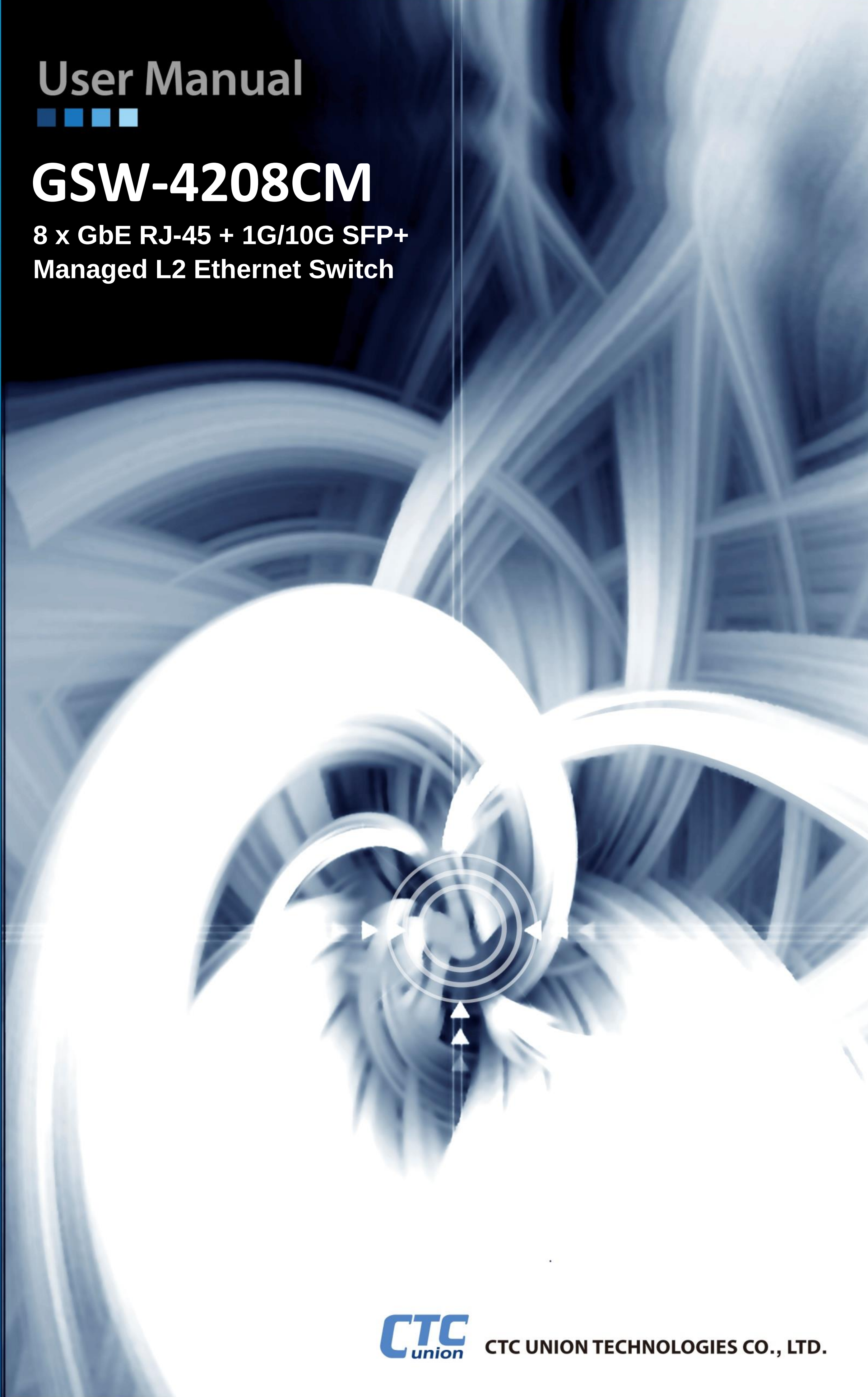
User Manual

GSW-4208CM

8 x GbE RJ-45 + 1G/10G SFP+
Managed L2 Ethernet Switch



CTC UNION TECHNOLOGIES CO., LTD.

LEGAL

The information in this publication has been carefully checked and is believed to be entirely accurate at the time of publication. CTC Union Technologies assumes no responsibility, however, for possible errors or omissions, or for any consequences resulting from the use of the information contained herein. CTC Union Technologies reserves the right to make changes in its products or product specifications with the intent to improve function or design at any time and without notice and is not required to update this documentation to reflect such changes.

CTC Union Technologies makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does CTC Union assume any liability arising out of the application or use of any product and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

CTC Union products are not designed, intended, or authorized for use in systems or applications intended to support or sustain life, or for any other application in which the failure of the product could create a situation where personal injury or death may occur. Should the Buyer purchase or use a CTC Union product for any such unintended or unauthorized application, the Buyer shall indemnify and hold CTC Union Technologies and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim of personal injury or death that may be associated with such unintended or unauthorized use, even if such claim alleges that CTC Union Technologies was negligent regarding the design or manufacture of said product.

WARNING:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause harmful interference in which case the user will be required to correct the interference at his own expense. NOTICE: (1) The changes or modifications not expressively approved by the party responsible for compliance could void the user's authority to operate the equipment. (2) Shielded interface cables and AC power cord, if any, must be used in order to comply with the emission limits.

CISPR PUB.22 Class A COMPLIANCE:

This device complies with EMC directive of the European Community and meets or exceeds the following technical standard. EN 55022 - Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment. This device complies with CISPR Class A.

WARNING:

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

CE NOTICE

Marking by the symbol CE indicates compliance of this equipment to the EMC directive of the European Community. Such marking is indicative that this equipment meets or exceeds the following technical standards: EN 55022:2006+A1:2007, Class A, EN55024:2010.

GSW-4208CM

8 x GbE RJ-45 + 1G/10G SFP+ Managed L2 Ethernet Switch

User Manual

Version 0.9c July, 2022

This document is the current official release manual. Contents are subject to change without prior notice. Please check CTC Union's website for any updated manual or contact us by E-mail at sales@ctcu.com. Please address any comments for improving this manual or to point out omissions or errors to marketing@ctcu.com. Thank you.

Table of Contents

CHAPTER 1. INTRODUCTION

1.1. Welcome

Welcome and thank you for purchasing GSW-4208CM Managed Ethernet Switch. We hope this product is everything you wanted and more. Our Product Managers and R&D team have placed a "quality first" motto in our development of this series of Gigabit Ethernet switches with the desire of providing a highly stable and reliable product that will give years of trouble free operation.

In this chapter we will provide general introduction to GSW-4208CM including product features and specifications. Chapter 2 will describe panels, mounting and installation methods, LED definitions and reset pushbutton. All the models in this series utilize almost identical management interfaces, whether using serial console and CLI (command line interface) commands, Telnet, HTTP (Web GUI) or SNMP (Simple Network Management Protocol). Chapter 4 will detail all of the configuration settings by using an easy to point and click Web interface which can be accessed from any available web browser.

1.2. Product Description

GSW-4208CM is a brand new generation Ethernet switch designed to make conversion between 8-Port 100M/1000M RJ-45 and 2-port 1G/10G fiber optics with SFP+ optical modules. Traditionally, transmission distance of Gigabit Ethernet over fiber interface can be extended from 550m to 100km using the flexibility of any third party pluggable SFP modules. GSW-4208CM is fully compliant with IEEE 802.3, 802.3u, 802.3ab and 802.3z standards. End-users can simply connect their devices, such as Ethernet home gateway, wireless access point or NIC on PC/laptop the RJ-45 ports of the CPE switch. No Ethernet crossover cables are required and link status can be easily monitored from the comprehensive LED display.

When GSW-4208CM is deployed as a stand-alone solution, it incorporates an easy to use Web user interface for operation, administration and maintenance both local and remotely. All of the enabled Layer 2 features and functions of GSW-4208CM can be configured and monitored via web interface and SNMP management.

1.3. Product Features

- 8 x 10M/100M/1G RJ-45 + 2 x 1G/10G SFP+
- Supports IEEE802.3az EEE (Energy Efficient Ethernet) Management to optimize power consumption
- STP, RSTP, MSTP, QoS, Traffic classification QoS, CoS, Bandwidth control for Ingress and Egress, broadcast storm control, DiffServ, IEEE802.1q VLAN, MAC based VLAN, IP subnet based VLAN, Protocol based VLAN, VLAN translation, MVR, Dynamic IEEE 802.3ad LACP Link Aggregation, Static Link Aggregation, IGMP/MLD snooping V1/V2/V3, etc.
- Security: Port based and MAC based IEEE802.1X, ACL, TACACS
- CLI, Web based management, SNMP v1/v2c/v3, Telnet for management
- Software upgrade via FTP, TFTP and HTTP, dual partitioned flash for quick recovery from upgrade failure
- DHCP client/Relay/Snooping/Snooping option 82/Relay option 82
- RMON, MIB II, port mirroring, event syslog, DNS, NTP/SNTP, IEEE802.1ab LLDP
- Supports IPv6 Telnet server/ICMP v6, SNMP, HTTP, SSH/SSL, NTP/SNTP, TFTP, QoS, ACL
- CE, FCC Certified

1.4. Product Specifications

Standards	IEEE 802.3	10Base-T 10Mbit/s Ethernet
	IEEE 802.3u	100Base-TX, 100Base-FX, Fast Ethernet
	IEEE 802.3ab	1000Base-T Gbit/s Ethernet over twisted pair
	IEEE 802.3z	1000Base-X Gbit/s Ethernet over Fiber-Optic
	IEEE 802.3ae	10G Ethernet over Fiber-Optic
	IEEE 802.1Q	Virtual LANs (VLAN)
	IEEE 802.1X	Port-based Network Access Control, Authentication
	IEEE 802.3x	Flow control for Full Duplex
	IEEE 802.1ad	Stacked VLANs, Q-in-Q
	IEEE 802.1p	LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization
	IEEE 802.1ab	Link Layer Discovery Protocol (LLDP)
	IEEE 802.3az	EEE (Energy Efficient Ethernet)
Switch	VLAN Groups	up to 4096
	Switching Fabric	68Gbps
	Data Processing	Store and Forward
	Flow Control	IEEE 802.3x for full duplex mode, back pressure for half duplex mode
	Jumbo Frame Size	10240Bytes
	MAC Table	16K
Connectors	LAN	8 x 10M/100M/1G RJ-45 port Auto detect speed, auto negotiate duplex, auto MDI/MDI-X function, Full/Half duplex
	Fiber	2 x 1G/10G dual speed mode SFP+ slots, supporting DDMI
Ethernet	Network Cable	UTP/STP Cat.5e cable or above
	EIA/TIA-568	100-ohm (100m)
	Protocol	CSMA/CD
	Reverse Polarity	auto detect/correct
	Protection	Present
	Overload Current Protection	Present
	CPU Watch Dog	Present
Power	Power Supply	AC power input 100~240V; DC power input 18~60VDC, 1A
LED	LED Indicators	PWR 1, PWR 2, ALM (For single power models), LAN (1~8), Fiber (9~10)

CHAPTER 2. INSTALLATION

This section describes panels of GSW-4208CM. The front panel of GSW-4208CM provides LAN ports, SFP fiber slot and power input port. LED indicators are also located on the front panel to provide real-time indications of link status. See below for detailed descriptions.

2.1. Panels

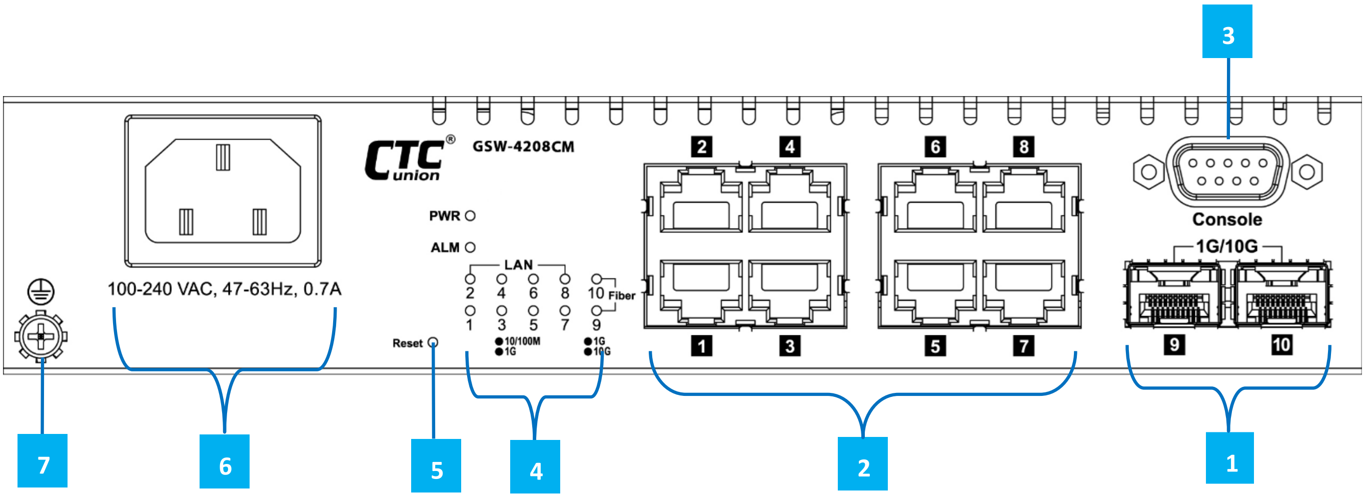


Figure 1. Front Panel with a AC Power Supply

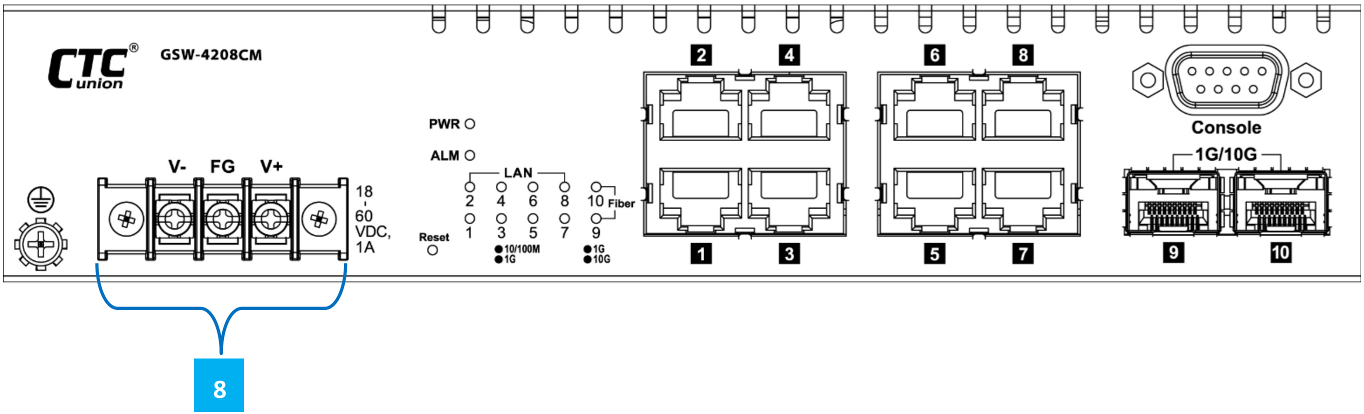


Figure 2. Front Panel with a DC Power Supply

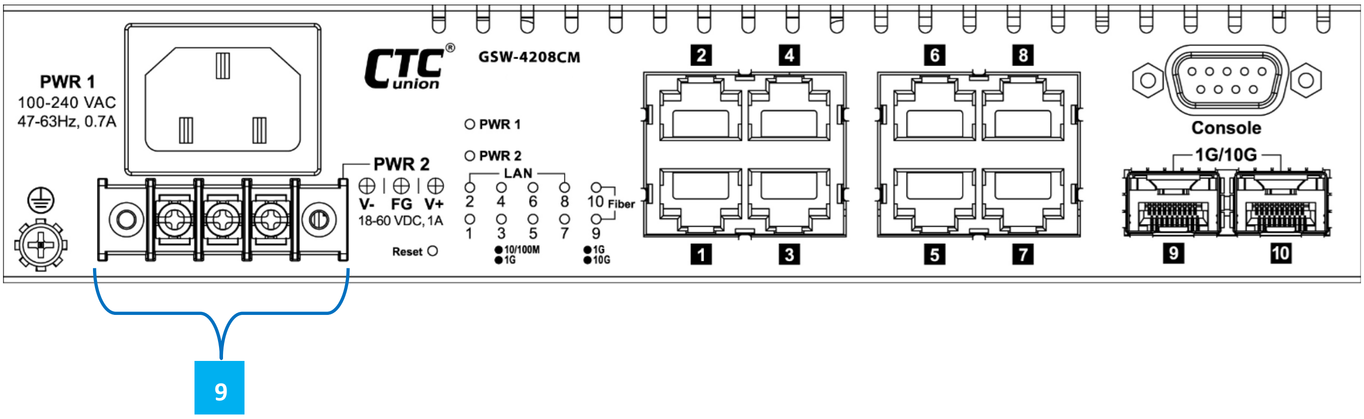


Figure 3. Front Panel with One AC and One DC Power Supply

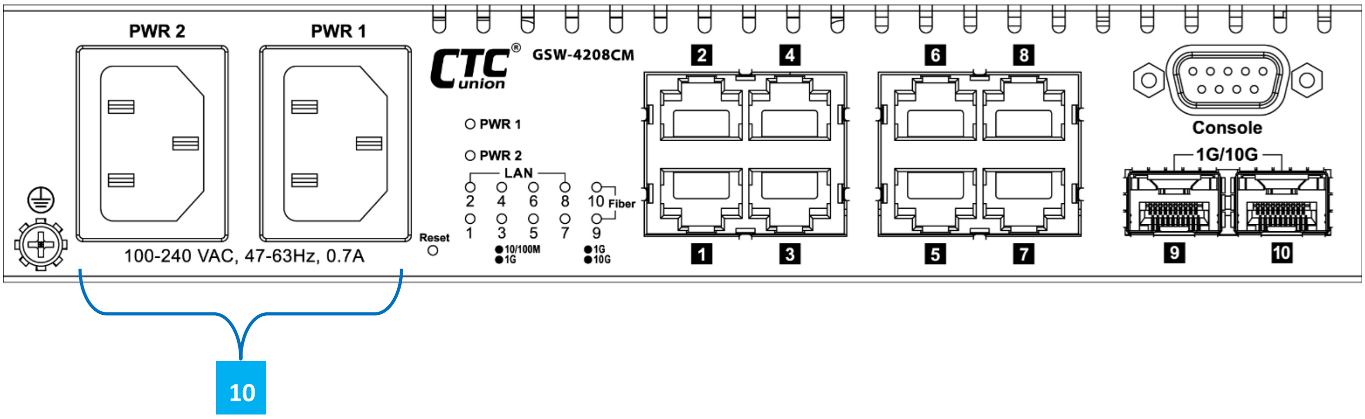


Figure 4. Front Panel with Two AC Power Supplies

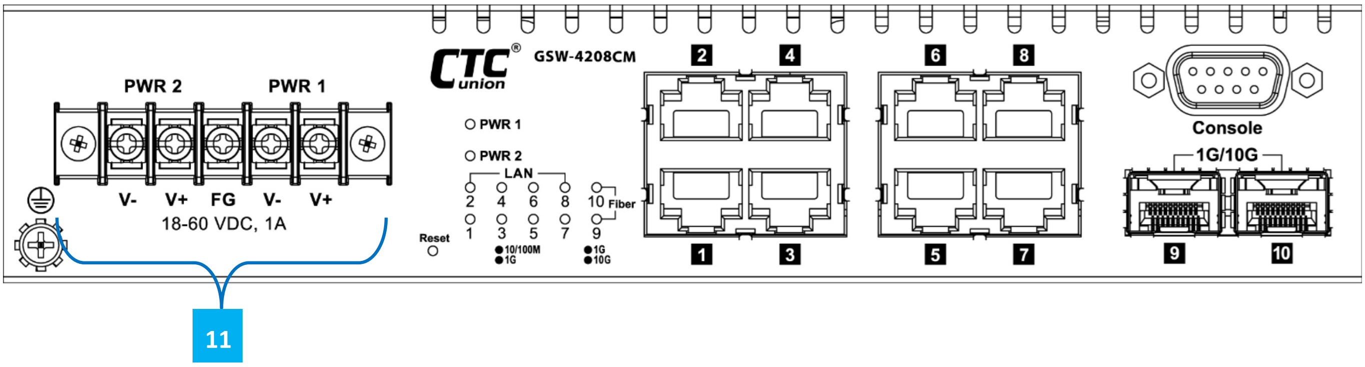


Figure 5. Front Panel with two DC Power Supplies

Index No.	Description
1	2 x 1G/10G SFP slots
2	8 x 10/100/1000M RJ-45 ports
3	RS-232 console port
4	LED indicators
5	Reset-to-default push button
6	One AC power supply
7	Grounding connection screw
8	One DC power supply
9	One AC and one DC power supply
10	Two AC power supplies
11	Two DC power suplies

Table 1. Index Reference Table

2.2. Connections

2.2.1. LAN Connections

GSW-4208CM provides 8 RJ-45 LAN ports on the front panel that support speed of 10M/100M/1G. Each of these LAN ports has associated LEDs, displayed on the front panel, which indicate the active link state and the detected speed of the interface. A green color indicates a link and a speed of 10/100Mbps, while amber color indicates a link and speed of 1Gbps.

2.2.2. Fiber Connections

GSW-4208CM utilizes two SFP modules for fiber transmission. The fiber ports have an associated status LED to indicate the presence or absence of fiber link and will also flash when there is Ethernet activity on the port. The SFP cage may insert any standard SFP module and be configured for 1G or 10G operation. There is no 'lock out' mechanism, so any third party SFP, compliant with MSA, can be used in GSW-4208CM.

2.2.3. Console Connection

The D-Sub 9 is an RS-232 console terminal port for local management. Connect one end of the provided DB-9 cable to the device, the other end to your local PC. Pinouts for RS-232 DB-9 connector are illustrated below.

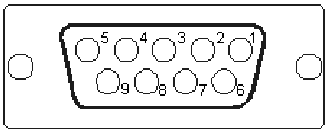
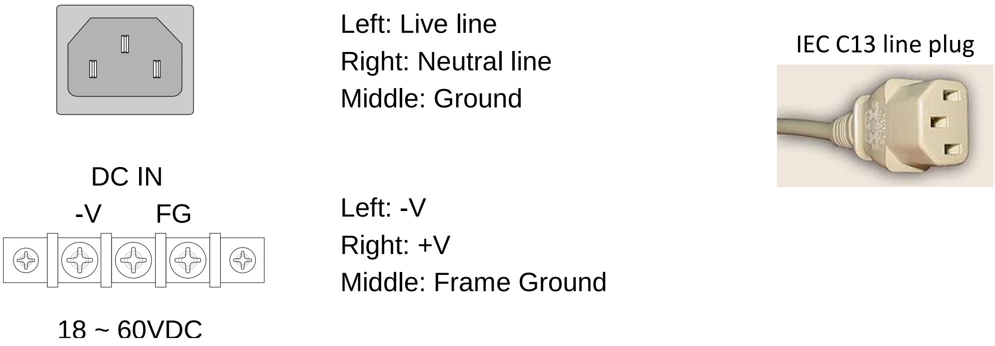


Figure 6. RS-232 (Female) Pinout

2.2.4. Power

GSW-4208CM provides two power options for power input. When AC power module is available, AC power is supplied to GSW-4208CM through a standard IEC C14 3-prong receptacle, located on the front panel. Any national power cord with IEC C13 line plug may be used to connect AC power to the power module. With a DC48 power module, DC voltage is connected to the terminal block. GSW-4208CM should always be grounded through the protective earth lead of the power cable in AC installations, or via the frame ground connection for DC installations.



Left: Live line
Right: Neutral line
Middle: Ground

Left: -V
Right: +V
Middle: Frame Ground

Figure 7. IEC (AC) & Terminal Block (DC) Power Connector Pin Assignment

2.2.5. Earth Grounding

Prior to connecting to the power, it is important to connect the ground wire to the earth. Follow steps below to install ground wire:

Step 1. Prepare one suitable ground screw and one grounding cable.
Step 2. Attach the grounding screw to the ring terminal of the grounding cable. Make sure that the grounding cable is long enough to reach the earth.
Step 3. Use a screwdriver (or other tools) to fasten the grounding screw on the earth ground hole securely.

2.3. LED Indicators

LED indicators are located on the front panel of the unit. Each port has a corresponding LED indicator that provides a visual and real-time indication of the current operating state. A description of these LED indicators is provided below.

LED	Color	Status	Meaning
PWR 1 PWR 2	Green	On	The switch is receiving power.
		Off	The switch does not receive power.
	Amber	On	There is only one power input (one power input either PWR 1 or PWR 2 does not receive power).
ALM* (Alarm)	Amber	On	This indicates an alarm has occurred.
		Off	The switch operates normally.
Fiber 9~10	Amber	On	The fiber port link is up and operating at 10Gbps.
		Blinking	The fiber port is receiving and transmitting traffic.
		Off	The fiber port link is down.
	Green	On	The fiber port link is up and operating at 1Gbps.
		Blinking	The fiber port is receiving and transmitting traffic.
		Off	The fiber port link is down.
LAN 1~8	Amber	On	When the LAN port is up and operating at 1Gbps.
		Blinking	The LAN port is receiving and transmitting traffic.
		Off	The LAN port link is down.
	Green	On	When the LAN port is up and operating at 10/100Mbps.
		Blinking	The LAN port is receiving and transmitting traffic.
		Off	The LAN port link is down.

* This LED indicator is for single power input model.

2.4. Reset Push-Button

The "Reset" push-button provides the following two functions:

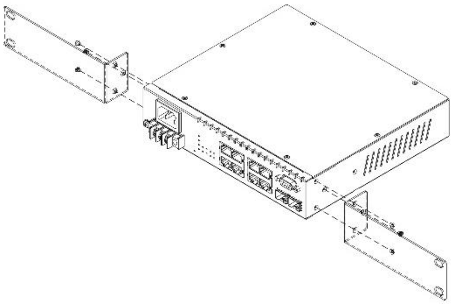
Function	Press and hold for~	LED Status	Description
Reboot	1~6 seconds	PWR LED blinks	Using a ball-point pen, press the "Reset" button and hold for 1~6 seconds then release. The switch will clear all unsaved settings and restart.
Reset to factory defaults	> 6 seconds	PWR LED blinks rapidly	Using a ball-point pen, press the "Reset" button and hold for 6 seconds or longer then release to set running configurations to factory defaults, including the original factory default IP address. If the IP address of the switch is unknown, it may be necessary to do a factory default reset. The IP address will then be the known default.

2.5. Mechanical Assembly

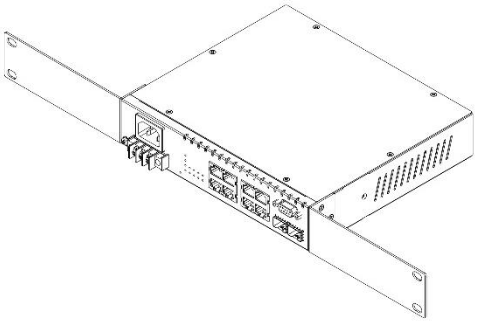
GSW-4208CM can be placed on the table top or mounted in the rack or the wall. If you choose to install in the rack, it only requires 1U space (1 3/4") in a standard EIA 19 inch rack. It is highly recommended that the unit be placed in a rack. The GSW-4208CM is delivered completely assembled, except for the rack mount brackets. No provision is made for bolting the GSW-4208CM to a tabletop. See diagrams below for detailed descriptions on how to install the rack brackets.

2.5.1. Rack Mounting (Single Unit Assembly)

1. Using the provided screws to install the rack brackets to the device.

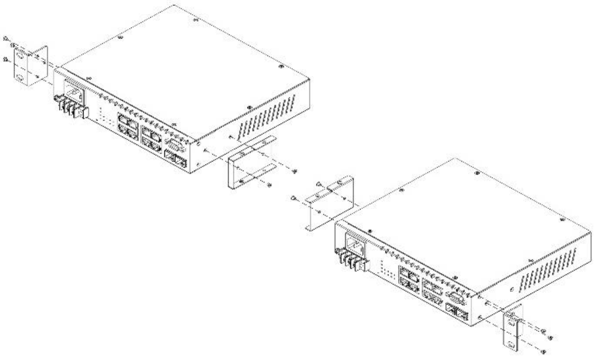


2. Once rack brackets are securely installed onto the device, you can now using the screws to fasten the device to the rack.

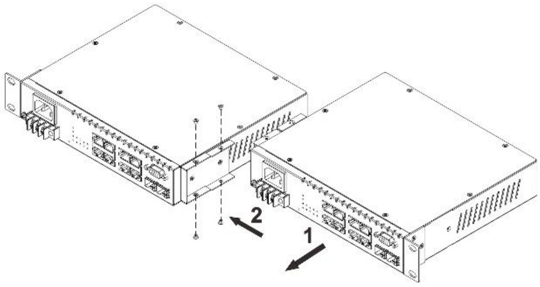


2.5.2. Rack Mounting (Two Units Assembly)

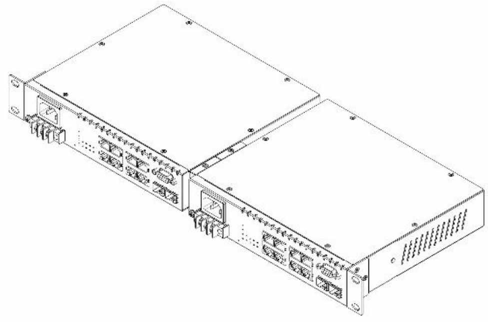
1. Using the provided screws to install the brackets to the device. Please note that rack brackets should be installed on the outer side of the device.



2. Connect two devices together and fasten securely using the provided screws.

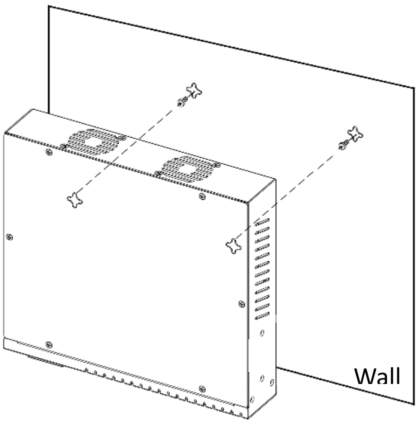


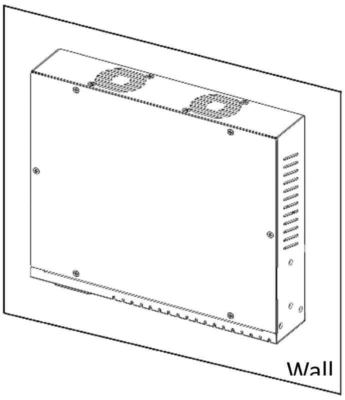
3. Once rack brackets and two devices are securely installed, you can now use the screws to fasten two devices to the rack.



2.5.3. Wall Mounting

Measure the distance between two mounting holes and fix screws on the wall. Please note that leave screws approximately 1/4 inch unfastened to hang the device.





CHAPTER 3. COMMAND LINE INTERFACE (CLI) PROVISIONING

3.1. Introduction

The GSW-4208CM Managed Ethernet switch provides a number of configuration/management methods. The first method of configuration/management uses a command line interface (CLI) via Console/Telnet/SSH access and is familiar to most network engineers. This requires that networking be configured so that the device can be accessed via a LAN port. Accessing the GSW-4208CM from a network allows for both local and remote management.

For engineers that are not comfortable using CLI, this device should be managed using any standard Web Browser in a more user friendly 'point-and-click' method. Therefore, in most configuration scenarios, Console/Telnet/SSH will only be used by experienced networking engineers.

After the device has been properly configured for the application and placed into service, a third method of configuration/management can be employed using Simple Network Management Protocol (SNMP). The operator will use SNMP management software to manage and monitor the GSW-4208CM switches on a network. This requires some configuration of the device to allow SNMP management. In addition, the network management platform will need to import and compile the proprietary MIB (management information base) file so that the management software knows "how" to manage the GSW-4208CM.

3.2. Console Operation

Using the provided accessory cable, connect the "CONSOLE" port to the PC terminal communications port (DB9). Run any terminal emulation program (HyperTerminal, PuTTY, TeraTerm Pro, etc.) and configure the communication parameters as follows:

Speed: 115,200
Data: 8 bits
Parity: none
Stop bits: 1
Flow Control: None

From a cold start, the following screen will be displayed. At the "Username" prompt, **enter 'admin' with no password**.

```
Username: admin
Password:
#
```

3.3. Telnet Connection

To use Command Line Interface (CLI), you must access the device through a Telnet/ssh connection via TCP/IP network over Ethernet. For initial operation, use the default TCP/IP settings (10.1.1.1) to login GSW-4208CM. This device supports up to 15 simultaneous Telnet sessions. Each session will disconnect automatically after a period of idle time specified by exec-timeout command.

Default TCP/IP settings of GSW-4208CM:

IP Address: 10.1.1.1
Subnet Mask: 255.255.255.0
Username: admin
Password: None (Leave this field blank)

3.4. CLI Modes

The Command Line Interface (CLI) is mainly divided into four basic modes; these are User mode, EXEC mode, Config mode and Config Interface mode. After entering the username and password, you start from the EXEC mode (prompted with "#"). The commands available in User mode and EXEC mode are limited. For more advanced configurations, you must enter Config mode or Config Interface mode. In each mode, a question mark (?) at the system prompt can be issued to obtain a list of commands available for each command mode. The following table provides a brief overview of modes available in this device.

Mode	Prompt	Enter Method	Exit Method
User mode	>	enable	disable
EXEC mode	#	Enter authorized username and password	Exit, end, logout
Global Config Mode	(config)#	Enter "configure terminal" after "#"	End, exit, end, do logout
Config Interface Mode	(config-if)#	Specify interface, interface type and number after (config)#	End, exit, end, do logout

3.5. Quick Keys

There are several useful quick keys you can use when editing command lines.

Keyboard	Action
?	Issue "?" to get a list of commands available in the current mode.
Up arrow key	To view the previous entered commands.
Down arrow key	To view the previous entered commands.
Tab key	To complete an unfinished command.

3.6. Command Syntax

Commands introduced in this user manual are written using the coherent symbols and easy-to-understand syntax and style. Although users can issue Help command to complete a desired command in CLI, it is useful to understand frequently-used symbols and syntax conventions. The following table lists the syntax conventions used in this user manual together with an example.

Example: (config-if-vlan)# ip address { { <address> <netmask> } | { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] } }

Symbol	Function	Example	Explanation
< > (Angle bracket)	Enter a value, alphanumeric strings or keywords.	<address> <netmask>	Enter IP address and subnet mask.
[ ] (Square bracket)	This is an optional parameter.	[fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]]	Fallback parameter is an optional item.
{ } (Curly bracket)	A curly bracket has the following two functions: 1. If there are more than two options available, a curly bracket can be used to separate them. 2. The outer curly bracket means that this is a must parameter. At least one value should be specified.	{ { <address> <netmask> } | { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] } }	At least specify one option to complete the command.
| (Vertical bar)	Use a vertical bar to separate options.	{ { <address> <netmask> } | { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] } }	Enter IP address or use DHCP to assign IP address automatically.

3.7. Basic Configurations

This section introduces users how to change the default IP address to the desired one and save the current running configurations to startup configurations. For detailed introductions to commands, please see section 3.8, 3.9, 3.10 & 3.11.

3.7.1. Configuring IPv4 Address

IP address: 192.168.0. 101
Subnet mask: 255.255.255.0

```
# config terminal
(config)# interface vlan 1
(config-if-vlan)# ip address 192.168.0.101 255.255.255.0
(config-if-vlan)# exit
(config)# exit
# show ip interface brief
Vlan Address                          Method     Status
---- -------------------------------- ---------------- ------
1    192.168.0.101/24                 Manual      DOWN
```

3.7.2. Enter Config Interface Mode

- Enter Port 1’s Config Interface mode.

```
# config terminal
(config)# interface GigabitEthernet 1/1
(config-if)#
```

Note: 1/1 means Ethernet Interface 1, Port 1.

- Enter Port 1~3’s Config Interface mode.

```
# config terminal
(config)# interface GigabitEthernet 1/1-3
(config-if)#
```

Note: 1/1-3 means Ethernet Interface 1, Port 1 to Port 3.

- Enter Port 1~3 & Port 5’s Config Interface mode.

```
# config terminal
(config)# interface GigabitEthernet 1/1-3,5
(config-if)#
```

Note: 1/1-3,5 means Ethernet Interface 1, Port 1 to Port 3 and Port 5.

3.7.3. Save Configurations

```
# copy running-config startup-config
Building configuration...
% Saving 1469 bytes to flash:startup-config
#
```

3.7.4. Restart the Device

```
# reload cold
% Cold reload in progress, please stand by.
#

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

RedBoot> fi lo -d managed
Image loaded from 0x80040000-0x80ae54cc
RedBoot> go

Press ENTER to get started
```

3.7.5. Load Factory Defaults

Load factory default settings

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

Load factory defaults but keep IP settings

```
# reload defaults keep-ip
% Reloading defaults, attempting to keep VLAN 1 IP address. Please stand by.
```

3.7.6. Show System and Software Information

```
#    show version

MAC Address          : 00-02-ab-f8-7d-70
Previous Restart     : Cold
```

```
System Contact       :
System Name          :
System Location      :
System Time          : 2022-05-17T10:59:49+00:00
System Uptime        : 00:28:39

Bootloader
------------------
Image                : RedBoot (bootload)
Version              : version 1_5-0dd76c3
Date                 : 02:42:50, Sep   8 2021


Active Image
------------------
Image                : linux (primary)
Version              : 1.000
Date                 : 2022-05-17T10:39:59+08:00
Upload filename      : GSW-4208CM-Series.mfi

Backup Image
------------------
Image                : linux (primary)
Version              : 1.000
Date                 : 2021-10-29T00:45:17+00:00
Upload filename      : GSW-4208CM-Series_v1.000.mfi
------------------
SID : 1
------------------
Port Count           : 10
Product              : GSW-4208CM
Software Version     : V1.000
Build Date           : 2022-05-17T10:39:59+08:00
```

3.7.7. Show Running Configurations

```
# show running-config
Building configuration...
username admin privilege 15 password none
!
vlan 1
!
!
!
no smtp server
spanning-tree mst name 00-02-ab-00-00-01 revision 0
```

```
!
interface GigabitEthernet 1/1
  no spanning-tree
!
interface GigabitEthernet 1/2
  no spanning-tree
!
interface GigabitEthernet 1/3
  no spanning-tree
!
interface GigabitEthernet 1/4
  no spanning-tree
!
-- more --, next page: Space, continue: g, quit: ^C
```

3.7.8. Show History Commands

```
# show history
    config t
    exit
    config t
    ip arp ex
    exit
```

```
> show history
  config t
    interface GigabitEthernet 1/3
    exit
    interface GigabitEthernet 1/1-2
    exit
    flowcontrol on
    exit
    show interface * status
    disable
    show clock detail
    show dot1x
    show history
```

3.7.9. Help

Help command can be issued in User, Exec, and Global Config mode to get a hint message describing how to use "show" command to get help from CLI.

```
# help
Help may be requested at any point in a command by entering
a question mark '?'.    If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
```

```
Two styles of help are provided:
1. Full help is available when you are ready to enter a
      command argument (e.g. 'show ?') and describes each possible
      argument.
2. Partial help is provided when an abbreviated argument is entered
      and you want to know what arguments match the input
      (e.g. 'show pr?'.)
```

3.7.10. Logout

To close an active terminal session, issue the “logout” command in User or EXEC mode.

```
(config)# exit
# logout

Press ENTER to get started
```

```
# disable
> logout

Press ENTER to get started
```

3.8. Commands in User Mode

When you successfully login in Command Line Interface, you are in EXEC Mode (prompted with “#”). To enter User mode, issue “disable” command after # prompt. Then you will be directed to User mode with “>” prompt.

```
Username: admin
Password:
#
# disable
>
```

In User mode, only limited commands are available. These commands are used for clearing statistics, entering Exec mode and pinging the specified destination. To configure a function, you should enter Config mode or Config Interface mode.

3.8.1. > clear ip acd

Syntax: > clear ip acd

Explanation: Clear IPv4 address conflict detection (ACD) results.

3.8.2. > clear ipv6 dhcp relay statistics

Syntax: > clear ipv6 dhcp relay statistics [interface vlan <vlan_id>]

Explanation: Clear IPv6 DHCP relay statistics.

3.8.3. > enable

Syntax: > enable [<new_priv>]

[<new_priv: 0-15>]: Choose a privilege level.

Explanation: Enter the EXEC mode.

3.8.4. > exit

Syntax: > exit

Explanation: Return to the previous mode. Issuing this command in User mode will logout the Command Line Interface.

3.8.5. > help

Syntax: > help

Explanation: Provide help messages.

3.8.6. > logout

Syntax: > logout

Explanation: Logout the Command Line Interface.

3.8.7. > ping ipv6

Syntax: > ping ipv6 { <domain_name> | <ip_addr> } [repeat <count>] [saddr <src_addr>] [sif { <port_type> <src_if> | vlan <vlan_id> }] [size <size>] [data <data_value>] [{ verbose | quiet }]

Parameters:

{ <domain_name> | <ip_addr> }: Specify IPv6 address or domain name that you want to ping.

[repeat <count>]: The number of packets that are sent to the destination IP or host.

saddr <src_addr>: This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

[sif { <port_type> <src_if> | vlan <vlan_id> } }]: Specify source interface information for PING function.

sif { <port_type> <src_if>: This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

vlan <vlan_id>: This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the Source Port Number or the IP Address for the source interface.

[size <size>]: The size of the packet.

data <data_value>**:** Specify the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

{ verbose | quiet }: "quiet" option will not print the result of each ping request but will only show the final result.

Explanation: To carry out ping tests on the specified destination IPv6 address or host.

3.8.8. > ping ip

Syntax: > ping ip { <domain_name> | <ip_addr> } [ttl <ttl_value>] [repeat <count>] [{ saddr <src_addr> | sif { <port_type> <src_if> | vlan <vlan_id> } }] [size <size>] [data <data_value>] [{ verbose | quiet }]

Parameters:

{ <domain_name> | <ip_addr> }: Specify IPv4 address or domain name that you want to ping.

[ttl <ttl_value>]: Specify the Time-To-Live (TTL) field value in the IPv4 header. The default value is 64. The valid range is 1-255.

[repeat <count>]: The number of packets that are sent to the destination IP or host.

[{ saddr <src_addr> | sif { <port_type> <src_if> | vlan <vlan_id> } }]: Specify source interface information for PING function.

saddr <src_addr>: This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

sif { <port_type> <src_if>: This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

vlan <vlan_id>: This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the Source Port Number or the IP Address for the source interface.

[size <size>]: The size of the packet.

data <data_value>**:** Specify the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

{ verbose | quiet }: "quiet" option will not print the result of each ping request but will only show the final result.

Explanation: To carry out ping tests on the specified destination IPv4 address or host.

3.8.9. show commands

In User mode, “show” commands can be issued to display current status or settings of a certain command. They will be introduced in Section 3.9 “Commands in Config Mode”.

3.9. Commands in EXEC Mode

3.9.1. # clear access management statistics

Syntax: # clear access management statistics

Explanation: Clear access (HTTP, HTTPs, SNMP, Telnet, SSH) management statistics.

3.9.2. # clear access-list ace statistics

Syntax: # clear access-list ace statistics

Explanation: Clear access list entry statistics.

3.9.3. # clear dot1x statistics

Syntax: # clear dot1x statistics [interface (<port_type> [<v_port_type_list>])]

Parameter:

[interface (<port_type> [<v_port_type_list>])]: Specify the interface that you want to clear.

Explanation: Clear (the specified interfaces') dot1x statistics.

3.9.4. # clear ip acd

Syntax: # clear ip acd

Explanation: Clear IPv4 address conflict detection (ACD) results.

3.9.5. # clear ip arp

Syntax: # clear ip arp

Explanation: Clear ARP cache.

3.9.6. # clear ip dhcp detailed statistics

Syntax: # clear ip dhcp detailed statistics { server | client | snooping | relay | helper | all } [interface (<port_type> [<in_port_list>])]

Explanation: Clear IP DHCP statistics.

Parameter:

{ server | client | snooping | relay | helper | all }: Specify the type of information that you want to clear.

[interface (<port_type> [<in_port_list>])]: Specify the interface type and port number.

3.9.7. # clear ip dhcp relay statistics

Syntax: # clear ip dhcp relay statistics

Explanation: Clear IP DHCP Relay statistics.

3.9.8. # clear ip dhcp server binding <ip>

Syntax: # clear ip dhcp server binding <ip>

Parameter:

<ip>: Specify the IP address for this server binding setup.

Explanation: Clear DHCP server binding cache in relation to the specified IP address.

3.9.9. # clear ip dhcp server binding { automatic | manual | expired }

Syntax: # clear ip dhcp server binding { automatic | manual | expired }

Parameter:

{ automatic | manual | expired }: Specify the server binding mode.

Explanation: Clear automatic, manual or expired server binding caches.

3.9.10. # clear ip dhcp server statistics

Syntax: # clear ip dhcp server statistics

Explanation: Clear DHCP server statistics.

3.9.11. # clear ip dhcp snooping statistics

Syntax: # clear ip dhcp snooping statistics [interface (<port_type> [<in_port_list>])]

Explanation: Clear IP DHCP Snooping statistics.

3.9.12. # clear ip igmp snooping

Syntax: # clear ip igmp snooping [vlan <v_vlan_list>] statistics

Explanation: Clear IP IGMP Snooping statistics.

3.9.13. # clear ip statistics

Syntax: # clear ip statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

Explanation: Clear IPv4 statistics for system, interface and ICMP.

3.9.14. # clear ipv6 dhcp relay statistics

Syntax: # clear ipv6 dhcp relay statistics [interface vlan <vlan_id> [interface vlan <rel_vlan_id]]

Explanation: Clear IPv6 DHCP relay statistics.

3.9.15. # clear ipv6 mld snooping

Syntax: # clear ipv6 mld snooping [vlan <v_vlan_list>] statistics

Explanation: Clear statistics for IPv6 MLD Snooping.

3.9.16. # clear ipv6 neighbors

Syntax: # clear ipv6 neighbors

Explanation: Clear the table for IPv6 neighbors.

3.9.17. # clear ipv6 statistics

Syntax: # clear ipv6 statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

Explanation: Clear IPv6 statistics for system, interface and ICMP.

3.9.18. # clear known-host-keys

Syntax: # clear known-host-keys

Explanation: Clear the cache of known hosts' SSH keys.

3.9.19. # clear lacp statistics

Syntax: # clear lacp statistics

Explanation: Clear LACP statistics.

3.9.20. # clear link-oam statistics

Syntax: # clear link-oam statistics [interface (<port_type> [plist])]

Explanation: Clear Link OAM statistics.

3.9.21. # clear lldp statistics

Syntax: # clear lldp statistics { interface (<port_type> [<port_type> [<plist >])] | global }

Explanation: Clear LLDP statistics of specified interfaces or clear LLDP global statistics.

