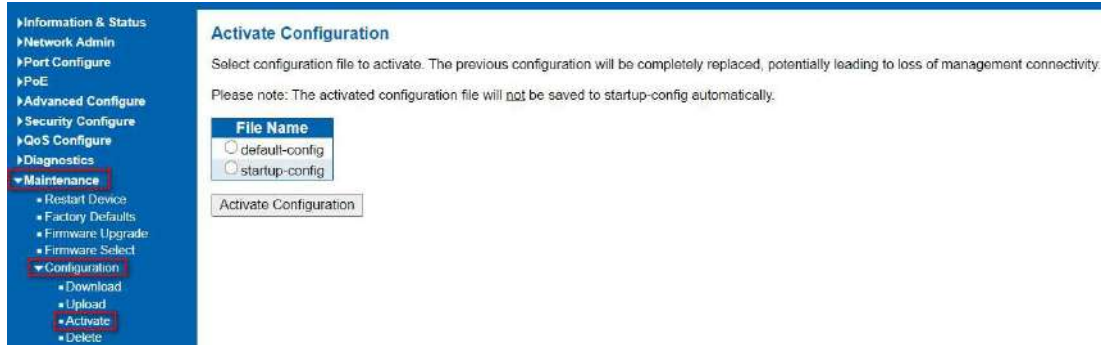
File Name	Parameters
<input type="radio"/> running-config	<input checked="" type="radio"/> Replace <input type="radio"/> Merge
<input type="radio"/> startup-config	
<input type="radio"/> Create new file	<input type="text"/>

Upload Configuration

9.5.3 Activate Configuration

Activate Configuration

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



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

9.5.4 Delete Configuration File



9.5.5 Glossary

ACE

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

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.

AES

AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

AMS

AMS is an acronym for Auto Media Select. AMS is used for dual media ports (ports supporting both copper (cu) and fiber (SFP) cables. AMS automatically determines if a SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and cu cables are inserted, the port will select the preferred media.

APS

APS is an acronym for Automatic Protection Switching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

ARP

ARP is an acronym for Address Resolution Protocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection 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 the switch device.

CC

CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM

CCM is an acronym for Continuity Check Message. It is a OAM frame transmitted from a MEP to its peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for Cisco Discovery Protocol.

DEI

DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

DHCP

DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

DSCP

DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

FTP

FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

HTTP

HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW). HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested

WEB

Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending

requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection. HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logins. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is no longer considered an adequate degree of encryption for commercial exchange.

ICMP

ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier. There will be only one IGMP Querier that wins Querier election on a particular link.

IMAP

IMAP is an acronym for Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server. IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server. The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network. IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new

version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for IP MultiCast. IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

IPMC Profile

IPMC Profile is an acronym for IP MultiCast Profile. IPMC Profile is used to deploy the access control on IP multicast streams.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping 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.

LACP

LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.

LLC

The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1-byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP

LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LLQI

LLQI (Last Listener Query Interval) is the maximum response time used to calculate the Maximum Response Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).

LOC

LOC is an acronym for Loss of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as switch criteria by EPS

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC

addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP

MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MLD Querier

A router sends MLD Query messages onto a particular link. This router is called the Querier. There will be only one MLD Querier that wins Querier election on a particular link.

MSTP

In 2002, the IEEE introduced an evolution of RSTP: the Multiple Spanning Tree Protocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

NAS

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

OAM

OAM is an acronym for Operation Administration and Maintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this.

Optional TLVs.

A LLDP frame contains multiple TLVs. For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLV is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

PCP

PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for Powered Device. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implements the Ethernet physical layer (IEEE-802.3).

PING

Ping (Packet InterNet Grouper) is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

Ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

PoE

PoE is an acronym for Power Over Ethernet. Power over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN Access Points (AP), IP cameras and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3

POP3 is an acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE

PPPoE is an acronym for Point-to-Point Protocol over Ethernet. It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

Private VLAN

In a private VLAN, PVLANS provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

PTP

PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

QCE

QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCI

QCI is an acronym for QoS Class Identifier. This is a special identifier defining the quality of packet communication provided by LTE (Long Term Evolution, marketed as 4G LTE).

QCL

QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution.

Therefore, QoS is the set of techniques to manage network resources.

QoS class

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one-to-one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

Querier Election

Querier election is used to dedicate the Querier, the only one router sends Query messages, on a particular link. Querier election rule defines that IGMP Querier or MLD Querier with the lowest IPv4/IPv6 address wins the election.

RARP

RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for Remote Authentication Dial in User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI

RDI is an acronym for Remote Defect Indication. It is a OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP.

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

SAMBA

Samba is a program running under UNIX-like operating systems (not the Brazilian dance) that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.

Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".

sFlow

sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector.

Additional information can be found at <http://sflow.org>.

SHA

SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack Protocol using ROUting Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

Switch ID

Switch IDs (1-1) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

SyncE

SyncE is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

TACACS+

TACACS+ is an acronym for Terminal Access Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame. The 3-bits provide 8 priority levels (0~7).

TCP

TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for TELeType NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

ToS

ToS is an acronym for Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP

TKIP is an acronym for Temporal Key Integrity Protocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

UDP

UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

VLAN

Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

WEP

WEP is an acronym for Wired Equivalent Privacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio, and are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).

WiFi

WiFi is an acronym for Wireless Fidelity. It is meant to be used generically when referring to any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA

WPA is an acronym for Wi-Fi Protected Access. It was created in response to several serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK

WPA-PSK is an acronym for Wi-Fi Protected Access - Pre-Shared Key. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPA-Radius

WPA-Radius is an acronym for Wi-Fi Protected Access - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode

security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia).