3.9.22. # clear logging

Syntax: # clear logging [informational] [notice] [warning] [error] [switch <switch_list>]

Explanation: Clear specific syslog events.

3.9.23. # clear mac address-table

Syntax: # clear mac address-table

Explanation: Clear MAC address table.

3.9.24. # clear mvr

Syntax: # clear mvr [vlan <v_vlan_list> | name <mvr_name>] statistics

Explanation: Clear MVR statistics.

3.9.25. # clear port-security dynamic

Syntax: # clear port-security dynamic [{ address <mac> [vlan <vlan_on_mac>]}| { interface (<port_type> [<plist>]) [vlan < vlan_on_interface>] | vlan <vlan>}

Explanation: Clear port security information.

3.9.26. # clear spanning-tree

Syntax: # clear spanning-tree { { statistics [interface (<port_type> [<v_port_type_list>])] } | { detected-protocols [interface (<port_type> [<v_port_type_list_1>])] } }

Explanation: Clear specific interfaces' Spanning Tree statistics.

3.9.27. # clear statistics

Syntax: # clear statistics [interface] (<port_type> [<v_port_type_list>])

Explanation: Clear Fast Ethernet and/or Gigabit Ethernet interfaces' statistics.

3.9.28. # clear system led status

Syntax: # clear system led status [switch <switch_list>] {fatal | software | post | ztp | stack-firmware | all}

Explanation: Clear error status of system LED.

3.9.29. # config terminal

Syntax: # config terminal

Explanation: Enter the Global Config mode.

Example:

```
# config t
(config)#
```

3.9.30. # copy

Syntax: # copy { startup-config | running-config | <source_path> } { startup-config | running-config | <destination_path> } [syntax-check]

{ startup-config | running-config | <source_path> }: Specify the file type that you want to copy from. This can be "startup-config", "running-config" or a specific source file in flash or TFTP server.

{ startup-config | running-config | <destination_path> }: Specify the file type that you want to copy to. This can be "startup-config", "running-config" or a specific destination file in flash or TFTP server.

Explanation: Save running configurations to startup configurations.

Example: Save running configurations to startup configurations.

```
# copy running-config startup-config
Building configuration...
% Saving 1596 bytes to flash:startup-config
#
```

Explanation: Save startup configurations to running configurations.

Example: Save running configurations to startup configurations.

```
# copy startup-config running-config
Building configuration...
% Saving 1596 bytes to flash:startup-config
#
```

Explanation: Save running configurations to Flash 201

```
# copy running-config Flash:201
Building configuration...
% Saving 1487 bytes to flash:201
# dir
Directory of flash:
   r- 1970-01-01 00:00:00     284 default-config
   rw 2015-01-01 01:56:32    1487 startup-config
   rw 2015-01-01 01:56:49    1487 201
3 files, 3258 bytes total.
```

3.9.31. # delete

Syntax: # delete <path>

Explanation: Delete a file saved in Flash.

Parameters:

<Path : word>: Name of the file in Flash to be deleted.

Example: Delete a file named 201 in Flash.

```
# dir
Directory of flash:
    r- 1970-01-01 00:00:00      284 default-config
    rw 2015-01-01 01:56:32     1487 startup-config
    rw 2015-01-01 01:56:49     1487 201
3 files, 3258 bytes total.
# delete flash:201
# dir
Directory of flash:
    r- 1970-01-01 00:00:00      284 default-config
    rw 2015-01-01 01:56:32     1487 startup-config
2 files, 1771 bytes total.
```

3.9.32. # dir

Explanation: Display files in flash.

Example:

```
# dir
Directory of flash:
    r- 1970-01-01 00:00:00      284 default-config
    rw 2015-01-01 01:56:32     1487 startup-config
    rw 2015-01-01 01:56:49     1487 201
```

3.9.33. # disable & # enable

Explanation: Return to user mode or enter exec mode.

```
# disable
>
>
> enable
#
"
```

3.9.34. # dot1x initialize

Syntax: # dot1x initialize [interface (<port_type> [<plist>])

[interface (<port_type> [<plist>])]: Specify the type of interface that you intend to use. “*” means all interfaces.

<plist>: Specify the ports that apply to this command.

Explanation: To initialize dot1x function in an interface immediately.

3.9.35. # firmware swap

Syntax: # firmware swap

Explanation: Use the other standby firmware image file uploaded to flash.

3.9.36. # firmware upgrade

Syntax: # firmware upgrade <url_file> [ftp-active]

Parameter:

<url_file >: Specify the uniform resource locator for firmware upgrade. It is a specific character string that constitutes a reference to a resource. See the firmware upgrade example provided below.

[ftp-active]: When FTP is used for firmware upgrade, you can add "ftp-active" to indicate that FTP is running under active mode.

[save-host-key]: Save SSH host key in local cache.

Explanation: Upgrade the firmware image.

Example: Upgrade the new firmware image via TFTP, FTP & HTTP server.

TFTP

```
# firmware upgrade tftp://10.1.1.223/switch.dat
Downloaded "/switch.dat", 5211062 bytes
Waiting for firmware update to complete
Starting flash update - do not power off device!
Erasing image...
Programming image...
Flash update succeeded.

RedBoot> fi lo -d managed
RedBoot> go

Press ENTER to get started
```

SFTP

```
# firmware upgrade sftp://account:password@10.1.1.223/switch.dat save-host-key
Fetching...
looking up 10.1.1.223
connecting non-blocking to 10.1.1.223:21
connection: No error
setting passive mode
opening data connection
initiating transfer
Waiting for firmware update to complete
Starting flash update - do not power off device!
Erasing image...
Programming image...

RedBoot> fi lo -d managed
RedBoot> go

Press ENTER to get started
```

FTP

```
# firmware upgrade ftp://account:password@10.1.1.223/switch.dat
Fetching...
looking up 10.1.1.223
connecting non-blocking to 10.1.1.223:21
connection: No error
setting passive mode
opening data connection
initiating transfer
Waiting for firmware update to complete
Starting flash update - do not power off device!
Erasing image...
Programming image...

RedBoot> fi lo -d managed
RedBoot> go
```

```
Press ENTER to get started
```

HTTP

```
# firmware upgrade http://account:password@10.1.1.223:8080/fwfolder/switch.dat
Fetching...
looking up 10.1.1.223
connecting non-blocking to 10.1.1.223:8080
connection: No error
requesting http://10.1.1.223:8080/fwfolder/switch.dat
Waiting for firmware update to complete
Starting flash update - do not power off device!
Erasing image...
Programming image...
Flash update succeeded.

RedBoot> fi lo -d managed
RedBoot> go

Press ENTER to get started
```

3.9.37. # ip dhcp retry interface vlan

Syntax: # ip dhcp retry interface vlan <vlan_id>

Parameter:

<vlan_id>: Specify the valid VLAN ID for DHCP query.

Explanation: Restart the DHCP query process.

3.9.38. # ipv6 dhcp-client restart

Syntax: # ipv6 dhcp-client restart [interface vlan <v_vlan_list>]

Parameter:

<v_vlan_list>: Specify the VLANs associated with the IP interface.

Explanation: Restart the IPv6 client service.

3.9.39. # link-oam remote-loopback

Syntax: # link-oam remote-loopback { start | stop } interface (<port_type> [<v_port_type_list>])

Explanation: Start or stop Link OAM remote loockback function on the specified interface.

Parameter:

{ start | stop }: To start or stop remote loopback function.

interface (<port_type> [<v_port_type_list>]): Specify the specific interface that is used for remote loopback function.

3.9.40. # logout

Syntax: # logout

Explanation: Logout from the device.

3.9.41. # more

Syntax: # more <path>

<path>: Specify the filename.

Explanation: Display file in Flash or in TFTP server.

3.9.42. # ping ip

Syntax: # ping ip { <domain_name> | <ip_addr> } [ttl <ttl_value>] [repeat <count>] [{ saddr <src_addr> | sif { <port_type> <src_if> | vlan <vlan_id> } }] [size <size>] [data <data_value>] [{ verbose | quiet }]

Explanation: To carry out ping tests on the specified destination IPv4 address or host.

Parameters:

{ <domain_name> | <ip_addr> }: Specify IPv4 address or domain name that you want to ping.

[ttl <ttl_value>]: Specify the Time-To-Live (TTL) field value in the IPv4 header. The default value is 64. The valid range is 1-255.

[repeat <count>]: The number of packets that are sent to the destination IP or host.

[{ saddr <src_addr> | sif { <port_type> <src_if> | vlan <vlan_id> } }]: Specify source interface information for PING function.

saddr <src_addr>: This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

sif { <port_type> <src_if>: This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

vlan <vlan_id>: This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the Source Port Number or the IP Address for the source interface.

[size <size>]: The size of the packet.

data <data_value>**:** Specify the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

{ verbose | quiet }: "quiet" option will not print the result of each ping request but will only show the final result.

3.9.43. # ping ipv6

Syntax: # ping ipv6 { <domain_name> | <ip_addr> } [repeat <count>] [saddr <src_addr>] [sif { <port_type> <src_if> | vlan <vlan_id> }] [size <size>] [data <data_value>] [{ verbose | quiet }]

Explanation: To carry out ping tests on the specified destination IPv6 address or host.

Parameters:

{ <domain_name> | <ip_addr> }: Specify IPv6 address or domain name that you want to ping.

[repeat <count>]: The number of packets that are sent to the destination IP or host.

saddr <src_addr>: This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

[sif { <port_type> <src_if> | vlan <vlan_id> } }]: Specify source interface information for PING function.

sif { <port_type> <src_if>: This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

vlan <vlan_id>: This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the Source Port Number or the IP Address for the source interface.

[size <size>]: The size of the packet.

data <data_value>**:** Specify the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

{ verbose | quiet }: "quiet" option will not print the result of each ping request but will only show the final result.

3.9.44. # reload cold

Syntax: # reload cold

Explanation: Perform a cold reload on the system.

3.9.45. # reload defaults

Syntax: # reload defaults [keep-ip]

Parameters:

[keep-ip]: Keep VLAN 1 IP setting.

Explanation: Restore the device to factory default settings.

3.9.46. # send

Syntax: # send { * | <session_list> | console 0 | vty <vty_list> } <message>

Explanation: Send messages to other tty lines.

Parameters:

{ * | <session_list> | console 0 | vty <vty_list> }: Choose one of the options.

* : Specify “*” to denote all tty users.

<session_list>: Specify a session number between 0 and 16.

console 0: This means primary terminal line.

<vty_list>: Send a message to a virtual terminal.

<message>: Enter a message in 128 characters that you want to send.

3.9.47. # terminal editing

Syntax: # terminal editing

Explanation: Enable command line editing.

Show: > show terminal
# show terminal

Negation: # no terminal editing

3.9.48. terminal exec-timeout

Syntax: # terminal exec-timeout <0-1440>

Parameters:

<0-1440>: Specify the timeout value in minutes.

Explanation: Set up terminal timeout value.

Show: > show terminal
# show terminal

Negation: # no terminal exec-timeout

3.9.49. # terminal history size

Syntax: # terminal history size <0-32>

Parameters:

<0-32>: Specify the current history size. “0” means to disable.

Explanation: Set up terminal history size.

Show: > show terminal
# show terminal

Negation: # no terminal history size

3.9.50. # terminal length

Syntax: # terminal length <0 or 3-512>

Parameters:

<0 or 3-512>: Specify the lines displayed on the screen. "0" means no pausing.

Explanation: Set up terminal length.

Show: > show terminal
# show terminal

Negation: # no terminal length

3.9.51. # terminal width

Syntax: # terminal width <0 or 40-512>

Parameters:

<0 or 40-512>: Specify the width displayed on the screen. "0" means unlimited width.

Explanation: Set up terminal display width.

Show: > show terminal
# show terminal

Negation: # no terminal width

3.9.52. # traceroute ip

Syntax: # traceroute ip { <domain_name> | <ip_addr> } [dscp <dscp>] [timeout <timeout>] [{ saddr <src_addr> | sif { <port_type> <src_if> | vlan <vlan_id> } }] [probes <probes>] [firstttl <firstttl>] [maxttl <maxttl>] [icmp] [numeric]

Explanation: This command allows you to perform a traceroute test over IPv4 towards a remote host. Traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network.

Parameters:

{ <domain_name> | <ip_addr> }: The destination IP Address.

[dscp <dscp>]: This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-

63.

[probes <probes>]: Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

[timeout <timeout>]: Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.

[firstttl <firstttl>]: Determines the value of the Time-To-Live (TTL) field in the IPv4 header in the first packet sent. The default number is 1. The valid range is 1-30.

[maxttl <maxttl>]: Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.

saddr <src_addr>: This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

[{ sif { <port_type> <src_if> | vlan <vlan_id> }]: Specify source interface information for traceroute function.

sif { <port_type> <src_if>: This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

vlan <vlan_id>:This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the Source Port Number or the IP Address for the source interface.

[icmp]: By default, the traceroute command will use UDP datagrams. Selecting this option forces it to use ICMP ECHO packets instead.

[numeric]: By default the traceroute command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

3.9.53. # traceroute ipv6

Syntax: # traceroute ipv6 { <domain_name> | <ip_addr> } [dscp <dscp>] [timeout <timeout>] [saddr <src_addr>] [sif { <port_type> <src_if> | vlan <vlan_id> }] [probes <probes>] [maxttl <maxttl>] [numeric]

Explanation: This command allows you to perform a traceroute test over IPv6 towards a remote host. Traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network.

Parameters:

{ <domain_name> | <ip_addr> }: The destination IP Address.

[dscp <dscp>]: This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-63.

[probes <probes>]: Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

[timeout <timeout>]: Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.

[maxttl <maxttl>]: Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.

saddr <src_addr>: This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

[sif { <port_type> <src_if> | vlan <vlan_id> } }]: Specify source interface information for traceroute function.

sif { <port_type> <src_if>: This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

vlan <vlan_id>:This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the Source Port Number or the IP Address for the source interface.

[numeric]: By default the traceroute command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

3.9.54. show commands

In Exec mode, “show” commands can be issued to display current status or settings of a certain command. They will be introduced in Section 3.9 “Commands in Config Mode”.

3.10. Commands in Config Mode

To enter Global Config Mode, you need to type the following command under "#":

```
# config terminal
(config)#
```

3.10.1. (config)# aaa

3.10.1.1. (config)# aaa accounting

Syntax: (config)# aaa accounting { console | telnet | ssh } tacacs { [commands <priv_lvl>] [exec] }}

Explanation: Configure the command and exec (login) authentication method for the client.

Parameters:

{ console | telnet | ssh }: Specify one of the authentication clients.

{ [commands <priv_lvl>] [exec] }: Use the remote TACACS server for accounting. Enable the accounting of all commands with a privilege level. Valid level values are 0 to 15. Specify "exec" to enable exec (login) accounting.

Negation: (config)# no aaa accounting { console | telnet | ssh }

Show: # show aaa

3.10.1.2. (config)# aaa authentication login

Syntax: (config)# aaa authentication login { console | telnet | ssh | http } { { local | radius | tacacs } [{ local | radius | tacacs } [{ local | radius | tacacs }]] }

Explanation: Configure the authentication method for the client.

Parameters:

{ console | telnet | ssh | http }: Specify one of the authentication clients.

{ { local | radius | tacacs } [{ local | radius | tacacs } [{ local | radius | tacacs }]] }: Specify one of the authentication methods for the specified client. At least one method needs to be specified. Users can specify three methods at most.

local: Use the local user database on the switch for authentication.

radius: Use remote RADIUS server(s) for authentication.

tacacs: Use remote TACACS+ server(s) for authentication.

NOTE: *Methods that involve remote servers will time out if the remote servers are offline. In this case the next method is tried. Each method is tried and continues until a method either approves or rejects a user. If a remote server is used for* *primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.*

Example: Set the Console client to use remote RADIUS server(s) for authentication.

```
# config t
(config)# aaa authentication login console radius
```

Negation: (config)# no aaa authentication login { console | telnet | ssh | http }

Show: # show aaa

3.10.1.3. (config)# aaa authorization

Syntax: (config)# aaa authorization { console | telnet | ssh } tacacs commands <priv_lvl> [config-commands]

Explanation: Use this command to limit the CLI commands available to a user.

Parameters:

{ console | telnet | ssh }: Specify one of the authentication clients that applies to this rule.

<priv_lvl> : Use the remote TACACS server for authorization. Authorize all commands with a privilege level. Valid level values are 0 to 15.

[config-commands]: Specify "config-commands" to authorize configuration commands.

Negation: (config)# no aaa authorization { console | telnet | ssh }

Show: # show aaa

3.10.2. (config)# access management

Syntax: (config)# access management <access_id> <access_vid> <start_addr> [to <end_addr>] { [web] [snmp] [telnet] | all }

Explanation: Create an access management rule.

Parameters:

<access_id: 1-16>: Specify an ID for this access management entry.

<access_vid>: Indicates the VLAN ID for the access management entry.

<start_addr> [to <end_addr>]: Indicate the starting and ending IP address for the access management entry.

{ [web] [snmp] [telnet] | all }: Specify matched hosts can access the switch from which interface.

Example: Allow IP 192.168.0.1 to 192.168.0.10 to access the device via Web, SNMP and Telnet.

```
# config t
(config)# access management 1 1 192.168.0.1 to 192.168.0.10 all
```

Negation: (config)# no access management
(config)# no access management <access_id>

Show: # show access management [statistics | <access_id_list>]

Clear: # clear access management statistics

3.10.3. (config)# access-list

3.10.3.1. (config)# access-list [update] ace

Syntax: There are several commands for "access-list" depending on the frame type you used.

1. **Frame Type : Non-IPv6**

(config)# access-list { ace | pre-ace | bypass-ace } [update] <ace_id> [next { <ace_id_next> | last }] [ingress interface { [<port_type> <ingress_port_list>] } | any }] [policy <policy> [policy-bitmask <policy_bitmask>]] [tag { tagged | untagged | any }] [vid { <vid> | any }] [tag-priority { <tag_priority> | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7 | any }] [frame-type **non-ipv6** [action { permit | deny | filter interface (<port_type> [<fliter_port_list>]] [rate-limiter { <rate_limiter_id> | disable }] [mirror [disable]] [logging [disable]] [shutdown [disable]] [lookup-second [disable]]

2. **Frame Type: Ethernet Type**

(config)# access-list { ace | pre-ace | bypass-ace } [update] <ace_id> [next { <ace_id_next> | last }] [ingress interface <ingress_port_list> | any] [policy <policy> [policy-bitmask <policy_bitmask>]] [tag { tagged | untagged | any }] [vid { <vid> | any }] [tag-priority { <tag_priority> | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7 | any }] [frame-type **etype** [etype-value { <etype_value> | any }] [smac { <etype_smac> | any }] [dmac { <etype_dmac> | any }] [action { permit | deny | filter interface [<fliter_port_list>] [rate-limiter { <rate_limiter_id> | disable }] [mirror [disable]] [logging [disable]] [shutdown [disable]] [lookup-second [disable]]

3. **Frame Type: ARP**

(config)# access-list { ace | pre-ace | bypass-ace } [update] <ace_id> [next { <ace_id_next> | last }] [ingress interface <ingress_port_list> | any] [policy <policy> [policy-bitmask <policy_bitmask>]] [tag { tagged | untagged | any }] [vid { <vid> | any }] [tag-priority { <tag_priority> | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7 | any }] [dmac-type { unicast | multicast | broadcast | any }] [frame-type [arp-opcode { arp | rarp | other | any }] [arp-flag [arp-request

{ <arp_flag_request> | any }] [arp-smac { <arp_flag_smac> | any }] [arp-tmac { <arp_flag_tmac> | any }] [arp-len { <arp_flag_len> | any }] [arp-ip { <arp_flag_ip> | any }] [arp-ether { <arp_flag_ether> | any }]] [action { permit | deny | filter { switchport <filter_switch_port_list> | interface (<port_type> [<fliter_port_list>]) } }] [rate-limiter { <rate_limiter_id> | disable }] [mirror [disable]] [logging [disable]] [shutdown [disable]] [lookup-second [disable]]

4. Frame Type: IPv4/ipv4-icmp/ipv4-udp/ipv4-tcp

(config)# access-list { ace | pre-ace | bypass-ace } [update] <ace_id> [next { <ace_id_next> | last }] [ingress { switch <ingress_switch_id> | switchport { <ingress_switch_port_id> | <ingress_switch_port_list> } | interface { <port_type> <ingress_port_id> | (<port_type> [<ingress_port_list>]) } | any }] [policy <policy> [policy-bitmask <policy_bitmask>]] [tag { tagged | untagged | any }] [vid { <vid> | any }] [tag-priority { <tag_priority> | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7 | any }] [frame-type { **ipv4** [sip { <sipv4> | any }] [dip { <dipv4> | any }] [ip-protocol { <ipv4_protocol> | any }] [ip-flag [ip-ttl { <ip_flag_ttl> | any }] [ip-options { <ip_flag_options> | any }] [ip-fragment { <ip_flag_fragment> | any }]]] | **ipv4-icmp** [sip { <sipv4_icmp> | any }] [dip { <dipv4_icmp> | any }] [icmp-type { <icmpv4_type> | any }] [icmp-code { <icmpv4_code> | any }] [ip-flag [ip-ttl { <ip_flag_icmp_ttl> | any }] [ip-options { <ip_flag_icmp_options> | any }] [ip-fragment { <ip_flag_icmp_fragment> | any }]]] | **ipv4-udp** [sip { <sipv4_udp> | any }] [dip { <dipv4_udp> | any }] [sport { <sportv4_udp_start> [to <sportv4_udp_end>] | any }] [dport { <dportv4_udp_start> [to <dportv4_udp_end>] | any }] [ip-flag [ip-ttl { <ip_flag_udp_ttl> | any }] [ip-options { <ip_flag_udp_options> | any }] [ip-fragment { <ip_flag_udp_fragment> | any }]]] | **ipv4-tcp** [sip { <sipv4_tcp> | any }] [dip { <dipv4_tcp> | any }] [sport { <sportv4_tcp_start> [to <sportv4_tcp_end>] | any }] [dport { <dportv4_tcp_start> [to <dportv4_tcp_end>] | any }] [ip-flag [ip-ttl { <ip_flag_tcp_ttl> | any }] [ip-options { <ip_flag_tcp_options> | any }] [ip-fragment { <ip_flag_tcp_fragment> | any }]] [tcp-flag [tcp-fin { <tcpv4_flag_fin> | any }] [tcp-syn { <tcpv4_flag_syn> | any }] [tcp-rst { <tcpv4_flag_rst> | any }] [tcp-psh { <tcpv4_flag_psh> | any }] [tcp-ack { <tcpv4_flag_ack> | any }] [tcp-urg { <tcpv4_flag_urg> | any }]]] [action { permit | deny | filter { switchport <filter_switch_port_list> | interface (<port_type> [<fliter_port_list>]) } }] [rate-limiter { <rate_limiter_id> | disable }] [mirror [disable]] [logging [disable]] [shutdown [disable]] [lookup-second [disable]]

5. Frame Type: IPv6/ipv6-icmp/ipv6-udp/ipv6-tcp

(config)# access-list { ace | pre-ace | bypass-ace } [update] <ace_id> [next { <ace_id_next> | last }] [ingress { switch <ingress_switch_id> | switchport { <ingress_switch_port_id> | <ingress_switch_port_list> } | interface { <port_type> <ingress_port_id> | (<port_type> [<ingress_port_list>]) } | any }] [policy <policy> [policy-bitmask <policy_bitmask>]] [tag { tagged | untagged | any }] [vid { <vid> | any }] [tag-priority { <tag_priority> | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7 | any }] [frame-type **ipv6** [next-header { <next_header> | any }] [sip { <sipv6> [sip-bitmask <sipv6_bitmask>] | any }] [hop-limit { <hop_limit> | any }] | **ipv6-icmp** [sip { <sipv6_icmp> [sip-bitmask <sipv6_bitmask_icmp>] | any }] [icmp-type { <icmpv6_type> | any }] [icmp-code { <icmpv6_code> | any }] [hop-limit { <hop_limit_icmp> | any }] | **ipv6-udp** [sip { <sipv6_udp> [sip-bitmask <sipv6_bitmask_udp>] | any }] [sport

{ <sportv6_udp_start> [to <sportv6_udp_end>] | any }] [dport { <dportv6_udp_start> [to <dportv6_udp_end>] | any }] [hop-limit { <hop_limit_udp> | any }] | **ipv6-tcp** [sip { <sipv6_tcp> [sip-bitmask <sipv6_bitmask_tcp>] | any }] [sport { <sportv6_tcp_start> [to <sportv6_tcp_end>] | any }] [dport { <dportv6_tcp_start> [to <dportv6_tcp_end>] | any }] [hop-limit { <hop_limit_tcp> | any }] [tcp-flag [tcp-fin { <tcpv6_flag_fin> | any }] [tcp-syn { <tcpv6_flag_syn> | any }] [tcp-rst { <tcpv6_flag_rst> | any }] [tcp-psh { <tcpv6_flag_psh> | any }] [tcp-ack { <tcpv6_flag_ack> | any }] [tcp-urg { <tcpv6_flag_urg> | any }]] }] [action { permit | deny | filter { switchport <filter_switch_port_list> | interface (<port_type> [<fliter_port_list>]) } }] [rate-limiter { <rate_limiter_id> | disable }] [mirror [disable]] [logging [disable]] [shutdown [disable]] [lookup-second [disable]]

Explanation: Configure an access control list.

Parameters:

{ace | pre-ace | bypass-ace}: Specify which access list you want to create. Bypass-ace has the highest priority in the list (which means bypass-ace rules will be checked first) and followed by Pre-ace and ace.

<AceId : 1-1024>: Specify access control list ID that applies to this rule.

[action {deny | filter | permit}]: Specify the action that applies to this rule.

[dmac-type {any| broadcast | multicast | unicast }]: Specify destination MAC type that applies to this rule.

[frame-type {any| arp|etype|ipv4|ipv4-icmp|ipv4-tcp|ipv4-udp|ipv6|ipv6-icmp|ipv6-tcp|ipv6-udp}]: Specify the frame type that applies to this rule.

[ingress {any | interface <PORT_TYPE> }]: Specify the ingress port.

[logging]: Enable logging function.

[mirror]: Enable the function of mirroring frames to destination mirror port.

[next { <AceId : 1-1024>|last}]: Insert the current ACE ID before the next ACE ID or put the ACE ID to the last one.

[policy <PolicyId : 0-255>]: Specify the policy ID.

[rate-limiter {<RateLimiterId : 1-16>|disable}]: Specify the rate limit ID or disable this function.

[shutdown]: Enable shutdown function.

[tag {any|tagged|untagged}]: Specify whether frames should be tagged or untagged.

[tag-priority {0-1| 0-3| 2-3| 4-5| 4-7| 6-7| <TagPriority : 0-7>|any}]: Specify the priority value.

[vid { <Vid : 1-4095>|any}]: Specify the VLAN ID.

Show: # show access-list [interface [(<port_type> [<v_port_type_list>])]] [rate-limiter [<rate_limiter_list>]] [ace statistics [<ace_list>]] [pre-ace statistics [<special_ace_list>]] [bypass-ace statistics [<bypass_ace_list>]]

Negation: (config)# no access-list {ace | pre-ace} <ace_list>

(config)# no access-list bypass-ace <ace_list>

Clear: # clear access-list ace statistics

3.10.3.2. (config)# access-list rate-limiter

Syntax: access-list rate-limiter [<rate_limiter_list>] { pps <pps_rate> | 10pps <pps10_rate> | 100pps <pps100_rate> | 25kbps <kpbs25_rate> | 100kbps <kpbs100_rate> }

Explanation: Configure rate limiter that applies to each rate limit ID.

Parameters:

[<rate_limiter_list>]: Specify the "rate limit ID". The allowed rate limit ID range is from1~16.

pps <pps_rate> | 10pps <pps10_rate> | 100pps <pps100_rate> | 25kbps <kpbs25_rate> | 100kbps <kpbs100_rate> }: Specify the limit rate.

Show: # show access-list rate-limiter [<RateLimiterList : 1~16>]

3.10.4. (config)# aggregation mode

Syntax: (config)# aggregation mode { [smac] [dmac] [ip] [port] }

Explanation: Configure aggregation mode.

Parameters:

[smac]: All traffic from the same Source MAC address is output on the same link in a trunk.

[dmac]: All traffic with the same Destination MAC address is output on the same link in a trunk.

[ip]: All traffic with the same source and destination IP address is output on the same link in a trunk.

[port]: All traffic with the same source and destination TCP/UDP port number is output on the same link in a trunk.

Negation: (config)# no aggregation mode

Show: # show aggregation [mode]

3.10.5. (config)# banner

3.10.5.1. (config)# banner [motd] <banner>

Syntax: (config)# banner [motd | login |exec] <banner>

Parameters:

[motd | login |exec]: Specify the purpose of this banner.

<banner>: Type in banner message.

Explanation: Configure the banner message of the day, login message or exec message.

Negation: (config)# no banner [motd | login |exec]

3.10.5.2. (config)# banner exec <banner>

Syntax: (config)# banner exec <banner>

Explanation: Display the configured message when successfully entering Exec mode.

Negation: (config)# no banner exec

3.10.5.3. (config)# banner login <banner>

Syntax: (config)# banner login <banner>

Explanation: Display the configured message when prompted for login ID and password.

Negation: (config)# no banner login

3.10.6. (config)# clock

3.10.6.1. (config)# clock summer-time <word16> date

Syntax: clock summer-time <word16> date [<start_month_var> <start_date_var> <start_year_var> <start_hour_var> <end_month_var> <end_date_var> <end_year_var> <end_hour_var> [<offset_var>]]

Explanation: Configure daylight saving time. This is used to set the clock forward or backward according to the configurations set for a defined Daylight Saving Time duration. “Recurring” command is used to repeat the configuration every year.

Parameters:

summer-time <word16>: Specify a description for this day-light setting.

date [<start_month_var> <start_date_var> <start_year_var> <start_hour_var> <end_month_var> <end_date_var> <end_year_var> <end_hour_var> [<offset_var>]]

<start_month_var:1-12>: Specify the starting month.

<start_date_var: 1-31>: Specify the starting day.

<start_year_var:2000-2097>: Specify the starting year.

<start_hour_var: hh:mm>: Specify the time to start.

<end_month_var:1-12>: Specify the ending month.

<end_date_var: 1-31>: Specify the ending day.

<end_year_var:2000-2097>: Specify the ending year.

<end_hour_var: hh:mm>: Specify the time to start.

[<offset_var: 1-1440>]: Specify the number of minutes to add during Daylight Saving Time. The allowed range is 1 to 1440.

Negation: (config)# no clock summer-time

Show: > show clock
> show clock detail
# show clock
# show clock detail

3.10.6.2. (config)# clock summer-time <word16> recurring

Syntax: (config)# clock summer-time <word16> recurring [<start_week_var> <start_day_var> <start_month_var> <start_hour_var> <end_week_var> <end_day_var> <end_month_var> <end_hour_var> [<offset_var>]]

Explanation: Configure daylight saving time. This is used to set the clock forward or backward according to the configurations set for a defined Daylight Saving Time duration. “Recurring” command is used to repeat the configuration every year.

Parameters:

summer-time <word16>: Specify a description for this day-light setting.

recurring [<start_week_var> <start_day_var> <start_month_var> <start_hour_var> <end_week_var> <end_day_var> <end_month_var> <end_hour_var> [<offset_var>]]

<start_week_var:1-5>: Specify the starting week.

<start_day_var: 1-31>: Specify the starting day.

<start_month_var:1-12>: Specify the starting month.

<start_hour_var: hh:mm>: Specify the time to start.

<end_week_var:1-5>: Specify the ending week.

<end_day_var: 1-31>: Specify the ending day.

<end_month_var: 1-12>: Specify the ending month.

<end_hour_var: hh:mm>: Specify the time to end.

[<offset_var: 1-1440>]: Specify the number of minutes to add during Daylight Saving Time. The allowed range is 1 to 1440.

Negation: (config)# no clock summer-time

Show: # show clock
# show clock detail

3.10.6.3. (config)# clock timezone

Syntax: (config)# clock timezone <word> <-23-23> [<0-59>]

Explanation: Configure a timezone used in the switch.

Parameters:

<word16>: Specify the name of the timezone.

<-23-23>: Hours offset from UTC.

[<0-59>]: Minutes offset from UTC.

Negation: (config)# no clock timezone

Show: # show clock
# show clock detail

3.10.7. (config)# ddmi

Syntax: (config)# ddmi

Explanation: To enable DDMI function. When enabled, users can view DDMI information of the inserted transceivers.

Negation: (config)# no ddmi

Show: # show ddmi

3.10.8. (config)# default access-list rate-limiter

Syntax: (config)# default access-list rate-limiter [<rate_limiter_list>]

Explanation: To default the specified rate-limiter ID.

Parameters:

[<rate_limiter_list: 1-16>]: Specify a rate limiter ID.

Example: To default rate-limiter 1.

```
# config t
(config)# default access-list rate-limiter 1
```

3.10.9. (config)# dot1x

3.10.9.1. (config)# dot1x system-auth-control

Syntax: (config)# dot1x system-auth-control

Explanation: To enable 802.1x service.

Example: Enable 802.1x service.

```
# config t
(config)# dot1x system-auth-control
```

Negation: (config)# no dot1x system-auth-control

Show: > show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]
# show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]

3.10.9.2. (config)# dot1x re-authentication

Syntax: (config)# dot1x re-authentication

Explanation: Set clients to be re-authenticated after an interval set in "Re-authenticate" field. Re-authentication can be used to detect if a new device is attached to a switch port.

Example: Enable re-authentication function.

```
# config t
(config)# dot1x re-authentication
```

Negation: (config)# no dot1x re-authentication

Show: > show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]
# show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]

3.10.9.3. (config)# dot1x authentication timer re-authenticate

Syntax: (config)# dot1x authentication timer re-authenticate <1-3600>

Explanation: Specify the time interval for a connected device to be re-authenticated. By default, the re-authenticated period is set to 3600 seconds. The allowed range is 1 - 3600 seconds.

Parameters:

<1-3600>: Specify a re-authentication value between 1 and 3600.

Example: Set re-authentication timer to 100.

```
# config t
(config)# dot1x authentication timer re-authenticate 100
```

Negation: (config)# no dot1x authentication timer re-authenticate

3.10.9.4. (config)# dot1x timeout tx-period

Syntax: (config)# dot1x timeout tx-period <v_1_to_65535>

Explanation: Specify the time that the switch waits for a supplicant response during an authentication session before transmitting a Request Identify EAPOL packet. By default, it is set to 30 seconds.

Parameters:

<v_1_to_65535>: Specify a timeout value between 1 and 65535 (seconds).

Example: Set EAPOL timeout to 30 seconds.

```
# config t
(config)# dot1x timeout tx-period 30
```

Negation: (config)# no dot1x timeout tx-period

3.10.9.5. (config)# dot1x authentication timer inactivity

Syntax: (config)# dot1x authentication timer inactivity <10-1000000>

Explanation: Specify the period that is used to age out a client’s allowed access to the switch via 802.1X and MAC-based authentication. The default period is 300 seconds. The allowed range is 10 - 1000000 seconds.

Parameters:

<10-1000000>: Specify a value between 10 and 1000000 (seconds).

Example: Set the aging time to 300 seconds.

```
# config t
(config)# dot1x authentication timer inactivity 300
```

Negation: (config)# no dot1x authentication timer inactivity

3.10.9.6. (config)# dot1x timeout quiet-period

Syntax: (config)# dot1x timeout quiet-period <v_10_to_1000000>

Explanation: The time after an EAP Failure indication or RADIUS timeout that a client is not allowed access. This setting applies to ports running Single 802.1X, Multi 802.1X, or MAC-based authentication. By default, hold time is set to 10 seconds. The allowed range is 10 - 1000000 seconds.

Parameters:

<10-1000000>: Specify a value between 10 and 1000000 (seconds).

Example: Set hold time to 30 seconds.

```
# config t
(config)# dot1x timeout quiet-period 30
```

Negation: (config)# no dot1x timeout quiet-period

3.10.9.7. (config)# dot1x feature

Syntax: (config)# dot1x feature { [guest-vlan] [radius-qos] [radius-vlan] }

Explanation: Enable the specified feature.

Parameters:

{ [guest-vlan] [radius-qos] [radius-vlan] }:

[guest-vlan]: Enable guest VLAN. A Guest VLAN is a special VLAN typically with limited network access. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

[radius-qos]: Enable RADIUS assigned QoS.

[radius-vlan]: Enable RADIUS VLAN. RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature.

Example: Enable guest VLAN service.

```
# config t
(config)# dot1x feature guest-vlan
```

Negation: (config)# no dot1x feature { [guest-vlan] [radius-qos] [radius-vlan] }

3.10.9.8. (config)# dot1x guest-vlan

Syntax: (config)# dot1x guest-vlan <value>

Explanation: Configure a guest VLAN ID.

Parameters:

<value:1-4095>: Specify the guest VLAN ID. The allowed VLAN ID range is from 1 to 4095.

Negation: (config)# no dot1x guest-vlan

3.10.9.9. (config)# dot1x guest-vlan supplicant

Syntax: (config)# dot1x guest-vlan supplicant

Explanation: Enable Guest VLAN supplicant function. The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. When enabled, the switch does not maintain the EAPOL packet history and allows clients that fail authentication to access the guest VLAN, regardless of whether EAPOL packets had been detected on the interface. Clients that fail authentication can access the guest VLAN.

Negation: (config)# no dot1x guest-vlan supplicant

3.10.9.10. (config)# dot1x max-requth-req

Syntax: (config)# dot1x max-reauth-req <value>

Explanation: The maximum number of times the switch transmits an EAPOL Request Identity frame without receiving a response before adding a port to the Guest VLAN. The value can only be changed when the Guest VLAN option is globally enabled. The range is 1 – 255.

Parameters:

<value:1-255>: Specify a value between 1 and 255.

Negation: (config)# no dot1x max-reauth-req

3.10.10. (config)# enable

3.10.10.1. (config)# enable password

Syntax: (config)# enable password <password>

Explanation: Configure enable password.

Parameters:

password <password>: Specify the enable mode password.

3.10.10.2. (config)# enable password level

Syntax: (config)# enable password [level <priv: 1-15>] <password>

Explanation: Configure enable password and privilege level.

Parameters:

[level <priv: 1-15>]: Specify the privilege level for this password.

<password>: Specify the enable mode password.

Negation: (config)# no enable password [level <priv>]

3.10.10.3. (config)# enable secret

Syntax: (config)# enable secret { 0 | 5 } [level <priv: 1-15>] <password>

Parameters:

{ 0 | 5 }: Specify “0” to denote unencrypted secret (cleartext). Specify “5” to denote encrypted secret (MD5).

[level <priv: 1-15>]: Specify the privilege level for this password.

<password>: Specify the enable mode password.

Explanation: Configure enable secret password and privilege level.

Negation: (config)# no enable secret { [0 | 5] } [level <priv>]

3.10.11. (config)# green-ethernet eee optimize-for-power

Syntax: (config)# green-ethernet eee optimize-for-power

Explanation: Enables the EEE function for this switch.

Example: Enable EEE function for optimized power.

```
# config t
(config)# green-ethernet eee optimize-for-power
```

Negation: (config)# no green-ethernet eee optimize-for-power

show: # show green-ethernet [interface (<port_type> [<port_list>])]
  # show green-ethernet eee [interface (<port_type> [<port_list>])]
  # show green-ethernet energy-detect [interface (<port_type> [<port_list>])]
  # show green-ethernet short-reach [interface (<port_type> [<port_list>])]

3.10.12. config)# gvrp

3.10.12.1. (config)# gvrp

Syntax: (config)# gvrp

Explanation: Globally enable GVRP function.

Parameters: None.

Example: Globally enable GVRP function.

```
# config t
(config)# gvrp
(config)#
```

Negation: (config)# no gvrp

3.10.12.2. (config)# gvrp max-vlans

Syntax: (config)# gvrp max-vlans <maxvlans>

Explanation: Set up the maximum number of VLANs can be learned via GVRP.

Parameters:

<maxvlans>: Specify the number of VLANs learned via GVRP.

Example: Set the maximum number of VLANs can be learned via GVRP to 20.

```
# config t
(config)# gvrp
(config)# gvrp max-vlans 20
```

Negation: (config)# no gvrp max-vlans <maxvlans>

3.10.12.3. (config)# gvrp time

Syntax: (config)# gvrp time { [join-time <jointime>] [leave-time <leavetime>] [leave-all-time <leavealltime>] }

Explanation: Set up the maximum number of VLANs can be learned via GVRP.

Parameters:

[join-time <jointime>]: Specify the amount of time in units of centi-seconds that PDUs are transmitted. The default value is 20 centi-seconds. The valid value is 1~20.

[leave-time <leavetime>]: Specify the amount of time in units of centi-seconds that the device waits before deleting the associated etry. The leave time is activated by a “Leave All-time” message sent/received and cancelled by the Join message. The default value is 60 centi-seconds.

NOTE: *The “LeaveAll-time” parameter must be greater than the “Leave-time” parameter.*

[leave-all-time <leavealltime>]: Specify the amount of time that “LeaveAll” PDUs are created. A LeaveAll PDU indicates that all registrations are shortly de-registered. Participants will need to rejoin in order to maintain registration. The valid value is 1000 to 5000 centi-seconds. The factory default 1000 centi-seconds.

NOTE: *The “LeaveAll-time” parameter must be greater than the “Leave-time” parameter.*

Negation: (config)# no gvrp time { [join-time <jointime>] [leave-time <leavetime>] [leave-all-time <leavealltime>] }

3.10.13. (config)# hostname

Syntax: (config)# hostname <WORD>

Explanation: Specify a descriptive name for this switch.

Parameters:

<WORD32>: Specify a descriptive name for this device. Indicate the hostname for this device. Alphabets (A-Z; a-z), digits (0-9) and minus sign (-) can be used. However, space characters are not allowed. The first character must be an alphabet character. The first and last character must not be a minus sign. The allowed string length is 0 – 255.

Example: Set the hostname to AccessSW.

```
# config t
(config)# hostname AccessSW
```

Negation: (config)# no hostname

Show: > show version
# show version

3.10.14. (config)# interface

3.10.14.1. (config)# interface (<port_type> [<plist>])

Syntax: (config)# interface (<port_type> [<plist>])

Explanation: Enter Config Interface mode for this specific interface.

Parameters:

<port_type> [<plist>]: Specify the port type and port number.

Example: Enter Config Interface mode for Gigabit Ethernet port 1.

```
# config t
(config)#
(config)# interface GigabitEthernet 1/1
(config-if)#
```

Show: > show interface (<port_type> [<in_port_list>]) switchport [access | trunk | hybrid]
> show interface (<port_type> [<v_port_type_list>]) capabilities
> show interface (<port_type> [<v_port_type_list>]) statistics [{ packets | bytes | errors | discards | filtered | { priority [<priority_v_0_to_7>] } }] [{ up | down }]
> show interface (<port_type> [<v_port_type_list>]) status
> show interface (<port_type> [<v_port_type_list>]) veriphy
> show interface vlan [<vlist>]

# show interface (<port_type> [<in_port_list>]) switchport [access | trunk | hybrid]
# show interface (<port_type> [<v_port_type_list>]) capabilities

# show interface (<port_type> [<v_port_type_list>]) statistics [{ packets | bytes | errors | discards | filtered | { priority [<priority_v_0_to_7>] } }] [{ up | down }]
# show interface (<port_type> [<v_port_type_list>]) status
# show interface (<port_type> [<v_port_type_list>]) veriphy
# show interface vlan [<vlist>]

Clear: # clear statistics { [interface] (<port_type> [<v_port_type_list>]) }

3.10.14.2. (config)# interface llag

Syntax: (config)# interface llag <llag_id>

Explanation: Enter Config Interface LLAG (Local Link Aggregation Group)mode.

Parameters:

<llag_id>: Specify LLAG group ID number. The valid range is 1~3.

3.10.14.2.1. (config-llag)# lacp failover

Syntax: (config-llag)# lacp failover <revertive | non-revertive>

Explanation: This command only applies to LACP-enabled groups. It determines if the group can automatically perform link re-calculation when links with higher priority becomes available.

Parameters:

<revertive | non-revertive>: Configure the group to revertive or no-revertive.

Negation: (config-llag)# no lacp failover <revertive | non-revertive>

3.10.14.2.2. (config-llag)# lacp max-bundle

Syntax: (config-llag)# lacp max-bundle <v_unit>

Explanation: This command only applies to LACP-enabled groups. It determines the maximum number of active bundled LACP ports allowed in an aggregation group.

Parameters:

<v_unit >: Specify the maximum number of bundled LACP ports. The valid range is 1~7.

Negation: (config-llag)# no lacp max-bundle <v_unit>

3.10.14.3. (config)# interface vlan

Syntax: (config)# interface vlan <vlist>

Explanation: Enter Config Interface VLAN mode for this specific interface.

Example: Enter Config Interface VLAN 1 for port 1.

```
# config t
(config)#
(config)# interface vlan 1
(config-if-vlan)#
```

3.10.15. (config)# ip

3.10.15.1. (config)# ip arp inspection

Syntax: (config)# ip arp inspection

Explanation: Enable ARP inspection function.

Negation: (config)# no ip arp inspection

Show: > show ip arp inspection [interface (<port_type> [<in_port_type_list>]) | vlan <in_vlan_list>]
# show ip arp inspection [interface (<port_type> [<in_port_type_list>]) | vlan <in_vlan_list>]

Clear: # clear ip arp

3.10.15.2. (config)# ip arp inspection entry interface

Syntax: (config)# ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>

Explanation: Create ARP static entry.

Parameters:

<port_type> <in_port_type_id>: Specify the port type and port number.

<vlan_var>: Specify a configured VLAN ID.

<mac_var>: Specify an allowed source MAC address in ARP request packets.

<ipv4_var>: Specify an allowed source IP address in ARP request packets.

Negation: (config)# no ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>

Show: # show ip arp inspection entry [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])]

Clear: # clear ip arp

3.10.15.3. (config)# ip arp inspection translate

Syntax: (config)# ip arp inspection translate [interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>]

Explanation: Translate the dynamic entry to static one.

Parameters:

<port_type> <in_port_type_id>: Specify the port type and port number.

<vlan_var>: Specify a configured VLAN ID.

<mac_var>: Specify an allowed source MAC address in ARP request packets.

<ipv4_var>: Specify an allowed source IP address in ARP request packets.

Show: # show ip arp inspection entry [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])]

3.10.15.4. (config)# ip arp inspection vlan

Syntax: (config)# ip arp inspection vlan <in_vlan_list>

Explanation: Specify ARP inspection is enabled on which VLAN.

Parameters:

<in_vlan_list>: Specify a list of VLAN ID to be used for ARP inspection.

Negation: (config)# no ip arp inspection vlan <in_vlan_list>

Show: < show ip arp
# show ip arp

Clear: # clear ip arp

3.10.15.5. (config)# ip arp inspection vlan <in_vlan_list> logging

Syntax: (config)# ip arp inspection vlan <in_vlan_list> logging { deny | permit | all }

Explanation: Enable log function.

Parameters:

{ deny | permit | all }: Specify one of the log types.

Deny: Log denied entries.

Permit: Log permitted entries.

All: Log all entries.

Negation: (config)# no ip arp inspection vlan <in_vlan_list> logging

Show: < show ip arp
# show ip arp

Clear: # clear ip arp

3.10.15.6. (config)# ip dhcp excluded-address

Syntax: (config)# ip dhcp excluded-address <low_ip> [<high_ip>]

Parameters:

<low_ip> [<high_ip>]: Specify the IP address range that will not be used for DHCP IP assignment.

Explanation: Configure IP addresses that are not used for DHCP IP allocation.

Example: Exclude IP address 1.2.3.4 to 1.2.3.10 from DHCP IP allocation pool..

```
# config t
(config)# ip dhcp excluded-address 1.2.3.4 1.2.3.10
(config)# exit
# show ip dhcp excluded-address
    Low Address     High Address
    --------------- ---------------
01   1.2.3.4         1.2.3.10

#
```

Negation: (config)# no ip dhcp excluded-address <low_ip> [<high_ip>]

Show: # show ip dhcp excluded-address

3.10.15.7. (config)# ip dhcp pool

Syntax: (config)# ip dhcp pool <pool_name>

Parameters:

<pool_name>: Specify the DHCP pool name in 32 characters.

Explanation: Configure the pool name for DHCP IP addresses.

Negation: (config)# no ip dhcp pool <pool_name>

Show: # show ip dhcp pool

3.10.15.7.1. (config-dhcp-pool)# broadcast

Syntax: (config-dhcp-pool)# broadcast <ip>

Explanation: Specify the broadcast address in use on the client’s subnet for the specified IP dhcp pool.

Parameters:

<ip>: Specify the broadcast address in use on the client’s subnet

Negation: (config-dhcp-pool)# no broadcast

Show: < show ip dhcp pool [<pool_name>]
# show ip dhcp pool [<pool_name>]

3.10.15.7.2. (config-dhcp-pool)# client-identifier

Syntax: (config-dhcp-pool)# client-identifier { fqdn <identifier> | mac-address <mac> }

Explanation: Specify client's unique identifier to be used when the pool is the type of host.

Parameters:

{ fqdn <identifier> | mac-address <mac> }: Specify the client identifier either in FQDN (Fully Qualified Domain Name) or MAC address format.

Negation: (config-dhcp-pool)# no client-identifier

Show: < show ip dhcp pool [<pool_name>]
# show ip dhcp pool [<pool_name>]

3.10.15.7.3. (config-dhcp-pool)# client-name

Syntax: (config-dhcp-pool)# client-name <host_name>

Explanation: Specify the name of client to be used when the pool is the type of host.

Parameters:

<host_name>: Specify the name of client to be used when the pool is the type of host.

Negation: (config-dhcp-pool)# no client-name

Show: < show ip dhcp pool [<pool_name>]
# show ip dhcp pool [<pool_name>]

3.10.15.7.4. (config-dhcp-pool)# default-router

Syntax: (config-dhcp-pool)# default-router <ip> [<ip1> [<ip2> [<ip3>]]]

Explanation: Specify a list of IP addresses for routers on the clients' subnet.

Parameters:

<ip> [<ip1> [<ip2> [<ip3>]]]: Specify a list of IP addresses for routers on the clients' subnet.

Negation: (config-dhcp-pool)# no default-router

Show: < show ip dhcp pool [<pool_name>]
# show ip dhcp pool [<pool_name>]

3.10.15.7.5. (config-dhcp-pool)# dns-server

Syntax: (config-dhcp-pool)# dns-server <ip> [<ip1> [<ip2> [<ip3>]]]

Explanation: Specify a list of Domain Name System name servers available to the client.

Parameters:

<ip> [<ip1> [<ip2> [<ip3>]]]: Specify a list of Domain Name Servers available to the client.

Negation: (config-dhcp-pool)# no dns-server

Show: < show ip dhcp pool [<pool_name>]
# show ip dhcp pool [<pool_name>]

3.10.15.7.6. (config-dhcp-pool)# domain-name

Syntax: (config-dhcp-pool)# domain-name <domain_name>

Explanation: Specify a list of Domain Name System name servers available to the client.

Parameters:

<domain_name>: Specify the domain name that a client use when resolving hostname via DNS.

Negation: (config-dhcp-pool)# no domain-name

Show: < show ip dhcp pool [<pool_name>]
# show ip dhcp pool [<pool_name>]

3.10.15.7.7. (config-dhcp-pool)# hardware-address

Syntax: (config-dhcp-pool)# hardware-address <mac>

Explanation: Specify client's hardware (MAC) address to be used when the pool is the type of host.

Parameters:

<mac>: Specify client's hardware (MAC) address to be used when the pool is the type of host.

Negation: (config-dhcp-pool)# no hardware-address

Show: < show ip dhcp pool [<pool_name>]
# show ip dhcp pool [<pool_name>]

3.10.15.7.8. (config-dhcp-pool)# host

Syntax: (config-dhcp-pool)# host <ip> <subnet_mask>

Explanation: Specify the Network IP and subnet mask of the DHCP address pool.

Parameters:

<ip>: Specify the network IP of the DHCP address pool.

<subnet_mask>: Specify subnet mask of the DHCP address pool.

Negation: (config-dhcp-pool)# no host

Show: < show ip dhcp pool [<pool_name>]
# show ip dhcp pool [<pool_name>]

3.10.15.7.9. (config-dhcp-pool)# lease

Syntax: (config-dhcp-pool)# lease { <day> [<hour> [<min>]] | infinite }

Explanation: Specify lease time that a client needs to send requests to the DHCP server for renewed IP address.

Parameters:

{ <day> [<hour> [<min>]] | infinite }: Specify lease time that a client needs to send requests to the DHCP server for renewed IP address. Specify "infinite" to mean the lease time is infinite.

Negation: (config-dhcp-pool)# no lease

Show: < show ip dhcp pool [<pool_name>]
# show ip dhcp pool [<pool_name>]

3.10.15.7.10. (config-dhcp-pool)# netbios-name-server

Syntax: (config-dhcp-pool)# netbios-name-server <ip> [<ip1> [<ip2> [<ip3>]]]

Explanation: Specify a list of NBNS name servers.

Parameters:

[<ip1> [<ip2> [<ip3>]]]: Specify a list of NBNS name servers IP in order of preference.

Negation: (config-dhcp-pool)# no netbios-name-server

Show: < show ip dhcp pool [<pool_name>]
# show ip dhcp pool [<pool_name>]

3.10.15.7.11. (config-dhcp-pool)# netbios-node-type

Syntax: (config-dhcp-pool)# netbios-node-type { b-node | h-node | m-node | p-node }

Explanation: Specify NetBIOS node type option to allow Netbios over TCP/IP clients as described in RFC 1001/1002.

Parameters:

{ b-node | h-node | m-node | p-node }: Specify NetBIOS node type.

Negation: (config-dhcp-pool)# no netbios-node-type

Show: < show ip dhcp pool [<pool_name>]
# show ip dhcp pool [<pool_name>]

3.10.15.7.12. (config-dhcp-pool)# netbios-scope

Syntax: (config-dhcp-pool)# netbios-scope <netbios_scope>

Explanation: Specify the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002.

Parameters:

<netbios_scope>: Specify NetBIOS scope identifier.

Negation: (config-dhcp-pool)# no netbios-scope

Show: < show ip dhcp pool [<pool_name>]
# show ip dhcp pool [<pool_name>]

3.10.15.7.13. (config-dhcp-pool)# network

Syntax: (config-dhcp-pool)# network <ip> <subnet_mask>

Explanation: The pool defines a pool of IP addresses to service more than one DHCP client

Parameters:

<ip> <subnet_mask>: Specify IP address and subnet mask for this specific IP address.

Negation: (config-dhcp-pool)# no network

Show: < show ip dhcp pool [<pool_name>]
# show ip dhcp pool [<pool_name>]

3.10.15.7.14. (config-dhcp-pool)# nis-domain-name

Syntax: (config-dhcp-pool)# nis-domain-name <domain_name>

Explanation: Specify the name of the client's NIS domain.

Parameters:

<domain_name>: Specify NIS domain name.

Negation: (config-dhcp-pool)# no nis-domain-name

Show: < show ip dhcp pool [<pool_name>]
# show ip dhcp pool [<pool_name>]

3.10.15.7.15. (config-dhcp-pool)# nis-server

Syntax: (config-dhcp-pool)# nis-server <ip> [<ip1> [<ip2> [<ip3>]]]

Explanation: Specify a list of IP addresses indicating NIS servers available to the client.

Parameters:

[<ip1> [<ip2> [<ip3>]]]: Specify a list of IP addresses indicating NIS servers available to the client.

Negation: (config-dhcp-pool)# no nis-server

Show: < show ip dhcp pool [<pool_name>]

# show ip dhcp pool [<pool_name>]

3.10.15.7.16. (config-dhcp-pool)# ntp-server

Syntax: (config-dhcp-pool)# ntp-server <ip> [<ip1> [<ip2> [<ip3>]]]

Explanation: Specify a list of IP addresses indicating NTP servers available to the client.

Parameters:

[<ip1> [<ip2> [<ip3>]]]: Specify a list of IP addresses indicating NTP servers available to the client.

Negation: (config-dhcp-pool)# no ntp-server

Show: < show ip dhcp pool [<pool_name>]
# show ip dhcp pool [<pool_name>]

3.10.15.7.17. (config-dhcp-pool)# vendor class-identifier

Syntax: (config-dhcp-pool)# vendor class-identifier <class_id> specific-info <hexval>

Explanation: Identify the vendor type and vendor specific information. DHCP server will deliver the corresponding option 43 specific information to the client that sends option 60 vendor class identifier.

Parameters:

<class_id>: Specify the specifc vendor class identifier (option 60).

<hexval>: Specify specific information.

Negation: (config-dhcp-pool)# no vendor class-identifier <class_id>

Show: < show ip dhcp pool [<pool_name>]
# show ip dhcp pool [<pool_name>]

3.10.15.8. (config)# ip dhcp relay

Syntax: (config)# ip dhcp relay

Explanation: Enable DHCP relay function.

Example: Enable DHCP relay function.

```
# config t
(config)# ip dhcp relay
```

Negation: (config)#   no ip dhcp relay

Show: > show ip dhcp relay [statistics]
    # show ip dhcp relay [statistics]

Clear: # clear ip dhcp relay statistics

3.10.15.9. (config)# ip dhcp relay information option

Syntax: (config)# ip dhcp relay information option

Explanation: Enable DHCP Relay option 82 function.   Please note that "Relay Mode" must be enabled before this function is able to take effect.

Example: Enable DHCP Relay option 82 function

```
# config t
(config)# ip dhcp relay information option
```

Negation: (config)# no ip dhcp relay information option

3.10.15.10. (config)# ip dhcp relay information policy {drop | keep |replace}

Syntax: (config)# ip dhcp relay information policy { drop | keep | replace }

Explanation: Specify DHCP Relay information reforwarding policy action.

Parameters:

{ drop | keep | replace }: Specify one of the relay information policy options.

drop: Drop the packet when it receives a DHCP message that already contains relay information.

keep: Keep the client's DHCP information.

replace: Replace (rewrite) the DHCP client packet information with the switch's relay information. This is the default setting.

Example: Keep the client's DHCP information.

```
# config t
(config)# ip dhcp relay information policy keep
```

Negation: (config)# no ip dhcp relay information policy

3.10.15.11. (config)# ip dhcp server

Syntax: (config)# ip dhcp server

Explanation: Enable DHCP server function globally.

Example: Enable DHCP server function.

```
# config t
(config)# ip dhcp server
```

Negation: (config)# no ip dhcp server

Show: > show ip dhcp server
# show ip dhcp server

3.10.15.12. (config)# ip dhcp snooping

Syntax: (config)# ip dhcp snooping

Explanation: Enable DHCP snooping function globally. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

Example: Enable DHCP snooping function.

```
# config t
(config)# ip dhcp snooping
```

Negation: (config)# no ip dhcp snooping

Show: > show ip dhcp snooping [interface (<port_type> [<in_port_list>])]
# show ip dhcp snooping [interface (<port_type> [<in_port_list>])]
# show ip dhcp snooping table

Clear: # clear ip dhcp snooping statistics [interface (<port_type> [<in_port_list>])]

3.10.15.13. (config)# ip dns proxy

Syntax: (config)# ip dns proxy

Explanation: Enable DNS (Domain Name System) proxy function.

Example: Enable DNS (Domain Name System) proxy function.

```
# config t
(config)# ip dns proxy
```

Negation: (config)# no ip dns proxy

3.10.15.14. (config)# ip helper-address

Syntax: (config)# ip helper-address <v_ipv4_ucast>

Explanation: Configure DHCP Relay server IPv4 address.

Parameters:

<v_ipv4_ucast>: Specify DHCP Relay server IPv4 address that is used by the switch's DHCP relay agent

Negation: (config)# no ip helper-address

3.10.15.15. (config)# ip http secure-server

Syntax: (config)# ip http secure-server

Explanation: Enable the HTTPS operation mode. When the current connection is HTTPS and HTTPS mode operation is disabled, web browser will automatically redirect to an HTTP connection.

Example: Enable the HTTPS operation mode.

```
# config t
(config)# ip http secure-server
```

Negation: (config)# no ip http secure-server

Show: # show ip http server secure status

3.10.15.16. (config)# ip http secure-redirect

Syntax: (config)# ip http secure-redirect

Explanation: Enable the HTTPS redirect mode operation. It applies only if HTTPS mode is "Enabled". Automatically redirects HTTP of web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled.

Example: Enable HTTPs automatic redirect mode.

```
# config t
(config)# ip http secure-redirect
```

Negation: (config)# no ip http secure-redirect

Show: # show ip http server secure status

3.10.15.17. (config)# ip igmp host-proxy

Syntax: (config)# ip igmp host-proxy [leave-proxy]

Explanation: When enabled, the switch suppresses leave messages unless received from the last member port in the group. IGMP leave proxy suppresses all unnecessary IGMP leave messages so that a non-querier switch forwards an IGMP leave packet only when the last dynamic member port leaves a multicast group.

Parameters:

[leave-proxy]: The parameter is optional. Enable leave-proxy function.

Negation: (config)# no ip igmp host-proxy [leave-proxy]

Show: # show ip igmp snooping detail

3.10.15.18. (config)# ip igmp snooping

Syntax: (config)# ip igmp snooping

Explanation: Globally enable IGMP Snooping feature. When enabled, this device will monitor network traffic and determine which hosts will receive multicast traffic. The switch can passively monitor or snoop on IGMP Query and Report packets transferred between IP multicast routers and IP multicast service subscribers to identify the multicast group members. The switch simply monitors the IGMP packets passing through it, picks out the group registration information and configures the multicast filters accordingly.

Negation: (config)# no ip igmp snooping

Show: # show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]

Clear: # clear ip igmp snooping [vlan <v_vlan_list>] statistics

3.10.15.19. (config)# ip igmp snooping vlan

Syntax: (config)# ip igmp snooping vlan <v_vlan_list>

Explanation: Enable IGMP function for specific VLANs**.**

Parameters:

<v_vlan_list>: Specify valid IGMP VLANs.

Negation: (config)# no ip igmp snooping vlan [<v_vlan_list>]

Show: # show ip igmp snooping

Clear: # clear ip igmp snooping [vlan <v_vlan_list>] statistics

3.10.15.20. (config)# ip igmp ssm-range

Syntax: (config)# ip igmp ssm-range <v_ipv4_mcast> <ipv4_prefix_length>

Explanation: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Parameters:

<v_ipv4_mcast>: Specify valid IPv4 multicast address.

<ipv4_prefix_length>: Specify the prefix length ranging from 4 to 32.

Negation: (config)# no ip igmp ssm-range

3.10.15.21. (config)# ip igmp unknown-flooding

Syntax: (config)# ip igmp unknown-flooding

Explanation: Set forwarding mode for unregistered (not-joined) IP multicast traffic. Select the checkbox to flood traffic.

Negation: (config)# no ip igmp unknown-flooding

3.10.15.22. (config)# ip name-server

Syntax: (config)# ip name-server { <v_ipv4_ucast> | dhcp [interface vlan <v_vlan_id>] }

Explanation: Set up DNS IP address manually or obtain DNS IP address via specific VLAN DHCP server.

Parameters:

<v_ipv4_ucast>: Manually specify unicast IPv4 name server address.

dhcp [interface vlan <v_vlan_id>]: Configure DNS IP address via specific VLAN DHCP server.

Negation: (config)# no ip name-server

Show: > show ip name-server
# show ip name-server

3.10.15.23. (config)# ip route

Syntax: (config)# ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>

Explanation: Configure a static IP route.

Parameters:

<v_ipv4_addr>: Specify IPv4 address. The IP route is the destination IP network or host address of this route. Valid format is dotted decimal notation.

<v_ipv4_netmask>: The route mask is a destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Only a default route will have a mask length of 0 (as it will match anything).

<v_ipv4_gw>: This is the IP address of the gateway. Valid format is dotted decimal notation. Gateway and Network must be of the same type.

Example: Add a new ip route with the following settings.

```
# config t
(config)# ip route 192.168.1.240 255.255.255.0 192.168.1.254
```

Negation: (config)# no ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>

Show: > show ip route
# show ip route

3.10.15.24. (config)# ip routing

Syntax: (config)# ip routing

Explanation: Enable IPv4 and IPv6 routing.

Example: Enable IPv4 and IPv6 routing.

```
# config t
(config)# ip routing
```

Negation: (config)# no ip routing

Show: > show ip route

> show ipv6 route [interface vlan <vlan_list>]

# show ip route

# show ipv6 route [interface vlan<vlan_list>]

```
# show ip route
127.0.0.1/32 via 127.0.0.1 <UP HOST>
224.0.0.0/4 via 127.0.0.1 <UP>
# show ipv6 route interface vlan 1
::1/128 via ::1 <UP HOST>
```

3.10.15.25. (config)# ip source binding interface

Syntax: (config)# ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mask_var>

Explanation: Create a static entry.

Parameters:

<port_type> <in_port_type_id>: Specify a port type and port number to which a static entry is bound.

<vlan_var>: Specify VLAN ID that has been configured.

<ipv4_var>: Specify a valid IPv4 address.

<mask_var>: Specify the subnet mask for the entered IP address.

Negation: (config)# no ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mask_var>

Show: # show ip source binding [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])]

3.10.15.26. (config)# ip ssh

Syntax: (config)# ip ssh

Explanation: Enable SSH mode.

Example: Enable SSH mode.

```
# config t
(config)# ip ssh
```

Negation: (config)# no ip ssh

Show: # show ip ssh

NOTE: *SSH is preferred to Telnet, unless the management network is trusted. Telnet passes authentication credentials in plain text, making those credentials susceptible to packet capture and analysis. SSH provides a secure authentication method. The SSH in this device uses version 2 of SSH protocol.*

3.10.15.27. (config)# ip verify source

Syntax: (config)# ip verify source

Explanation: Enable IP source guard function.

Negation: (config)# no ip verify source

Show: > show ip verify source [interface (<port_type> [<in_port_type_list>])]
# show ip verify source [interface (<port_type> [<in_port_type_list>])]

3.10.15.28. (config)# ip verify source translate

Syntax: (config)# ip verify source translate

Explanation: Translate Dynamic entries to Static ones.

3.10.16. (config)# ipmc

3.10.16.1. (config)# ipmc profile

Syntax: (config)# ipmc profile

Explanation: Enable IPMC (IP multicast) profile globally.

Negation: (config)# no ipmc profile

Show: # show ipmc profile

3.10.16.2. (config)# ipmc profile <profile_name>

Syntax: (config)# ipmc profile <profile_name>

Parameters:

<profile_name: word16>: Specify the desired profile name in 16 characters. When entered is pressed, the command will change to (config-ipmc-profile)#.

Explanation: Set up an IPMC profile.

Example: Create an IPMC profile named “goldpass”.

```
# config t
(config)# ipmc profile goldpass
(config-ipmc-profile)#
```

Negation: (config)# no ipmc profile <profile_name>

Show: # show ipmc profile [<profile_name>] [detail]

3.10.16.2.1. (config-ipmc-profile)# default range

Syntax: (config-ipmc-profile)# default range <entry_name>

Parameters:

<entry_name: word16>: Specify an entry name in 16 characters for this IPMC profile.

Explanation: To set default IPMC Profile Rule for a specific IPMC Profile.

Example: To default IPMC Profile Rule (Entry 1) for specific IPMC Profile.

```
# config t
(config)# ipmc profile goldpass
(config-ipmc-profile)# default range 1
```

Negation: (config-ipmc-profile)# no range <entry_name>

Show: # show ipmc profile
#show ipmc profile [<profile_name>] [detail]

3.10.16.2.2. (config-ipmc-profile)# description

Syntax: (config-ipmc-profile)# description <profile_desc>

Parameters:

<profile_desc: line 64>: Additional description for the designated profile in 64 characters.

Explanation: Specify descriptive information for the designated profile.

Example: Provide descriptive information for IPMC profile goldpass.

```
# config t
(config)# ipmc profile goldpass
(config-ipmc-profile)# description 1stclasscustomer
```

Negation: (config-ipmc-profile)# no description

Show: # show ipmc profile
#show ipmc profile [<profile_name>] [detail]

3.10.16.2.3. (config-ipmc-profile)# range

Syntax: (config-ipmc-profile)# range <entry_name> { permit | deny } [log] [next <next_entry>]

Parameters:

<entry_name>: Specify an entry name.

{ permit | deny }: Specify the action taken upon receiving the Join/Report frame that has the group address matches the address range of the rule.

Permit: Group address matches the range specified in the rule will be learned.

Deny: Group address matches the range specified in the rule will be dropped.

[log]: Log when matching

[next <next_entry>]: Specify next entry used in profile

Explanation: To set action of an entry for a specific IPMC profile.

Negation: (config-ipmc-profile)# no range <entry_name>

Show: # show ipmc profile
#show ipmc profile [<profile_name>] [detail]

3.10.16.3. (config)# ipmc range

Syntax: (config)# ipmc range <entry_name> { <v_ipv4_mcast> [<v_ipv4_mcast_1>] | <v_ipv6_mcast> [<v_ipv6_mcast_1>] }

Explanation: Specify the multicast IP range. The available IP range is from 224.0.0.0~239.255.255.255.

Parameters:

<entry_name>: The name used in specifying the address range.

{ <v_ipv4_mcast> [<v_ipv4_mcast_1>] | <v_ipv6_mcast> [<v_ipv6_mcast_1>] }: Specify the multicast IP range. The available IP range is from 224.0.0.0~239.255.255.255.

Negation: (config)# no no ipmc range <entry_name>

Show: # show ipmc profile [<profile_name>] [detail]

3.10.17. (config)# ipv6

3.10.17.1. (config)# ipv6 dhcp snooping

Syntax: (config)# ipv6 dhcp snooping

Explanation: Enable IPv6 DHCP Snooping mode. When DHCPv6 snooping mode operation is enabled, the DHCPv6 client request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

Negation: (config)# no ipv6 dhcp snooping

Show: > show ipv6 dhcp snooping
# show ipv6 dhcp snooping

3.10.17.2. (config)# ipv6 dhcp snooping uh-unknown

Syntax: (config)# ipv6 dhcp snooping nh-unknown {drop | allow}

Explanation: Specify how unknown IPv6 "next-header" values should be treated. The switch needs to parse all IPv6 packets to a DHCPv6 client to determine if it is in fact a DHCPv6 message. If an unknown IPv6 extension header is encountered the parsing cannot continue. See RFC 7610, section 5, item 3 for details.

Parameters:

{drop | allow}: Two options are available for this command:

Drop: Drop packets with unknown IPv6 extension headers. This is the most secure option but may result in traffic disruptions.

Allow: Allow packets with unknown IPv6 extension headers. This is a less secure option but prevents traffic disruptions.

Show: > show ipv6 dhcp snooping
# show ipv6 dhcp snooping

3.10.17.3. (config)# ipv6 mld host-proxy

Syntax: (config)# ipv6 mld host-proxy

Explanation: Enable IPv6 MLD proxy. When MLD proxy is enabled, the switch exchanges MLD messages with the router on its upstream interface, and performs the host portion of the MLD task on the upstream interface as follows:

- When queried, it sends multicast listener reports to the group.

- When a host joins a multicast group to which no other host belongs, it sends unsolicited multicast listener reports to that group.
- When the last host in a particular multicast group leaves, it sends an unsolicited multicast listener done report to the all-routers address (FF02::2) for MLDv1.

Example: Enable IPv6 MLD Proxy.

```
# config t
(config)# ipv6 mld host-proxy
(config)#
```

Negation: (config)# no ipv6 mld host-proxy

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.10.17.4. (config)# ipv6 mld host-proxy leave-proxy

Syntax: (config)# ipv6 mld host-proxy leave-proxy

Explanation: Enable IPv6 MLD leave proxy. To prevent multicast router from becoming overloaded with leave messages, MLD snooping suppresses leave messages unless received from the last member port in the group. When the switch acts as the querier, the leave proxy feature will not function.

Example: Enable IPv6 MLD leave proxy.

```
# config t
(config)# ipv6 mld host-proxy leave-proxy
(config)#
```

Negation: (config)# no ipv6 mld host-proxy leave-proxy

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.10.17.5. (config)# ipv6 mld snooping

Syntax: (config)# ipv6 mld snooping

Explanation: Enable MLD Snooping feature globally. When enabled, this device will monitor network traffic and determine which hosts would like to receive multicast traffic. The switch can passively monitor or snoop on MLD Listener Query and Report packets transferred between IP multicast routers and IP multicast service subscribers to identify the multicast group members. The switch simply monitors the IGMP packets passing through it, picks out the group registration information and configures the multicast filters accordingly.

Example: Enable IPv6 MLD snooping.

```
# config t
(config)# ipv6 mld snooping
(config)#
```

Negation: (config)# no ipv6 mld snooping

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.10.17.6. (config)# ipv6 mld snooping vlan

Syntax: (config)# ipv6 mld snooping vlan <v_vlan_list>

Parameters:

<v_vlan_list>: Specify VLAN ID for MLD.

Negation: (config)# no ipv6 mld snooping vlan [<v_vlan_list>]

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
> show ipv6 mld snooping mrouter [detail]
# show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show ipv6 mld snooping mrouter [detail]

Clear: # clear ipv6 mld snooping [vlan <v_vlan_list>] statistics

3.10.17.7. (config)# ipv6 mld ssm-range

Syntax: (config)# ipv6 mld ssm-range <v_ipv6_mcast> <ipv6_prefix_length>

Parameters:

<v_ipv6_mcast>: Specify valid IPv6 multicast address.

<ipv6_prefix_length>: Specify prefix length range from 8 to 128.

Explanation: Specify SSM (Source-Specific Multicast) Range. This setting allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Example: Configure MLD SSM with the ff3e::7728/128 settings.

```
# config t
(config)# ipv6 mld ssm-range ff3e::7728 128
```

Negation: (config)# no ipv6 mld ssm-range

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.10.17.8. (config)# ipv6 mld unknown-flooding

Syntax: (config)# ipv6 mld unknown-flooding

Explanation: Enable forwarding mode for unregistered (not-joined) IP multicast traffic.

Example: To flood unregistered IPv6 multicast traffic

```
# config t
(config)# ipv6 mld unknown-flooding
```

Negation: (config)# no ipv6 mld unknown-flooding

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
> show ipv6 mld snooping mrouter [detail]
# show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show ipv6 mld snooping mrouter [detail]

3.10.17.9. (config)# ipv6 route

Syntax: (configure)# ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }

Parameters:

<v_ipv6_subnet>: Specify IPv6 route address.

{ <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }: Specify one of the options. This could be either IPv6 next hop unicast address or an interface.

Explanation: Configure a static IPv6 route.

Negation: (config)# no ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }

Show: # show ipv6 route [interface vlan <v_vlan_list>]

3.10.17.10. (config)# ipv6 source binding interface

Syntax: (configure)# ipv6 source binding interface <port_type> <port_type_id> [vlan <vlan_id>] <ipv6_ucast> <mac_ucast>

Explanation: Create a static IPv6 entry.

Parameters:

<port_type> <in_port_type_id>: Specify a port type and port number to which a static entry is bound.

<vlan_var>: Specify VLAN ID that has been configured.

<ipv6_ucast>: Specify a valid IPv6 address.

<mac_ucast>: Specify the MAC address for this entry.

Negation: (config)# no ipv6 source binding interface <port_type> <port_type_id> [vlan <vlan_id>] <ipv6_ucast> <mac_ucast>

Show: # show ipv6 source binding [dhcpv6-snooping | static] [interface (<port_type> [<port_list>])]

3.10.17.11. (config)# ipv6 verify source

Syntax: (config)# ipv6 verify source

Explanation: Enable IPv6 Source Guard.

Negation: (config)# no ip verify source

Show: > show ipv6 verify source [interface (<port_type> [<port_list>])]
# show ipv6 verify source [interface (<port_type> [<port_list>])]

3.10.17.12. (config)# ipv6 verify source translate

Syntax: (config)# ipv6 verify source translate

Explanation: Translate dynamic IPv6 entries to static ones.

3.10.18. (config)# lacp system-priority

Syntax: (configure)# lacp system-priority <v_1_to_65535>

Parameters:

<v_1_to_65535>: The priority of the port. The allowed value range is from 1 to 65535.

Explanation: Configure system priority for LACP function. The lower number means greater priority. This priority value controls which ports will be active and which ones will be in a backup role.

Example: Set LACP system priority value to 100.

```
# config t
(config)# lacp system-priority 100
```

Negation: (config)# no lacp system-priority <v_1_to_65535>

Show: # show lacp { internal | statistics | system-id | neighbour }

3.10.19. (config)# line

Syntax: (configure)# line { <0~16> | console 0 | vty <0~15> }

Explanation: Enter the specific line. When Enter is pressed, the command line changes to "(config-line)#".

Parameters:

{ <0~16> | console 0 | vty <0~15> }: Specify one of the options.

<0~16> : List of line numbers.

console 0: Console line connection.

vty <0~15>: VTY lines are the Virtual Terminal lines of the device, used solely to control inbound Telnet connections. They are virtual, in the sense that they are a function of software - there is no hardware associated with them.

Example: Enter Console 0 mode.

```
# config t
(config)# line console 0
(config-line)#
```

Show: > show line [alive]
# show line [alive]

3.10.19.1. (config-line)# do

Syntax: (config-line)# do <command>

Explanation: To run EXEC. commands.

Parameters:

<command>: Enter the EXEC. command

Example: Show aaa settings.

```
# config t
(config)# line console 0
(config-line)# do show aaa
console : local
telnet  : local
ssh     : local
http    : local
(config-line)#
```

3.10.19.2. (config-line)# editing

Syntax: (config-line)# editing

Explanation: Enable command line editing.

Negation: (config-line)# no editing

Show: > show line [alive]
# show line [alive]

3.10.19.3. (config-line)# end

Syntax: (config-line)# end

Explanation: Return to EXEC. mode.

Example: Return to EXEC. mode.

```
# config t
(config)# line console 0
(config-line)# end
#
```

3.10.19.4. (config-line)# exec-banner

Syntax: (config-line)# exec-banner

Explanation: Enable the display of EXEC banner.

Example: Enable the display of EXEC banner.

```
# config t
(config)# line console 0
(config-line)# exec-banner
```

Negation: (config-line)# no exec-banner

Show: > show line [alive]
# show line [alive]

3.10.19.5. (config-line)# exec-timeout

Syntax: (config-line)# exec-timeout <min> [<sec>]

Parameters:

<min>: Specify timeout in minutes. The allowed range is 0 to 1440. Specify "0" to disable timeout function (CLI session will never timeout.)

[<sec>]: Specify timeout in seconds. The allowed range is 0 to 3600.

Negation: (config-line)# no exec-timeout

Show: > show line [alive]
# show line [alive]

3.10.19.6. (config-line)# exit

Syntax: (config-line)# exit

Explanation: Return to Config mode.

Example: Return to Config mode.

```
# config t
(config)# line console 0
(config-line)# exit
(config)#
```

3.10.19.7. (config-line)# help

Syntax: (config-line)# help

Explanation: Show the Help explanation.

Example: Show Help explanation.

```
# config t
(config)# line console 0
(config-line)# help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what Parameters match the input
   (e.g. 'show pr?'.)
```

3.10.19.8. (config-line)# history size

Syntax: (config-line)# history size <history_size>

Explanation: Control how many history commands are displayed.

Parameters:

<history_size>: The allowed range is 0 to 32. 0 means “disable”.

Example: Set history size to 10.

```
# config t
(config)# line console 0
(config-line)# history size 10
```

Negation: (config-line)# no history size

Show: > show line [alive]

# show line [alive]

3.10.19.9. (config-line)# length

Syntax: (config-line)# length <length>

Explanation: Configure the number of lines displayed on the screen.

Parameters:

<length>: Specify the number of lines displayed on the screen. The allowed range is 3 to 512. Specify “0” for no pausing.

Example: Display 20 lines on the screen.

```
# config t
(config)# line console 0
(config-line)# length 20
(config-line)#
```

Negation: (config-line)# no length

Show: > show line [alive]
# show line [alive]

3.10.19.10. (config-line)# location

Syntax: (config-line)# location <location>

Explanation: Configure the descriptive location of this device.

Parameters:

<location>: Location description for the terminal. The characters allowed are 32.

Example: Configure the location “cabinet5a”.

```
# config t
(config)# line console 0
(config-line)# location cabinet5a
(config-line)#
```

Negation: (config-line)# no location

Show: > show line [alive]
# show line [alive]

3.10.19.11. (config-line)# motd-banner

Syntax: (config-line)# motd-banner

Explanation: Enable the display of motd (message of the day) banner.

Example: Enable motd banner.

```
# config t
(config)# line console 0
(config-line)# motd-banner
(config-line)#
```

Negation: (config-line)# no motd-banner

Show: > show line [alive]
# show line [alive]

3.10.19.12. (config-line)# privilege level

Syntax: (config-line)# privilege level <privileged_level>

Explanation: Configure the privilege level for the terminal line.

Parameters:

<privileged_level>: Privilege level for the terminal line. The allowed range is 0 to 15.

Example: Change the privilege level to 5 for vty 1.

```
# config t
(config)# line vty 1
(config-line)# privilege level 5
(config-line)#
```

Negation: (config-line)# no privilege level

Show: > show line [alive]
# show line [alive]

3.10.19.13. (config-line)# width

Syntax: (config-line)# width <width>

Explanation: Configure the width of the terminal line.

Parameters:

<width>: Specify the width of the terminal line. The allowed range is 40 to 512. Specify “0” for unlimited width.

Example: Change of width of vty 1 to 60.

```
# config t
(config)# line vty 1
(config-line)# width 60
(config-line)#
```

Negation: (config-line)# no width

Show: > show line [alive]
# show line [alive]

3.10.20. (config)# lldp

3.10.20.1. (config)# lldp holdtime

Syntax: (config)# lldp holdtime <val>

Explanation: This setting defines how long LLDP frames are considered valid and is used to compute the TTL. The default is 4.

Parameters:

<val>: Specify the holdtime value. The allowed value is 2 to 10.

Example: Set the holdtime to 5.

```
# config t
(config)# lldp holdtime 5
```

Negation: (config)# no lldp holdtime

3.10.20.2. (config)# lldp reinit

Syntax: (config)# lldp reinit <val>

Explanation: Configure a delay between the shutdown frame and a new LLDP initialization.

Parameters:

<val>: Specify a value between 1 and 10 (seconds).

Example: Set the LLDP re-initiation value to 3.

```
# config t
(config)# lldp reinit 3
```

Negation: (config)# no lldp reinit

3.10.20.3. (config)# lldp timer

Syntax: (config)# lldp timer <val>

Explanation: Configure the interval between LLDP frames are sent to its neighbors for updated discovery information. The default is 30 seconds.

Parameters:

<val>: Specify a value between 5 and 32768 (seconds).

Example: Set the LLDP timer value to 35.

```
# config t
(config)# lldp timer 35
```

Negation: (config)# no lldp timer

3.10.20.4. (config)# lldp transmission-delay

Syntax: (config)# lldp transmission-delay <val>

Parameters:

<val>: Specify a value between 1 and 8192 (seconds).

Explanation: Configure a delay between the LLDP frames that contain changed configurations. Tx Delay cannot be larger than 1/4 of the Tx interval value.

Example: Set the LLDP transmission delay value to 2.

```
# config t
(config)# lldp transmission-delay 2
```

Negation: (config)# no lldp transmission-delay

3.10.20.5. (config)# lldp med datum

Syntax: (config)# lldp med datum { wgs84 | nad83-navd88 | nad83-mllw }

Explanation: The Map Datum is used for the coordinates given in above options.

Parameters:

{ wgs84 | nad83-navd88 | nad83-mllw }: Specify one of the options.

WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.

NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Example: Set the map datum to wgs84.

```
# config t
(config)# lldp med datum wgs84
```

Negation: (config)# no lldp med datum

3.10.20.6. (config)# lldp med fast

Syntax: (config)# lldp med fast <v_1_to_10>

Explanation: Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy. With this in mind, LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. With Fast start repeat count it is possible to specify the number of times the fast start transmission is repeated. The recommended value is 4 times, giving that 4 LLDP frames with a 1 second interval will be transmitted, when a LLDP frame with new information is received. It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including between Network Connectivity Devices, or to other types of links.

Parameters:

<v_1_to_10>: Specify a valid value between 1 and 10.

Example: Set the value to 5.

```
# config t
(config)# lldp med fast 5
```

Negation: (config)# no lldp med fast

3.10.20.7. (config)# lldp med location-tlv altitude

Syntax: (config)# lldp med location-tlv altitude { meters | floors } <v_word11>

Explanation: Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). “meters” means meters of Altitude defined by the vertical datum specified; while, “floors” means altitude in a form more relevant in buildings which have different floor-to-floor dimensions.

Parameters:

{ meters | floors }: Specify one of the options.

<v_word11>: Specify a value for the specified option.

Example: Set the altitude value to “floors 10”.

```
# config t
(config)# lldp med location-tlv altitude floors 10
```

Negation: (config)# no lldp med location-tlv altitude

3.10.20.8. (config)# lldp med location-tlv civic-addr

Syntax: (config)# lldp med location-tlv civic-addr { country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code } <v_string250>

Explanation: Configure civic address information.

Parameters:

{ country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code }: Specify one of the options.

country: The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

state: National subdivisions (state, canton, region, province, prefecture).

county: County, parish, gun (Japan), district.

city: City, township, shi (Japan) - Example: Copenhagen.

district: City division, borough, city district, ward, chou (Japan).

block: Neighbourhood, block.

street: Street - Example: Poppelvej.

leading-street-direction: Example: N.

trailings-street-suffix: Example: SW.

street-suffix: Ave, Platz.

house-no: Specify house number.

house-no-suffix: Example: A, 1/2.

landmark: Landmark or vanity address - Example: Columbia University.

additional-info: Example: South Wing.

Name: Example: Flemming Jahn.

zip-code: Postal/zip code - Example: 2791.

building: Building (structure). Example: Low Library.

apartment: Unit (Apartment, suite). Example: Apt 42.

floor: Example: 4.

room-number: Room number - Example: 450F.

place-type: Example: Office.

postal-community-name: Example: Leonia.

p-o-box: Example: 12345.

additional code: Example: 1320300003.

Example: Set the country code to “UK”.

```
# config t
(config)# lldp med location-tlv civic-addr country UK
```

Negation: (config)# no lldp med location-tlv civic-addr { country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code }

3.10.20.9. (config)# lldp med location-tlv elin-addr

Syntax: (config)# lldp med location-tlv elin-addr <v_word25>

Explanation: Configure a value for Emergency Location Information.

Parameters:

<v_word25>: A value for Emergency Location Information (ELIN).

Example: Set the emergency location information to “911”.

```
# config t
(config)# lldp med location-tlv elin-addr 911
```

Negation: (config)# no lldp med location-tlv elin-addr

3.10.20.10. (config)# lldp med location-tlv latitude

Syntax: (config)# lldp med location-tlv latitude { north | south } <v_word8>

Explanation: Configure a value for latitude. Latitude value should be between 0 and 90.

Parameters:

{ north | south }: Specify one of the options, either north or south.

<v_word8>: Specify latitude value for the selected option.

Example: Set the north latitude to 5.

```
# config t
(config)# lldp med location-tlv latitude north 5
```

Negation: (config)# no lldp med location-tlv latitude

3.10.20.11. (config)# lldp med location-tlv longitude

Syntax: (config)# lldp med location-tlv longitude { west | east } <v_word9>

Explanation: Configure a value for longitude. Longitude value should be between 0 and 180.

Parameters:

{ west | east }: Specify one of the options, either west or east.

<v_word9>: Specify longitude value for the selected option.

Example: Set the west longitude to 90.

```
# config t
(config)# lldp med location-tlv longitude west 90
```

Negation: (config)# no lldp med location-tlv longitude

3.10.20.12. (config)# lldp med media-vlan-policy

Syntax: (config)# lldp med media-vlan-policy <policy_index> { voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling } { tagged <v_vlan_id> | untagged } [l2-priority <v_0_to_7>] [dscp <v_0_to_63>]

Explanation: Configure a LLDP MED policy ID for a service.

Parameters:

<policy_index>: Specify a policy ID. The valid range is from 0 to 31.

{ voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling }: Specify one of the services for this policy ID.

{ tagged <v_vlan_id> | untagged }: Specify whether this service is tagged or untagged. When “tagged” is specified, a VLAN ID should be provided.

[l2-priority <v_0_to_7>]: Specify a value for L2 priority. The valid value is from 0 to 7.

[dscp <v_0_to_63>]: Specify a value for DSCP. The valid value is from 0 to 63.

Example: Create a policy ID 1 for tagged Voice VLAN.

```
# config t
(config)# lldp med media-vlan-policy 1 voice tagged 100 l2-priority 7 DSCP 63
```

Negation: (config)# no lldp med media-vlan-policy <policies_list>

Show: > show lldp med media-vlan-policy [<v_0_to_31>]
# show lldp med media-vlan-policy [<v_0_to_31>]

3.10.21. (config)# logging

3.10.21.1. (config)# logging on

Syntax: (config)# logging on <idx>

Explanation: This sets the server mode operation. When the mode of operation is enabled (on), the syslog message will send out to syslog server (at the server address). The syslog protocol is based on UDP communication and received on UDP port 514. Syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out, even if the syslog server does not exist. When the mode of operation is disabled, no syslog packets are sent out.

Parameters:

<idx>: Specify the syslog server ID number. The available ID range is 1~4.

Example: Enable log server 1 operation.

```
# config t
(config)# logging on 1
```

Negation: (config)# no logging on

Show: # show logging

Clear: # clear logging [info] [warning] [error] [switch <switch_list>]

3.10.21.2. (config)# logging host

Syntax: (config)# logging host <idx> { <ipv4_addr> | <domain_name> }

Parameters:

<idx>: Specify the syslog server ID for this entry. The valid range is 1~3.

{ <ipv4_addr> | <domain_name> }: Specify the domain name of the log server or IPv4 address of the log server.

Explanation: Configure log server address.

Example: Use IPv4 address to configure log server.

```
# config t
(config)# logging host 192.168.1.253
```

Negation: (config)# no logging host

Show: # show logging
# show logging <logging_id: 1-4294967295>
# show logging [info] [warning] [error]

3.10.21.3. (config)# logging host <idx> level

Syntax: (config)# logging host <id> level { informational | notice | warning | error }

Explanation: Configure what kind of messages will send to syslog server.

Parameters:

<idx>: Specify the log server ID (1~4)

{ informational | notice | warning | error }: Specify one of the log message options that will be sent to syslog server.

informational: Send specific messages which severity code is less than or equal to Informational type (6).

notice: Send specific messages which severity code is less than or equal to Notice type (5).

Warning: Send specific messages which severity code is less than or equal to Warning type (4).

Error: Send specific messages which severity code is less than or equal to Error type (3).

Example: Send error messages to log server 1.

```
# config t
(config)# logging level 1 error
```

Show: # show logging
# show logging <logging_id: 1-4294967295>
# show logging [info] [warning] [error]

3.10.21.4. (config)# logging source

Syntax: (config)# logging source <source_name> [level { informational | notice | warning | error }]

Explanation: Configure log source and its severity level.

Parameters:

<source_name>: Specify the source name.

[level { informational | notice | warning | error } : Specify the log notification level.

Negation: (config)# no logging source <source_name> level { informational | notice | warning | error }

Show: # show logging

Clear: # clear logging [informational] [notice] [warning] [error] [switch <switch_list>]

3.10.22. (config)# loop-protect

3.10.22.1. (config)# loop-protect

Syntax: (config)# loop-protect

Explanation: Enable loop protection function.

```
# config t
(config)# loop-protect
```

Negation: (config)# no loop-protect

Show: # show loop-protect [interface (<port_type> [<plist>])]

3.10.22.2. (config)# loop-protect shutdown-time

Syntax: (config)# loop-protect shutdown-time <t>

Explanation: Configure the period for which a port will be kept disabled.

Parameters:

<t: 0-604800>: Specify a shutdown time value. The valid values are from 0 to 604800 seconds. 0 means that a port is kept disabled until next device restart.

Example: Set the shutdown time value to 180 seconds.

```
# config t
(config)# loop-protect shutdown-time 180
```

Negation: (config)# no loop-protect shutdown-time

Show: # show loop-protect [interface (<port_type> [<plist>])]

3.10.22.3. (config)# loop-protect transmit-time

Syntax: (config)# loop-protect transmit-time <t>

Explanation: Configure the interval between each loop protection PDU sent on each port.

Parameters:

<t: 1-10>: Specify a transmit time value. The valid values are from 1 to 10 seconds.

Example: Set the transmit time value to 5 seconds.

```
# config t
(config)# loop-protect transmit-time 5
```

Negation: (config)# no loop-protect transmit-time

Show: # show loop-protect [interface (<port_type> [<plist>])]

3.10.23. (config)# mac

3.10.23.1. (config)# mac address-table aging-time

Syntax: (config)# mac address-table aging-time <v_0_10_to_1000000>

Explanation: Configure the aging time for a learned MAC to be appeared in MAC learning table.

Parameters:

<v_0_10_to_1000000>: Specify an aging time value for MAC address table. The valid values are from 10 to 1000000 (seconds). Using "0" to disable aging time function.

Example: Set the aging time to 600 seconds.

```
# config t
(config)# mac address-table aging-time 600
```

Negation: (config)# no mac address-table aging-time
(config)# no mac address-table aging-time <v_0_10_to_1000000>

Show: > show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]
# show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]
# show mac address-table aging-time

3.10.23.2. (config)# mac address-table static

Syntax: (config)# mac address-table static <v_mac_addr> vlan <v_vlan_id> interface (<port_type> [<v_port_type_list>])

Explanation: Configure the static MAC address mapping table.

Parameters:

<v_mac_addr>: Specify MAC address in “xx:xx:xx:xx:xx:xx” format.

vlan <v_vlan_id>: Specify the VLAN ID for this entry.

interface (<port_type> [<v_port_type_list>]): Specify the interface port type and the port number.