WPS

WPS is an acronym for Wi-Fi Protected Setup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

WRED

WRED is an acronym for Weighted Random Early Detection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

WTR

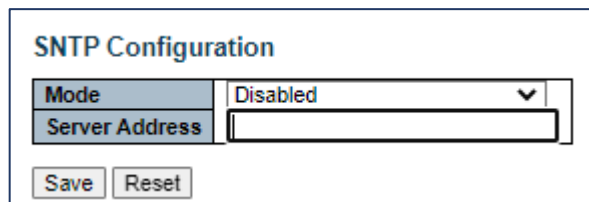
WTR is an acronym for Wait to Restore. This is the time a failure on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.

9.5.6 Appendix

Setting a system time as Syslog Messaging and System information.

In order for the Vi35136 to display the correct time for Syslog messaging and system information it must have an external time and date reference. If Time and Date are not or cannot be referred to a common source all switch functions that display time and date will be correct.

One solution is to use the SNTP (Network Time Protocol setting



SNTP Configuration	
Mode	Disabled
Server Address	
Save	Reset

This requires the switch have access to an external NTP IP address for an external NTP clock. Often is this not allowed for closed security applications.

An alternative is to use the Time and Date generated from a server or computer normally use to operate VMS software as part of any internal network.

Step 1: Acquiring Internal Time and Date Reference

- a. After power up go to the Time zone Information Configuration.
- b. Use the drop-down menu to select the correct format for your region. The chooses are:
 1. MM-DD-YYYY
 2. DD-MM-YYYY
 3. YYYY-MM-DD
- c. Wait for the screen to acquire the time and date. If no time and date is acquired than no reference exists

d. Press Save

Important: You must wait for the switch to acquire the time and date prior to pressing Save

Timezone Information Configuration

System Timezone Offset (minutes)	-420
Date Format	MM-DD-YYYY ▼
UTC time	8/18/2022, 11:04:29 AM

e. To confirm the Time and Date to the Syslog screen under Information and Settings:

1. View the screen and confirm the information is correct and matches the Time/Date settings you programmed

System Log Information

Level	All ▼
Clear Level	All ▼

The total number of entries is 8 for the given level.

Start from ID with entries per page.

ID	Level	Time	Message
22	Notice	08-18-2022T10:37:22-07:00	LINK-UPDOWN: Interface GigabitEthernet 1/2, changed state to down.
23	Notice	08-18-2022T10:37:22-07:00	LINK-UPDOWN: Interface GigabitEthernet 1/4, changed state to down.
24	Notice	08-18-2022T10:37:26-07:00	LINK-UPDOWN: Interface GigabitEthernet 1/2, changed state to up.
25	Notice	08-18-2022T10:37:26-07:00	LINK-UPDOWN: Interface GigabitEthernet 1/4, changed state to up.
26	Notice	08-18-2022T10:45:28-07:00	LINK-UPDOWN: Interface GigabitEthernet 1/2, changed state to down.
27	Notice	08-18-2022T10:45:28-07:00	LINK-UPDOWN: Interface GigabitEthernet 1/4, changed state to down.
28	Notice	08-18-2022T10:45:33-07:00	LINK-UPDOWN: Interface GigabitEthernet 1/2, changed state to up.
29	Notice	08-18-2022T10:45:33-07:00	LINK-UPDOWN: Interface GigabitEthernet 1/4, changed state to up.

Step 2: External Syslog Capture- Defining which alerts are displayed

a. Prior to setting the system configuration follow the above steps – they must be set correctly

b. Under Network Admin go to the Syslog

1. Enable the Server mode- this must be a computer on your network that is capable of being accessed by the switch.
2. Enter the computer/server IP address and note it must be on the same network as the switch.
3. Set the Syslog Level- this will define the type of alert that is both broadcast and entered in the switch's GUI Syslog. The choices are"

1. Error
2. Warning
3. Notice

Server Mode	Enabled
Server Address	192.168.0.102
Syslog Level	Informational

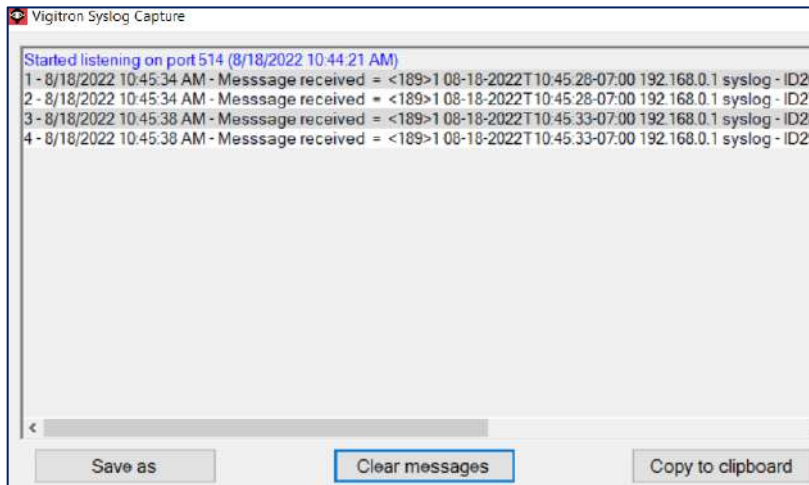
Error

Warning

Notice

Informational

- c. You will need a separate software program running on your computer/server to capture the messages.
- d. Vigitron provides a free and without obligation SysCap Utility program
- e. Contact Vigitron at Support@vigitron.com for more information



The date will be dependent on the format settings. Time will be displayed only in 24-hour format. If power is lost the time and date will revert to a default value and the procedure must be repeated