Example: Add a static MAC address “11:11:22:22:33:33” to MAC address table.

```
# config t
(config)# mac address-table static 11:11:22:22:33:33 vlan 1 interface
GigabitEthernet 1/1-2
```

Negation: (config)# no mac address-table static <v_mac_addr> vlan <v_vlan_id> interface (<port_type> [<v_port_type_list>])

Show: > show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]
# show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]

Clear: # clear mac address-table

3.10.24. (config)# monitor session

Syntax: (config)# monitor session <session_number> [destination { interface (<port_type> [<di_list>]) | remote vlan <drvid> reflector-port <port_type> <rportid> } | source { interface (<port_type> [<si_list>]) [both | rx | tx] | remote vlan <srvid> | vlan <source_vlan_list> | cpu [both | rx | tx] }]

Explanation: Configure which port traffic should be mirrored to.

Parameters:

<session_number <1-5>: Specify a session number (1 to 5) to this entry.

[destination { interface (<port_type> [<di_list>]) | remote vlan <drvid> reflector-port <port_type> <rportid> } | source { interface (<port_type> [<si_list>]) [both | rx | tx] | remote vlan <srvid> | vlan <source_vlan_list> | cpu [both | rx | tx] }]: Specify the mirroring source.

Negation: (config)# no monitor session <session_number> [destination { interface (<port_type> [<di_list>]) | remote vlan <drvid> reflector-port <port_type> <rportid> } | source { interface (<port_type> [<si_list>]) [both | rx | tx] | remote vlan <srvid> | vlan <source_vlan_list> | cpu [both | rx | tx] }]

3.10.25. (config)# mvr

3.10.25.1. (config)# mvr

Syntax: (config)# mvr

Explanation: Enable MVR function.

Example: Enable MVR function.

```
# config t
(config)# mvr
```

Negation: (config)# no mvr

Show: > show mvr

# show mvr

3.10.25.2. (config)# mvr name <mvr_name> channel

Syntax: (config)# mvr name <mvr_name> channel <profile_name>

Explanation: Configure MVR name and channel.

Parameters:

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

<profile_name>: Specify a channel name for this MVR entry. The allowed characters are 16.

Example: Set up a MVR entry “video1” and its corresponding channel profile name “1”.

```
# config t
(config)# mvr name video1 channel 1
```

Negation: (config)# no mvr name <mvr_name> channel

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

# show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]

3.10.25.3. (config)# mvr name <mvr_name> frame priority

Syntax: (config)# mvr name <mvr_name> frame priority <cos_priority>

Explanation: Configure the priority for transmitting IGMP/MLD control frames for the specified MVR entry.

Parameters:

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

<cos_priority>: Specify a Cos priority for this MVR entry. The allowed range is from 0 to 7.

Example: Set up a MVR entry “video1” and its corresponding priority value “0”.

```
# config t
(config)# mvr name video1 frame priority 0
```

Negation: (config)# no mvr name <mvr_name> frame priority

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]
# show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]

3.10.25.4. (config)# mvr name <mvr_name> frame tagged

Syntax: (config)# mvr name <mvr_name> frame tagged

Explanation: Tagged IGMP/MLD frames will be sent.

Parameters:

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

Example: Set “video1” MVR entry to send tagged IGMP/MLD frames.

```
# config t
(config)# mvr name video1 frame tagged
```

Negation: (config)# no mvr name <mvr_name> frame tagged

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]
# show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]

3.10.25.5. (config)# mvr name <mvr_name> {election | igmp-address<v_ipv4_ucast>}

Syntax: (config)# mvr name <mvr_name> {election | igmp-address<v_ipv4_ucast>}

Explanation: Enable to join IGMP election in the VLAN or configure IGMP IPv4 address for the specified MVR entry.

Parameters:

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

<v_ipv4_ucast>: Specify the IPv4 unicast address as source address used in IP header for IGMP control frames.

Example: Set up a MVR entry “video1” and its corresponding IGMP address “10.1.1.100”.

```
# config t
(config)# mvr name video1 igmp-address 10.1.1.100
```

Negation: (config)# no mvr vlan <mvr_name> igmp-address

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]
# show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]

3.10.25.6. (config)# mvr name <mvr_name> last-member-query-interval

Syntax: (config)# mvr name <mvr_name> last-member-query-interval <ipmc_lmqi>

Explanation: Configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership.

Parameters:

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

<ipmc_lmqi>: Specify the LMQI (Last Member Query Interval) value. By default, LMQI is set to 5 tenths of a second (0.5 second). The allowed range is from 0 to 31744 tenths of a second.

Example: Set LMQI value to 600 tenths of a second.

```
# config t
(config)# mvr name video1 last-member-query-interval 600
```

Negation: (config)# no mvr vlan <mvr_name> last-member-query-interval

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.10.25.7. (config)# mvr name <mvr_name> mode

Syntax: (config)# mvr name <mvr_name> mode { dynamic | compatible }

Explanation: Configure MVR mode.

Parameters:

<mvr_name>: Specify a name for this MVR entry. The allowed characters are 16.

{ dynamic | compatible }: Specify one of the options.

Dynamic: MVR allows dynamic MVR membership reports on source ports. (This is the default mode.)

Compatible: MVR membership reports are forbidden on source ports.

Example: Set MVR mode to dynamic.

```
# config t
(config)# mvr name video1 mode dynamic
```

Negation: (config)# no mvr name <mvr_name> mode

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.10.25.8. (config)# mvr vlan <v_vlan_list>

Syntax: (config)# mvr vlan <v_vlan_list> [name <mvr_name>]

Explanation: Configure a MVR VLAN and its corresponding MVR name.

Parameters:

<v_vlan_list>: Specify multicast VLAN ID.

[name <mvr_name>]: Specify a name for this MVR entry. This argument is optional.

Example: Set up MVR VLAN 201 and its corresponding name.

```
# config t
(config)# mvr vlan 201 video1
```

Negation: (config)# no mvr vlan <v_vlan_list>

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.10.25.9. (config)# mvr vlan <v_vlan_list> channel

Syntax: (config)# mvr vlan <v_vlan_list> channel <profile_name>

Explanation: Configure MVR name and channel.

Parameters:

<v_vlan_list>: Specify MVR VLAN ID for this entry.

<profile_name>: Specify a channel name for this MVR entry. The allowed characters are 16.

Example: Set up Set up MVR VLAN 201 and its corresponding channel.

```
# config t
(config)# mvr vlan 201 channel 1
```

Negation: (config)# no mvr vlan <v_vlan_list> channel

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.10.25.10. (config)# mvr vlan <v_vlan_list> frame priority

Syntax: (config)# mvr vlan <v_vlan_list> frame priority <cos_priority>

Explanation: Configure the priority for transmitting IGMP/MLD control frames for the specified MVR VLAN ID.

Parameters:

<v_vlan_list>: Specify MVR VLAN ID for this entry.

<cos_priority>: Specify a Cos priority for this MVR entry. The allowed range is from 0 to 7.

Example: Set up a MVR VLAN 201 and its corresponding priority value “0”.

```
# config t
(config)# mvr vlan 201 frame priority 0
```

Negation: (config)# no mvr vlan <v_vlan_list> frame priority

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.10.25.11. (config)# mvr vlan <v_vlan_list> frame tagged

Syntax: (config)# mvr vlan <v_vlan_list> frame tagged

Explanation: Tagged IGMP/MLD frames will be sent.

Parameters:

<v_vlan_list>: Specify MVR VLAN ID for this entry.

Example: Set MVR VLAN 201 to send tagged IGMP/MLD frames.

```
# config t
(config)# mvr vlan 201 frame tagged
```

Negation: (config)# no mvr vlan <v_vlan_list> frame tagged

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.10.25.12. (config)# mvr vlan <v_vlan_list> igmp-address

Syntax: (config)# mvr vlan <v_vlan_list> igmp-address <v_ipv4_ucast>

Explanation: Configure IGMP IPv4 address for the specified MVR entry.

Parameters:

<v_vlan_list>: Specify MVR VLAN ID for this entry.

<v_ipv4_ucast>: Specify the IPv4 unicast address as source address used in IP header for IGMP control frames.

Example: Set up a MVR VLAN 201 and its corresponding IGMP address "10.1.1.100".

```
# config t
(config)# mvr vlan 201 igmp-address 10.1.1.100
```

Negation: (config)# no mvr vlan <v_vlan_list> igmp-address

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.10.25.13. (config)# mvr vlan <v_vlan_list> last-member-query-interval

Syntax: (config)# mvr vlan <v_vlan_list> last-member-query-interval <ipmc_lmqi>

Explanation: Configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership.

Parameters:

<v_vlan_list>: Specify MVR VLAN ID for this entry.

<ipmc_lmqi>: Specify the LMQI (Last Member Query Interval) value. By default, LMQI is set to 5 tenths of a second (0.5 second). The allowed range is from 0 to 31744 tenths of a second.

Example: Set LMQI value to 600 tenths of a second.

```
# config t
(config)# mvr vlan 201 last-member-query-interval 600
```

Negation: (config)# no mvr vlan <v_vlan_list> last-member-query-interval

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.10.25.14. (config)# mvr vlan <v_vlan_list> mode

Syntax: (config)# mvr vlan <v_vlan_list> mode { dynamic | compatible }

Explanation: Configure MVR mode.

Parameters:

<v_vlan_list>: Specify MVR VLAN ID for this entry.

{ dynamic | compatible }: Specify one of the options.

Dynamic: MVR allows dynamic MVR membership reports on source ports. (This is the default mode.)

Compatible: MVR membership reports are forbidden on source ports.

Example: Set MVR mode to dynamic.

```
# config t
(config)# mvr vlan 201 mode dynamic
```

Negation: (config)# no mvr vlan <v_vlan_list> mode

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.10.25.15. (config)# mvr vlan <v_vlan_list> {election | igmp-address <v_ipv4_ucast>}

Syntax: (config)# mvr vlan <v_vlan_list> {election | igmp-address <v_ipv4_ucast>}

Explanation: Enable to join IGMP querier or configure IGMP IPv4 address for the specified MVR entry.

Parameters:

<v_vlan_list>: Specify MVR VLAN ID for this entry.

<v_ipv4_ucast>: Specify the IPv4 unicast address as source address used in IP header for IGMP control frames.

Example: Set up a MVR VLAN 201 and its corresponding IGMP address “10.1.1.100”.

```
# config t
(config)# mvr vlan 201 igmp-address 10.1.1.100
```

Negation: (config)# no mvr vlan <v_vlan_list> igmp-address

Show: > show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]
# show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]

3.10.26. (config)# ntp

3.10.26.1. (config)# ntp

Syntax: (config)# ntp

Explanation: Enable NTP function.

Example: Enable NTP function.

```
# config t
(config)# ntp
```

Negation: (config)# no ntp

Show: # show ntp status

3.10.26.2. (config)# ntp server

Syntax: (config)# ntp server <index_var> ip-address { <ipv4_var> | <ipv6_var> | <name_var> }

Explanation: Configure a list of NTP server's address.

Parameters:

< index_var: 1-5>: Specify the index number of NTP server. The allowed range is from 1 to 5. The NTP servers are tried in numeric order. If 'Server 1' is unavailable, the NTP client will try to contact 'Server 2'.

{ <ipv4_var> | <ipv6_var> | <name_var> }: Specify one of the three options.

ipv4_var>: IPv4 address.

<ipv6_var>: IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once.

<name_var>: The domain name for NTP server.

Example: Set the NTP server 1 to 192.168.1.253.

```
# config t
(config)# ntp server 1 ip-address 192.168.1.253
```

Negation: (config)# no ntp server <index_var>

Show: # show ntp status

3.10.27. (config)# port-security

3.10.27.1. (config)# port-security

Syntax: (config)# port-security

Explanation: Enable port security function globally.

Example: Enable port security function globally.

```
# config t
(config)# port-security
```

Negation: (config)# no port-security

Show: > show port-security switch [interface (<port_type> [<v_port_type_list>])]
# show port-security switch [interface (<port_type> [<v_port_type_list>])]

3.10.27.2. (config)# port-security aging

Syntax: (config)# port-security aging

Explanation: Enable port security aging function. If enabled, secured MAC addresses are subject to aging as discussed in "Aging time" command. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Example: Enable port security aging function.

```
# config t
(config)# port-security aging
```

Negation: (config)# no port-security aging

Show: > show port-security port [interface (<port_type> [<v_port_type_list>])]
# show port-security port [interface (<port_type> [<v_port_type_list>])]

3.10.27.3. (config)# port-security aging time

Syntax: (config)# port-security aging time <v_10_to_10000000>

Explanation: Configure a desired aging time value. If "Aging" is enabled, secured MAC addresses are subject to aging as discussed this command. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Parameters:

<v_10_to_10000000>: Specify the aging time value. The allowed range is between 10 and 10,000,000 seconds.

Example: Set the aging time value to 1800 seconds.

```
# config t
(config)# port-security aging time 1800
```

Negation: (config)# no port-security aging time

Show: > show port-security port [interface (<port_type> [<v_port_type_list>])]
# show port-security port [interface (<port_type> [<v_port_type_list>])]

3.10.27.4. (config)# port-security hold time

Syntax: (config)# port-security hold time <v_10_to_10000000>

Explanation: Configure a desired hold time value in seconds. This value is used to determine how long a MAC address is held in the MAC table if it has been found to vilate the limit. The default value 300 seconds but can be changed to the desired value from 10 to 10000000 seconds. The reason for holding a violating MAC address in MAC table is primarily to ensure that the same MAC address doesn't give rise to continuous notifications (if notifications on violation count is enabled).

Parameters:

<v_10_to_10000000>: Specify the hold time value. The allowed range is between 10 and 10,000,000 seconds.

Negation: (config)# no port-security hold time

Show: > show port-security port [interface (<port_type> [<v_port_type_list>])]

# show port-security port [interface (<port_type> [<v_port_type_list>])]

3.10.28. (config)# prompt

Syntax: (config)# prompt <prompt>

Explanation: Set up prompt message before prompted mode symbol.

Parameters:

<prompt>]: The prompt message should begin with a "%" sign and then a character. Available prompt messages include the following:

%h = hostname
%%= percent sign
%s= space
%t= tab
%D= date
%T= time
%Z= date and time

Negation: (config)# no prompt

Example: Set the current date and time as a prompt message.

```
# config t
(config)# prompt %Z
2019-10-03T17:33:25+00:00(config)#
```

3.10.29. (config)# privilege

Syntax: (config)# privilege { exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool } level <privilege> <cmd>

Explanation: This command is used to change the privilege level of commands available in Configuration mode.

Parameters:

{ exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile }: Specify the group command that you want to configure.

level <privilege>: Specify the privilege level. The allowed range is 0 to 15.

<cmd>: Initial valid words and literals of the command to modify, in 128 characters.

Example: The following example sets the privilege level to 15 for any Exec mode (user or privileged) command.

```
# config t
(config)# privilege exec level 15 host
```

Negation: (config)# no privilege { exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile } level <0-15> <cmd>

Show: > show privilege
# show privilege

3.10.30. (config)# qos

3.10.30.1. (config)# qos map cos-dscp

Syntax: (config)# qos map cos-dscp <cos> dpl <dpl> dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Parameters:

cos-dscp <cos>: Map COS to DSCP. Indicate the Class of Service level. The allowed range is 0 to 7. A CoS class of 0 has the lowest priority, while 7 has the highest priority.

dpl <dpl>: Specify the Drop Precedence Level. The allowed range is 0 to 7.

dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }: Specify one of the DSCP values.

<dscp_num: 0-63>: The allowed number is from 0 to 63.

be: Default PHB (DSCP 0) for best effort traffic.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43: Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7: Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

ef: Expedited Forwarding PHB (DSCP 46).

va: Voice Admit PHB (DSCP 44).

Explanation: Configure the COS-DSCP mapping.

Example: The following example sets DPL to 4, DSCP to cs4.

```
# config t
(config)# qos map cos-dscp 4 dpl 4 dscp cs4
```

Negation: (config)# no qos map cos-dscp <cos> dpl <dpl>

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.10.30.2. (config)# qos map dscp-classify

Syntax: (config)# qos map dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Explanation: Configure the DSCP Ingress classification.

Parameters:

dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }: Specify one of the DSCP values.

<dscp_num: 0-63>: The allowed number is from 0 to 63.

be: Default PHB (DSCP 0) for best effort traffic.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43: Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7: Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

ef: Expedited Forwarding PHB (DSCP 46).

va: Voice Admit PHB (DSCP 44).

Example: The following example sets DSCP Ingress classification to cs4.

```
# config t
(config)# qos map dscp-classify cs4
```

Negation: (config)# no qos map dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.10.30.3. (config)# qos map dscp-cos

Syntax: (config)# qos map dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } cos <cos> dpl <dpl>

Explanation: Configure the DSCP-based QoS Ingress classification.

Parameters:

dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }: Specify one of the DSCP values.

<dscp_num: 0-63>: The allowed number is from 0 to 63.

be: Default PHB (DSCP 0) for best effort traffic.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43: Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7: Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

ef: Expedited Forwarding PHB (DSCP 46).

va: Voice Admit PHB (DSCP 44).

cos <cos>: Indicate the Class of Service level. The allowed range is 0 to 7. A CoS class of 0 has the lowest priority, while 7 has the highest priority.

dpl <dpl>: Specify the Drop Precedence Level. The allowed range is 0 to 7.

Negation: (config)# no qos map dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.10.30.4. (config)# qos map dscp-egress-translation

Syntax: (config)# qos map dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } to { <dscp_num_tr> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Explanation: Configure the DSCP Egress Mapping Table.

Parameters:

dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }: Specify one of the DSCP values.

<dscp_num: 0-63>: The allowed number is from 0 to 63.

be: Default PHB (DSCP 0) for best effort traffic.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43: Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7: Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

ef: Expedited Forwarding PHB (DSCP 46).

va: Voice Admit PHB (DSCP 44).

Example: The following example maps cs4 to cs5.

```
# config t
(config)# qos map dscp-egress-translation cs4 to cs5
```

Negation: (config)# no qos map dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } <dpl>

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.10.30.5. (config)# qos map dscp-ingress-translation

Syntax: (config)# qos map dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } to { <dscp_num_tr> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Explanation: Configure the DSCP Ingress Mapping Table.

Parameters:

dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }: Specify one of the DSCP values.

<dscp_num: 0-63>: The allowed number is from 0 to 63.

be: Default PHB (DSCP 0) for best effort traffic.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43: Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7: Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

ef: Expedited Forwarding PHB (DSCP 46).

va: Voice Admit PHB (DSCP 44).

Example: The following example maps cs4 to cs5.

```
# config t
(config)# qos map dscp-ingress-translation cs4 to cs5
```

Negation: (config)# no qos map dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.10.30.6. (config)# qos map egress

Syntax: (config)# qos map egress <map_id>

Explanation: Enter the egress map configuration page.

Parameters:

<map_id>: Specify the Egress map ID.

3.10.30.6.1. (config-qos-map-egress)# key

Syntax: (config-qos-map-egress)# key { class | class-dpl | dscp | dscp-dpl }

Explanation: Specify the key type that will be used to filter the map rules when applying the map.

Parameters:

key { class | class-dpl | dscp | dscp-dpl }: Specify the key type.

class: Use classified CoS ID as the key.

class-dpl: Use classified CoS ID and DPL as the key.

dscp: Use classified DSCP as the key.

dscp-dpl: Use classified DSCP and DPL as the key.

Show: > show qos
# show qos

3.10.30.6.2. (config-qos-map-egress)# map dscp

Syntax: (config-qos-map-egress)# map { { { dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } } |[dpl <dpl_num>] } to { [pcp <pcp>] [dei <dei>] [dscp <dscp>] [path-cosid <path_cosid>] }*1

Explanation: Specify the rule key and the action.

Parameters:

dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va }: Indicate a specific DSCP.

dpl <dpl_num>: Indicate DPL value. The valid DPL value range is 0~3.

to { [pcp <pcp>] [dei <dei>] [dscp <dscp>] [path-cosid <path_cosid>]: Specify PCP, DEI, DSCP, Path CoS ID values.

PCP: Assign a PCP value. The valid range is 0~7.

DEI: Assign a DEI value. The valid range is 0~1.

DSCP: Assign a DSCP value. The valid range is 0~63.

Path CoS ID: Assign a path CoS ID value. The valid range is 0~7.

Show: > show qos
# show qos
# show qos maps egress

3.10.30.6.3. (config-qos-map-egress)# map

Syntax: (config-qos-map-egress)# map { { { dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } } | { class <cosid_num> } } [dpl <dpl_num>] } to { [pcp <pcp>] [dei <dei>] [dscp <dscp>] }*1

Explanation: Map DSCP values, CoS, and DPL value to PCP, DEI and DSCP values.

Parameters:

{ { { dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } } | { class <cosid_num> } } [dpl <dpl_num>] } to { [pcp <pcp>] [dei <dei>] [dscp <dscp>] }*1: Map DSCP values, CoS, and DPL value to PCP, DEI and DSCP values.

Show: # show qos maps egress

3.10.30.6.4. (config-qos-map-egress)# action

Syntax: (config-qos-map-egress)# action { [pcp] [dei] [dscp] }*1

Explanation: Specify the rule key and the action.

Parameters:

action { [pcp] [dei] [dscp] }*1: Indicate the action type to filter the map rules.

Show: > show qos
# show qos
# show qos maps egress

3.10.30.7. (config)# qos map ingress

Syntax: (config)# qos map ingress <map_id>

Explanation: Enter the ingress map configuration page.

Parameters:

<map_id>: Specify the Ingress map ID.

3.10.30.7.1. (config-qos-map-ingress)# map dscp

Syntax: (config-qos-map-ingress)# map { { dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } } to { [cos <cos>] [dpl <dpl>] [pcp <pcp>] [dei <dei>] [dscp <dscp>] [path-cosid <path_cosid>] }*1

Explanation: Specify the rule key and the action.

Parameters:

dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42| af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va }: Indicate a specific DSCP.

to { [cos <cos>] [dpl <dpl>] [pcp <pcp>] [dei <dei>] [dscp <dscp>] [path-cosid <path_cosid>] }: Specify CoS ID, DPL, PCP, DEI, DSCP, Path CoS ID values.

COS: Assign a CoS ID value. The valid range is 0~7.

DPL: Assign a DPL value. The valid range is 0~3.

PCP: Assign a PCP value. The valid range is 0~7.

DEI: Assign a DEI value. The valid range is 0~1.

DSCP: Assign a DSCP value. The valid range is 0~63.

Path CoS ID: Assign a path CoS ID value. The valid range is 0~7.

Show: > show qos
# show qos
# show qos maps ingress

3.10.30.7.2. (config-qos-map-ingress)# map pcp

Syntax: (config-qos-map-inress)# map { { pcp <pcp_num> [dei <dei_num>] } } to { [class <cosid>] [cos <cos>] [dpl <dpl>] [pcp <pcp>] [dei <dei>] [dscp <dscp>] [path-cosid <path_cosid>] [tc <tc>] }*1

Explanation: Specify the rule key and the action.

Parameters:

pcp <pcp_num>: Indicate a PCP value. The valid PCP value range is 0~7.

dpl <dpl_num>: Indicate DPL value. The valid DPL value range is 0~3.

to { [pcp <pcp>] [dei <dei>] [dscp <dscp>] [path-cosid <path_cosid>]: Specify PCP, DEI, DSCP, Path CoS ID values.

PCP: Assign a PCP value. The valid range is 0~7.

DEI: Assign a DEI value. The valid range is 0~1.

DSCP: Assign a DSCP value. The valid range is 0~63.

Path CoS ID: Assign a path CoS ID value. The valid range is 0~7.

Show: > show qos
# show qos
# show qos maps egress

3.10.30.7.3. (config-qos-map-ingress)# map action

Syntax: (config-qos-map-ingress)# action { [class] [cos] [dpl] [pcp] [dei] [dscp] }*1

Explanation: Specify the rule key and the action.

Parameters:

action { [class] [cos] [dpl] [pcp] [dei] [dscp] }*1: Indicate the action type to filter the map rules.

Show: > show qos
# show qos
# show qos maps ingress

3.10.30.8. (config)# qos qce refresh

Syntax: (config)# qos qce refresh

Explanation: To refresh QCE.

Example: Refresh QCE.

```
# config t
(config)# qos qce refresh
```

3.10.30.9. (config)# qos qce update

Syntax: (config)# qos qce { [update] } <qce_id> [{ next <qce_id_next> } | last] [interface (<port_type> [<port_list>])] [smac { <smac> | <smac_24> | any }] [dmac { <dmac> | unicast | multicast | broadcast | any }] [tag { [type { untagged | tagged | c-tagged | s-tagged | any }] [vid { <ot_vid> | any }] [pcp { <ot_pcp> | any }] [dei { <ot_dei> | any }] }*1] [inner-tag { [type { untagged | tagged | c-tagged | s-tagged | any }] [vid { <it_vid> | any }] [pcp { <it_pcp> | any }] [dei { <it_dei> | any }] }*1] [frame-type { any | { etype [{ <etype_type> | any }] } | { llc [dsap { <llc_dsap> | any }] [ssap { <llc_ssap> | any }] [control { <llc_control> | any }] } | { snap [{ <snap_data> | any }] } | { ipv4 [proto { <pr4> | tcp | udp | any }] [sip { <sip4> | any }] [dip { <dip4> | any }] [dscp { <dscp4> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any }] [fragment { yes | no | any }] [sport { <sp4> | any }] [dport { <dp4> | any }] } | { ipv6 [proto { <pr6> | tcp | udp | any }] [sip { <sip6> | any }] [dip { <dip6> | any }] [dscp { <dscp6> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any }] [sport { <sp6> | any }] [dport { <dp6> | any }] } }] [action { [cos { <action_cos> | default }] [dpl { <action_dpl> | default }] [pcp-dei { <action_pcp> <action_dei> | default }] [dscp { <action_dscp_dscp> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | default }] [policy { <action_policy> | default }] }*1]

Explanation: To update the QCE.

Parameters:

{ [update] }: Update the QCE.

<qce_id>: Specify the QCE ID.

[{ next <qce_id_next> } | last]: Put this QCE next to the specified one or to the last one.

[interface (<port_type> [<port_list>])]: Specify port type and port number that apply to this updated QCE rule.

[smac { <smac> | <smac_24> | any }]: Set up the matched SMAC.

[dmac { <dmac> | unicast | multicast | broadcast | any }]: Set up the matached DMAC.

[tag { [type { untagged | tagged | c-tagged | s-tagged | any }]: Set up the matched tag type.
[vid { <ot_vid> | any }]: Specify a specific VID or VID range or specify “any” to allow any VIDs.

[pcp { <ot_pcp> | any }]: Specify a specific PCP or PCP range or specify “any” to allow any PCP values.

[dei { <ot_dei> | any }] }]: Specify a specific DEI or specify “any” to allow any DEI.

[frame-type { any | { etype [{ <etype_type> | any }] } | { llc [dsap { <llc_dsap> | any }] [ssap { <llc_ssap> | any }] [control { <llc_control> | any }] } | { snap [{ <snap_data> | any }] } | { ipv4 [proto { <pr4> | tcp | udp | any }] [sip { <sip4> | any }] [dip { <dip4> | any }] [dscp { <dscp4> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any }] [fragment { yes | no | any }] [sport { <sp4> | any }] [dport { <dp4> | any }] } | { ipv6 [proto { <pr6> | tcp | udp | any }] [sip { <sip6> | any }] [dip { <dip6> | any }] [dscp { <dscp6> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any }] [sport { <sp6> | any }] [dport { <dp6> | any }] } }]: Specify the frame type that applies to this QCE rule.

any: By default, any is used which means that all types of frames are allowed.

etype: This option can only be used to filter Ethernet II formatted packets. (Options: Any, Specific – 600-ffff hex; Default: ffff). Note that 800 (IPv4) and 86DD (IPv6) are excluded. A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).

llc: LLC refers to Link Logical Control and further provides three options.

dsap: DSAP stands for Destination Service Access Point address. By default, any is used. Specify “any” or indicate a value (0x00 to 0xFF).

ssap: SSAP stands for Source Service Access Point address. By default, any is used. Specify “any” or indicate a value (0x00 - 0xFF).

control: Control field may contain command, response, or sequence information depending on whether the LLC frame type is Unnumbered, Supervisory, or Information. By default, any is used. Specify “any” or indicate a value (0x00 to 0xFF).

snap: SubNetwork Access Protocol can be distinguished by an OUI and a Protocol ID. (Options for PID: Any, Specific (0x00-0xffff); Default: Any) If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP. If the OUI is that of a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI isother than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.

ipv4:

proto: IPv4 frame type includes Any, TCP, UDP, Other. If “TCP” or “UDP” is specified, you might further define Sport (Source port number) and Dport (Destination port number).

sip: Specify source IP type. By default, any is used. Indicate self-defined source IP and submask format. The address and mask must be in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When the 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

dscp: By default, any is used. Indicate a DSCP value or a range of DSCP value.

fragment: By default, any is used. Datagrams sometimes may be fragmented to ensure they can pass through a network device that uses a maximum transfer unit smaller than the original packet's size.

ipv6:

proto: IPv6 protocol includes Any, TCP, UDP, Other. If "TCP" or "UDP" is specified, you may need to further define Sport (Source port number) and Dport (Destination port number).

sip: Specify source IP type. By default, any is used. You can also indicate self-defined source IP and submask format.

dscp: By default, any is used. You can also indicate a DSCP value or a range of DSCP value.

[action { [cos { <action_cos> | default }]: Specify the classification action taken on ingress frame if the parameters match the frame's content. If a frame matches the QCE, it will be put in the queue corresponding to the specified QoS class or placed in a queue based on basic classification rules.

[dpl { <action_dpl> | default }]: If a frame matches the QCE, the drop precedence level will be set to the specified value or left unchanged.

[pcp-dei { <action_pcp> <action_dei> | default }]: If a frame matches the QCE, the PCP or DEI value will be set to the specified one.

[dscp { <action_dscp_dscp> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | default }] [policy { <action_policy> | default }] }*1]: If a frame matches the QCE, the DSCP value will be set to the specified one.

Negation: (config)# no qos qce <qce_id_range>

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.10.30.10. (config)# qos storm

Syntax: (config)# qos storm { unicast | multicast | broadcast } <rate> [fps | kfps | kbps | mbps]

Explanation: Configure broadcast storm control rate for QoS

Parameters:

{ unicast | multicast | broadcast }: Specify the storm type that you want to configure.

{ { <rate> [kfps] } | { 1024 kfps } }: User-define storm frame rate or set storm rate to 1024 kfps.

Example: The following example sets broadcast storm control for QoS to 1024 kfps.

Negation: (config)# no qos storm { unicast | multicast | broadcast }

Show: # show qos storm

3.10.31. (config)# radius-server

3.10.31.1. (config)# radius-server attribute 32

Syntax: (config)# radius-server attribute 32 <id>

Explanation: Configure Radius attribute 32 string.

Parameters:

<id>: Specify Radius server identifier. The allowed characters are 1 to 253.

Example: Set RADIUS attribute 32 string to "cabinet5aSW".

```
# config t
(config)# radius-server attribute 32 cabinet5aSW
```

Negation: (config)# no radius-server attribute 32

Show: # show radius-server [statistics]

3.10.31.2. (config)# radius-server attribute 4

Syntax: (config)# radius-server attribute 4 <ipv4>

Explanation: Configure NAS IPv4 address.

Parameters:

<ipv4>: Specify NAS IPv4 address.

Example: Set NAS IPv4 address to 100.1.1.25.

```
# config t
(config)# radius-server attribute 4 100.1.1.25
```

Negation: (config)# no radius-server attribute 4

Show: # show radius-server [statistics]

3.10.31.3. (config)# radius-server attribute 95

Syntax: (config)# radius-server attribute 95 <ipv6>

Explanation: Configure NAS IPv6 address.

Parameters:

<ipv6>: Specify NAS IPv6 address.

Negation: (config)# no radius-server attribute 95

Show: # show radius-server [statistics]

3.10.31.4. (config)# radius-server deadtime

Syntax: (config)# radius-server deadtime <minutes>

Explanation: Configure RADIUS server deadtime value. Deadtime 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.

Parameters:

<deadtime>: Specify RADIUS server deadtime value. The valid range is 1 to 1440 (minutes).

Example: Set RADIUS server to 60.

```
# config t
(config)# radius-server deadtime 60
```

Negation: (config)# no radius-server deadtime

Show: # show radius-server [statistics]

3.10.31.5. (config)# radius-server host

Syntax: (config)# radius-server host <host_name> [auth-port <auth_port>] [acct-port <acct_port>] [timeout <seconds>] [retransmit <retries>] [key <key>]

Explanation: This command is used to configure Radius server.

Parameters:

<host_name>: Specify the hostname or IP address for the radius server. The allowed characters are 1 to 255.

[auth-port <auth_port>]: Specify the UDP port to be used on the RADIUS server for authentication.

[acct-port <acct_port>]: Specify the UDP port to be used on the RADIUS server for accounting.

[timeout <seconds>]: Specify a timeout value. If timeout value is specified here, it will replace the global timeout value. If you prefer to use the global value, leave this field blank.

[retransmit <retries>]: Specify a value for retransmit retry. If retransmit value is specified here, it will replace the global retransmit value. If you prefer to use the global value, leave this field blank.

[key <key>]: Specify a secret key. If secret key is specified here, it will replace the global secret key. If you prefer to use the global value, leave this field blank.

Negation: (config)# no radius-server host <host_name> [auth-port <auth_port>] [acct-port <acct_port>]

Show: # show radius-server [statistics]

3.10.31.6. (config)# radius-server key

Syntax: (config)# radius-server key <key>

Explanation: Configure RADIUS server key value. This key is shared between the RADIUS sever and the switch.

Parameters:

<key>: Specify RADIUS server secret key value. The valid range is 1 to 63.

Example: Set RADIUS server secret key to 803321.

```
# config t
(config)# radius-server key 803321
```

Negation: (config)# no radius-server key

3.10.31.7. (config)# radius-server retransmit

Syntax: (config)# radius-server retransmit <retries>

Explanation: Configure the number of times to retransmit request packets to an authentication server that does not respond. If the server does not respond after the last retransmit is sent, the switch considers the authentication server is dead.

Parameters:

<retries>: Specify RADIUS server retransmit value. The valid range is 1 to 1000.

Example: Set RADIUS server retransmit value to 5

```
# config t
(config)# radius-server retransmit 5
```

Negation: (config)# no radius-server retransmit

Show: # show radius-server [statistics]

3.10.31.8. (config)# radius-server timeout

Syntax: (config)# radius-server timeout <seconds>

Explanation: Configure the time the switch waits for a reply from an authentication server before it retransmits the request.

Parameters:

<seconds>: Specify RADIUS server timeout value. The valid range is 1 to 1000.

Example: Set RADIUS server timeout to 60

```
# config t
(config)# radius-server timeout 60
```

Negation: (config)# no radius-server timeout

Show: # show radius-server [statistics]

3.10.32. (config)# rmon

3.10.32.1. (config)# rmon alarm

Syntax: (config)# rmon alarm <id> <oid_str> <interval> { absolute | delta } rising-threshold <rising_threshold> [<rising_event_id>] falling-threshold <falling_threshold> [<falling_event_id>] { [rising | falling | both] }

Syntax: (config)# rmon alarm <id> { ifInOctets | ifInUcastPkts | ifInNUcastPkts | ifInDiscards | ifInErrors | ifInUnknownProtos | ifOutOctets | ifOutUcastPkts | ifOutNUcastPkts | ifOutDiscards | ifOutErrors } <ifIndex> <interval> { absolute | delta } rising-threshold <rising_threshold> [<rising_event_id>] falling-threshold <falling_threshold> [<falling_event_id>] { [rising | falling | both] }

Explanation: Configure RMON alarm settings. RMON Alarm configuration defines specific criteria that will generate response events. It can be set to test data over any specified time interval and can monitor absolute or changing values. Alarms can also be set to respond to rising or falling thresholds.

Parameters:

<id>: Indicates the index of the entry. The range is from 1 to 65535.

<oid_str>: The object number of the MIB variable to be sampled. Only variables of the type ifEntry.n.n may be

sampled. Possible variables are ifInOctets, ifInUcastPkts, ifInNUcastPkts, ifOutDiscards, ifErrors, ifInUnknownProtos, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts, ifOutDiscards, ifOutErrors.

<interval>: The polling interval for sampling and comparing the rising and falling threshold. The range is from 1to 2^31 (2147483647) seconds.

{ absolute | delta }: Test for absolute or relative change in the specified variable.

Absolute: The variable is compared to the thresholds at the end of the sampling period.

Delta: The last sample is subtracted from the current value and the difference is compared to the thresholds.

rising-threshold <rising_threshold>: If the current value is greater than the rising threshold and the last sample value is less than this threshold, then an alarm will be triggered. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold. The threshold range is -2147483647 to 2147483647.

[<rising_event_id>]: Indicates the rising index of an event. The range is 1 - 65535.

falling-threshold <falling_threshold>: If the current value is less than the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the failing threshold. (Range: -2147483647 to 2147483647)

[<falling_event_id>]: Indicates the falling index of an event. The range is 0 - 65535.

{ [rising | falling | both] }: Specify a method that is used to sample the selected variable and calculate the value to be compared against the thresholds.

rising: Trigger alarm when the first value is larger than the rising threshold.

falling: Trigger alarm when the first value is less than the falling threshold.

both: Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold.

Negation: (config)# no rmon alarm <id>

Show: # show rmon alarm [<id_list>]
# show rmon history [<id_list>]
# show rmon statistics [<id_list>]

3.10.32.2. (config)# rmon event

Syntax: (config)# rmon event <id> [log] [trap <community>] { [description <description>] }

Explanation: Configure RMON Event settings.

Parameters:

<id>: Specify an ID index. The range is 1 - 65535.

[log]: When the event is triggered, a RMON log entry will be generated.

[trap <community>]: A password-like community string sent with the trap. Although the community string can be set on this configuration page, it is recommended that it be defined on the SNMP trap configuration page prior to configuring it here. The allowed characters are 0 - 127.

{ [description <description>] }: Enter a descriptive comment for this entry.

Negation: (config)# no rmon event <id>

Show: # show rmon alarm [<id_list>]
# show rmon history [<id_list>]

3.10.33. (config)# snmp-server

3.10.33.1. (config)# snmp-server

Syntax: (config)# snmp-server

Explanation: Enable SNMP server service.

Example: Enable SNMP server service.

```
# config t
(config)# snmp-server
```

Negation: (config)# no snmp-server

Show: # show snmp

3.10.33.2. (config)# snmp-server access

Syntax: (configt)# snmp-server access <group_name> model { v1 | v2c | v3 | any } level { auth | noauth | priv } [read <view_name>] [write <write_name>]

Explanation: Configure SNMP access settings.

Parameters:

<group_name>: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

model { v1 | v2c | v3 | any }: Indicates the security model that this entry should belong to. Possible security models are:

any: Any security model accepted(v1|v2c|usm).

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

v3: User-based Security Model (USM) for SNMPv3.

level { auth | noauth | priv }: Indicates the security level that this entry should belong to. Possible security models are:

auth: Authentication and no privacy.

noauth: No authentication and no privacy.

priv: Authentication and privacy.

[read <view_name>]: The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

[write <write_name>]: The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

Negation: (config)# no snmp-server access <group_name> model { v1 | v2c | v3 | any } level { auth | noauth | priv }

Show: # show snmp access [<group_name> { v1 | v2c | v3 | any } { auth | noauth | priv }]

3.10.33.3. (config)# snmp-server community

Syntax: (config)# snmp-server community <v3_comm> [{ ip-range <v_ipv4_addr> <v_ipv4_netmask> | ipv6-range <v_ipv6_subnet> }] { <v3_sec> | encrypted <v3_sec_enc> }

Explanation: Configure SNMP server community v3 value.

Parameters:

<v3_comm>: Specify SNMPv3 community string.

[ip-range <v_ipv4_addr> <v_ipv4_netmask> | ipv6-range <v_ipv6_addr> <v_ipv6_netmask>]: Specify IPv4 or IPv6 address and subnet mask address.

Negation: (config)# no snmp-server community <word127>

Show: # show snmp

# show snmp community v3

3.10.33.4. (config)# snmp-server contact

Syntax: (config)# snmp-server contact <v_line255>

Explanation: Configure system contact information.

Parameters:

<v_line255>: Specify system contact information. This could be a person’s name, email address or other descriptions. The allowed string length is 0 – 255 and the allowed content is the ASCII characters from 32 – 126.

Example: Set system contact information to “admin@acme.com”

```
# config t
(config)# snmp-server contact admin@acme.com
```

Negation: (config)# no snmp-server contact

3.10.33.5. (config)# snmp-server engine-id local

Syntax: (config)# snmp-server engine-id local <engineID>

Explanation: Configure SNMP server v3 Engine ID value.

Parameters:

<engineID>: Indicates the SNMPv3 engine ID. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Changes to the Engine ID will clear all original local users.

Negation: (config)# no snmp-server engine-id local

Show: # show snmp

3.10.33.6. (config)# snmp-server host

Syntax: (config)# snmp-server host <conf_name>

Explanation: Configure SNMP server hostname.

Parameters:

<conf_name: word 32>**:** Specify a host name. Once “Enter” is pressed, the CLI prompt changes to (config-snmps-host)#.

Example: Set SNMP server hostname to RemoteSnmp

```
# config t
(config)# snmp-server host RemoteSnmp
(config-snmps-host)#
```

Negation: (config)# snmp-server host <conf_name>

Show: # show snmp host [<conf_name>] [system] [switch] [power] [interface] [aaa]

3.10.33.6.1. (config-snmps-host)# host <v_ipv6_ucast>

Syntax: (config-snmps-host)# host <v_ipv6_ucast> [<udp_port>] [traps | informs]

Explanation: Indicates the SNMP trap destination address.

Parameters:

<v_ipv6_ucast>: Specify the IPv6 address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). Also allowed is a valid hostname. A valid hostname is a string drawn from the alphabet (A-Z; a-z), digits (0-9), dot (.) and dash (-). Spaces are not allowed. The first character must be an alpha character, and the first and last characters cannot be a dot or a dash.

[<udp_port>]: Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535. The default SNMP trap port is 162.

[traps | informs]: Specify one of the options.

Negation: (config-snmps-host)# no host

3.10.33.6.2. (config-snmps-host)# host <v_ipv4_ucast>

Syntax: (config-snmps-host)# host { <v_ipv4_ucast> | <v_word45> } [<udp_port>] [traps | informs]

Explanation: Configure the SNMP trap destination IPv4 address.

Parameters:

{ <v_ipv4_ucast> | <v_word45> }: Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). Also allowed is a valid hostname. A valid hostname is a string drawn from the alphabet (A-Z; a-z), digits (0-9), dot (.) and dash (-). Spaces are not allowed. The first character must be an alpha character, and the first and last characters cannot be a dot or a dash.

[<udp_port>]: Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535. The default SNMP trap port is 162.

[traps | informs]: Specify one of the options.

Negation: (config-snmps-host)# no host

3.10.33.6.3. (config-snmps-host)# version

Syntax: (config-snmps-host)# version { v1 [<v1_comm>] | v2 [<v2_comm>] | v3 [probe | engineID <v_word10_to_32>] [<securtyname>] }

Parameters:

{ v1 [<v1_comm>] | v2 [<v2_comm>] | v3 [probe | engineID <v_word10_to_32>] [<securtyname>] }: Specify one of the SNMP versions.

v1 [v1_comm]: Support SNMPv1 and trap community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 0x21 to 0x7E.

v2 [v2_comm]: Support SNMPv2c and trap community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 0x21 to 0x7E.

v3 [probe | engineID <v_word10_to_32>] [<securtyname>]: Support SNMPv3.

[probe | engineID <v_word10_to_32>]: Indicates the SNMP trap probe security engine ID or SNMP trap security engine ID. SNMPv3 sends traps and informs use USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

[<securtyname>]: Indicates the SNMP trap security name. SNMPv3 traps and informs use USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Explanation: Configure SNMP version and its corresponding values.

Example: Support SNMPv2c version.

```
# config t
(config-snmps-host)# version v2 public
```

Negation: (config-snmps-host)# no version

3.10.33.6.4. (config-snmps-host)# informs retries

Syntax: (config-snmps-host)# informs retries <retries> timeout <timeout>

Explanation: Configure SNMP trap retry times and timeout.

Parameters:

<retries>: Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.

<timeout>: Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.

Negation: (config-snmps-host)# no informs

3.10.33.6.5. (config-snmps-host)# shutdown

Syntax: (config-snmps-host)# shutdown

Parameters: None.

Explanation: Disable the SNMP trap mode.

Example: Disable the SNMP trap mode.

```
# config t
(config-snmps-host)# shutdown
```

Negation: (config-snmps-host)# no shutdown

3.10.33.7. (config)# snmp-server location

Syntax: (config)# snmp-server location <v_line255>

Parameters:

<v_line255>: Specify the descriptive location of this device. The allowed string length is 0 – 255.

Example: Set the location to “Cabinet A22”

```
# config t
(config)# snmp-server location Cabinet A22
```

Negation: (config)# no snmp-server location

3.10.33.8. (config)# snmp-server security-to-group model

Syntax: (configt)# snmp-server security-to-group model { v1 | v2c | v3 } name <security_name> group <group_name>

Explanation: Configure SNMPv3 Group settings.

Parameters:

{ v1 | v2c | v3 }: Indicates the security model that this entry should belong to.

<security_name>: A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

<group_name>: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

Negation: (config)# no snmp-server security-to-group model { v1 | v2c | v3 } name <security_name>

Show: # show snmp security-to-group [{ v1 | v2c | v3 } <security_name>]

3.10.33.9. (config)# snmp-server trap

Syntax: (config)# snmp-server trap

Explanation: Enable SNMP server trap function.

Example: Enable SNMP server trap function.

```
# config t
(config)# snmp-server trap
```

Negation: (config)# no snmp-server trap

Show: # show snmp

3.10.33.10. (config)# snmp-server user

Syntax: (configt)# snmp-server user <username> engine-id <engineID> [{ md5 { <md5_passwd> | { encrypted <md5_passwd_encrypt> } } | sha { <sha_passwd> | { encrypted <sha_passwd_encrypt> } } } [priv { des | aes } { <priv_passwd> | { encrypted <priv_passwd_encrypt> } }]]

Explanation: Configure SNMPv3 User settings.

Parameters:

<username: word 32>: A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

engine-id <engineID>: An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it is a remote user.

[{ md5 { <md5_passwd> | { encrypted <md5_passwd_encrypt> } } | sha { <sha_passwd> | { encrypted <sha_passwd_encrypt> } } }: Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

md5 <md5_passwd>: An optional flag to indicate that this user uses MD5 authentication protocol. A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32 characters. For SHA authentication protocol, the allowed string length is 8 to 40 characters. The allowed content is ASCII characters from 0x21 to 0x7E.

encrypted <md5_passwd_encrypt>: Specify the encrypted MD5 password.

sha <sha_passwd>: An optional flag to indicate that this user uses SHA authentication protocol. A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32 characters. For SHA authentication protocol, the allowed string length is 8 to 40 characters. The allowed content is ASCII characters from 0x21 to 0x7E.
encrypted <sha_passwd_encrypt>: Specify the encrypted SHA password.

[priv { des | aes } { <priv_passwd> | { encrypted <priv_passwd_encrypt> } }]]: Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

DES: An optional flag to indicate that this user uses DES authentication protocol.

AES: An optional flag to indicate that this user uses AES authentication protocol.

<priv_passwd>: A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

encrypted <priv_passwd_encrypt>: Specify the encrypted privacy password.

Negation: (config)# no snmp-server user <username> engine-id <engineID>

Show: #show snmp user [<username> <engineID>]

3.10.33.11. (config)# snmp-server view

Syntax: (configt)# snmp-server view <view_name> <oid_subtree> { include | exclude }

Explanation: Configure SNMPv3 MIB view name.

Parameters:

<view_name>: A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

<oid_subtree>: The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128.

{ include | exclude }: Indicates the view type that this entry should belong to. Possible view types are:

included: An optional flag to indicate that this view subtree should be included.

excluded: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.

Negation: (config)# no snmp-server view <view_name> <oid_subtree>

Show: # show snmp view [<view_name> <oid_subtree>]

3.10.34. (config)# spanning-tree

3.10.34.1. (config)# spanning-tree aggregation

Syntax: (config)# spanning-tree aggregation

Explanation: Enable aggregation mode of Spanning Tree.

Example: Enter aggregation mode.

```
# config t
(config)# spanning-tree aggregation
(config-stp-aggr)#
```

Show: # show spanning-tree

3.10.34.1.1. (config-stp-aggr)# spanning-tree

Syntax: (config-stp-aggr)# spanning-tree

Explanation: Enable Spanning Tree under aggregation mode.

Negation: (config-stp-aggr)# no spanning-tree

Show: # show spanning-tree

3.10.34.1.2. (config-stp-aggr)# spanning-tree auto-edge

Syntax: (config-stp-aggr)# spanning-tree auto-edge

Explanation: Enable auto edge function. When enabled, a port is automatically determined to be at the edge of the network when it receives no BPDUs.

Negation: (config-stp-aggr)# no spanning-tree auto-edge

Show: # show spanning-tree

3.10.34.1.3. (config-stp-aggr)# spanning-tree bpdu-guard

Syntax: (config-stp-aggr)# spanning-tree bpdu-guard

Explanation: Enable BPDU guard function. This feature protects ports from receiving BPDUs. It can prevent loops by shutting down a port when a BPDU is received instead of putting it into the spanning tree discarding state. If enabled, the port will disable itself upon receiving valid BPDU's.

Negation: (config-stp-aggr)# no spanning-tree bpdu-guard

Show: # show spanning-tree

3.10.34.1.4. (config-stp-aggr)# spanning-tree edge

Syntax: (config-stp-aggr)# spanning-tree edge

Explanation: If an interface is attached to end nodes, you can set it to “Edge”.

Negation: (config-stp-aggr)# no spanning-tree edge

Show: # show spanning-tree

3.10.34.1.5. (config-stp-aggr)# spanning-tree link-type

Syntax: (config-stp-aggr)# spanning-tree link-type { point-to-point | shared | auto }

Explanation: Configure the link type attached to an interface.

Parameters:

{ point-to-point | shared | auto }: Select the link type attached to an interface.

point-to-point: It is a point-to-point connection.

shared: It is a shared medium connection

auto: The switch automatically determines whether the interface is attached to a point-to-point link or shared medium.

Negation: (config-stp-aggr)# no spanning-tree link-type

Show: # show spanning-tree

3.10.34.1.6. (config-stp-aggr)# spanning-tree mst <instance> cost

Syntax: (config-stp-aggr)# spanning-tree mst <instance> cost { <cost> | auto }

Explanation: Configure MSTI and its' path cost value.

Parameters:

mst <instance: 0-15>: Specify MST instance number. Specify "0" to denote CIST. Specify "1-15" to denote MSTI 1-15.

cost { <cost> | auto }: Specify a Path cost value that is used to determine the best path between devices. Valid values are 1 to 200000000. If "auto" mode is specified, the system automatically detects the speed and duplex mode to decide the path cost. Please note that path cost takes precedence over port priority.

Negation: (config-stp-aggr)# no spanning-tree mst <instance> cost

Show: # show spanning-tree

3.10.34.1.7. (config-stp-aggr)# spanning-tree mst <instance> port-priority

Syntax: (config-stp-aggr)# spanning-tree mst <instance> port-priority <prio>

Explanation: Configure MSTI and its' port priority.

Parameters:

mst <instance: 0-15>: Specify MST instance number. Specify "0" to denote CIST. Specify "1-15" to denote MSTI 1-15.

port-priority <prio>: Specify a port priority value.

Negation: (config-stp-aggr)# no spanning-tree mst <instance> port-priority

Show: # show spanning-tree

3.10.34.1.8. (config-stp-aggr)# spanning-tree restricted-role

Syntax: (config-stp-aggr)# spanning-tree restricted-role

Explanation: Enable restricted role function. If enabled, this causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority.

Negation: (config-stp-aggr)# no spanning-tree restricted-role

Show: # show spanning-tree

3.10.34.1.9. (config-stp-aggr)# spanning-tree restricted-tcn

Syntax: (config-stp-aggr)# spanning-tree restricted-tcn

Explanation: Enable restricted TCN function. If enabled, this causes the port not to propagate received topology change notifications and topology changes to other ports.

Negation: (config-stp-aggr)# no spanning-tree restricted-tcn

Show: # show spanning-tree

3.10.34.2. (config)# spanning-tree edge bpdu-filter

Syntax: (config)# spanning-tree edge bpdu-filter

Explanation: Enable edge BPDU filtering function. The purpose of Port BPDU Filtering is to prevent the switch from sending BPDU frames on ports that are connected to end devices.

Example: Enable edge BPDU filtering function.

```
# config t
(config)# spanning-tree edge bpdu-filter
```

Negation: (config)# no spanning-tree edge bpdu-filter

Show: # show spanning-tree

3.10.34.3. (config)# spanning-tree edge bpdu-guard

Syntax: (config)# spanning-tree edge bpdu-guard

Explanation: Enable edge BPDU guard function. Edge ports generally connect directly to PC, file servers or printers. Therefore, edge ports are configured to allow rapid transition. Under normal situations, edge ports should not receive configuration BPDUs. However, if they do, this probably is due to malicious attacks or mis-settings. When edge ports receive configuration BPDUs, they will be automatically set to non-edge ports and start a new spanning tree calculation process.

BPDU Guard is therefore used to prevent the device from suffering malicious attacks. With this function enabled, when edge ports receive configuration BPDUs, STP disables those affected edge ports. After a period of recovery time, those disabled ports are re-activated.

Example: Enable edge BPDU guard function.

```
# config t
(config)# spanning-tree edge bpdu-guard
```

Negation: (config)# no spanning-tree edge bpdu-guard

Show: # show spanning-tree

3.10.34.4. (config)# spanning-tree mode

Syntax: (config)# spanning-tree mode { stp | rstp | mstp }

Parameters:

{ stp | rstp | mstp }: Specify one of the STP protocol versions.

Explanation: Configure the desired STP protocol version.

Example: Set the spanning tree mode to MSTP.

```
# config t
(config)# spanning-tree mode mstp
```

Negation: (config)# no spanning-tree mode

Show: # show spanning-tree

3.10.34.5. (config)# spanning-tree mst <instance> priority <prio>

Syntax: (config)# spanning-tree mst <instance> priority <prio>

Parameters:

<instance: 0-7>: Specify an instance ID. “0” means CIST. “1-7” means MSTI 1-7.

<prio: 0-61440>: Specify a priority value.

Explanation: Specify an appropriate priority for a MSTI instance. Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Note that lower numeric values indicate higher priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Example: Map MST Instance 1 to priority 61440.

```
# config t
(config)# spanning-tree mst 1 priority 61440
```

Negation: (config)# no spanning-tree mst <instance> priority

Show: # show spanning-tree

3.10.34.6. (config)# spanning-tree mst <instance> vlan <v_vlan_list>

Syntax: (config)# spanning-tree mst <instance> vlan <v_vlan_list>

Parameters:

<instance: 0-7>: Specify an instance ID. “0” means CIST. “1-7” means MSTI 1-7.

<v_vlan_list>: Specify a list of VLANs for the specified MST instance. Separate VLANs with a comma and use hyphen to denote a range of VLANs. (Example: 2,5,20-40)

Explanation: Specify VLANs mapped to a certain MSTI. Both a single VLAN and a range of VLANs are allowed.

Example: Map MST Instance 1 to VLAN 90 and VLAN 101-105.

```
# config t
(config)# spanning-tree mst 1 vlan 90,101-105
```

Negation: (config)# no spanning-tree mst <instance> vlan

3.10.34.7. (config)# spanning-tree mst forward-time

Syntax: (config)# spanning-tree mst forward-time <fwdtime>

Parameters:

<fwdtime: 4-30>: Specify forward delay value between 4 and 30 (seconds).

Explanation: Fort STP bridges, the Forward Delay is the time spent in each Listening and Learning state before the Forwarding state is entered. This delay occurs when a new bridge comes onto a network.

Example: Set the forward delay to 15 seconds.

```
# config t
(config)# spanning-tree mst forward-time 15
```

Negation: (config)# no spanning-tree mst forward-time

Show: # show spanning-tree

3.10.34.8. (config)# spanning-tree mst max-age

Syntax: (config)# spanning-tree mst max-age <maxage> [forward-time <fwdtime>]

Parameters:

<maxage: 6-40>: Specify the max age value. The valid range is from 6 to 40.

[forward-time <fwdtime>]: Fort STP bridges, the Forward Delay is the time spent in each Listening and Learning state before the Forwarding state is entered. This delay occurs when a new bridge comes onto a network. Valid values are 4-30 seconds.

Explanation: If another switch in the spanning tree does not send out a hello packet for a period of time, it is considered to be disconnected. Valid values are 6 to 40 seconds, and Max Age values must be smaller than or equal to (Forward Delay-1)*2.

Example: Set the max age to 20 seconds.

```
# config t
(config)# spanning-tree mst max-age 20
```

Negation: (config)# no spanning-tree mst max-age

Show: # show spanning-tree

3.10.34.9. (config)# spanning-tree mst max-hops

Syntax: (config)# spanning-tree mst max-hops <maxhops>

Parameters:

<maxhops>: Specify the maximum hop count value. The valid range is from 6 to 40.

Explanation: The maximum number of hops allowed for MST region before a BPDU is discarded. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the BPDU is discarded. The default hop count is 20. The allowed range is 6-40.

Example: Set the maximum hop count to 20.

```
# config t
(config)# spanning-tree mst max-hops 20
```

Negation: (config)# no spanning-tree mst max-hops

Show: # show spanning-tree

3.10.34.10. (config)# spanning-tree mst name

Syntax: (config)# spanning-tree mst name <name> revision <v_0_to_65535>

Parameters:

name <name>: Specify a name for this MSTI. By default, the switch's MAC address is used. The maximum length is 32 characters. In order to share spanning trees for MSTI, bridges must have the same configuration name and revision value.

revision <v_0_to_65535>: Specify a revision number for this MSTI. The allowed range is 0 – 65535.

Explanation: Configure a name and revision number for this MSTI.

Negation: (config)# no spanning-tree mst name

Show: # show spanning-tree

3.10.34.11. (config)# spanning-tree recovery interval

Syntax: (config)# spanning-tree recovery interval <interval>

Parameters:

<interval>: The time that has to pass before a port in the error-disabled state can be enabled. The allowed range is 30 – 86400 (seconds).

Explanation: When enabled, a port that is in the error-disabled state can automatically be enabled after a certain time.

Example: Set the spanning tree recovery interval to 50.

```
# config t
(config)# spanning-tree recovery interval 50
```

Negation: (config)# no spanning-tree recovery interval

Show: # show spanning-tree

3.10.34.12. (config)# spanning-tree transmit hold-count

Syntax: (config)# spanning-tree transmit hold-count <holdcount>

Parameters:

<holdcount:1-10>: Specify the transmit hold-count. The allowed transmit hold count is 1 to 10.

Explanation: The number of BPDU sent by a bridge port per second. When exceeded, transmission of the next BPDU will be delayed. By default, it is set to 6. The allowed transmit hold count is 1 to 10. Please note that increasing this value might have a significant impact on CPU utilization and decreasing this value might slow down convergence. It is recommended to remain Transmit Hold Count to the default setting.

Example: Set the spanning tree transmit hold-count to 6.

```
# config t
(config)# spanning-tree transmit hold-count 6
```

Negation: (config)# no spanning-tree transmit hold-count

Show: # show spanning-tree

3.10.35. (config)# switchport

3.10.35.1. (config)# switchport vlan mapping

Syntax: (config)# switchport vlan mapping <group ID> <vlan_list> <translation_vlan>

Explanation: VLAN Translation is especially useful for users who want to translate the original VLAN ID to a new VLAN ID so as to exchange data across different VLANs and improve VLAN scaling. VLAN translation replaces an incoming C-VLAN tag with an S-VLAN tag instead of adding an additional tag. When configuring VLAN Translation, both ends of the link normally must be able to replace tags appropriately. In other words, both ends must be configured to translate the C-VLAN tag to S-VLAN tag and S-VLAN tag to C-VLAN tag appropriately in a network. Note that only access ports support VLAN translation.   It is not recommended to configure VLAN Translation on trunk ports.

Parameters:

<group ID: 1-7>: Indicate the Group ID that applies to this translation rule.

<vlan_list>: Indicate the VLAN ID that will be mapped to a new VID.

<translation_vlan>: Indicate the new VID to which VID of ingress frames will be changed.

Example: Map the group ID 5 with VLAN ID 100 to be translated to 201.

```
# config t
(config)# switchport vlan mapping 5 100 201
```

Negation: (config)# no switchport vlan mapping <group> <v_vlan_id_from>

3.10.35.2. (config)# switchport vlan mapping <gid> { both | ingress | egress } <vid> <tvid>

Syntax: (config)# switchport vlan mapping <gid> { both | ingress | egress } <vid> <tvid>

Explanation: Map a VLAN to a translated VLAN.

Parameters:

<group ID: 1-7>: Indicate the Group ID that applies to this rule.

{ both | ingress | egress } : Specify the direction of the VLAN Translation. The direction can be 'Ingress', where the translation takes place on the VLAN ID of frames entering the switch port, 'Egress', where the translation takes place on the VLAN ID of frames exiting the switch port, or 'Both', where the translation takes place on both of the above directions.

<vid>: Indicate the VLAN ID that will be mapped to a new VID.

<tvid>: Indicate the new VID to which VID of ingress frames will be changed.

Negation: (config)# no switchport vlan mapping <gid> { both | ingress | egress } <vid>

3.10.36. (config)# tacacs-server

3.10.36.1. (config)# tacacs-server timeout

Syntax: (config)# tacacs-server timeout <seconds>

Explanation: The time the switch waits for a reply from a TACACS+ server before it retransmits the request.

Parameters:

<seconds:1-1000>: Specify a value for timeout. The allowed timeout range is between 1 and 1000.

Negation: (config)# no tacacs-server timeout

Show: # show tacacs-server

3.10.36.2. (config)# tacacs-server deadtime

Syntax: (config)# tacacs-server deadtime <minutes>

Explanation: Deadtime 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.

Parameters:

<minutes:1-1440>: Specify a value for tacacs-server deadtime. The allowed deadtime range is between 1 to 1440 minutes.

Negation: (config)# no tacacs-server deadtime

Show: # show tacacs-server

3.10.36.3. (config)# tacacs-server key

Syntax: (config)# tacacs-server key { [unencrypted] <unencrypted_key> | encrypted <encrypted_key> }

Explanation: Specify the secret key up to 63 characters. This is shared between a TACACS+ sever and the switch.

Parameters:

{ [unencrypted] <unencrypted_key> | encrypted <encrypted_key> }: Specify a shared secret key value (either unencrypted or encrypted).

Negation: (config)# no tacacs-server key

Show: # show tacacs-server

3.10.36.4. (config)# tacacs-server host

Syntax: (config)# tacacs-server host <host_name> [port <port>] [timeout <seconds>] [key <key>]

Explanation: Configure radius server settings.

Parameters:

<host_name>: Specify a hostname or IP address for the TACACS+ server.

[port <port>]: Specify the TCP port number to be used on a TACACS+ server for authentication.

[timeout <seconds>]: If timeout value is specified here, it will replace the global timeout value. If you prefer to use the global value, leave this field blank.

[key <key>]: If secret key is specified here, it will replace the global secret key. If you prefer to use the global value, leave this field blank.

Negation: (config)# no tacacs-server host <host_name> [port <port>]

Show: # show tacacs-server

3.10.37. (config)# thermal-protect

3.10.37.1. (config)# thermal-protect grp

Syntax: (config)# thermal-protect grp <grp_list> temperature <new_temp>

Explanation: Configure the temperature threshold by groups.

Parameters:

grp <grp_list>: Specify the temperature group number. The valid group value is 0~3.

temperature <new_temp>: Specify the threshold temperature for the specified group. The valid temperature range is 0~255.

Negation: (config)# no thermal-protect grp <grp_list>

Show: # show thermal-protect [interface (<port_type> [<plist>])]

3.10.37.2. (config)# thermal-protect fan mode

Syntax: (config)# thermal-protect fan { mode { on | off | auto } }

Explanation: Configure the mode of the fans to protect the device.

Parameters:

{ mode { on | off | auto } }: Fans can be turned on or off manually. Or, if you want to turn on fans automatically when the temperature of the device reaches a certain level, then you can specify “auto”.

Show: # show thermal-protect fan

3.10.37.3. (config)# thermal-protect fan temp-on

Syntax: (config)# thermal-protect fan { temp-on <temp_on_num> }

Explanation: Configure the temperature of the device. Once the temperature of the device reaches this configured temperature, fans will be turned on automatically.

Parameters:

> { temp-on <temp_on_num> }: Specify the threshold temperature. Once the temperature of the device reaches this configured temperature, fans will be turned on automatically.

Show: # show thermal-protect fan

3.10.38. (config)# upnp

3.10.38.1. (config)# upnp

Syntax: (config)# upnp

Explanation: Enable upnp operation.

Example: Enable upnp operation

```
# config t
(config)# upnp
(config)#
```

Negation: (config)# no upnp

Show: # show upnp

3.10.38.2. (config)# upnp advertising-duration

Syntax: (config)# upnp advertising-duration <v_100_to_86400>

Parameters:

> <v_100_to_86400>: Specify the advertising duration. The allowed range is 100 to 86400 (seconds).

Explanation: This defines how often an UPnP advertisement is sent. The duration is carried in Simple Service Discover Protocol (SSDP) packets which informs a control point how often it should receive a SSDP advertisement message from the switch. By default, the advertising duration is set to 100 seconds. However, due to the unreliable nature of UDP, it is recommended to set to the shorter duration since the shorter the duration, the fresher is UPnP status.

Example: Set the upnp advertising duration to 150 seconds.

```
# config t
(config)# upnp advertising-duration 150
```

Negation: (config)# no upnp advertising-duration

Show: # show upnp

3.10.38.3. (config)# upnp ip-addressing-mode

Syntax: (config)# upnp ip-addressing-mode { dynamic | static }

Explanation: Determine IP addressing mode.

Parameters:

{ dynamic | static }: Specify IP addressing mode.

dynamic: 'dymanic' is the default selection for UPnP. UPnP module helps users choosing the IP address of the switch device. It finds the first available sytem IP address.

static: User specifies the IP interface VLAN for choosing the IP address of the switch device.

Negation: (config)# no upnp ip-addressing-mode

Show: # show upnp

3.10.38.4. (config)# upnp static interface vlan

Syntax: (config)# upnp static interface vlan <v_vlan_id>

Explanation: Determine IP VLAN interface for UPnP applications.

Parameters:

<v_vlan_id>: Specify a specific IP VLAN interface. It will only be applied when IP addressing mode is static.

Negation: (config)# no upnp static interface vlan

Show: # show upnp

3.10.39. (config)# username

3.10.39.1. (config)# username { default-administrator | <input_username>} privilege<priv>password encrypted

Syntax: (config)# username { default-administrator | <input_username>} privilege <priv> password encrypted <encry_password>

Explanation: By default, there is only one user, 'admin', assigned the highest privilege level of 15. Use this command to configure a new user account.

Parameters:

username { default-administrator | <input_username>}: Specify a new username. The allowed characters are 31.

privilege <priv: 0-15>: Specify the privilege level for this new user account. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

password encrypted <encry_password: 4-44>: Specify the encrypted password for this new user account. The ENCRYPTED (hidden) user password. Notice the ENCRYPTED password will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.

Example: Create the new user account with the following settings.

```
# config t
(config)# username mis4jack privilege 15 password encrypted jack30125
```

Negation: (config)# no username <username>

Show: > show users

# show users

3.10.39.2. (config)# username { default-administrator | <input_username>} privilege<priv>password none

Syntax: (config)# username { default-administrator | <input_username>} privilege <priv> password none

Explanation: By default, there is only one user, 'admin', assigned the highest privilege level of 15. Use this command to configure a new user account without password

Parameters:

username { default-administrator | <input_username>}: Specify a new username. The allowed characters are 31.

privilege <priv: 0-15>: Specify the privilege level for this new user account. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default, most groups' privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

password none: No password for this user account.

Example: Create the new user account with the following settings.

```
# config t
(config)# username mis4jack privilege 15 password none
```

Negation: (config)# no username <username>

Show: > show users
# show users

3.10.39.3. (config)# username { default-administrator | <input_username>} privilege<priv>password unencrypted

Syntax: (config)# username { default-administrator | <input_username>} privilege <priv> password unencrypted <password>

Explanation: By default, there is only one user, 'admin', assigned the highest privilege level of 15. Use this command to configure a new user account with unencrypted password.

Parameters:

username { default-administrator | <input_username>}: Specify a new username. The allowed characters are 31.

privilege <priv: 0-15>: Specify the privilege level for this new user account. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default, most groups' privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

password unencrypted <password: line31>: Specify the unencrypted password for this user account. The UNENCRYPTED (Plain Text) user password. Any printable characters including space is accepted.

Example: Create the new user account with the following settings.

```
# config t
(config)# username mis4jack privilege 15 password unencrypted jack30125
```

Negation: (config)# no username <username>

Show: > show users

# show users

3.10.40. (config)# vlan

3.10.40.1. (config)# vlan

Syntax: (config)# vlan <vlist>

Explanation: Configure allowed VLANs.

Parameters:

<vlist>: This shows the allowed access VLANs. This setting only affects ports set in “Access” mode. Ports in other modes are members of all VLANs specified in “Allowed VLANs” field. By default, only VLAN 1 is specified. More allowed access VLANs can be entered by specifying the individual VLAN ID separated by comma. If you want to specify a range, separate it by a dash. For example, 1, 5,10,12-15,100. Once Enter is pressed, the prompt changes to (config-vlan)#

Example: Add VID 1,5,10,12-15,100 to the allowed VLAN list.

```
# config t
(config)# vlan 1,510,12-15,100
(config-vlan)#
```

Negation: (config)# no vlan { { ethertype s-custom-port } | <vlan_list> }

3.10.40.2. (config)# vlan ethertype s-custom-port

Syntax: (config)# vlan ethertype s-custom-port <etype>

Explanation: Configure ether type used for customer s-ports.

Parameters:

ethertype s-custom-port <etype>: Specify ether type used for customer s-ports. The valid range is 0x0600 to 0xffff.

Example: Set ether type for customer s-port to 0x88a8.

```
# config t
(config)# vlan ethertype s-custom-port 0x88a8
```

Negation: (config)# no vlan { { ethertype s-custom-port } | <vlan_list> }

3.10.40.3. (config)# vlan protocol

Syntax: (config)# vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } } group <grp_id>

Explanation: The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

Parameters:

protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } }: There are three frame types available for selection; these are “Ethernet”, “SNAP”, and “LLC”. The value field will need to be changed accordingly.

eth2 (Ethernet): Ether Type (etype) value. By default, it is set to 0x0800. The range allowed is 0x0600 to 0xffff.

SNAP: This includes OUI (Organizationally Unique Identifier) and PID (Protocol ID) values.

OUI: A value in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value in the ranges of 0x00-0xff.

PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type field value for the protocol running on top of SNAP. If the OUI is that of a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of the OUI field is 00-

00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI is other than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.

LLC (Logical Link Control): This includes DSAP (Destination Service Access Point) and SSAP (Source Service Access Point) values. By default, the value is 0xff. Valid range is 0x00 to 0xff.

group <grp_id>: Indicate the descriptive name for this entry. This field only allows 16 alphabet characters (a-z; A-Z) or integers (0-9).

Example: Set VLAN protocol to eth2 0x88a8.

```
# config t
(config)# vlan protocol eth2 0x88a8 group a12
```

Negation: (config)# no vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } } group <grp_id>

Show: # show vlan protocol [eth2 { <etype> | arp | ip | ipx | at }] [snap { <oui> | rfc-1042 | snap-8021h } <pid>] [llc <dsap> <ssap>]

3.10.41. (config)# voice vlan

3.10.41.1. (config)# voice vlan

Syntax: (config)# voice vlan

Explanation: Enable voice vlan for voice traffic.

Negation: (config)# no voice vlan

Show: # show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]

3.10.41.2. (config)# voice vlan aging-time

Syntax: (config)# voice vlan aging-time <aging_time>

Explanation: Set voice vlan secure learning aging time.

Parameters:

<AgingTime : 10-10000000>: Specify voice vlan learning aging time. The allowed range is 10-10000000.

Negation: (config)# no voice vlan aging-time

Show: # show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]

3.10.41.3. (config)# voice vlan class

Syntax: (config)# voice vlan class { <traffic_class> | low | normal | medium | high }

Explanation: Set voice vlan secure learning aging time.

Parameters:

{ <traffic_class> | low | normal | medium | high }: Specify voice vlan class value or prioritize voice vlan.

<traffic_class: 0-7>: Specify voice vlan class value. The valid value is 0~7.

Negation: (config)# no voice vlan class

Show: # show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]

3.10.41.4. (config)# voice vlan oui <oui> [description <description>]

Syntax: (config)# voice vlan oui <oui> [description <description>]

Explanation: Set voice vlan secure learning aging time.

Parameters:

<oui>: Specify OUI value.

[description <description>]: Enter the description for this OUI.

Negation: (config)# no voice vlan oui <oui>

Show: # show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]

3.10.41.5. (config)# voice vlan vid

Syntax: (config)# voice vlan vid <vid>

Explanation: Set voice VLAN ID.

Parameters:

<vid>: Specify voice VLAN ID.

Negation: (config)# no voice vlan vid

Show: # show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]

3.10.42. (config)# web privilege group

Syntax: (config)# web privilege group <group_name> level { [configRoPriv <configRoPriv>] [configRwPriv <configRwPriv>] [statusRoPriv <statusRoPriv>] [statusRwPriv <statusRwPriv>] }*1

Explanation: Assign web privilege level to the specified group.

Parameters:

group <group_name>: This name identifies the privilege group. Valid words are Aggregation' 'DHCP' 'Dhcp_Client' 'Diagnostics' 'EEE' 'ERPS' 'Green_Ethernet' 'IP2' 'IPMC_Snooping' 'LACP' 'LLDP' 'Loop_Protect' 'MAC_Table' 'MVR' 'Maintenance' 'Mirroring' 'NTP' 'POE' 'PTP' 'Ports' 'Private_VLANs' 'QoS' 'RPC' 'SMTP' 'Security' 'Smart_Config' 'Spanning_Tree' 'System' 'Timer' 'UPnP' 'VCL' 'VLAN_Translation' 'VLANs' 'XXRP' 'u-Ring'

level { [cro <cro: 0-15>] [crw <crw: 0-15>] [sro <sro: 0-15>] [srw <srw: 0-15>] }*1: Every group has an authorization Privilege level for the following sub groups:

configRoPriv (configuration read-only): The privilege level is 1 to 15.

configRwPriv (configuration/execute read-write): The privilege level is 1 to 15.

statusRoPriv (status/statistics read-only): The privilege level is 1 to 15.

statusRwPriv (status/statistics read-write): The privilege level is 1 to 15.

User Privilege should be the same or greater than the authorization Privilege level to have access to that group.

Example: Assign Aggregation group to crw (configuration/excute read-write) level 15.

```
# config t
(config)# web privilege group aggregation level crw 15
(config)# exit
# show web privilege group level
Group Name                     Privilege Level
                              CRO CRW SRO SRW
-------------------------------- --- --- --- ---
Aggregation                    5   15   5   10
DHCP                           5   10   5   10
Dhcpv6_Client                  5   10   5   10
Diagnostics                    5   10   5   10
Eth_Link OAM                   5   10   5   10
Firmware                       5   10   5   10
Green_Ethernet                 5   10   5   10
GVRP                           5   10   5   10
IP                             5   10   5   10
LACP                           5   10   5   10
LLDP                           5   10   5   10
IPMC Snooping                  5   10   5   10
Loop_Protect                   5    10   5   10
MAC_Table                      5   10   5   10
Maintenance                    15   15  15  15
Mirroring                      5   10   5   10
MVR                            5   10   5   10
NTP                            5   10   5   10
POE                            5   10   5   10
Ports                          5   10   1   10
-- more --, next page: Space, continue: g, quit: ^C
```

Negation: (config)# no web privilege group <group_name> level

Show: > show web privilege group <group_name> level
# show web privilege group <group_name> level

3.11. Commands in Config Interface Mode

To enter Global Config Interface Mode, you need to type one of the following commands after "(config)#" prompt:

```
# config terminal
(config)# interface GigabitEthernet 1/1
(config-if)#
```

3.11.1. (config-if)# access-list

3.11.1.1. (config-if)# access-list action

Syntax: (config-if)# access-list action { permit|deny}

Explanation: Configure a specific port’s action option.

Parameters:

{ permit|deny}: Permit or deny frames on a specific port.

Show: # show access-list [interface [(<port_type> [<v_port_type_list>])]]

3.11.1.2. (config-if)# access-list logging

Syntax: (config-if)# access-list logging

Explanation: Enable a specific port’s logging function.

Show: # show access-list [interface [(<port_type> [<v_port_type_list>])]]

Negation: (config-if)# no access-list logging

3.11.1.3. (config-if)# access-list mirror

Syntax: (config-if)# access-list mirror

Explanation: Enable a specific port's mirroring function on an ACL basis. If enabled, frames received on this port will be mirror.

Show: # show access-list [interface [(<port_type> [<v_port_type_list>])]]

Negation: (config-if)# no access-list mirror

3.11.1.4. (config-if)# access-list policy

Syntax: (config-if)# access-list policy <policy_id>

Parameters:

<policy_id:0-255>: Specify a policy ID that applies to this specific port.

Explanation: Apply a policy ID to a specific port.

Show: # show access-list [interface [(<port_type> [<v_port_type_list>])]]

Negation: (config-if)# no access-list policy

3.11.1.5. (config-if)# access-list port-state

Syntax: (config-if)# access-list port-state

Explanation: Enable a specific port's port state.

Negation: (config-if)# no access-list port-state

3.11.1.6. (config-if)# access-list rate-limiter

Syntax: (config-if)# access-list rate-limiter <rate_limiter_id>

Parameters:

<rate_limiter_id:1-16>: Specify a rate limiter ID to a specific port.

Explanation: Apply a rate limiter ID to a specific port.

Negation: (config-if)# no access-list rate-limiter

3.11.1.7. (config-if)# access-list shutdown

Syntax: (config-if)# access-list shutdown

Explanation: Shutdown this port when specified rules are matched.

Negation: (config-if)# no access-list shutdown

3.11.1.8. (config-if)# access-list {redirect }

Syntax: (config-if)# access-list { redirect } interface { <port_type> <port_type_id> | (<port_type> [<port_type_list>]) }

Parameters:

{ redirect }: Redirect this port's frames to the specified port.

interface { <port_type> <port_type_id> | (<port_type> [<port_type_list>]) }: Specify the redirect or copy port type and port list.

Explanation: Redirect or copy this port's frames to the specified port.

Negation: (config-if)# no access-list { redirect | port-copy }

3.11.2. (config-if)# aggregation group

Syntax: (config-if)# aggregation group <v_uint> mode { [active | on | passive] }

Explanation: Add this specific interface to the specified aggregation group.

Parameters:

<unit>: Specify the aggregation group ID.

{ [active | on | passive] }: Configure the specified interface to active LACP, passive LACP or static aggregation.

Negation: (config-if)# no aggregation group

Show: # show aggregation [mode]

3.11.3. (config-if)# description

Syntax: (config-if)# description <desc_str>

Explanation: Specify a descriptive information for the selected interface.

Negation: (config-if)# no description

3.11.4. (config-if)# dot1x

3.11.4.1. (config-if)# dot1x port-control

Syntax: (config-if)# dot1x port-control { force-authorized | force-unauthorized | auto | single | multi | mac-based }

Parameters:

{ force-authorized | force-unauthorized | auto | single | multi | mac-based }: Specify one of the authentication modes on the selected interfaces. This setting works only when NAS is globally enabled. The following modes are available:

force-authorized: In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

force unauthorized: In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

auto (Port-Based 802.1X): This mode requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.

single (802.1X): In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the “Port Security” module is used to secure a supplicant's MAC address once successfully authenticated.

multi (802.1X): In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the “Port Security” module.

mac-based: Unlike port-based 802.1X, MAC-based authentication do not transmit or receive EAPOL frames. In MAC-based authentication, 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.

Example: Set Gigabit Ethernet port 1 & 2’s admin state to “auto”

```
# config t
(config)# interface gigabitethernet 1/1-2
(config-if)# dot1x port-control auto
```

Negation: (config-if)# no dot1x port-control

3.11.4.2. (config-if)# dot1x guest-vlan

Syntax: (config-if)# dot1x guest-vlan

Explanation: Enable the guest VLAN on the selected interfaces.

Parameters: None.

Example: Enable guest VLAN on port 1-2.

```
# config t
(config)# interface gigabitethernet 1/1-2
(config-if)# dot1x guest-vlan
```

Negation: (config-if)# no dot1x guest-vlan

3.11.4.3. (config-if)# dot1x radius-qos

Syntax: (config-if)# dot1x radius-qos

Explanation: Enable RADIUS Assigned QoS on the selected interfaces.

Parameters: None.

Example: Enable RADIUS Assigned QoS on port 1-2.

```
# config t
(config)# interface gigabitethernet 1/1-2
(config-if)# dot1x radius-qos
```

Negation: (config-if)# no dot1x radius-qos

3.11.4.4. (config-if)# dot1x radius-vlan

Syntax: (config-if)# dot1x radius-vlan

Explanation: Enable RADIUS Assigned VLAN on the selected interfaces.

Parameters: None.

Example: Enable RADIUS Assigned VLAN on port 1-2.

```
# config t
(config)# interface gigabitethernet 1/1-2
(config-if)# dot1x radius-vlan
```

Negation: (config-if)# no dot1x radius-vlan

3.11.4.5. (config-if)# dot1x re-authenticate

Syntax: (config-if)# dot1x re-authenticate

Explanation: Schedules reauthentication to whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. This command only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

Show: > show dot1x statistics { eapol | radius | all } [interface (<port_type> [<v_port_type_list>])]
# show dot1x statistics { eapol | radius | all } [interface (<port_type> [<v_port_type_list>])]

3.11.5. (config-if)# duplex

Syntax: (config-if)# duplex { half | full | auto [half | full] }

Explanation: Configure port's duplex mode.

Parameters:

{ half | full | auto [half | full] }: Specify the duplex mode for this specific interface.

Example: Set port 1's duplex mode to auto.

```
# config t
(config)# interface gigabitethernet 1/1
(config-if)# duplex auto
```

Negation: (config-if)# no duplex

Show: > show interface (<port_type> [<v_port_type_list>]) status
# show interface (<port_type> [<v_port_type_list>]) status

3.11.6. (config-if)# excessive-restart

Syntax: (config-if)# excessive-restart

Explanation: Restart backoff algorithm after 16 collisions (No excessive-restart means discard frames after 16 collisions.)

Negation: (config-if)# no excessive-restart

Show: > show interface (<port_type> [<v_port_type_list>]) status
# show interface (<port_type> [<v_port_type_list>]) status

3.11.7. (config-if)# flowcontrol { on | off }

Syntax: (config-if)# flowcontrol { on | off }

Explanation: Enable or disable flow control for this specific interface.

Parameters:

{ on | off }: Enable or disable flow control.

Negation: (config-if)# no flowcontrol

Show: > show interface (<port_type> [<v_port_type_list>]) status
# show interface (<port_type> [<v_port_type_list>]) status

3.11.8. (config-if)# frame-length-check

Syntax: (config-if)# frame-length-check

Explanation: Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actually payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. Note: No drop counters count frames dropped due to frame length mismatch.

Negation: (config-if)# no frame-length-size

3.11.9. (config-if)# green-ethernet

3.11.9.1. (config-if)# green-ethernet eee

Syntax: (config-if)# green-ethernet eee

Explanation: Enable EEE (Energy-Efficient Ethernet) on the selected interface.

Negation: (config-if)# no green-ethernet eee

Show: # show green-ethernet eee [interface (<port_type> [<port_list>])]

3.11.9.2. (config-if)# green-ethernet urgent-queues

Syntax: (config-if)# green-ethernet eee urgent-queues [<urgent_queue_range_list>]

Explanation: It is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

Parameters:

[<urgent_queue_range_list>]: Specify urgent queue range. The allowed range is from 1 to 8.

Negation: (config-if)# no green-ethernet eee urgent-queues [<urgent_queue_range_list>]

3.11.9.3. (config-if)# green-ethernet energy-detect

Syntax: (config-if)# green-ethernet energy-detect

Explanation: Enable power saving function for this specific interface when there is no link partner.

Negation: (config-if)# no green-ethernet energy-detect

Show: # show green-ethernet energy-detect [interface (<port_type> [<port_list>])]

3.11.9.4. (config-if)# green-ethernet short-reach

Syntax: (config-if)# green-ethernet short-reach

Explanation: Enable power saving for ports which is connect to link partner with short cable.

Negation: (config-if)# no green-ethernet short-reach

Show: # show green-ethernet short-reach [interface (<port_type> [<port_list>])]

3.11.10. (config-if)# gvrp

Syntax: (config-if)# gvrp

Explanation: Enable GVRP function on the specified interfaces.

Parameters: None.

Example: Enable GVRP function on port 1~2.

```
# config t
(config)# interface GigabitEthernet 1/1-2
(config-if)# gvrp
(config-if)#
```

Negation: (config-if)# no gvrp

3.11.11. (config-if)# ip

3.11.11.1. (config-if)# ip arp inspection check-vlan

Syntax: (config-if)# ip arp inspection check-vlan

Explanation: Enable check vlan function.

Negation: (config-if)# no ip arp inspection check-vlan

3.11.11.2. (config-if)# ip arp inspection logging

Syntax: (config-if)# ip arp inspection logging { deny | permit | all }

Explanation: Enable log function on a specific interface.

Parameters:

{ deny | permit | all }: Specify one of the log types.

deny: Log denied entries.

permit: Log permitted entries.

all: Log all entries.

Negation: (config-if)# no ip arp inspection logging

3.11.11.3. (config-if)# ip arp inspection trust

Syntax: (config-if)# ip arp inspection trust

Explanation: Enable trust state on the selected interfaces.

Negation: (config-if)# no ip arp inspection trust

3.11.11.4. (config-if)# ip dhcp snooping trust

Syntax: (config-if)# ip dhcp snooping trust

Explanation: Set this interface to DHCP Snooping trusted port.

Negation: (config-if)# no ip dhcp snooping trust

Show: > show ip dhcp snooping [interface (<port_type> [<in_port_list>])]
# show ip dhcp snooping [interface (<port_type> [<in_port_list>])]

3.11.11.5. (config-if)# ip igmp snooping filter

Syntax: (config-if)# ip igmp snooping filter <profile_name>

Explanation: Use this command to filter specific multicast traffic on a per port basis.

Parameters:

<profile_name>: Specify the configured multicast groups that are denied on a port. When a certain multicast group is selected on a port, IGMP join reports received on a port are dropped.

Negation: (config-if)# no ip igmp snooping filter

Show: > show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.11.11.6. (config-if)# ip igmp snooping immediate-leave

Syntax: (config-if)# ip igmp snooping immediate-leave

Explanation: Enable fast leave function on a specific port. When a leave packet is received, the switch immediately removes it from a multicast service without sending an IGMP group-specific (GS) query to that interface.

Negation: (config-if)# no ip igmp snooping immediate-leave

Show: > show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.11.11.7. (config-if)# ip igmp snooping max-groups

Syntax: (config-if)# ip igmp snooping max-groups <throttling>

Explanation: Specify the maximum number of multicast groups that a port can join at the same time.

Parameters:

<throttling>: This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new IGMP join reports will be dropped. By default, unlimited is selected. The allowed range can be specified is 1 to 10.

Negation: (config-if)# no ip igmp snooping max-groups

Show: > show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.11.11.8. (config-if)# ip igmp snooping mrouter

Syntax: (config-if)# ip igmp snooping mrouter

Explanation: Set this interface to Router port. If IGMP snooping cannot locate the IGMP querier, you can manually designate a port which is connected to a known IGMP querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Negation: (config-if)# no ip igmp snooping mrouter

Show: > show ip igmp snooping mrouter [detail]
# show ip igmp snooping mrouter [detail]

3.11.11.9. (config-if)# ip verify source

Syntax: (config-if)# ip verify source

Explanation: Enable IP Source Guard on this interface

Negation: (config-if)# no ip verify source

Show: > show ip verify source [interface (<port_type> [<in_port_type_list>])]
# show ip verify source [interface (<port_type> [<in_port_type_list>])]

3.11.11.10. (config-if)# ip verify source limit

Syntax: (config-if)# ip verify source limit <0-2>

Explanation: Specify the maximum number of dynamic clients that can be learned on a port. The available options are 0, 1, 2. If the port mode is enabled and the maximum number of dynamic clients is equal 0, the switch will only forward IP packets that are matched in static entries for a given port.

Parameters:

<0-2>: Specify the maximum number of dynamic clients that can be learned on a port.

Negation: (config-if)# no ip verify source limit

Show: > show ip verify source [interface (<port_type> [<in_port_type_list>])]
# show ip verify source [interface (<port_type> [<in_port_type_list>])]

3.11.12. (config-if)# ipv6

3.11.12.1. (config-if)# ipv6 mld snooping filter

Syntax: (config-if)# ipv6 mld snooping filter <profile_name>

Explanation: Use this command to filter specific multicast traffic on a per port basis.

Parameters:

<profile_name>: Specify the configured multicast groups that are denied on a port. When a certain multicast group is selected on a port, IGMP join reports received on a port are dropped.

Negation: (config-if)# no ipv6 mld snooping filter

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]
# show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3.11.12.2. (config-if)# ipv6 mld snooping immediate-leave

Syntax: (config-if)# ipv6 igmp snooping immediate-leave

Explanation: Enable fast leave function on a specific port. When a leave packet is received, the switch immediately removes it from a multicast service without sending an IGMP group-specific (GS) query to that interface.

Negation: (config-if)# no ipv6 mld snooping immediate-leave

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]
# show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]

3.11.12.3. (config-if)# ipv6 mld snooping max-groups

Syntax: (config-if)# ipv6 mld snooping max-groups <throttling>

Explanation: Specify the maximum number of multicast groups that a port can join at the same time.

Parameters:

<throttling>: This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new IGMP join reports will be dropped. By default, unlimited is selected. The allowed range can be specified is 1 to 10.

Negation: (config-if)# no ipv6 mld snooping max-groups

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]
# show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]

3.11.12.4. (config-if)# ipv6 mld snooping mrouter

Syntax: (config-if)# ipv6 mld snooping mrouter

Explanation: Set this interface to Router port. If IGMP snooping cannot locate the IGMP querier, you can manually designate a port which is connected to a known IGMP querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Negation: (config-if)# no ipv6 mld snooping mrouter

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]
> show ipv6 mld snooping mrouter [detail]
# show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]
# show ipv6 mld snooping mrouter [detail]

3.11.12.5. (config-if)# ipv6 verify source

Syntax: (config-if)# ipv6 verify source

Explanation: Enable IPv6 Source Guard on this interface

Negation: (config-if)# no ipv6 verify source

Show: > show ipv6 verify source [interface (<port_type> [<in_port_type_list>])]
# show ipv6 verify source [interface (<port_type> [<in_port_type_list>])]

3.11.12.6. (config-if)# ipv6 verify source limit

Syntax: (config-if)# ipv6 verify source limit <max_dynamic_clients>

Explanation: Specify the maximum number of dynamic clients that can be learned on a port. The available options are 0~32. If the port mode is enabled and the maximum number of dynamic clients is equal 0, the switch will only forward IPv6 packets that are matched in static entries for a given port.

Parameters:

<max_dynamic_clients>: Specify the maximum number of dynamic clients that can be learned on a port. The values available are 0~32.

Negation: (config-if)# no ipv6 verify source limit

Show: > show ipv6 verify source [interface (<port_type> [<in_port_type_list>])]
# show ipv6 verify source [interface (<port_type> [<in_port_type_list>])]

3.11.13. (config-if)# lacp

3.11.13.1. (config-if)# lacp

Syntax: (config-if)# lacp

Explanation: Enable LACP on this interface.

Example: Enable LACP on port 1.

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)# lacp
(config-if)#
```

Negation: (config-if)# no lacp

Show: # show lacp { internal | statistics | system-id | neighbour }

Clear: # clear lacp statistics

3.11.13.2. (config-if)# lacp port-priority <v_1_to_65535>

Syntax: (config-if)# lacp port-priority <v_1_to_65535>

Explanation: Configure a LACP key for this interface.

Parameters:

<v_1_to_65535>}: Specify a LACP port priority for this interface. The lower number means greater priority. This priority value controls which ports will be active and which ones will be in a backup role.

Negation: (config-if)# no lacp port-priority <v_1_to_65535>

Show: # show lacp { internal | statistics | system-id | neighbour }

3.11.13.3. (config-if)# lacp timeout { fast | slow }

Syntax: (config-if)# lacp timeout { fast | slow }

Explanation: Configure timeout mode.

Parameters:

{ fast | slow }: The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.

Negation: (config-if)# no lacp timeout { fast | slow }

Show: # show lacp { internal | statistics | system-id | neighbour }

3.11.14. (config-if)# lldp

3.11.14.1. (config-if)# lldp cdp-aware

Syntax: (config-if)# lldp cdp-aware

Explanation: Configures if the interface shall be CDP aware (CDP discovery information is added to the LLDP neighbor table).

Example: Set interface 1 to CDP aware.

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)# lldp cdp-aware
```

Negation: (config-if)# no lldp cdp-aware

Show: > show lldp neighbors [interface (<port_type> [<v_port_type_list>])]
# show lldp neighbors [interface (<port_type> [<v_port_type_list>])]

3.11.14.2. (config-if)# lldp med media-vlan policy-list

Syntax: (config-if)# lldp med media-vlan policy-list <v_range_list>

Explanation: To apply MED Media-VLAN policy of LLDP on this interface.

Parameters:

<v_range_list>: Assign a policy to this interface.

Negation: (config-if)# no lldp med media-vlan policy-list <v_range_list>

Show: > show lldp med media-vlan-policy [<v_0_to_31>]
# show lldp med media-vlan-policy [<v_0_to_31>]

3.11.14.3. (config-if)# lldp med transmit-tlv

Syntax: (config-if)# lldp med transmit-tlv [capabilities] [location] [network-policy]

Explanation: To configure LLDP-MED TLV Type for specific interface.

Parameters:

[capabilities]: Enable transmission of the optional capabilities TLV.

[location]: Enable transmission of the optional location TLV.

[network-policy]: Enable transmission of the optional network policy TLV.

Negation: (config-if)# no lldp med transmit-tlv [capabilities] [location] [network-policy]

Show: > show lldp med media-vlan-policy [<v_0_to_31>]
# show lldp med media-vlan-policy [<v_0_to_31>]

3.11.14.4. (config-if)# lldp med type { connectivity | end-point }

Syntax: (config-if)# lldp med type { connectivity | end-point }

Explanation: Any LLDP-MED device operates as a specific type of LLDP-MED device, which may be either a Network Connectivity Device or a specific Class of Endpoint Device, as defined below.

A Network Connectivity Device is a LLDP-MED Device that provides access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. A LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

1. LAN Switch/Router

2. IEEE 802.1 Bridge

3. IEEE 802.3 Repeater (included for historical reasons)

4. IEEE 802.11 Wireless Access Point

5. Any device that supports the IEEE 802.1AB and MED extensions that can relay IEEE 802 frames via any method.

An Endpoint Device is a LLDP-MED Device that sits at the network edge and provides some aspect of IP communications service, based on IEEE 802 LAN technology.

The main difference between a Network Connectivity Device and an Endpoint Device is that only an Endpoint Device can start the LLDP-MED information exchange.

Even though a switch always should be a Network Connectivity Device, it is possible to configure it to act as an Endpoint Device, and thereby start the LLDP-MED information exchange (In the case where two Network Connectivity Devices are connected together).

Negation: (config-if)# no lldp med type

Show: > show lldp med media-vlan-policy [<v_0_to_31>]
# show lldp med media-vlan-policy [<v_0_to_31>]

3.11.14.5. (config-if)# lldp receive

Syntax: (config-if)# lldp receive

Explanation: The switch will analyze LLDP information received from neighbours.

Negation: (config-if)# no lldp receive

Show: > show lldp statistics [interface (<port_type> [<v_port_type_list>])]
# show lldp statistics [interface (<port_type> [<v_port_type_list>])]

3.11.14.6. (config-if)# lldp tlv-select

Syntax: (config-if)# lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name }

Explanation: To configure LLDP-MED TLV attributes for specific interface.

Parameters:

{ management-address | port-description | system-capabilities | system-description | system-name }: Specify a LLDP TLV attribute. LLDP uses several attributes to discover neighbour devices. These attributes contains type, length, and value descriptions and are referred to TLVs. Details such as port description, system name, system description, system capabilities, management address can be sent from this device.

Negation: (config-if)# no lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name }

Show: > show lldp neighbors [interface (<port_type> [<v_port_type_list>])]
# show lldp neighbors [interface (<port_type> [<v_port_type_list>])]

3.11.14.7. (config-if)# lldp transmit

Syntax: (config-if)# lldp transmit

Explanation: To configure LLDP Tx only mode for specific interface

Negation: (config-if)# no lldp transmit

Show: # show lldp statistics [interface (<port_type> [<v_port_type_list>])]

3.11.15. (config-if)# loop-protect

3.11.15.1. (config-if)# loop-protect

Syntax: (config-if)# loop-protect

Explanation: Enable loop protection function on this interface.

Negation: (config-if)# no loop-protect

Show: # show loop-protect [interface (<port_type> [<plist>])]

3.11.15.2. (config-if)# loop-protect action

Syntax: (config-if)# loop-protect action { [shutdown] [log] }

Explanation: Configure the action taken when loops are detected on a port.

Parameters:

> { [shutdown] [log] }: When a loop is detected on a port, the loop protection will immediately take appropriate actions. Actions will be taken include "Shutdown Port", "Shutdown Port and Log" or "Log Only".

Negation: (config-if)# no loop-protect action

Show: # show loop-protect [interface (<port_type> [<plist>])]

3.11.15.3. (config-if)# loop-protect tx-mode

Syntax: (config-if)# loop-protect tx-mode

Explanation: Enable a port to actively generate loop protection PDUs.

Negation: (config-if)# no loop-protect tx-mode

Show: # show loop-protect [interface (<port_type> [<plist>])]

3.11.16. (config-if)# mac

3.11.16.1. (config-if)# mac address-table learning

Syntax: (config)# mac address-table learning [secure]

Explanation: Set this interface to secure mode.

Parameters:

[secure]: Only static MAC entries listed in "Static MAC Table Configuration" are learned. Others will be dropped.

***NOTE:** Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.*

Negation: (config-if)# no mac address-table learning [secure]

Show: > show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]
# show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]

Clear: # clear mac address-table

3.11.16.2. (config-if)# mac address-table unknown-unicast destination

Syntax: mac address-table unknown-unicast destination

Explanation: Allow egress frames with unknown unicast MAC address to the specified port or ports.

Negation: (config-if)# no mac address-table unknown-unicast destination

Show: # show mac address-table unknown-unicast destination

3.11.17. (config-if)# media-type

Syntax: (config-if)# media-type { rj45 | sfp | dual }

Explanation: Configure the media type supported for this specific interface.

Parameters:

{ rj45 | sfp | dual }: The options are RJ-45, SFP, or dual (both RJ-45 & SFP are supported.).

Negation: (config-if)# no media-type

3.11.18. (config-if)# mtu

Syntax: (config-if)# mtu <max_length>

Explanation: Configure the maximum transmission unit for this specific interface.

Parameters:

<max_length: 1518-10240>}: Specify the MTU. The range is 1518 to 10240 bytes.

Negation: (config-if)# no mtu

Show: # show interface (<port_type> [<v_port_type_list>]) status

3.11.19. (config-if)# mvr

3.11.19.1. (config-if)# mvr immediate-leave

Syntax: (config-if)# mvr immediate-leave

Explanation: Enable immediate leave function. When enabled, the device immediately removes a port from a multicast stream as soon as it receives leave message for that group. This option only applies to an interface configured as MVR receivers.

Example: Enable immediate leave function on port 1.

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)# mvr immediate-leave
```

Negation: (config-if)# no mvr immediate leave

3.11.19.2. (config-if)# mvr name

Syntax: (config-if)# mvr name <mvr_name> type { source | receiver }

Explanation: Configure port role of specific MVR profile for specific interface.

Parameters:

<mvr_name>: Specify a MVR name. The maximum length of the MVR name string is 16. Both alphabets and numbers are allowed for use.

{ source | receiver }: Specify MVR port role.

source: MVR source port.

receiver: MVR receiver port.

Negation: (config-if)# no mvr name <mvr_name> type

3.11.19.3. (config-if)# mvr vlan

Syntax: (config-if)# mvr vlan <v_vlan_list> type { source | receiver }

Explanation: Configure port role of a specific MVR VLAN ID for this specific interface.

Parameters:

<v_vlan_list>: MVR Multicast VLAN list

{ source | receiver }: Specify MVR port role.

source: MVR source port.

receiver: MVR receiver port.

Negation: (config-if)# no mvr immediate leave

3.11.20. (config-if)# port-security

3.11.20.1. (config-if)# port-security

Syntax: (config-if)# port-security

Explanation: Enable the port security function on the selected ports.

Example: Enable Gigabit Ethernet port 1-2's port security function.

```
# config t
(config)# interface Gigabitethernet 1/1-2
(config-if)# port-security
```

Negation: (config-if)# no port-security

Show: > show port-security switch [interface (<port_type> [<v_port_type_list>])]
# show port-security switch [interface (<port_type> [<v_port_type_list>])]

3.11.20.2. (config-if)# port-security maximum

Syntax: (config-if)# port-security maximum [<v_1_to_1024>]

Explanation: The maximum number of MAC addresses that can be secured on this port. The number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

Parameters:

[<v_1_to_1024>]: Specify a value between 1 and 1024.

Example: Limit Gigabit Ethernet port 1-2's MAC addresses can be learnt to 5.

```
# config t
(config)# interface gigabitethernet 1/1-2
(config-if)# port-security maximum 5
```

Negation: (config-if)# no port-security maximum

Show: > show port-security port [interface (<port_type> [<v_port_type_list>])]
# show port-security port [interface (<port_type> [<v_port_type_list>])]

3.11.20.3. (config-if)# port-security maximum-violation

Syntax: (configt-if)# port-security maximum-violation [<v_1_to_1024>]

Explanation: The maximum number of MAC addresses that can be marked as violating on this port. The number cannot exceed 1024. This value is only used when Violation mode is "Restrict".

Parameters:

[<v_1_to_1024>]: Specify a value between 1 and 1024.

Negation: (configt-if)# no port-security maximum-violation

Show: > show port-security port [interface (<port_type> [<v_port_type_list>])]
# show port-security port [interface (<port_type> [<v_port_type_list>])]

3.11.20.4. (config-if)# port-security violation

Syntax: (config-if)# port-security violation { protect | restrict | shutdown }

Explanation: If the limit is exceeded, the specified action will take effect.

Parameters:

{ protect | restrict | shutdown }: Specify one of the actions taken when the limit is exceeded.

protect: Do not allow more than the specified limit of MAC addresses to access on a port. No action is further taken.

restrict: If Limit is reached, subsequent MAC addresses on the port will be counted and marked as violating. Such MAC addresses are removed from the MAC table when the hold time expires.

shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new addresses will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:
* Boot the switch
* Disable and re-enable Limit Control on the port or the switch
* Click the “Reopen” button

Negation: (config-if)# no port-security violation

Show: > show port-security port [interface (<port_type> [<v_port_type_list>])]
# show port-security port [interface (<port_type> [<v_port_type_list>])]

3.11.21. (config-if)# pvlan

3.11.21.1. (config-if)# pvlan

Syntax: (config-if)# pvlan <pvlan_list>

Explanation: This command is used to configure private VLANs. New Private VLANs can be added and existing VLANs can be modified. Private VLANs are based on the source port mask and there are no connections to VLANs which means that VLAN IDs and Private VLAN IDs can be identical. A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Parameters:

<pvlan_list>: Specify the private VLAN ID.

Negation: (config-if)# no pvlan <pvlan_list>

Show: # show pvlan <pvlan_list>

3.11.21.2. (config-if)# pvlan isolation

Syntax: (config-if)# pvlan isolation

Explanation: Enable Port Isolation function on this specific interface. Port Isolation is used to prevent communications between customer ports in a same Private VLAN. The port that is isolated from others cannot forward any unicast, multicast or broadcast traffic to any other ports in the same PVLAN.

Negation: (config-if)# no pvlan isolation

Show: # show pvlan isolation [interface (<port_type> [<plist>])]

3.11.22. (config-if)# qos

3.11.22.1. (config-if)# qos class

Syntax: (config-if)# qos class <cosid>

Explanation: Configure Class of Service ID on this selected interface.

Parameters:

<cosid>: Specify COS value (0-7).

Negation: (config-if)# no qos class

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.2. (config-if)# qos cos

Syntax: (config-if)# qos cos <cos>

Explanation: Configure CoS value on this selected interface.

Parameters:

<cos>: Specify COS value (1-7).

Negation: (config-if)# no qos cos

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.3. (config-if)# qos dei

Syntax: (config-if)# qos dei <dei>

Explanation: Configure DEI (Drop Eligible Indicator) value on this selected interface.

Parameters:

<dei>: Specify DEI for untagged frames.

Negation: (config-if)# no qos dei

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.4. (config-if)# qos dpl

Syntax: (config-if)# qos dpl <dpl>

Explanation: Configure DPL value on this selected interface.

Parameters:

<dpl>: Specify the default Drop Precedence Level

Negation: (config-if)# no qos dpl

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation]

[dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.5. (config-if)# qos dscp-classify

Syntax: (config-if)# qos dscp-classify { zero | selected | any }

Explanation: Configure a classification method.

Parameters:

{ zero | selected | any }: Specify a classification method.

zero: Classify if incoming DSCP is 0.

selected: Classify only selected DSCP for which classification is enabled in DSCP Translation table

any: Classify all DSCP.

Negation: (config-if)# no qos dscp-classify

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.6. (config-if)# qos dscp-remark

Syntax: (config-if)# qos dscp-remark { rewrite | remap | remap-dp }

Explanation: Configure port egress rewriting of DSCP values.

Parameters:

{ rewrite | remap | remap-dp }: Specify an option.

rewrite: Rewrite DSCP field with classified DSCP value.

remap: Frame with DSCP from analyzer is remapped and remarked with the remapped DSCP value. Depending on the frame’s DP level, the remapped DSCP value is either taken from the DSCP Translation table, Egress Remap DP0 or DP1 field.

remap-dp: Frame with DSCP from analyzer is remapped and remarked with the remapped DSCP value. The remapped DSCP value is always taken from the DSCP Translation table, Egress Remap DP0 field.

Negation: (config-if)# no qos dscp-remark

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.7. (config-if)# qos dscp-translate

Syntax: (config-if)# qos dscp-translate

Explanation: Configure DSCP ingress translation of QoS for specific interface.

Negation: (config-if)# no qos dscp-translate

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.8. (config-if)# qos map cos-tag cos

Syntax: (config-if)# qos map cos-tag cos <cos> dpl <dpl> pcp <pcp> dei <dei>

Explanation: Configure (QoS class, DP level) to (PCP, DEI) Mapping of QoS for specific interface.

Parameters:

cos <cos: 0-7>: Specify a QoS class value.

dpl <dpl:0-1>: Specify a DPL value (0 or 1).

pcp <pcp: 0-7>: Specify a PCP (Priority Code Point) value.

dei <dei: 0-1>: Specify a DEI value (0 or 1).

Negation: (config-if)# no qos map cos-tag cos <cos> dpl <dpl>

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.9. (config-if)# qos map tag-cos pcp

Syntax: (config-if)# qos map tag-cos pcp <pcp> dei <dei> cos <cos> dpl <dpl>

Explanation: Configure (PCP, DEI) to (QoS class, DP level) Mapping of QoS for specific interface.

Parameters:

pcp <pcp: 0-7>: Specify a PCP (Priority Code Point) value.

dei <dei: 0-1>: Specify a DEI value (0 or 1).

cos <cos: 0-7>: Specify a QoS class value.

dpl <dpl:0-1>: Specify a DPL value (0 or 1).

Negation: (config-if)# no qos map tag-cos pcp <pcp> dei <dei>

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.10. (config-if)# qos pcp

Syntax: (config-if)# qos pcp <pcp>

Explanation: Configure PCP value for specific interface.

Parameters:

pcp <pcp: 0-7>: Specify a PCP (Priority Code Point) value.

Negation: (config-if)# no qos pcp

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.11. (config-if)# qos policer

Syntax: (config-if)# qos policer <rate> [kbps| mbps| fps | kfps] [flowcontrol]

Explanation: Configure PCP value for specific interface.

Parameters:

< rate >: Indicate the rate for the policer. By default, 500kbps is used. The allowed range for kbps and fps is 100 to 1000000. The allowed range for Mbps and kfps is 1 to 3300Mbps.

[kbps| mbps| fps | kfps]: Specify the desired rate unit. By default, kbps is used.

[flowcontrol]: Enable Flow Control. If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames

Negation: (config-if)# no qos policer

Show: # show qos

# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.12. (config-if)# qos queue-policer queue

Syntax: (config-if)# qos queue-policer queue <queue> <rate> [kbps | mbps]

Explanation: Configure Ingress Queue Policers Rate of QoS for specific interface.

Parameters:

<queue: 0-7>: Specify a queue or a range.

<rate: 1-13107100>: Specify Policer rate.

[kbps | mbps]: Specify the rate unit.

Negation: (config-if)# no qos queue-policer queue <queue>

Show: # show qos

# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.13. (config-if)# qos queue-shaper queue

Syntax: (config-if)# qos queue-shaper queue <queue> <rate> [kbps | mbps] [rate-type { line | data }]

Explanation: Configure Egress Queue Policers Rate of QoS for specific interface.

Parameters:

<queue: 0-7>: Specify a queue or a range.

<rate: 1-13107100>: Specify Policer rate.

[kbps | mbps]: Specify the rate unit. By default, kbps is used.

[rate-type { line | data }]: Specify the shaping rate type. It can operate on line or data rate

Negation: (config-if)# no qos queue-shaper queue <queue>

Show: # show qos

# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.14. (config-if)# qos shaper

Syntax: (config-if)# qos shaper <rate> [kbps | mbps] [rate-type { line | data }]

Explanation: Configure Egress Queue Policers Rate of QoS for specific interface.

Parameters:

<rate: 1-13107100>: Specify Policer rate.

[kbps | mbps]: Specify the rate unit. By default, kbps is used.

[rate-type { line | data }]: Specify the shaping rate type. It can operate on line or data rate

Negation: (config-if)# no qos shaper

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.15. (config-if)# qos tag-remark

Syntax: (config-if)# qos tag-remark { pcp <pcp> dei <dei> | mapped }

Explanation: Configure the appropriate remarking mode used by this port.

Parameters:

{ pcp <pcp> dei <dei> | mapped }: Specify a remarking mode.

pcp <pcp> dei <dei>: Specify PCP and DEI value.

mapped: Use the mapping of the classified QoS class values and DP levels to PCP/DEI values.

Negation: (config-if)# no qos tag-remark

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.16. (config-if)# qos trust dscp

Syntax: (config-if)# qos trust dscp

Explanation: Enable DSCP Classification of QoS for specific interface.

Negation: (config-if)# no qos trust dscp

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.17. (config-if)# qos trust tag

Syntax: (config-if)# qos trust tag

Explanation: Enable VLAN tag Classification of QoS for specific interface.

Negation: (config-if)# no qos trust tag

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.18. (config-if)# qos wred-group

Syntax: (config-if)# qos wred-group <wred_group>

Explanation: Assign QoS WRED group to this specific interface.

Parameter:

<wred_group>: Assign a group number to this specific interface. The allowed number is 1~3.

Negation: (config-if)# no qos wred-group <wred_group>

Show: # show qos wred
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.22.19. (config-if)# qos wrr

Syntax: (config-if)# qos wrr <w0> <w1> [<w2> [<w3> [<w4> [<w5> [<w6> [<w7>]]]]]]

Explanation: Assign weight for QoS queueing method. WRR stands for Weighted Round Robin and uses default queue weights. The number of packets serviced during each visit to a queue depends on the percentages you configure for the queues.

Parameters:

<w0: 1-100>: Specify weight for queue 0.

<w1: 1-100>: Specify weight for queue 1.

<w2: 1-100>: Specify weight for queue 2.

<w3: 1-100>: Specify weight for queue 3.

<w4: 1-100>: Specify weight for queue 4.

<w5: 1-100>: Specify weight for queue 5.

<w6: 1-100>: Specify weight for queue 6.

<w7: 1-100>: Specify weight for queue 7.

Negation: (config-if)# no qos wrr

Show: # show qos
# show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

3.11.23. (config-if)# shutdown

Syntax: (config-if)# shutdown

Explanation: Shutdown this specific interface.

Negation: (config-if)# no shutdown

Show: # show interface (<port_type> [<v_port_type_list>]) status

3.11.24. (config-if)# spanning-tree

3.11.24.1. (config-if)# spanning-tree

Syntax: (config-if)# spanning-tree

Explanation: Enable Spanning Tree on this interface.

Negation: (config-if)# no spanning-tree

Show: # show spanning-tree

3.11.24.2. (config-if)# spanning-tree auto-edge

Syntax: (config-if)# spanning-tree auto-edge

Explanation: Enable auto edge function on this interface. When enabled, a port is automatically determined to be at the edge of the network when it receives no BPDUs.

Negation: (config-if)# no spanning-tree auto-edge

Show: # show spanning-tree

3.11.24.3. (config-if)# spanning-tree bpdu-guard

Syntax: (config-if)# spanning-tree bpdu-guard

Explanation: Enable BPDU guard function on this interface. This feature protects ports from receiving BPDUs. It can prevent loops by shutting down a port when a BPDU is received instead of putting it into the spanning tree discarding state. If enabled, the port will disable itself upon receiving valid BPDU's.

Negation: (config-if)# no spanning-tree bpdu-guard

Show: # show spanning-tree

3.11.24.4. (config-if)# spanning-tree edge

Syntax: (config-if)# spanning-tree edge

Explanation: If an interface is attached to end nodes, you can set it to “Edge”.

Negation: (config-if)# no spanning-tree edge

Show: # show spanning-tree

3.11.24.5. (config-if)# spanning-tree link-type

Syntax: (config-if)# spanning-tree link-type { point-to-point | shared | auto }

Explanation: Configure the link type attached to an interface.

Parameters:

{ point-to-point | shared | auto }: Select the link type attached to an interface.

point-to-point: It is a point-to-point connection.

shared: It is a shared medium connection

auto: The switch automatically determines whether the interface is attached to a point-to-point link or shared medium.

Negation: (config-if)# no spanning-tree link-type

Show: # show spanning-tree

3.11.24.6. (config-if)# spanning-tree mst <instance> cost

Syntax: (config-if)# spanning-tree mst <instance> cost { <cost> | auto }

Explanation: Configure MSTI and its' path cost value.

Parameters:

mst <instance: 0-15>: Specify MST instance number. Specify "0" to denote CIST. Specify "1-15" to denote MSTI 1-15.

cost { <cost> | auto }: Specify a Path cost value that is used to determine the best path between devices. Valid values are 1 to 200000000. If "auto" mode is specified, the system automatically detects the speed and duplex mode to decide the path cost. Please note that path cost takes precedence over port priority.

Negation: (config-if)# no spanning-tree mst <instance> cost

Show: # show spanning-tree

3.11.24.7. (config-if)# spanning-tree mst <instance> port-priority

Syntax: (config-if)# spanning-tree mst <instance> port-priority <prio>

Explanation: Configure MSTI and its' port priority.

Parameters:

mst <instance: 0-15>: Specify MST instance number. Specify "0" to denote CIST. Specify "1-15" to denote MSTI 1-15.

port-priority <prio>: Specify a port priority value.

Negation: (config-if)# no spanning-tree mst <instance> port-priority

Show: # show spanning-tree

3.11.24.8. (config-if)# spanning-tree restricted-role

Syntax: (config-if)# spanning-tree restricted-role

Explanation: Enable restricted role function. If enabled, this causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority.

Negation: (config-if)# no spanning-tree restricted-role

Show: # show spanning-tree

3.11.24.9. (config-if)# spanning-tree restricted-tcn

Syntax: (config-if)# spanning-tree restricted-tcn

Explanation: Enable restricted TCN function. If enabled, this causes the port not to propagate received topology change notifications and topology changes to other ports.

Negation: (config-if)# no spanning-tree restricted-tcn

Show: # show spanning-tree

3.11.25. (config-if)# speed

Syntax: (config-if)# speed { 10g | 2500 | 1000 | 100 | 10 | auto { [10] [100] [1000] [2500] [10g] } }

Explanation: Configure port speed for this specific interface.

Negation: (config-if)# no speed

Show: # show interface (<port_type> [<v_port_type_list>]) status

3.11.26. (config-if)# switchport

3.11.26.1. (config-if)# switchport access vlan

Syntax: (config-if)# switchport access vlan <pvid>

Explanation: Configure access VLAN ID for this interface.

Parameters:

<pvid>: Indicate the access VLAN ID (PVID) for this interface.

Example: Set the interface 1's access VLAN ID to 10.

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)# switchport access vlan 10
(config-if)#
```

Negation: (config-if)# no switchport access vlan

Show: # show vlan status

3.11.26.2. (config-if)# switchport forbidden vlan

Syntax: (config-if)# switchport forbidden vlan { add | remove } <vlan_list>

Explanation: Add or remove a port from the forbidden VLAN list.

Parameters:

{ add | remove }: Add or remove this specific interface from the forbidden VLAN list.

<vlan_list>: Specify the VLAN ID.

Negation: (config-if)# no switchport access vlan

Show: > show switchport forbidden [{ vlan <vid> } | { name <name> }]
# show switchport forbidden [{ vlan <vid> } | { name <name> }]

3.11.26.3. (config-if)# switchport hybrid acceptable-frame-type

Syntax: (config-if)# switchport hybrid acceptable-frame-type { all | tagged | untagged }

Explanation: Configure the accepted frame types. Available options include "all" (accept all frames), "tagged" (accept only tagged frames), "untagged" (accept only untagged frames). This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, frame type is set to All.

Parameters:

{ all | tagged | untagged }: Specify the frame type for this interface. Available options include "all" (accept all frames), "tagged" (accept only tagged frames), "untagged" (accept only untagged frames).

Negation: (config-if)# no switchport hybrid acceptable-frame-type

Show: # show vlan status

3.11.26.4. (config-if)# switchport hybrid allowed vlan

Syntax: (config-if)# switchport hybrid allowed vlan { all | none | [add | remove | except] <vlan_list> }

Explanation: Configure allowed VLANs when this interface is in hybrid mode.

Parameters:

{ all | none | [add | remove | except] <vlan_list> }: Specify one of the options.

all: All VLANs.

none: No VLANs.

add: Add VLANs to the current list.

remove: Remove VLANs from the current list

except: All VLANs except the following specified in <vlan_list>.

<vlan_list>: Specify the VLAN list.

Negation: (config-if)# no switchport hybrid allowed vlan

Show: # show vlan status

3.11.26.5. (config-if)# switchport hybrid egress-tag

Syntax: (config-if)# switchport hybrid egress-tag { none | all [except-native] }

Explanation: Determines egress tagging of a port.

Parameters:

{ none | all [except-native] }: Determines egress tagging of a port.

none: All VLANs are untagged.

all: All VLANs are tagged.

all [except-native]: All VLANs except the configured PVID will be tagged.

Negation: (config-if)# no switchport hybrid egress-tag

Show: # show vlan status

3.11.26.6. (config-if)# switchport hybrid ingress-filtering

Syntax: (config-if)# switchport hybrid ingress-filtering

Explanation: Enable ingress filtering function on this specific interface. If Ingress Filtering is enabled and the ingress port is not a member of a VLAN, the frame from the ingress port is discarded. By default, ingress filtering is disabled.

Negation: (config-if)# no switchport hybrid ingress-filtering

Show: # show vlan status

3.11.26.7. config-if)# switchport hybrid native vlan

Syntax: (config-if)# switchport hybrid native vlan <pvid>

Explanation: Configures the VLAN identifier in Hybrid mode for the port. The allowed values are from 1 through 4095. The default value is 1.

Parameters:

<pvid>: Specify the port VLAN ID for this specific interface.

Negation: (config-if)# no switchport hybrid native vlan

Show: # show vlan status

3.11.26.8. (config-if)# switchport hybrid port-type

Syntax: (config-if)# switchport hybrid port-type { unaware | c-port | s-port | s-custom-port }

Explanation: Configures the port type in Hybrid mode for the port.

Parameters:

{ unaware | c-port | s-port | s-custom-port }: There are four port types available. Each port type's ingress and egress action is described in the following table.

Action Port Type	Ingress Action	Egress Action
Unaware	When a tagged frame is received on a port, ● If the tagged frame with TPID=0x8100, it becomes a double-tag frame and is forwarded. ● If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by Unaware port will be set to 0x8100. The final status of the frame after egressing are also affected by egress rule.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
C-port	When a tagged frame is received on a port, ● If a tagged frame with TIPID=0x8100, it is forwarded. ● If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by C-port will be set to 0x8100.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
S-port	When a tagged frame is received on a port, ● If a tagged frame with TPID=0x88A8, it is forwarded. ● If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded.	The TPID of frame transmitted by S-port will be set to 0x88A8
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
S-custom port	When a tagged frame is received on a port, ● If a tagged frame with TPID=0x88A8, it is forwarded. ● If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded.	The TIPID of frame transmitted by S-custom-port will be set to an self-customized value, which can be set by the user using the column of Ethertype for Custom S-ports.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	

Negation: (config-if)# no switchport hybrid port-type

Show: # show vlan status

3.11.26.9. (config-if)# switchport mode

Syntax: (config-if)# switchport mode { access | trunk | hybrid }

Explanation: Configure VLAN mode for this specific interface.

Parameters:

{ access | trunk | hybrid }: Specify the VLAN mode.

Negation: (config-if)# no switchport mode

Show: # show vlan status

3.11.26.10. (config-if)# switchport trunk allowed vlan

Syntax: (config-if)# switchport trunk allowed vlan { all | none | [add | remove | except] <vlan_list> }

Explanation: Configure allowed VLANs when this interface is in trunk mode.

Parameters:

{ all | none | [add | remove | except] <vlan_list> }: Specify one of the options.

all: All VLANs.

none: No VLANs.

add: Add VLANs to the current list.

remove: Remove VLANs from the current list.

except: All VLANs except the following specified in <vlan_list>.

<vlan_list>: Specify the VLAN list.

Negation: (config-if)# no switchport trunk allowed vlan

Show: # show vlan status

3.11.26.11. (config-if)# switchport trunk native vlan

Syntax: (config-if)# switchport trunk native vlan <pvid>

Explanation: Configure native VLAN ID in trunk mode for this specific interface.

Parameters:

<pvid>: Specify the port VLAN ID for this specific interface.

Negation: (config-if)# no switchport trunk native vlan

Show: # show running-config

3.11.26.12. (config-if)# switchport trunk vlan tag native

Syntax: (config-if)# switchport trunk vlan tag native

Explanation: Configure this specific interface to tag native VLAN traffic.

Negation: (config-if)# no switchport trunk vlan tag native

3.11.26.13. (config-if)# switchport vlan ip-subnet id

Syntax: (config-if)# switchport vlan ip-subnet id <vce_id> <ipv4> vlan <vid>

Explanation: IP Subnet-based VLAN configuration is to map untagged ingress frames to a specific VLAN if the source address is found in the IP subnet-to-VLAN mapping table. When IP subnet-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the IP subnet-to-VLAN mapping table. If an entry is found for that subnet, these frames are assigned to the VLAN indicated in the entry. If no IP subnet is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

Parameters:

<vce_id: 1-128>: Specify index of the entry. Valid range is 1~128.

<ipv4>: Specify IP address and subnet mask. The format is xx.xx.xx.xx/mm.mm.mm.mm.

<vid>: Indicate the VLAN ID.

Negation: (config-if)# no switchport vlan ip-subnet id <vce_id_list>

Show: # show vlan ip-subnet [id <subnet_id>]

3.11.26.14. (config-if)# switchport vlan mac

Syntax: (config-if)# switchport vlan mac <mac_addr> vlan <vid>

Explanation: This command is to set up VLANs based on source MAC addresses. When ingress untagged frames are received by a port, source MAC address is processed to decide which VLAN these untagged frames belong. When source MAC addresses do not match the rules created, untagged frames are assigned to the receiving port's native VLAN ID (PVID).

Parameters:

<mac_addr>: Indicate the source MAC address. Please note that the source MAC address can only map to one VLAN ID.

vlan <vid>: Map this MAC address to the associated VLAN ID.

Negation: (config-if)# no switchport vlan mac <mac_addr> vlan <vid>

Show: # show vlan mac [address <mac_addr>]

3.11.26.15. (config-if)# switchport vlan mapping <gid>

Syntax: (config-if)# switchport vlan mapping <grp_id>

Explanation: This command is used to map VLAN Translation to groups. In this way, a port is configured to use a number of VLAN translation mappings easily by simply configuring it to use a given group. The number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 10.

By default, each port is set to use the group with Group ID equal to the port number. For example, port 1 is by default set to use Group ID 1 (gid=1).

Parameters:

<gid>: Indicate a Group ID to this specified interface. The allowed value is 1~10.

Negation: (config-if)# no switchport vlan mapping

3.11.26.16. (config-if)# switchport vlan protocol group

Syntax: (config-if)# switchport vlan protocol group <grp_id> vlan <vid>

Explanation: Configure VLAN protocol group for this specific interface.

Parameters:

<grp_id: word 16>: Indicate the descriptive name for this entry. This field only allows 16 alphabet characters (a-z; A-Z) or integers (0-9).

<vid>: Specify the VLAN ID that applies to this rule.

Negation: (config-if)# no switchport vlan protocol group <grp_id> vlan <vid>

Show: # show vlan protocol [eth2 { <etype> | arp | ip | ipx | at }] [snap { <oui> | rfc-1042 | snap-8021h } <pid>] [llc <dsap> <ssap>]

3.11.26.17. (config-if)# switchport voice vlan discovery-protocol

Syntax: (config-if)# switchport voice vlan discovery-protocol { oui | lldp | both }

Explanation: Configure a method for detecting VoIP traffic. By default, OUI is used.

Parameters:

oui: Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address. OUI numbers are assigned to manufacturers and form the first three octets of a device MAC address. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.

lldp: Use LLDP (IEEE 802.1ab) to discover VoIP devices attached to a port. LLDP checks that the “telephone bit” in the system capability TLV is turned on or not.

both: Use both OUI table and LLDP to detect VoIP traffic on a port.

Negation: (config-if)# no switchport voice vlan discovery-protocol

Show: # show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]

3.11.26.18. (config-if)# switchport voice vlan mode

Syntax: (config-if)# switchport voice vlan mode { auto | force | disable }

Explanation: Configure Voice VLAN mode on a per port basis.

Parameters:

auto: Enable the Voice VLAN auto detection mode. When voice (VoIP) traffic is detected on a port, the port will be added as a tagged member to the Voice VLAN. When Auto mode is selected, you need to further decide a method for detecting voice traffic in "Discovery Protocol" field, either OUI or LLDP (802.1ab).

force: Enable Voice VLAN feature on a particular port.

disabled: Disable Voice VLAN feature on a particular port.

Negation: (config-if)# no switchport voice vlan mode

Show: # show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]

3.11.26.19. (config-if)# switchport voice vlan security

Syntax: (config-if)# switchport voice vlan security

Explanation: Enable security filtering feature on a per port basis. When enabled, any non-VoIP packets received on a port with Voice VLAN ID will be discarded. VoIP traffic is identified by source MAC addresses configured in the telephony OUI list or through LLDP which is used to discover VoIP devices attached to the switch.

Negation: (config-if)# no switchport voice vlan security

Show: # show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]

3.12. Commands in Config Interface VLAN Mode

To enter Config Interface VLAN Mode, you need to type the following command under "(config)#":

```
# config terminal
(config)# interface vlan 1
(config-if-vlan)#
```

Note: *VLAN ID used in the example above can be changed to the one applicable to your actual settings.*

3.12.1. (config-if-vlan)# ip

3.12.1.1. (config-if-vlan)#ip address

Syntax: (config-if-vlan)# ip address { { <address> <netmask> } | { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] } }

Explanation: Configure IPv4 address for this VLAN interface.

Parameters:

<address> <netmask>: Specify IPv4 address and subnet mask.

dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]]: Use DHCP server to automatically assign IP address.

fallback <fallback_address> <fallback_netmask>: specify Fallback IP address and subnet mask.

timeout <fallback_timeout>: Specify Fallback timeout value.

Negation: (config-if-vlan)# no ip address

Show: > show ip interface brief
# show ip interface brief

3.12.1.2. (config-if-vlan)# ip dhcp server

Syntax: (config-if-vlan)# ip dhcp server

Explanation: Enable DHCP server on this specific VLAN.

Negation: (config-if-vlan)# no ip dhcp server

Show: > show ip dhcp server
# show ip dhcp server

3.12.1.3. (config-if-vlan)# ip igmp snooping

Syntax: (config-if-vlan)# ip igmp snooping

Explanation: Enable IGMP Snooping on this specific VLAN.

Negation: (config-if-vlan)# no ip igmp snooping

Show: > show ip statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]
# show ip statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

3.12.1.4. (config-if-vlan)# ip igmp snooping compatibility

Syntax: (config-if-vlan)# ip igmp snooping compatibility { auto | v1 | v2 | v3 }

Explanation: Configure IGMP Snooping version used for this specific VLAN.

Parameters:

{ auto | v1 | v2 | v3 }: Specify one of the IGMP Snooping options.

auto: Compatible with Version 1, Version 2, and Version 3.

v1: Compatible with IGMP version 1.

v2: Compatible with IGMP version 2.

v3: Compatible with IGMP version 3.

Negation: (config-if-vlan)# no ip igmp snooping compatibility

3.12.1.5. (config-if-vlan)# ip igmp snooping last-member-query-interval

Syntax: (config-if-vlan)# ip igmp snooping last-member-query-interval <ipmc_lmqi>

Explanation: LMQI stands for Last Member Query Interval and is to configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The allowed range is 0~31744 tenths of a second.

Parameters:

<ipmc_lmqi: 0-31744>: Specify LMQI (Last Member Query Interval) value.

Negation: (config-if-vlan)# no ip igmp snooping last-member-query-interval

3.12.1.6. (config-if-vlan)# ip igmp snooping priority

Syntax: (config-if-vlan)# ip igmp snooping priority <cos_priority>

Explanation: Specify the priority for transmitting IGMP/MLD control frames. By default, priority is set to 0. Allowed priority values is 0-7.

Parameters:

<cos_priority: 0-7>: Specify COS for this specific VLAN. The valid range is 0 to 7.

Negation: (config-if-vlan)# no ip igmp snooping priority

3.12.1.7. (config-if-vlan)# ip igmp snooping querier

Syntax: (config-if-vlan)# ip igmp snooping querier { election | address <v_ipv4_ucast> }

Parameters:

{ election | address <v_ipv4_ucast> }: Elect the IGMP Snooping querier or use the specified IPv4 unicast address as a querier.

Explanation: Elect or specify IGMP Snooping querier IP address.

Negation: (config-if-vlan)# no ip igmp snooping querier { election | address }

3.12.1.8. (config-if-vlan)# ip igmp snooping query-interval

Syntax: (config-if-vlan)# ip igmp snooping query-interval <ipmc_qi>

Explanation: Specify IPMC Query interval value.

Parameters:

<ipmc_qi: 1-31744>: Specify IPMC Query interval value. The valid value is 1~31744.

Negation: (config-if-vlan)# no ip igmp snooping query-interval

3.12.1.9. (config-if-vlan)# ip igmp snooping query-max-response-time

Syntax: (config-if-vlan)# ip igmp snooping query-max-response-time <ipmc_qri>

Explanation: Specify IPMC Query Response time value.

Parameters:

<ipmc_qri>: Specify IPMC Query Response time value. The valid value is 1~31744.

Negation: (config-if-vlan)# no ip igmp snooping query-max-response-time

3.12.1.10. (config-if-vlan)# ip igmp snooping robustness-variable

Syntax: (config-if-vlan)# ip igmp snooping robustness-variable <ipmc_rv>

Explanation: The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2.

Parameters:

<ipmc_rv: 1-255>: Specify IPMC Robustness Variable value. The valid value is 1~255.

Negation: (config-if-vlan)# no ip igmp snooping robustness-variable

3.12.1.11. (config-if-vlan)# ip igmp snooping unsolicited-report-interval

Syntax: (config-if-vlan)# ip igmp snooping unsolicited-report-interval <ipmc_uri>

Explanation: The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. The allowed range for URI is 0 -31744 seconds.

Parameters:

<ipmc_uri: 0-31744>: Specify Unsolicited Report Interval value. The valid value is 0~31744.

Negation: (config-if-vlan)# no ip igmp snooping unsolicited-report-interval

3.12.2. (config-if-vlan)# ipv6

3.12.2.1. (config-if-vlan)# ipv6 address

Syntax: (config-if-vlan)# ipv6 address <subnet>

Explanation: Configure IPv6 address for this VLAN interface.

Parameters:

<subnet>: Specify IPv6 address in X:X:X:X::X/<0-128> format.

Negation: (config-if-vlan)# no ipv6 address [<ipv6_subnet>]

Show: > show ip interface brief

> show ipv6 interface [vlan <v_vlan_list> { brief | statistics }]

# show ip interface brief

# show ipv6 interface [vlan <v_vlan_list> { brief | statistics }]

3.12.2.2. (config-if-vlan)# ipv6 address {autoconfig | dhcp | rapid-commit}}

Syntax: (config-if-vlan)# ipv6 address {autoconfig | dhcp | rapid-commit}

Explanation: Configure how IPv6 address is obtained.

Parameters:

{autoconfig | dhcp | rapid-commit}: Manual configure IPv6 address or use DHCP server to obtain IPv6 address. Or configure DHCPv6 to support rapid commit option (DHCPv6 option 14). When rapid commint is endabled, the server recognizes the Rapid Commit option in Solicit messages sent from the DHCPv6 client.The server and client then use a two-message exchange (Solicit and Reply) to configure clients, rather than the default four-message exchange (Solicit, Advertise, Request, and Reply). The two-message exchange provides faster client configuration, and is beneficial in environments in which networks are under a heavy load.

Negation: (config-if-vlan)# no ipv6 address {autoconfig | dhcp | rapid-commit}

Show: > show ipv6 interface [vlan <v_vlan_list> { brief | statistics }]
# show ipv6 dhcp-client [interface vlan <v_vlan_list>]
#show ipv6 interface [vlan <v_vlan_list> { brief | statistics }]

3.12.2.3. (config-if-vlan)# ipv6 mld snooping

Syntax: (config-if-vlan)# ipv6 mld snooping

Explanation: Eanble MLD (Multicast Listener Discovery) Snooping on this specific VLAN.

Negation: (config-if-vlan)# no ipv6 mld snooping

Show: > show ipv6 statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]
# show ipv6 statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

3.12.2.4. (config-if-vlan)# ipv6 mld snooping compatibility

Syntax: (config-if-vlan)# ipv6 mld snooping compatibility { auto | v1 | v2 }

Explanation: Configure MLD Snooping version used for this specific VLAN.

Parameters:

{ auto | v1 | v2 | v3 }: Specify one of the MLD Snooping options.

auto: Compatible with Version 1, Version 2.

v1: Compatible with MLD version 1.

v2: Compatible with MLD version 2.

Negation: (config-if-vlan)# no ipv6 mld snooping compatibility

3.12.2.5. (config-if-vlan)# ipv6 mld snooping last-member-query-interval

Syntax: (config-if-vlan)# ipv6 mld snooping last-member-query-interval <ipmc_lmqi>

Explanation: LMQI stands for Last Member Query Interval and is to configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The allowed range is 0~31744 tenths of a second.

Parameters:

<ipmc_lmqi: 0-31744>: Specify LMQI (Last Member Query Interval) value.

Negation: (config-if-vlan)# no ipv6 mld snooping last-member-query-interval

(config-if-vlan)# ipv6 mld snooping priority <cos_priority>

Syntax: (config-if-vlan)# ipv6 mld snooping priority <cos_priority>

Explanation: Specify the priority for transmitting IGMP/MLD control frames. By default, priority is set to 0. Allowed priority values is 0 -7.

Parameters:

<cos_priority: 0-7>: Specify COS for this specific VLAN. The valid range is 0 to 7.

Negation: (config-if-vlan)# no ipv6 mld snooping priority

3.12.2.6. (config-if-vlan)# ipv6 mld snooping querier election

Syntax: (config-if-vlan)# ipv6 mld snooping querier election

Explanation: Enable MLD Snooping querier election function.

Negation: (config-if-vlan)# no ipv6 mld snooping querier election

3.12.2.7. (config-if-vlan)# ipv6 mld snooping query-interval <ipmc_qi>

Syntax: (config-if-vlan)# ipv6 mld snooping query-interval <ipmc_qi>

Explanation: Specify MLD Query interval value.

Parameters:

<ipmc_qi: 1-31744>: Specify IPMC Query interval value. The valid value is 1~31744.

Negation: (config-if-vlan)# no ipv6 mld snooping query-interval

3.12.2.8. (config-if-vlan)# ipv6 mld snooping query-max-response-time <ipmc_qri>

Syntax: (config-if-vlan)# ipv6 mld snooping query-max-response-time <ipmc_qri>

Explanation: Specify MLD Query Response time value.

Parameters:

<ipmc_qri>: Specify MLD Query Response time value. The valid value is 1~31744.

Negation: (config-if-vlan)# no ipv6 mld snooping query-max-response-time

3.12.2.9. (config-if-vlan)# ipv6 mld snooping robustness-variable <ipmc_rv>

Syntax: (config-if-vlan)# ipv6 mld snooping robustness-variable <ipmc_rv>

Explanation: The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2.

Parameters:

<ipmc_rv: 1-255>: Specify IPMC Robustness Variable value. The valid value is 1~255.

Negation: (config-if-vlan)# no ipv6 mld snooping robustness-variable

3.12.2.10. (config-if-vlan)# ipv6 mld snooping unsolicited-report-interval <ipmc_uri>

Syntax: (config-if-vlan)# ipv6 mld snooping unsolicited-report-interval <ipmc_uri>

Explanation: The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. The allowed range for URI is 0 -31744 seconds.

Parameters:

<ipmc_uri: 0-31744>: Specify Unsolicited Report Interval value. The valid value is 0~31744.

Negation: (config-if-vlan)# no ipv6 mld snooping unsolicited-report-interval

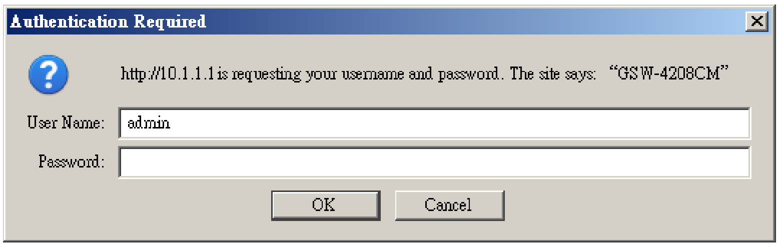
CHAPTER 4. WEB CONFIGURATION & OPERATION

4.1. Home Page

Using your favorite web browser, enter the IP address of the GSW-4208CM in the browser's location bar. The factory default address is 10.1.1.1.

4.1.1. Login

A standard login prompt will appear depending on the type of browser used. The example below is with Firefox browser.



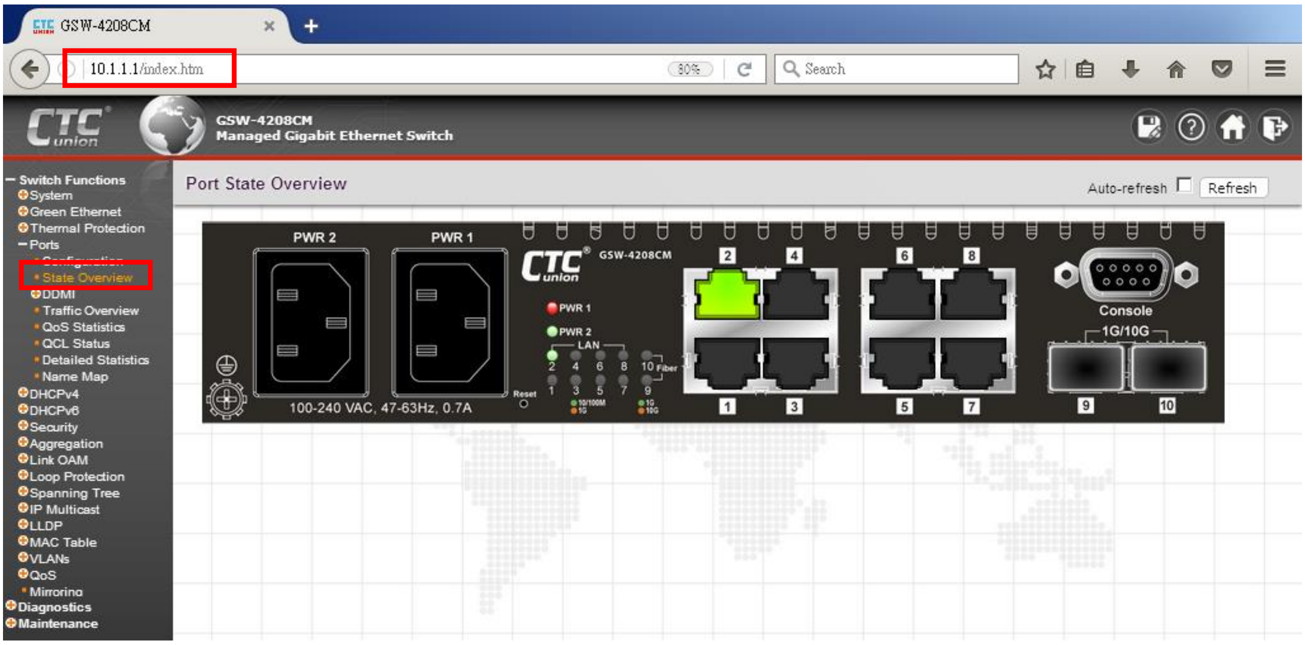
Authentication Required

http://10.1.1.1 is requesting your username and password. The site says: "GSW-4208CM"

User Name: admin

Password:

The GSW-4208CM factory default is username '**admin**' with **no password**.

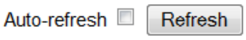


4.1.2. Port Status

The initial page, when logged in, displays a graphical overview of the port status for the electrical and optical ports. The status display can be reached by using the left side menu, and go to Ports>State Overview.

4.1.3. Refresh

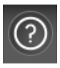
To update the screen, click the "Refresh" button. For automatic updating of the screen, the "Auto-refresh" tick box may be ticked. The screen will be auto refreshed every 5 seconds.



Unless connected directly on a local LAN, we recommend not using the auto-refresh function as it does generate a bit of traffic.

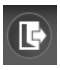
4.1.4. Help System

The device has an online "help" system to aid the engineer when setting the parameters of the device. Each functional setting page is accompanied by a specific "help" for that functional page. The user can display this help "pop up" at any time by clicking the "help" icon.

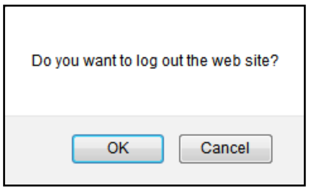


4.1.5. Logout

After completing configuration, we recommend logging out of the web GUI. This is easily accomplished by clicking the logout icon.



After clicking the logout icon, a confirmation screen will be displayed. Click "OK" to finish logging out or click "Cancel" to return to the web configuration GUI.

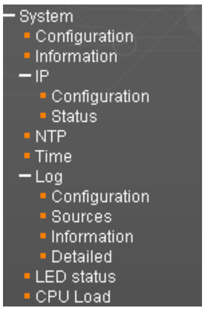


Do you want to log out the web site?

For the remainder of this section, each menu item will be explained one by one, in order as they descend down the menu screen, starting with the "System" menu.

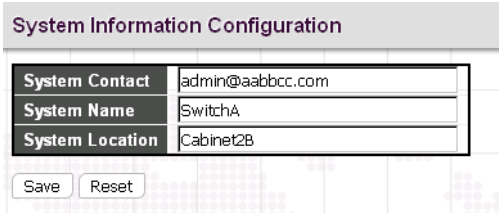
4.2. System

The configuration under the "System" menu includes device settings such as IP address, time server, etc.



4.2.1. System Configuration

The configuration information entered here will be reported in the standard SNMP MIB2 for 'sysContact' (OID 1.3.6.1.2.1.1.4), 'sysName' (OID 1.3.6.1.2.1.1.5) and 'sysLocation' (OID 1.3.6.1.2.1.1.6). Remember to click the 'Save' button after entering the configuration information.

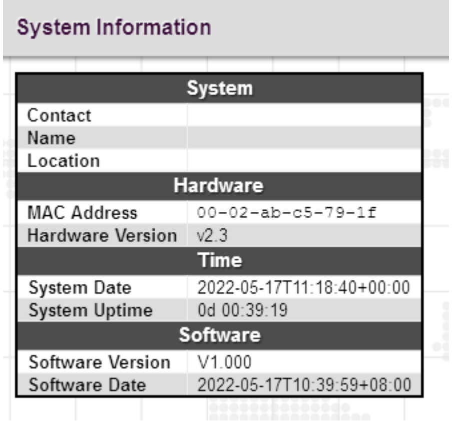


System Information Configuration

System Contact	admin@aabbcc.com
System Name	SwitchA
System Location	Cabinet2B

4.2.2. System Information

The system information screen will display the configuration information, the hardware MAC address and version, the system time, the system "uptime" and the software version and build date.



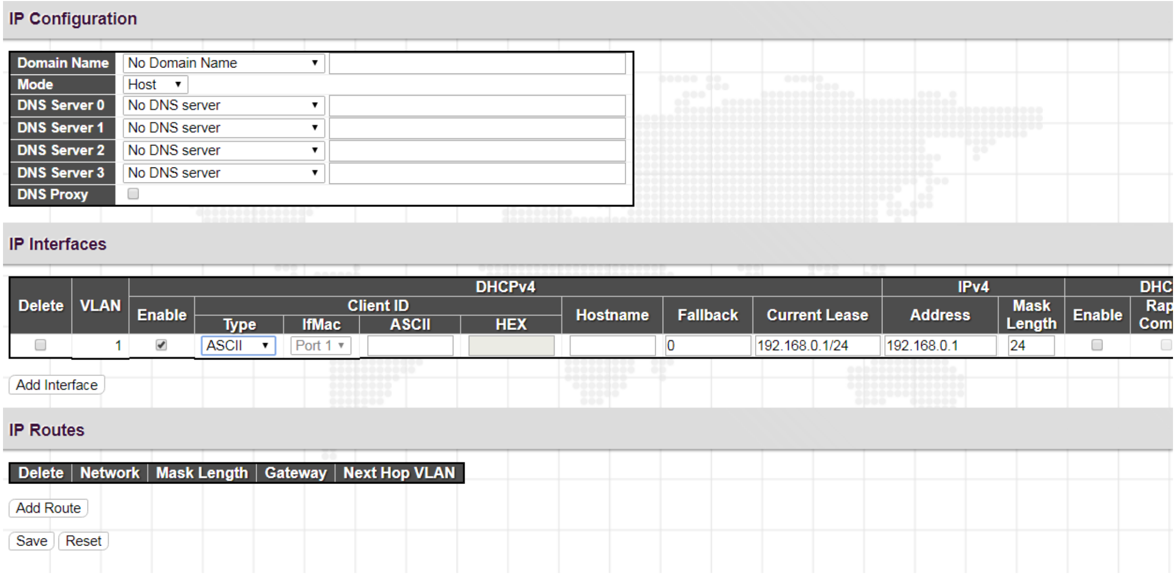
System Information

System	
Contact	
Name	
Location	
Hardware	
MAC Address	00-02-ab-c5-79-1f
Hardware Version	v2.3
Time	
System Date	2022-05-17T11:18:40+00:00
System Uptime	0d 00:39:19
Software	
Software Version	V1.000
Software Date	2022-05-17T10:39:59+08:00

4.2.3. IP

4.2.3.1. Configuration

Setup the IP configuration, interface and routes.



IP Configuration

Domain Name	No Domain Name ▾	
Mode	Host ▾	
DNS Server 0	No DNS server ▾	
DNS Server 1	No DNS server ▾	
DNS Server 2	No DNS server ▾	
DNS Server 3	No DNS server ▾	
DNS Proxy	☐	

IP Interfaces

Delete	VLAN	DHCPv4								IPv4		DHC	
		Enable	Client ID				Hostname	Fallback	Current Lease	Address	Mask Length	Enable	Rap Com
			Type	IfMac	ASCII	HEX							
☐	1	☑	ASCII ▾	Port 1 ▾				0	192.168.0.1/24	192.168.0.1	24	☐	☐

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN

IP Configuration

Domain Name: This setting controls the DNS name resolution done by the switch. The following modes are supported:

No Domain Name: No DNS server will be used.

Configured Domain Name: Explicitly provide the IP address of the DNS Server in dotted decimal notation.

From any DHCPv4 interfaces: The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used.

From this DHCPv6 interface: Specify from which DHCP-enabled interface a provided DNS server should be preferred.

Mode: This pull-down menu configures whether the IP stack should act as a Host or a Router. In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces. When configuring this device for multiple VLANs, the Router mode should be chosen. Router mode is the default mode.

DNS Server: This setting controls the DNS name resolution done by the switch. There are four servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution. The following modes are supported:

No DNS server: No DNS server will be used.

Configured IPv4: Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation. Make sure the configured DNS server could be reachable (e.g. via PING) for activating DNS service.

Configured IPv6: Explicitly provide the valid IPv6 unicast (except linklocal) address of the DNS Server. Make sure the configured DNS server could be reachable (e.g. via PING6) for activating DNS service.

From any DHCPv4 interfaces: The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.

From this DHCPv4 interface: Specify from which DHCPv4-enabled interface a provided DNS server should be preferred.

From any DHCPv6 interfaces: The first DNS server offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used.

From this DHCPv6 interface: Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.

DNS Proxy: When DNS proxy is enabled, the system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.

IP Interface

Click "Add Interface" to add a new IP interface. A maximum of 8 interfaces is supported.

VLAN: This is the VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.

DHCPv4

Enable: When this checkbox is enabled, the system will configure the IPv4 address and mask of the interface using the DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

Fallback: The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables fallback mechanism. The DHCP will keep retrying until a valid lease is obtained when fallback is disabled. The transmission delay is a randomization value that up to a maximum of 64 seconds. Legal values are 0 or 65 to 4294967295 seconds.

Current Lease: For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.

IPv4

Address: The IPv4 address of the interface is entered in dotted decimal notation. If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.

Mask Length: The IPv4 network mask is entered by a number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address. If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.

DHCPv6

Enable: When this checkbox is enabled, the system will configure the IPv6 address and mask of the interface using the DHCP protocol.

Rapid Commit: If this option is enabled, the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received. This option is only manageable when DHCPv6 client is enabled.

Current Lease: For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.

IPv6

Address: A IPv6 address is a 128-bit record represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, ::192.1.2.34. The field may be left blank if IPv6 operation on the interface is not desired.

Mask Length: The IPv6 network mask is entered by a number of bits (prefix length). Valid values are between 1 and 128 bits for an IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.

IP Routes

Network: The IP route is the destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0 or for IPv6 use the :: notation.

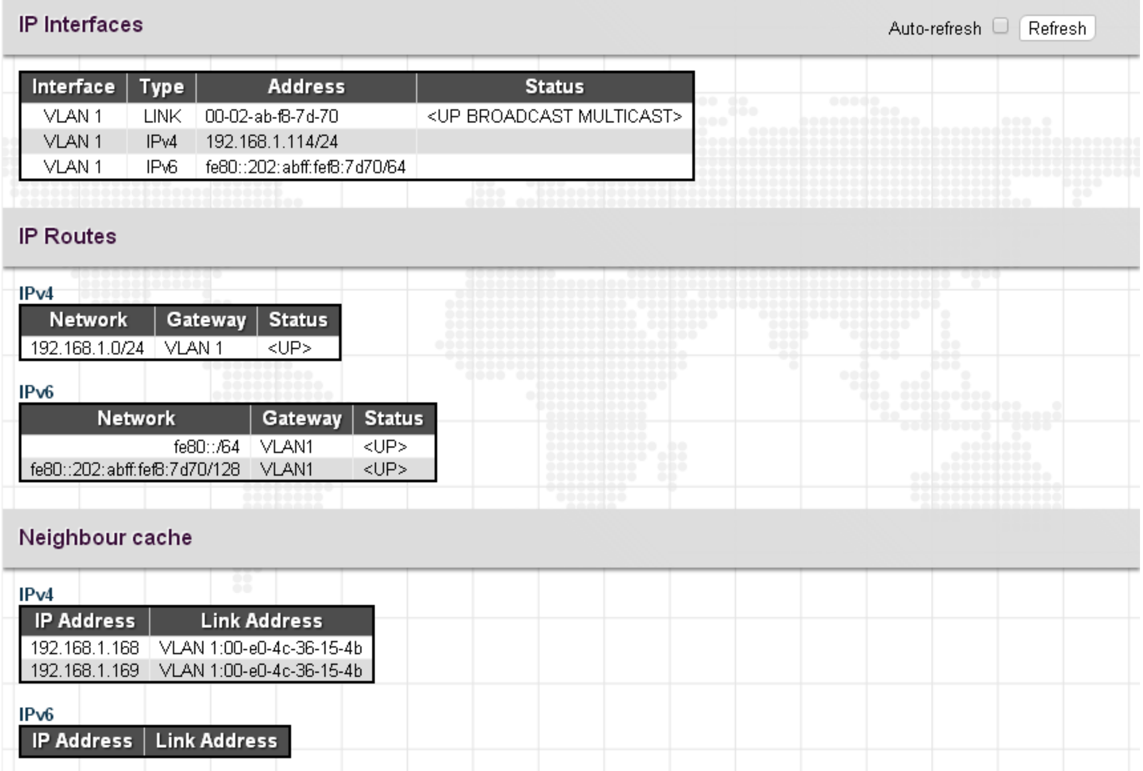
Route Mask: The route mask is a destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).

Gateway: This is the IP address of the gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.

Next Hop VLAN (Only for IPv6): The VLAN ID of the specific IPv6 interface associated with the gateway. The given VID ranging from 1 to 4095 will be effective only when the corresponding IPv6 interface is valid. If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway. If the IPv6 gateway address is not link-local, the device will ignore the next hop VLAN for the gateway.

4.2.3.2. System IP Status

Display the status of IP interfaces and routes.



IP Interfaces

Interface	Type	Address	Status
VLAN 1	LINK	00-02-ab-f8-7d-70	<UP BROADCAST MULTICAST>
VLAN 1	IPv4	192.168.1.114/24	
VLAN 1	IPv6	fe80::202:abff:fef8:7d70/64	

IP Routes

IPv4

Network	Gateway	Status
192.168.1.0/24	VLAN 1	<UP>

IPv6

Network	Gateway	Status
fe80::/64	VLAN1	<UP>
fe80::202:abff:fef8:7d70/128	VLAN1	<UP>

Neighbour cache

IPv4

IP Address	Link Address
192.168.1.168	VLAN 1:00-e0-4c-36-15-4b
192.168.1.169	VLAN 1:00-e0-4c-36-15-4b

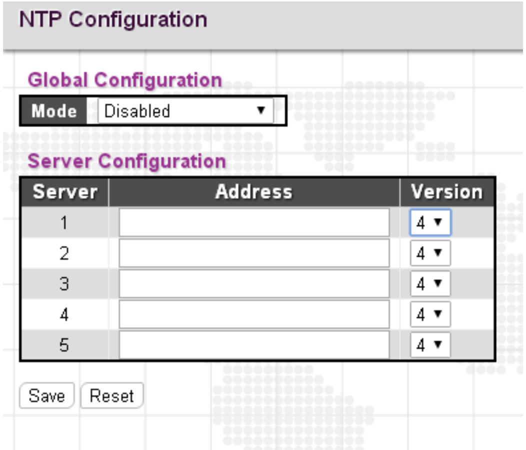
IPv6

IP Address	Link Address

Please refer to “System IP” for the configuration of the interfaces and routes. This page is informational only.

4.2.4. System NTP Configuration

Configure NTP (Network Time Protocol) on this page.



NTP Configuration

Global Configuration

Mode	Disabled

Server Configuration

Server	Address	Version
1		4
2		4
3		4
4		4
5		4

Global Configuration

Mode: Indicates the NTP mode operation. Possible modes are:

Enabled: Enable NTP client mode operation.

Disabled: Disable NTP client mode operation.

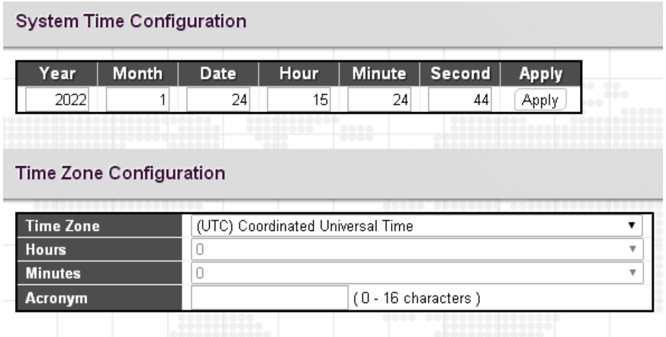
Server Configuration

Address: Provides the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Version: Select the NTP/SNTP protocol version.

4.2.5. Time

Setup the device time.

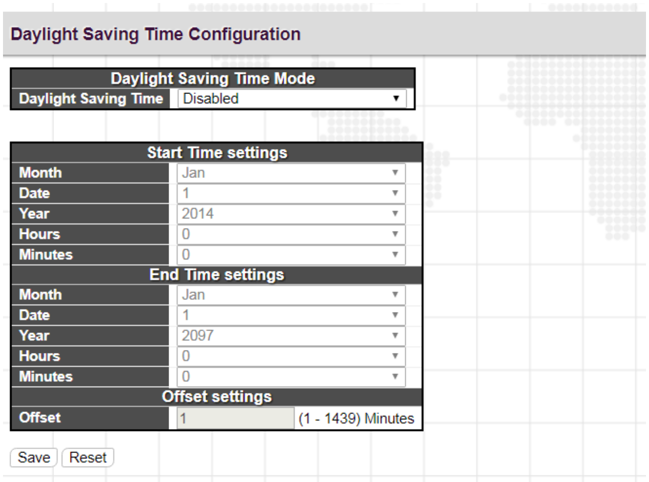


System Time Configuration

Year	Month	Date	Hour	Minute	Second	Apply
2022	1	24	15	24	44	Apply

Time Zone Configuration

Time Zone	(UTC) Coordinated Universal Time
Hours	0
Minutes	0
Acronym	(0 - 16 characters)



Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled

Start Time settings	
Month	Jan
Date	1
Year	2014
Hours	0
Minutes	0
End Time settings	
Month	Jan
Date	1
Year	2097
Hours	0
Minutes	0
Offset settings	
Offset	1 (1 - 1439) Minutes

Save Reset

System Time Configuration

The system automatically gets the time from your connected device (such as PC). If you want to use the time shown in this area, click “Apply” button to use this system time.

Time Zone Configuration

Time Zone: Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set. Select "Manual Setting" to set up your desired time.

Hours: When "Manual Setting" is selected, you can set up "Hour" parameter from the pull-down menu.

Minutes: When "Manual Setting" is selected, you can set up "Minutes" parameter from the pull-down menu.

Acronym: Set the acronym of the time zone.

Daylight Saving Time Configuration

This page is used to setup Daylight Saving Time Configuration.

Daylight Saving Time: This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default is Disabled)

Recurring & Non-Recurring Configurations:

Start time settings: Select the starting week, day, month, year, hours, and minutes.

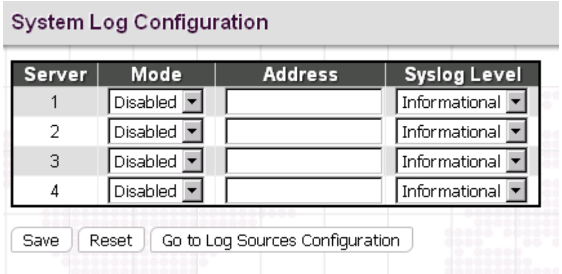
End time settings: Select the ending week, day, month, year, hours, and minutes.

Offset settings: Enter the number of minutes to add during Daylight Saving Time. The allowed range is 1 to 1440.

4.2.6. Log

4.2.6.1. Configuration

Configure System Log on this page.



System Log Configuration

Server	Mode	Address	Syslog Level
1	Disabled		Informational
2	Disabled		Informational
3	Disabled		Informational
4	Disabled		Informational

Server Mode: This sets the server mode operation. When the mode of operation is enabled, the syslog message will send out to syslog server (at the server address). The syslog protocol is based on UDP communication and received on UDP port 514. Syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out, even if the syslog server does not exist. When the mode of operation is disabled, no syslog packets are sent out.

Server Address: This sets the IPv4 host address of syslog server. If the switch provides DNS feature, it also can be a host name.

Syslog Level: This sets what kind of messages will send to syslog server. Possible levels are:

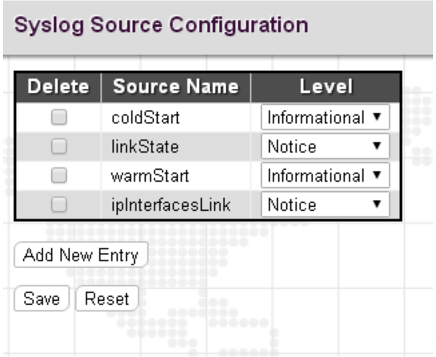
Informational: Send the specific messages which the severity code is less or equal than Informational (6).

Notice: Send the specific messages which the severity code is less or equal than Notice (5).

Warning: Send the specific messages which the severity code is less or equal than Warning (4).

Error: Send the specific messages which the severity code is less or equal than Error (3).

4.2.6.2. Sources



Syslog Source Configuration

Delete	Source Name	Level
□	coldStart	Informational
□	linkState	Notice
□	warmStart	Informational
□	ipInterfacesLink	Notice

Source Name: Indicates the name for the entry.

coldStart: The device performs a power on (Chip and CPU restart).

warmStart: The device restarts (CPU restarts only).

linkState: A port interface is link up or link down.

crcError: The device receives CRC error packets.

ddmiStatus: The current DDMI status.

psecLimitReached: Learned MAC addresses from all limit control enabled ports reach the upper limit (The upper limit is 1024).

loopDetected: A loop condition has been detected. (Loop Protection → Configuration)

entConfigChange: This stands for "Entity Configuration Change". When in stack condition, the device becomes "Master" in the topology. This device will also be in "Master" status since it is a standalone device.

newRoot: Spanning tree selects a new root.

topologyChange: In spanning tree protocol, a port state has changed.

lldpRemTablesChange: In LLDP, neighbor information has changed.

ipInterfacesLink: VLAN-IP interface link is up or down.

ipDhcpBound: The device obtains IPv4 address from DHCP server.

igmpJoinLeave: IGMP Snooping function detects that new devices would like to join or leave the multicast group.

powerSupply: The current power supply status.

configurationUpload: A configuration file has been uploaded to the device as a running configuration.

firmwareUpdate: Software has been uploaded to the device.

Level: Select the level of specified syslog source. Possible types are:

Error: Indicate the specific messages which severity code is Error (3).

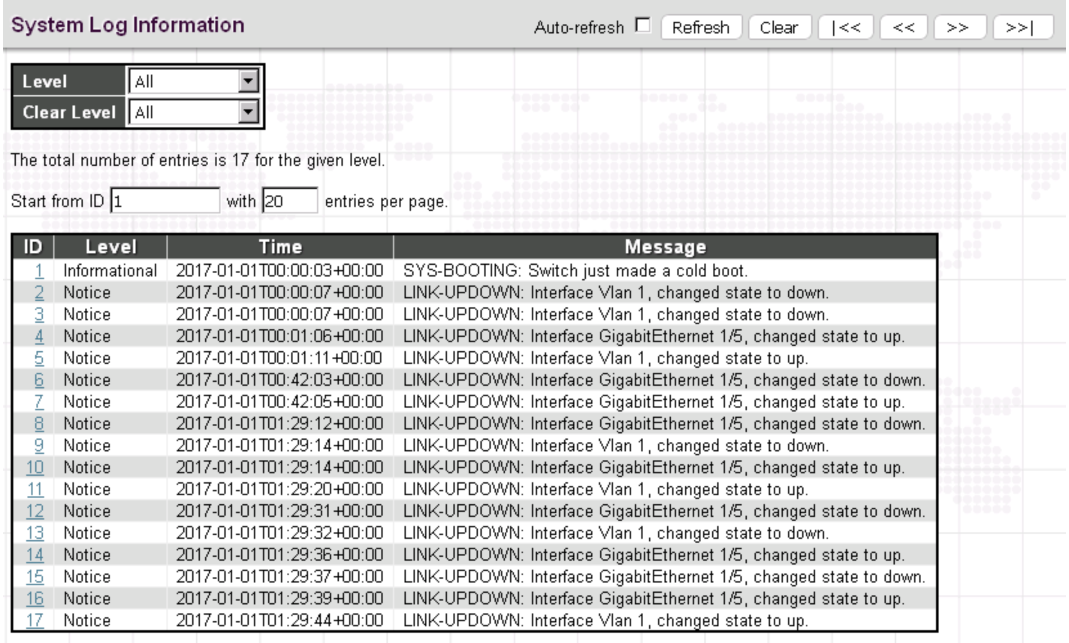
Warning: Indicate the specific messages which severity code is Warning (4).

Notice: Indicate the specific messages which severity code is Notice (5).

Informational: Indicate the specific messages which severity code is Informational (6).

4.2.6.3. Information

Displays the collected log information.



System Log Information

Level	All
Clear Level	All

The total number of entries is 17 for the given level.

Start from ID 1 with 20 entries per page.

ID	Level	Time	Message
1	Informational	2017-01-01T00:00:03+00:00	SYS-BOOTING: Switch just made a cold boot.
2	Notice	2017-01-01T00:00:07+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
3	Notice	2017-01-01T00:00:07+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
4	Notice	2017-01-01T00:01:06+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/5, changed state to up.
5	Notice	2017-01-01T00:01:11+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
6	Notice	2017-01-01T00:42:03+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/5, changed state to down.
7	Notice	2017-01-01T00:42:05+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/5, changed state to up.
8	Notice	2017-01-01T01:29:12+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/5, changed state to down.
9	Notice	2017-01-01T01:29:14+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
10	Notice	2017-01-01T01:29:14+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/5, changed state to up.
11	Notice	2017-01-01T01:29:20+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
12	Notice	2017-01-01T01:29:31+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/5, changed state to down.
13	Notice	2017-01-01T01:29:32+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
14	Notice	2017-01-01T01:29:36+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/5, changed state to up.
15	Notice	2017-01-01T01:29:37+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/5, changed state to down.
16	Notice	2017-01-01T01:29:39+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/5, changed state to up.
17	Notice	2017-01-01T01:29:44+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.

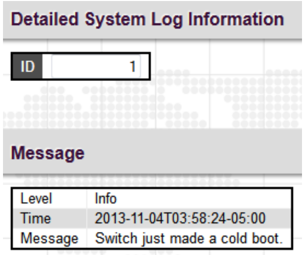
Level: Use this pull down to display all messages or messages of type info, warning or error.

Clear Level: Use this pull down to clear selected message types from the log.

Click a particular ID number to view its detailed log message. See ‘System Detailed Log’ section.

4.2.6.4. Detailed Log

Displays individual log records.



Detailed System Log Information

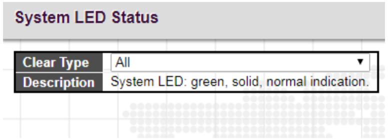
ID 1

Message

Level	Info
Time	2013-11-04T03:58:24-05:00
Message	Switch just made a cold boot.

View each log, by ID number.

4.2.7. LED Status



System LED Status

Clear Type	All
Description	System LED: green, solid, normal indication.

Clear Type: Select the suitable clear type.

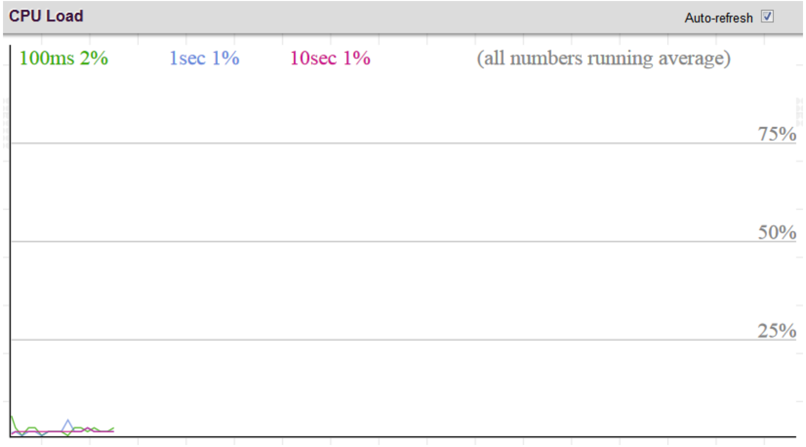
All: Clear all LED indication errors and back to normal status.

Fatal: Clear fatal error status of LED indication.

Software: Clear software error status of LED indication.

4.2.8. System CPU Load

This page displays the CPU load, using an SVG graph.



The load is measured as averaged over the last 100ms, 1sec 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. Automatic refresh occurs every 3 seconds.

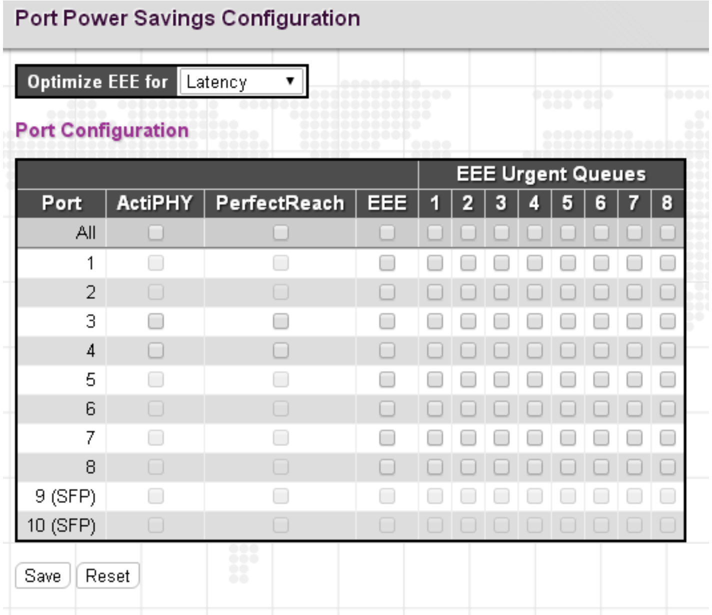
4.3. Green Ethernet

EEE is a power saving option that reduces the power usage when there is low or no traffic utilization. EEE was developed through the IEEE802.3az task force of the Institute of Electrical and Electronic Engineers (IEEE). EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is called wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP (Link Layer Discovery Protocol) protocol.

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode. For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for. When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic. For traffic that should not be held back, urgent queues may be assigned to reduce latency yet still result in overall power saving.

4.3.1. Configuration

Configure EEE (Energy-Efficient Ethernet) as well as Ethernet power savings.



Port Power Savings Configuration

Optimize EEE for: Latency ▾

Port Configuration

				EEE Urgent Queues							
Port	ActiPHY	PerfectReach	EEE	1	2	3	4	5	6	7	8
All	□	□	□	□	□	□	□	□	□	□	□
1	□	□	□	□	□	□	□	□	□	□	□
2	□	□	□	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□	□	□	□
4	□	□	□	□	□	□	□	□	□	□	□
5	□	□	□	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	□	□	□	□
7	□	□	□	□	□	□	□	□	□	□	□
8	□	□	□	□	□	□	□	□	□	□	□
9 (SFP)	□	□	□	□	□	□	□	□	□	□	□
10 (SFP)	□	□	□	□	□	□	□	□	□	□	□

Optimize EEE for: Enables/disables the EEE function for this switch. The two options are:

Power: Set to optimize EEE for best power saving.

Latency: Set to optimize EEE for least traffic latency.

Port Configuration

ActiPHY™: ActiPHY™ works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if an Ethernet cable is inserted. For ports with no cable connection, the PHY remains powered down to save energy.

PerfectReach™: PerfectReach™ is another power saving mechanism. PerfectReach™ works by determining the cable length and lowering the Ethernet transmit power for ports with short cables.

EEE (Energy-Efficient Ethernet): EEE is a power saving option that reduces the power usage when there is low or no traffic utilization. EEE was developed through the IEEE802.3az task force of the Institute of Electrical and Electronic Engineers (IEEE). EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is called wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP (Link Layer Discovery Protocol) protocol. EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode. For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for.

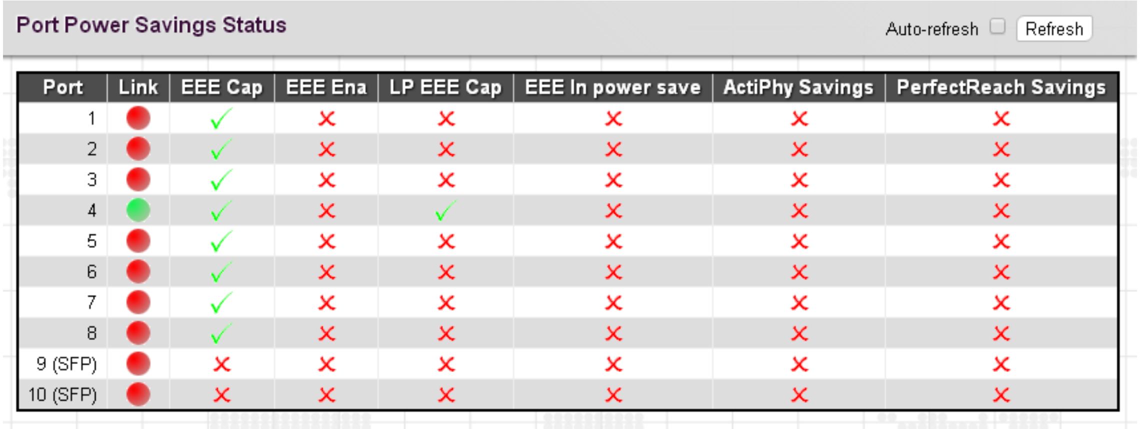
When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic. For traffic that should not be held back, urgent queues may be assigned to reduce latency yet still result in overall power saving.

EEE Urgent Queues: It is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

4.3.2. Status

Display the energy saving status for all ports.

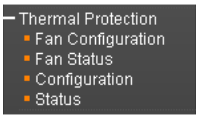


Port Power Savings Status

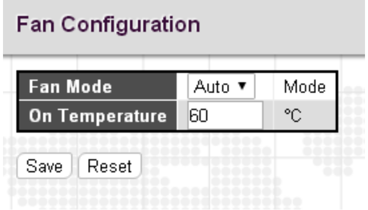
Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE In power save	ActiPhy Savings	PerfectReach Savings
1	🔴	✓	✕	✕	✕	✕	✕
2	🔴	✓	✕	✕	✕	✕	✕
3	🔴	✓	✕	✕	✕	✕	✕
4	🟢	✓	✕	✓	✕	✕	✕
5	🔴	✓	✕	✕	✕	✕	✕
6	🔴	✓	✕	✕	✕	✕	✕
7	🔴	✓	✕	✕	✕	✕	✕
8	🔴	✓	✕	✕	✕	✕	✕
9 (SFP)	🔴	✕	✕	✕	✕	✕	✕
10 (SFP)	🔴	✕	✕	✕	✕	✕	✕

4.4. Thermal Protection

This page allows the user to inspect and configure the current setting for controlling thermal protection. Thermal protection is used to protect the chip from getting overheated.



4.4.1. Fan Configuration



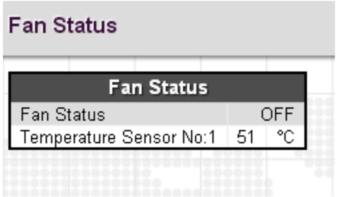
Fan Configuration

Fan Mode	Auto ▾	Mode
On Temperature	60	°C

Fan Mode: Turn on or turn off fans immediately. Selecting “Auto” when you want to turn on fans to cool down the device automatically when the temperature of the device gets too high.

On Temperature: The temperature which fans will be turned on. The accepted temperature is between the range -127 to 127.

4.4.2. Fan Status



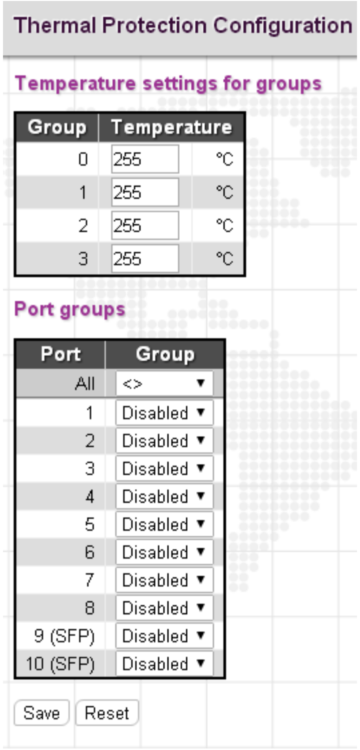
Fan Status

Fan Status		
Fan Status		OFF
Temperature Sensor No:1	51	°C

Fan Status: This field shows the current status of rear fans.

Temperature Sensor: The current temperature that the sensor detects.

4.4.3. Thermal Protection Configuration



Thermal Protection Configuration

Temperature settings for groups

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

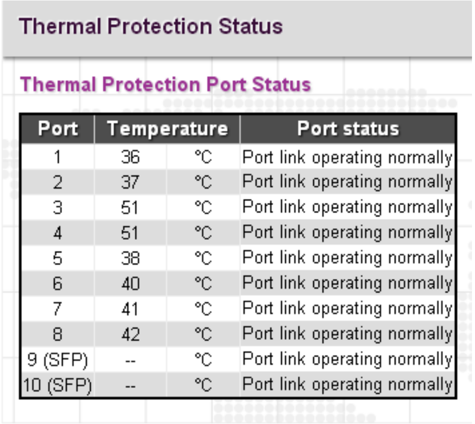
Port groups

Port	Group
All	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9 (SFP)	Disabled
10 (SFP)	Disabled

Temperature settings for priority groups: Specify the temperature at which the ports with the corresponding priority will be turned off. Temperatures between 0˚C and 255˚C are supported.

Port priorities: The priority the port belongs to. There are 4 priority levels supported.

4.4.3.1. Thermal Protection Status



Thermal Protection Status

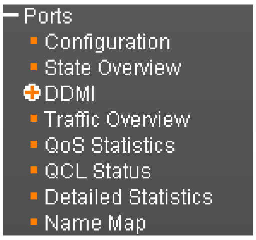
Thermal Protection Port Status

Port	Temperature		Port status
1	36	°C	Port link operating normally
2	37	°C	Port link operating normally
3	51	°C	Port link operating normally
4	51	°C	Port link operating normally
5	38	°C	Port link operating normally
6	40	°C	Port link operating normally
7	41	°C	Port link operating normally
8	42	°C	Port link operating normally
9 (SFP)	--	°C	Port link operating normally
10 (SFP)	--	°C	Port link operating normally

This page shows the current temperature of each port and port status.

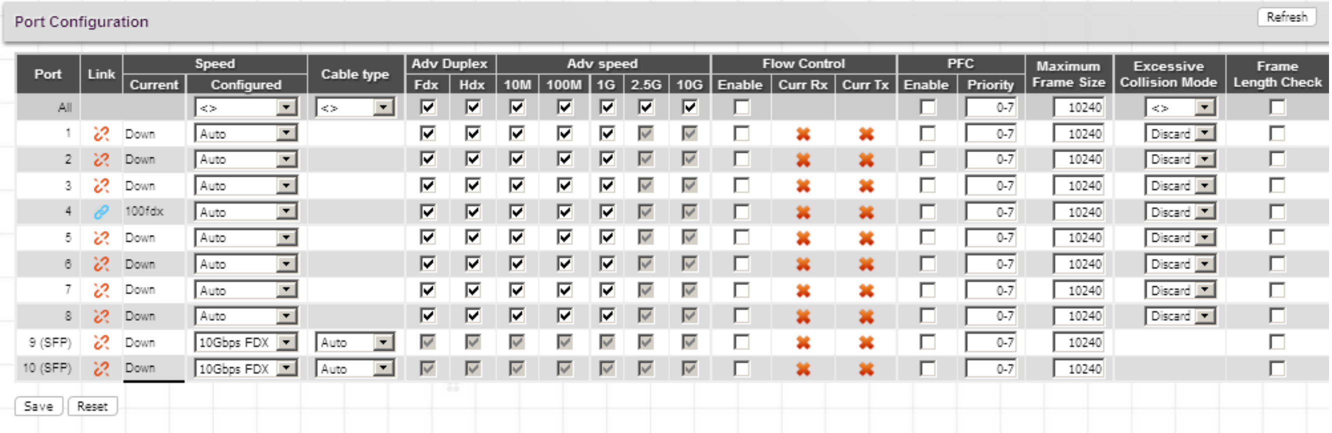
4.5. Ports

Configurations related to the fiber and electrical ports are performed under the Ports menu.



4.5.1. Ports Configuration

This page displays current port configurations and allows some configuration here.



Port Configuration

Refresh

Port	Link	Speed		Cable type	Adv Duplex		Adv speed					Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
		Current	Configured		Fdx	Hdx	10M	100M	1G	2.5G	10G	Enable	Curr Rx	Curr Tx	Enable	Priority			
All			<>	<>	☑	☑	☑	☑	☑	☑	☑	□			□	0-7	10240	<>	□
1		Down	Auto		☑	☑	☑	☑	☑	☑	☑	□	✖	✖	□	0-7	10240	Discard	□
2		Down	Auto		☑	☑	☑	☑	☑	☑	☑	□	✖	✖	□	0-7	10240	Discard	□
3		Down	Auto		☑	☑	☑	☑	☑	☑	☑	□	✖	✖	□	0-7	10240	Discard	□
4		100fdx	Auto		☑	☑	☑	☑	☑	☑	☑	□	✖	✖	□	0-7	10240	Discard	□
5		Down	Auto		☑	☑	☑	☑	☑	☑	☑	□	✖	✖	□	0-7	10240	Discard	□
6		Down	Auto		☑	☑	☑	☑	☑	☑	☑	□	✖	✖	□	0-7	10240	Discard	□
7		Down	Auto		☑	☑	☑	☑	☑	☑	☑	□	✖	✖	□	0-7	10240	Discard	□
8		Down	Auto		☑	☑	☑	☑	☑	☑	☑	□	✖	✖	□	0-7	10240	Discard	□
9 (SFP)		Down	10Gbps FDX	Auto	☑	☑	☑	☑	☑	☑	☑	□	✖	✖	□	0-7	10240		□
10 (SFP)		Down	10Gbps FDX	Auto	☑	☑	☑	☑	☑	☑	☑	□	✖	✖	□	0-7	10240		□

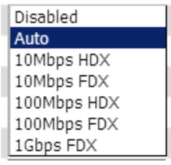
Save Reset

Port: This device is managed Gigabit switches with 8 electrical LAN ports numbered 1~8 and 2 fiber optical ports (for SFP module) numbered 9~10. Each logical port number is displayed in a row. The "All" settings will apply actions on all ports.

Link: The current link state for each port is displayed graphically. Blue indicates the link is up and red indicates that it is down.

Current Speed: This column provides the current link speed (Auto nego, 10, 100, 1G, 2.5G, 10G) and duplex (fdx=Full Duplex, hdx=Half Duplex) of each port.

Configured Speed: This pull down selects any available link speed for the given switch port. Only speeds supported by the specific port are shown.



Possible copper port settings are:

Disabled - Disables the switch port operation.

Auto - Port auto negotiating speed with the link partner, selecting the highest speed that is compatible with the link partner and negotiating the duplex mode.

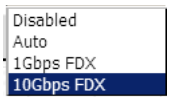
10Mbps HDX - Forces the port to 10Mbps half duplex mode.

10Mbps FDX - Forces the port to 10Mbps full duplex mode.

100Mbps HDX - Forces the port to 100Mbps half duplex mode.

100Mbps FDX - Forces the port to 100Mbps full duplex mode.

1Gbps FDX - Forces the port to 1Gbps full duplex.



Possible fiber port settings are:

Disabled - Disables the switch port operation.

Auto – The port auto negotiates 1G speed with the link partner.

1Gbps FDX - Forces the fiber port to 1Gbps full duplex mode.

10Gbps FDX - Forces the fiber port to 10Gbps full duplex mode.

Adv Duplex: When duplex is set to Auto (i.e. Auto Negotiation), the port will advertise the specified duplex either FDX or HDX to the link partner. By default, the port will advertise all the supported duplexes if the Duplex is Auto.

Adv Speed: When speed is set to Auto (i.e. Auto Negotiation), the port will advertise the specified speeds either 10M, 100M, 1G, 2.5G or 10G to the link partner. By default, the port will advertise all the supported speeds if the speed is Auto.

Flow Control: The “Current Rx” column indicates whether pause frames on the port are obeyed, and the “Current Tx” column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is also related to the setting for Configured Link Speed.

PFC: When PFC (802.1Qbb Priority Flow Control) is enabled on a port then flow control on a priority level is enabled. Through the Priority field, range (one or more) of priorities can be configured, for example: '0-3,7' which equals '0,1,2,3,7'. PFC is not supported through auto negotiation. “PFC” and “Flow Control” cannot both be enabled on the same port.

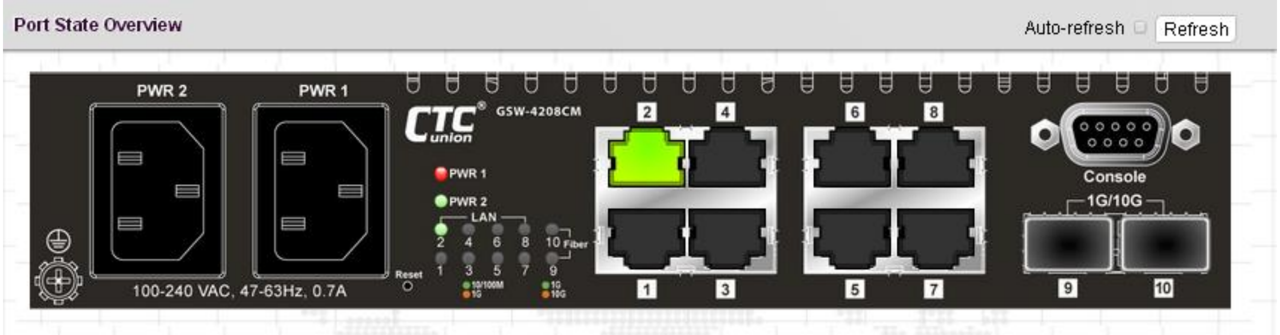
Maximum Frame Size: Enter the maximum frame size allowed for the switch port, including FCS. This switch supports up to 10240 byte packets.

Excessive Collision Mode: This setting configures the port transmit collision behavior to either "Discard" (Discard frame after 16 collisions - default) or "Restart" (Restart backoff algorithm after 16 collisions).

Frame Length Check: Tick the checkbox if you want to enable Frame Length Check function. If enabled and frames with incorrect frame length (less than 1536 bytes) in EtherType/Length field, frames will be dropped. If disabled, frames are not dropped due to frame length mismatch.

4.5.2. State Overview

Display an overview graphic of the switch.

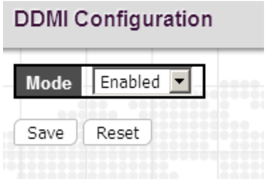


Port State Overview

This is the same graphic overview shown when first logging into the switch for management. The link status display can be updated by clicking the "Refresh" button. When "Auto-refresh" is checked, the display will be updated every 3 seconds. "Green" colored ports indicate a linked state of RJ-45 ports; while, "Amber" colored ports indicate a 1G linked state of SFP fiber ports and "Blue" colored ports indicate 10G linked state of SFP fiber ports. "Black" ports have no link and "Gray" ports mean ports are disabled.

4.5.3. DDMI

4.5.3.1. Configuration



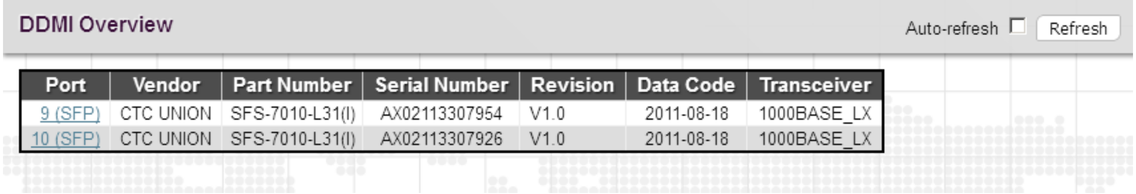
DDMI Configuration

Mode: Enabled

Mode: Enable or disable DDMI function.

4.5.3.2. Overview

This page provides status of SFP.



DDMI Overview

Port	Vendor	Part Number	Serial Number	Revision	Data Code	Transceiver
9 (SFP)	CTC UNION	SFS-7010-L31(I)	AX02113307954	V1.0	2011-08-18	1000BASE_LX
10 (SFP)	CTC UNION	SFS-7010-L31(I)	AX02113307926	V1.0	2011-08-18	1000BASE_LX

This page displays DDMI overview information.

Port: Shows DDMI port number.

Vendor: Vendor name SFP vendor name.

Part Number: Vendor PN Part number provided by SFP vendor.

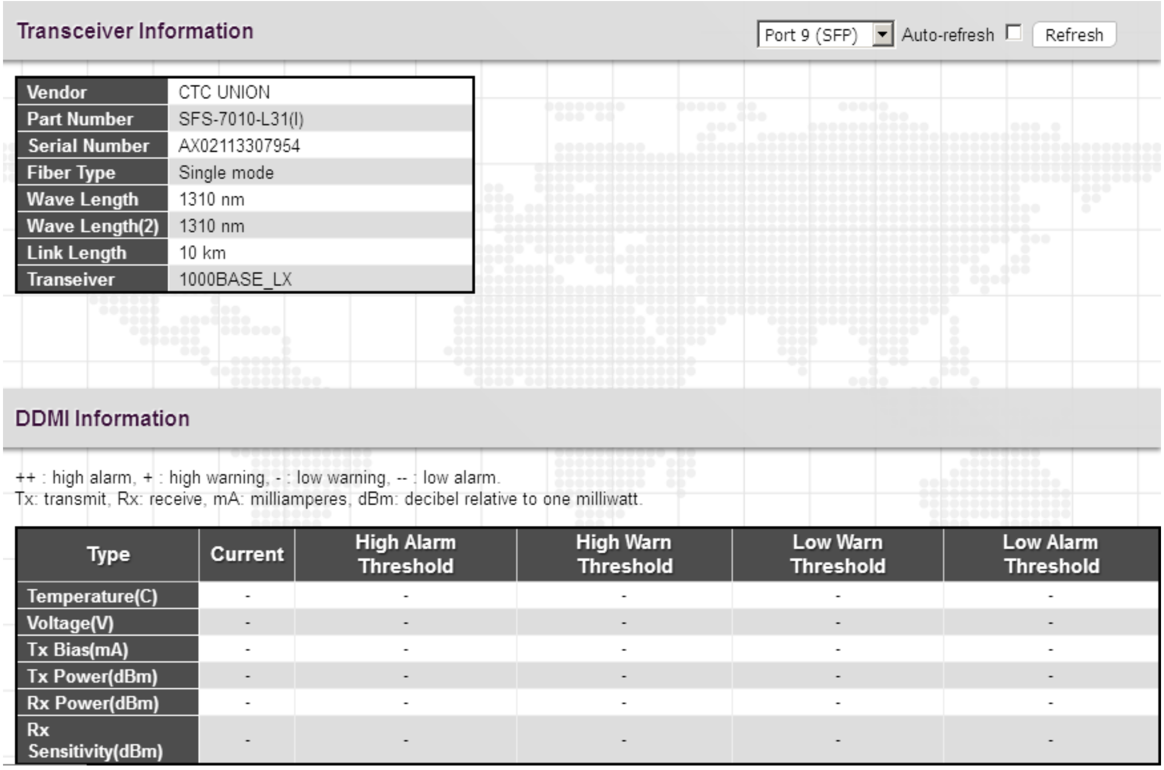
Serial Number: Vendor SN Serial number provided by vendor.

Revision: Vendor rev Revision level for part number provided by vendor.

Data Code: Vendor's manufacturing date code.

Transceiver: Shows transceiver compatibility.

4.5.3.3. Detailed



Transceiver Information

Vendor	CTC UNION
Part Number	SFS-7010-L31(I)
Serial Number	AX02113307954
Fiber Type	Single mode
Wave Length	1310 nm
Wave Length(2)	1310 nm
Link Length	10 km
Transeiver	1000BASE_LX

DDMI Information

++ : high alarm, + : high warning, - : low warning, -- : low alarm.
Tx: transmit, Rx: receive, mA: milliamperes, dBm: decibel relative to one milliwatt.

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	-	-	-	-	-
Voltage(V)	-	-	-	-	-
Tx Bias(mA)	-	-	-	-	-
Tx Power(dBm)	-	-	-	-	-
Rx Power(dBm)	-	-	-	-	-
Rx Sensitivity(dBm)	-	-	-	-	-

This page displays DDMI detailed information.

Transceiver Information

Vendor: Vendor name SFP vendor name.

Part Number: Vendor PN Part number provided by SFP vendor.

Serial Number: Vendor SN Serial number provided by vendor.

Revision: Vendor Revision level for part number provided by vendor.

Data Code: Date code Vendor's manufacturing date code.

Transceiver: Shows transceiver compatibility.

DDMI Information

Current: The current value of temperature, voltage, TX bias, TX power, and RX power.

High Alarm Threshold: The high alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

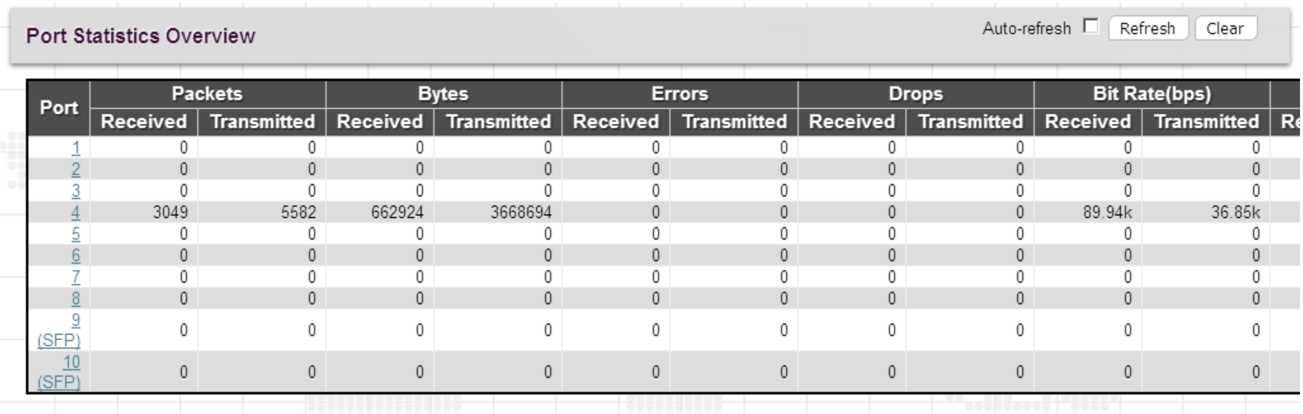
High Warn Threshold: The high warn threshold value of temperature, voltage, TX bias, TX power, and RX power.

Low Warn Threshold: The low warn threshold value of temperature, voltage, TX bias, TX power, and RX power.

Low Alarm Threshold: The low alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

4.5.4. Ports Traffic Overview

Displays a comprehensive overview of traffic on all ports.



Port	Packets		Bytes		Errors		Drops		Bit Rate(bps)		
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Re
1	0	0	0	0	0	0	0	0	0	0	
2	0	0	0	0	0	0	0	0	0	0	
3	0	0	0	0	0	0	0	0	0	0	
4	3049	5582	662924	3668694	0	0	0	0	89.94k	36.85k	
5	0	0	0	0	0	0	0	0	0	0	
6	0	0	0	0	0	0	0	0	0	0	
7	0	0	0	0	0	0	0	0	0	0	
8	0	0	0	0	0	0	0	0	0	0	
9 (SFP)	0	0	0	0	0	0	0	0	0	0	
10 (SFP)	0	0	0	0	0	0	0	0	0	0	

Port: The logical port for the data contained in the same row.

Packets: The number of received and transmitted packets per port.

Bytes: The number of received and transmitted bytes per port.

Errors: The number of frames received in error and the number of incomplete transmissions per port.

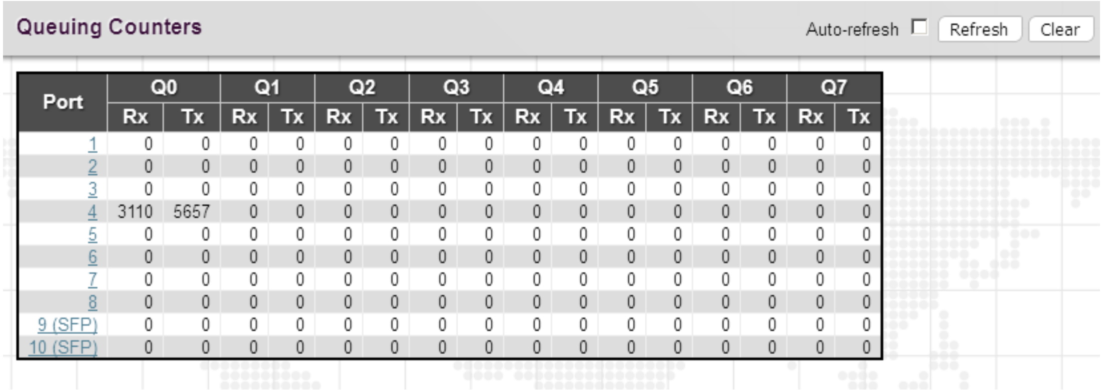
Drops: The number of frames discarded due to ingress or egress congestion.

Filtered: The number of received frames filtered by the forwarding process.

The counter display can be updated by clicking the "Refresh" button. When "Auto-refresh" is checked, the display will be updated every 3 seconds. Clicking the "Clear" button will zero all counters and start counting again.

4.5.5. QoS Statistics

This page provides statistics for the different queues for all switch ports.



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	3110	5657	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	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 (SFP)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10 (SFP)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

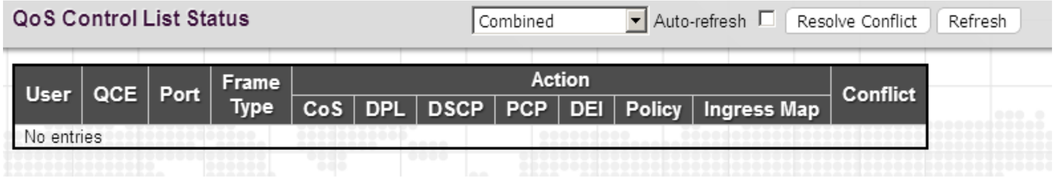
Port: The logical port for the settings contained in the same row.

Qn: There are 8 QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx: The number of received and transmitted packets per queue.

4.5.6. Ports QCL Status

This page shows the QCL status by different QCL users.



User	QCE	Port	Frame Type	Action							Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	Ingress Map	
No entries											

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.

User: Indicates the QCL user.

QCE#: Indicates the index of QCE.

Port: Indicate the port number associated with this QCE.

Frame Type: Indicates the type of frame to look for incoming frames. Possible frame types are:

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: Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP.

CoS: Classified QoS class; if a frame matches the QCE it will be put in the queue.

DPL: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column.

DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.

PCP: If a frame matches the QCE then PCP will be classified with the value displayed under PCP column.

DEI: If a frame matches the QCE then DEI will be classified with the value displayed under DEI column.

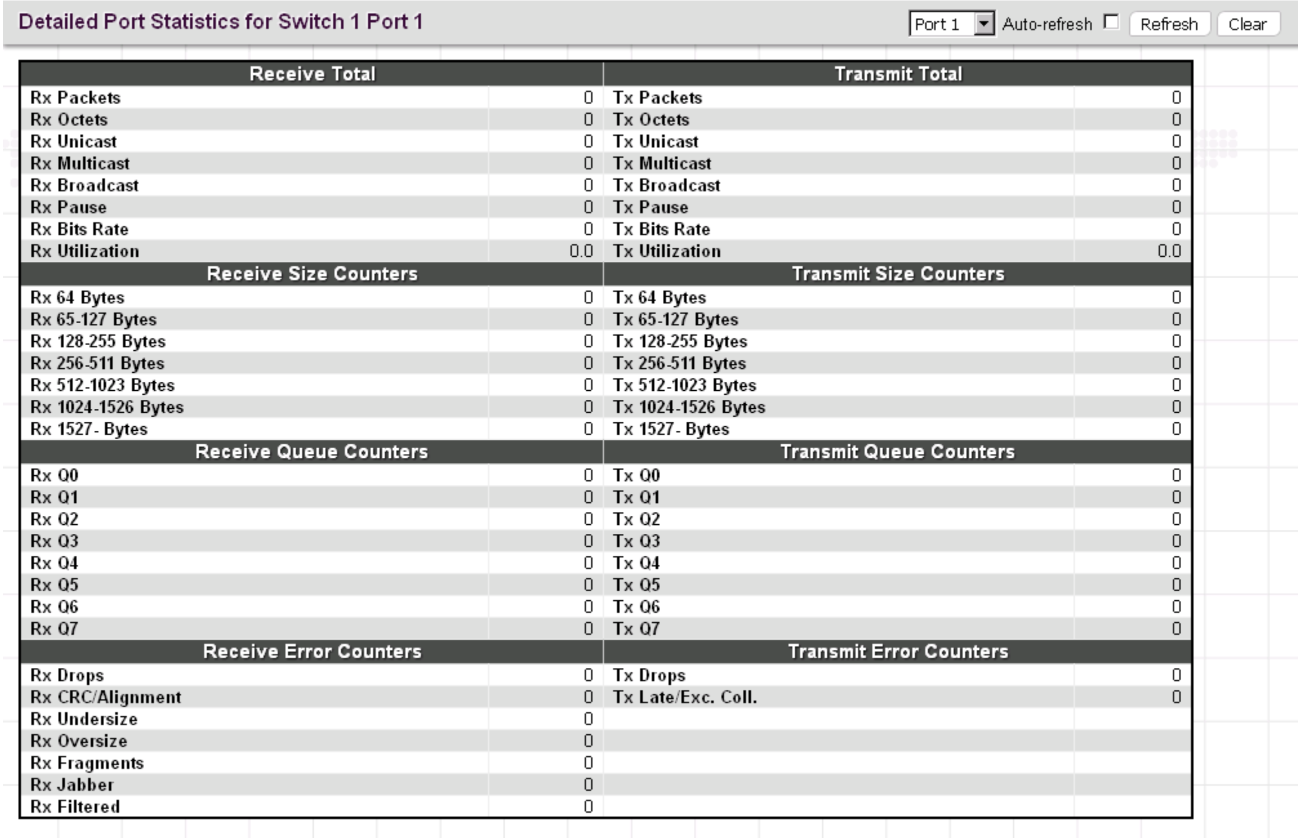
Policy: ACL policy number.

Ingress Map: Classify Ingress Map ID.

Conflict: Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications, it may happen that resources are required to add a QCE may not be available. In that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

4.5.7. Ports Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit. Use the port select pull down to select which switch port details to display.



Detailed Port Statistics for Switch 1 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
Rx Bits Rate	0	Tx Bits Rate	0
Rx Utilization	0.0	Tx Utilization	0.0
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
Rx Q7	0	Tx Q7	0
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

<u>Receive Total and Transmit Total</u>

Rx and Tx Packets: The number of received and transmitted (good and bad) packets.

Rx and Tx Octets: The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

Rx and Tx Unicast: The number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast: The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast: The number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause: A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE.

Receive and Transmit Size Counters

RX & TX 64 Bytes~1527: Displays the number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

RX & TX Q0~Q7: Displays the number of received and transmitted packets per input and output queue.

Receive Error Counters

Rx Drops: The number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment: The number of frames received with CRC or alignment errors.

Rx Undersize: The number of short [1] frames received with valid CRC.

Rx Oversize: The number of long [2] frames received with valid CRC.

Rx Fragments: The number of short [1] frames received with invalid CRC.

Rx Jabber: The number of long [2] frames received with invalid CRC.

Rx Filtered: The number of received frames filtered by the forwarding process.

[1] Short frames are frames that are smaller than 64 bytes.

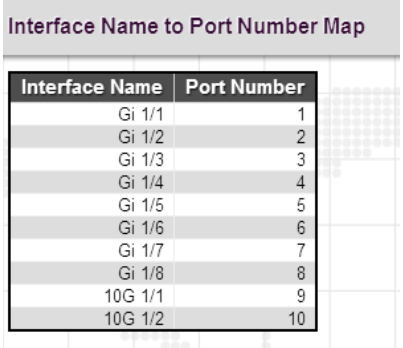
[2] Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

Tx Drops: The number of frames dropped due to output buffer congestion.

Tx Late/Exc. Coll.: The number of frames dropped due to excessive or late collisions.

4.5.8. Name Map



Interface Name to Port Number Map

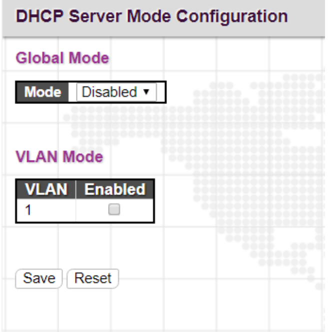
Interface Name	Port Number
Gi 1/1	1
Gi 1/2	2
Gi 1/3	3
Gi 1/4	4
Gi 1/5	5
Gi 1/6	6
Gi 1/7	7
Gi 1/8	8
10G 1/1	9
10G 1/2	10

This table shows the mapping of interface and port number. The interface name and port number are used interchangeable.

4.6. DHCPv4

4.6.1. Server

4.6.1.1. DHCP Server Mode Configuration



DHCP Server Mode Configuration

Global Mode

Mode: Disabled ▾

VLAN Mode

VLAN	Enabled
1	□

Global Mode

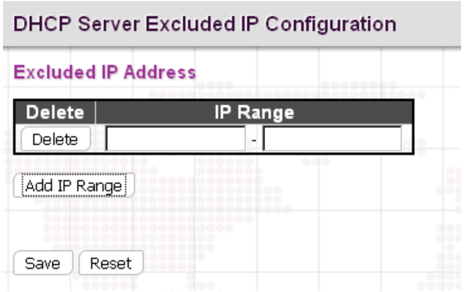
Mode: Enable or disable DHCP server mode. When enabled, this device can act as a DHCP server and provide IP address to clients that request for one.

VLAN Mode

Mode: Indicates the operation mode per VLAN.

Enabled: Enable DHCP server on the specified VLAN.

4.6.1.2. DHCP Server Excluded IP Configuration



DHCP Server Excluded IP Configuration

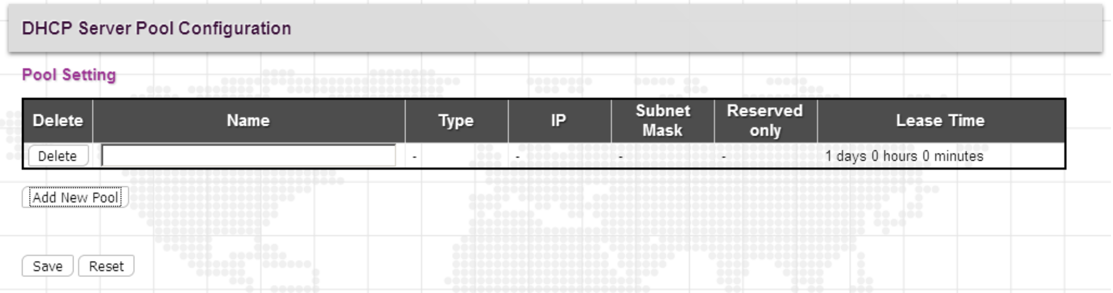
Excluded IP Address

Delete	IP Range
Delete	-

Click “Add IP Range” to set up IP pool range.

IP Range: Enter the starting and ending IP address that are not allocated to DHCP clients. The starting IP address must be smaller or equal to the ending IP address. If there is only one excluded IP address, it can be entered either in starting or ending IP address field. The total Excluded IP address ranges can be supported is 16.

4.6.1.3. DHCP Server Pool Configuration



DHCP Server Pool Configuration

Pool Setting

Delete	Name	Type	IP	Subnet Mask	Reserved only	Lease Time
Delete		-	-	-	-	1 days 0 hours 0 minutes

Click “Add New Pool” to add a new entry to the list. The maximum entries supported are 640.

Name: Enter the pool name for this entry. All printable characters are supported except white space. Click on the pool name after save to configure its detailed settings.

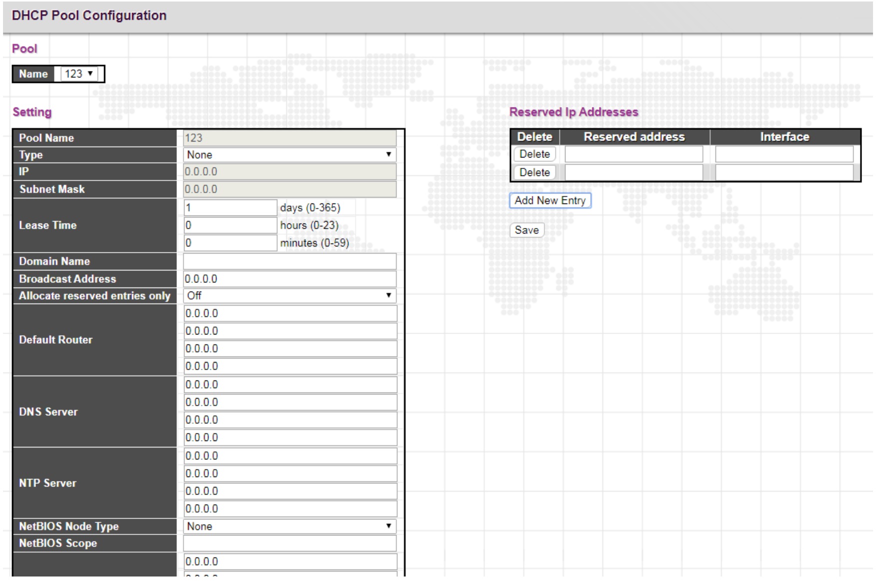
Type: Display which type the pool is. The displayed options include Network and Host. If “ – ” is displayed, it means this field has not been defined yet.

IP: Display network number of the DHCP address pool. If “ – ” is displayed, it means this field has not been defined yet.

Subnet Mask: Display subnet mask of the DHCP address pool. If “ – ” is displayed, it means this field has not been defined yet.

Lease Time: Display the lease time of the configured pool.

Click on the pool name to configure its detailed settings.



DHCP Pool Configuration

Pool

Name	123 ▾

Setting

Pool Name	123
Type	None ▾
IP	0.0.0.0
Subnet Mask	0.0.0.0
Lease Time	1 days (0-365) 0 hours (0-23) 0 minutes (0-59)
Domain Name	
Broadcast Address	0.0.0.0
Allocate reserved entries only	Off ▾
Default Router	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
DNS Server	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
NTP Server	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
NetBIOS Node Type	None ▾
NetBIOS Scope	
	0.0.0.0

Reserved Ip Addresses

Delete	Reserved address	Interface
Delete		
Delete		

Pool

Name: Select the pool name that you want to configure from the pull-down menu.

Setting

Pool Name: Display the pool name for this configured entry.

Type: Select the pool type.

Network: The pool defines a pool of IP addresses to service more than one DHCP client.

Host: The pool services for a specific DHCP client identified by client identifier or hardware address.

IP: Specify the network IP of the DHCP address pool.

Subnet Mask: Specify subnet mask of the DHCP address pool.

Lease Time: Specify lease time that a client needs to send requests to the DHCP server for renewed IP address. If all are 0's, then it means the lease time is infinite.

Domain Name: Specify the domain name that a client use when resolving hostname via DNS.

Broadcast Address: Specify the broadcast address in use on the client's subnet.

Default Router: Specify a list of IP addresses for routers on the clients' subnet.

DNS Server: Specify a list of Domain Name System name servers available to the client.

NTP Server: Specify a list of IP addresses indicating NTP servers available to the client.

NetBios Node Type: Select NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002.

NetBIOS Scope: Specify the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002.

NetBIOS Name Server: Specify a list of NBNS name servers listed in order of preference.

NIS Domain Name: Specify the name of the client's NIS domain.

NIS Server: Specify a list of IP addresses indicating NIS servers available to the client.

Client Identifier: Specify client's unique identifier to be used when the pool is the type of host.

Hardware Address: Specify client's hardware (MAC) address to be used when the pool is the type of host.

Client Name: Specify the name of client to be used when the pool is the type of host.

Vendor 1~4 Class Identifier: Specify to be used by DHCP client to optionally identify the vendor type and configuration of a DHCP client. DHCP server will deliver the corresponding option 43 specific information to the client that sends option 60 vendor class identifier.

Vendor 1~4 Specific Information: Specify vendor specific information according to option 60 vendor class identifier.

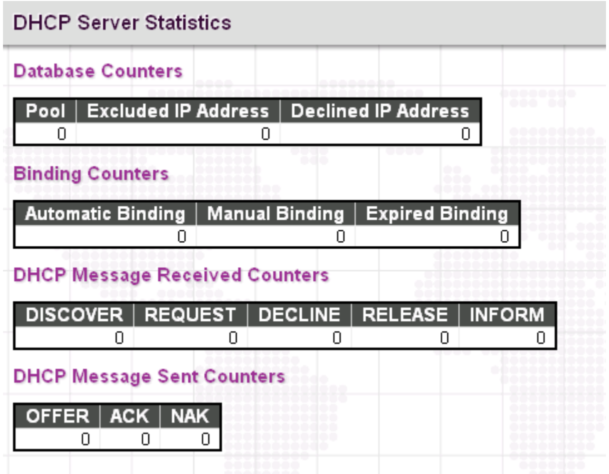
Reserved IP Address

Click the "Add New Entry" button to create a new rule.

Reserved Address: Specify the IP addresses reserved for the port interface.

Interface: Select the interface that uses the reserved IP address.

4.6.1.4. DHCP Server Statistics



DHCP Server Statistics

Database Counters

Pool	Excluded IP Address	Declined IP Address
0	0	0

Binding Counters

Automatic Binding	Manual Binding	Expired Binding
0	0	0

DHCP Message Received Counters

DISCOVER	REQUEST	DECLINE	RELEASE	INFORM
0	0	0	0	0

DHCP Message Sent Counters

OFFER	ACK	NAK
0	0	0

Database Counters

Pool: The number of pool that has been configured.

Excluded IP Address: The number of excluded IP address.

Declined IP Address: The number of declined IP address.

Binding Counters

Automatic Binding: The number of bindings with network-type pools.

Manual Binding: The number of bindings that the network engineer assigns an IP address to a client. In other words, the pool is of host type.

Expired Binding: The number of bindings that their lease time expired or they are cleared from Automatic or Manual type bindings.

DHCP Message Received Counters

Discover: The number of DHCP DISCOVER messages received.

Request: The number of DHCP REQUEST messages received.

Decline: The number of DHCP DECLINE messages received.

Release: The number of DHCP RELEASE messages received.

Inform: The number of DHCP INFORM messages received.

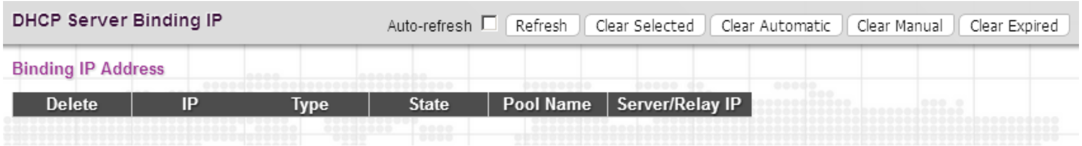
DHCP Message Sent Counters

OFFER: The number of DHCP OFFER messages sent.

ACK: The number of DHCP ACK messages sent.

NAK: The number of DHCP NAK messages sent.

4.6.1.5. DHCP Server Binding IP



DHCP Server Binding IP

Auto-refresh □ Refresh Clear Selected Clear Automatic Clear Manual Clear Expired

Binding IP Address

Delete	IP	Type	State	Pool Name	Server/Relay IP

IP: The IP address allocated to DHCP client.

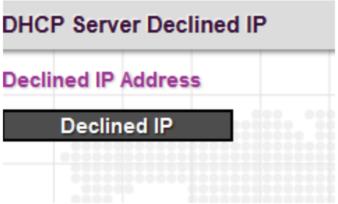
Type: The type of binding method. This field can be “Automatic”, “Manual” or “Expired”.

State: The state of binding. Possible states are “Committed”, “Allocated”, or “Expired”.

Pool Name: The pool that generates the binding.

Server/Relay IP: The DHCP server IP address or relay agent IP address which binding was negotiated.

4.6.1.6. DHCP Server Declined IP



DHCP Server Declined IP

Declined IP Address

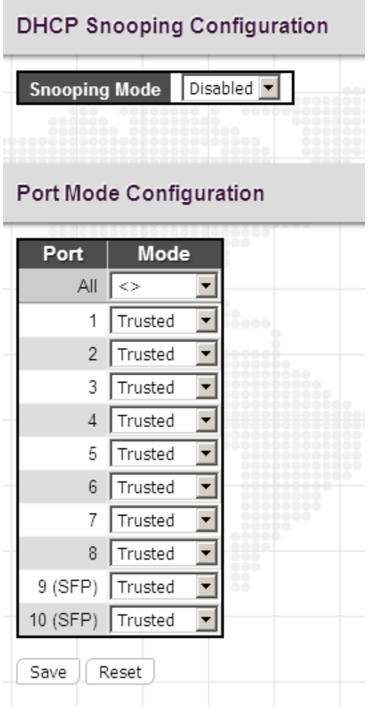
Declined IP

Declined IP: Displays a list of declined IP addresses.

4.6.2. Snooping

4.6.2.1. Configuration

DHCP Snooping allows the switch to protect a network from attacking by other devices or rogue DHCP servers. When DHCP Snooping is enabled on the switch, it can filter IP traffic on insecure (untrusted) ports that the source addresses cannot be identified by DHCP Snooping. The addresses assigned to connected clients on insecure ports can be carefully controlled by either using the dynamic binding registered with DHCP Snooping or using the static binding configured with IP Source Guard.



DHCP Snooping Configuration

Snooping Mode: Disabled

Port Mode Configuration

Port	Mode
All	<>
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted
8	Trusted
9 (SFP)	Trusted
10 (SFP)	Trusted

DHCP Snooping Configuration

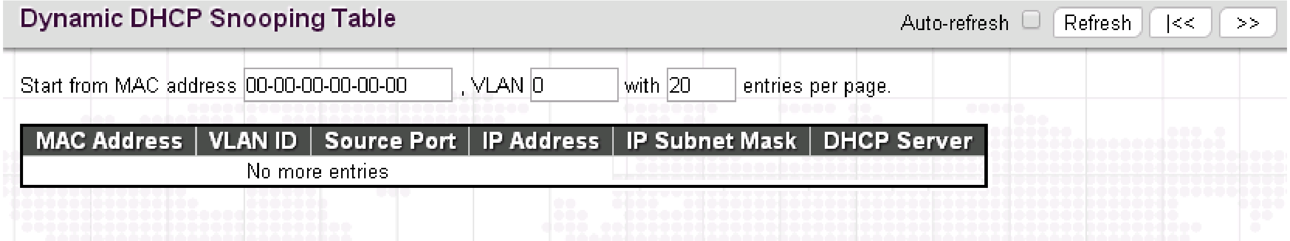
Snooping Mode: Enable or disable DHCP Snooping function globally. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

Port Mode Configuration

Port: Port number. "Port *" rules apply to all ports.

Mode: Select the DHCP Snooping port mode. Ports can be set to either “Trusted” or “Untrusted”.

4.6.2.2. Dynamic Table


Dynamic DHCP Snooping Table

Start from MAC address 00-00-00-00-00-00 , VLAN 0 with 20 entries per page.

MAC Address	VLAN ID	Source Port	IP Address	IP Subnet Mask	DHCP Server
No more entries					

DHCP clients who obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Items displayed include the following:

MAC Address: Client hardware MAC address

VLAN ID: VLAN number of the client interface

Source Port: The port number of the client that binds with IP address.

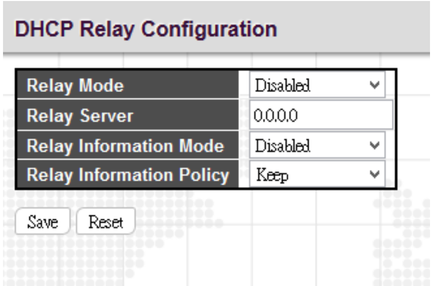
IP Address: Client IP address assigned from the DHCP server.

IP Subnet Mask: Client IP subnet mask.

DHCP Server: The DHCP Server that assigns IP address.

4.6.3. Relay

4.6.3.1. Relay Configuration


DHCP Relay Configuration

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

Relay Mode: Enable or disable the DHCP relay function.

Relay Server: Enter DHCP server IP address that is used by the switch's DHCP relay agent.

Relay Information Mode: Enable or disable DHCP Relay option 82 function. Please note that "Relay Mode" must be enabled before this function is able to take effect.

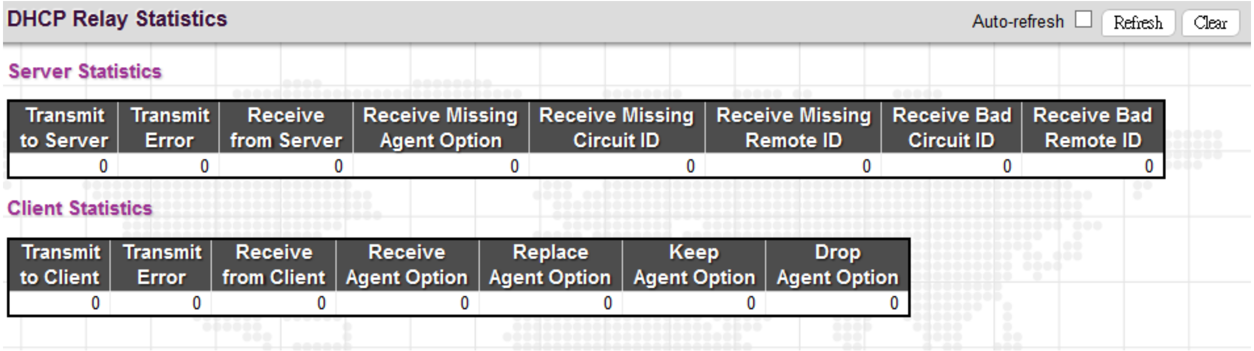
Relay Information Policy: Select Relay Information policy for DHCP client that includes option 82 information.

Replace: Replace the DHCP client packet information with the switch's relay information. This is the default setting.

Keep: Keep the client's DHCP information.

Drop: Drop the packet when it receives a DHCP message that already contains relay information.

4.6.3.2. 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

DHCP Relay Statistics

Transmit to Server: The number of packets that are relayed from client to server.

Transmit Error: The number of packets that resulted in errors while being sent to clients.

Receive from Client: The number of packets received from server.

Receive Missing Agent Option: The number of packets received without agent information options.

Receive Missing Circuit ID: The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID: The number of packets received with the Remote ID option missing.

Receive Bad Circuit ID: The number of packets whose Circuit ID option did not match known circuit ID.

Receive Bad Remote ID: The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Transmit to Client: The number of relayed packets from server to client.

Transmit Error: The number of packets that resulted in error while being sent to servers.

Receive from Client: The number of received packets from server.

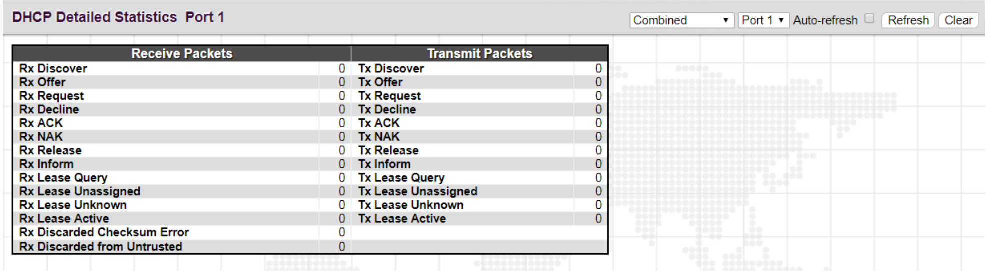
Receive Agent Option: The number of received packets with relay agent information option.

Replace Agent Option: The number of packets which were replaced with relay agent information option.

Keep Agent Option: The number of packets whose relay agent information was retained.

Drop Agent Option: The number of packets that were dropped which were received with relay agent information.

4.6.4. DHCP Detailed Statistics



DHCP Detailed Statistics Port 1

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		

Rx and Tx Discover: The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer: The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request: The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline: The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK: The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK: The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release: The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform: The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query: The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned: The number of lease unassigned (option 53 with value 11) packets received and transmitted.

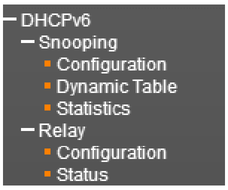
Rx and Tx Lease Unknown: The number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active: The number of lease active (option 53 with value 13) packets received and transmitted.

Rx Discarded checksum error: The number of discard packets that IP/UDP checksum is error.

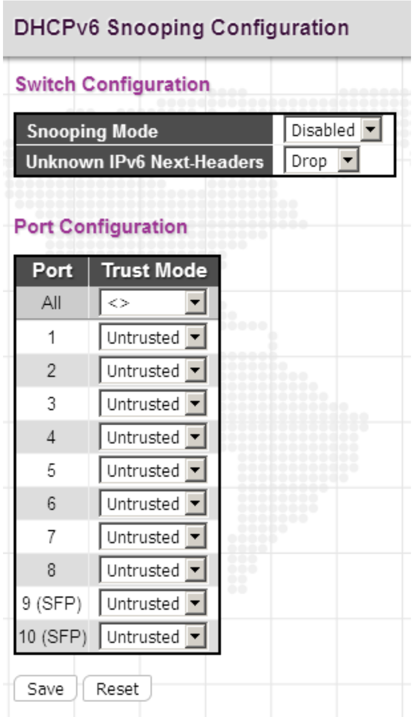
Rx Discarded from Untrusted: The number of discarded packets that are coming from untrusted port.

4.7. DHCPv6



4.7.1. Snooping

4.7.1.1. Configuration



DHCPv6 Snooping Configuration

Switch Configuration

Snooping Mode	Disabled
Unknown IPv6 Next-Headers	Drop

Port Configuration

Port	Trust Mode
All	<>
1	Untrusted
2	Untrusted
3	Untrusted
4	Untrusted
5	Untrusted
6	Untrusted
7	Untrusted
8	Untrusted
9 (SFP)	Untrusted
10 (SFP)	Untrusted

Switch Configuration

Snooping Mode: Enable or disable IPv6 DHCP Snooping mode. When DHCPv6 snooping mode operation is enabled, the DHCPv6 client request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

Unknown IPv6 Next Headers: Specify how unknown IPv6 "next-header" values should be treated. The switch needs to parse all IPv6 packets to a DHCPv6 client to determine if it is in fact a DHCPv6 message. If an unknown IPv6 extension header is encountered the parsing cannot continue. See RFC 7610, section 5, item 3 for details.

Drop: Drop packets with unknown IPv6 extension headers. This is the most secure option but may result in traffic disruptions.

Allow: Allow packets with unknown IPv6 extension headers. This is a less secure option but prevents traffic disruptions.

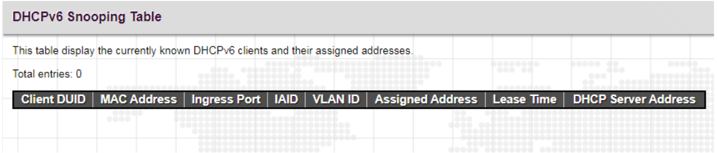
Port Configuration

Trust Mode: Select DHCPv6 snooping mode.

Trusted: Configure the port as trusted source of the DHCPv6 messages.

Untrusted: Configure the port as untrusted source of the DHCPv6 messages.

4.7.1.2. DHCPv6 Snooping Table



DHCPv6 Snooping Table

This table display the currently known DHCPv6 clients and their assigned addresses.

Total entries: 0

Client DUID	MAC Address	Ingress Port	IAID	VLAN ID	Assigned Address	Lease Time	DHCP Server Address

DUID: The DHCP Unique Identifier (DUID) for the client. DHCPv6 uses this value to uniquely identify a client host instead of just using the MAC address of one of its interface ports (as DHCPv4 does).

MAC Address: The MAC address for the client interface port that sent the DHCPv6 message.

Ingress Port: The local port on the snooping switch where client messages are received.

IAID: Each client may contain multiple interfaces and may request addresses for each of these in the same DHCPv6 message. The Identity Association ID (IAID) value uniquely identifies the interface in the scope of the client.

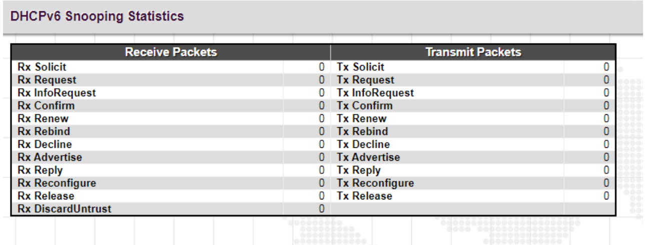
VLAN ID: The VLAN ID which is used by the client messages.

Assigned Address: The address assigned to the interface identified by the IAID value.

Lease Time: The lease time associated with the assigned address in seconds.

DHCP Server Address: The IPv6 address of the DHCP server which assigned the address to the client.

4.7.1.3. Statistics



DHCPv6 Snooping Statistics

Receive Packets		Transmit Packets	
Rx Solicit	0	Tx Solicit	0
Rx Request	0	Tx Request	0
Rx InfoRequest	0	Tx InfoRequest	0
Rx Confirm	0	Tx Confirm	0
Rx Renew	0	Tx Renew	0
Rx Rebind	0	Tx Rebind	0
Rx Decline	0	Tx Decline	0
Rx Advertise	0	Tx Advertise	0
Rx Reply	0	Tx Reply	0
Rx Reconfigure	0	Tx Reconfigure	0
Rx Release	0	Tx Release	0
Rx DiscardUntrust	0		

This page provides statistics for DHCPv6 snooping.

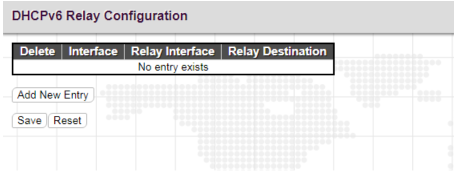
<u>General Receive and Transmit Packets</u>

The page contains both RX and TX counters for all known DHCPv6 message types.

Please refer to RFC 3315 for details on the various DHCPv6 message types.

4.7.2. Relay

4.7.2.1. Configuration



DHCPv6 Relay Configuration

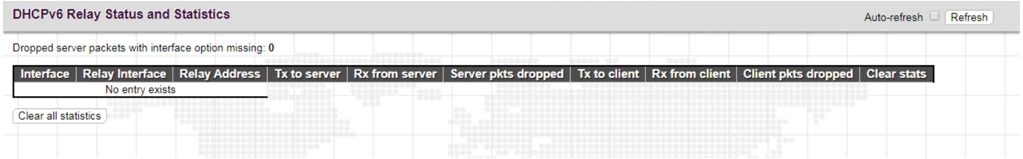
Delete	Interface	Relay Interface	Relay Destination
No entry exists			

Interface: VLAN Interface identification.

Relay Interface: Specify the interface used for relaying.

Relay Destination: Specify the IPv6 address of the DHCPv6 server that requests shall be relayed to.

4.7.2.2. Status and Statistics



DHCPv6 Relay Status and Statistics

Dropped server packets with interface option missing: **0**

Interface	Relay Interface	Relay Address	Tx to server	Rx from server	Server pkts dropped	Tx to client	Rx from client	Client pkts dropped	Clear stats
No entry exists									

Interface: Interface identification. The ID of the interface that receives client requests.

Relay Interface: Interface identification. The ID of the interface used for relaying.

Relay Address: An Ipv6 address represented as human readable test as specified in RFC5952. The IPv6 address that requests shall be relayed to. The default value 'ff05::1:3' means 'any DHCPv6 server'.

Tx to server: Integer number. Number of packets relayed to server.

Rx from server: Integer number. Number of packets received from server.

Server pkts dropped: Integer number. Number of packets from server that relay agent drops.

Tx to client: Integer number. Number of packets sent to client.

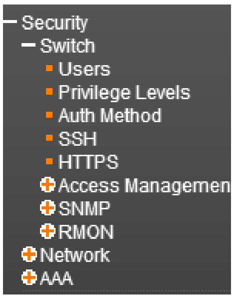
Rx from client: Integer number. Number of packets received from client.

Client pkts dropped: Integer number. Number of packets from client that relay agent drops.

Clear all statistics: Resets all statistics counters of relevant entry to zero.

4.8. Security

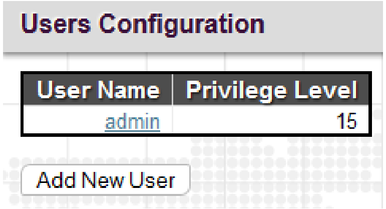
Under the security heading are three major icons, switch, network and AAA (Authentication and Accounting).



4.8.1. Switch

4.8.1.1. Users

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.



Users Configuration

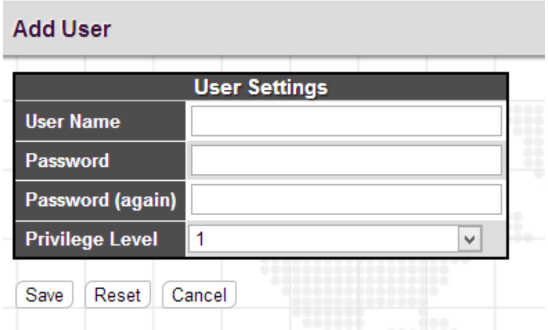
User Name	Privilege Level
admin	15

By default, there is only one user, 'admin'. It is assigned with the highest privilege level of 15.

User Name: The name identifying the user. Click the entries in User Name column to edit the existing users. Or click the "Add New User" button to insert a new user entry.

Privilege Level: The privilege level of the user.

<u>Add User</u>



Add User

User Settings	
User Name	
Password	
Password (again)	
Privilege Level	1

User Name: Enter the new user name.

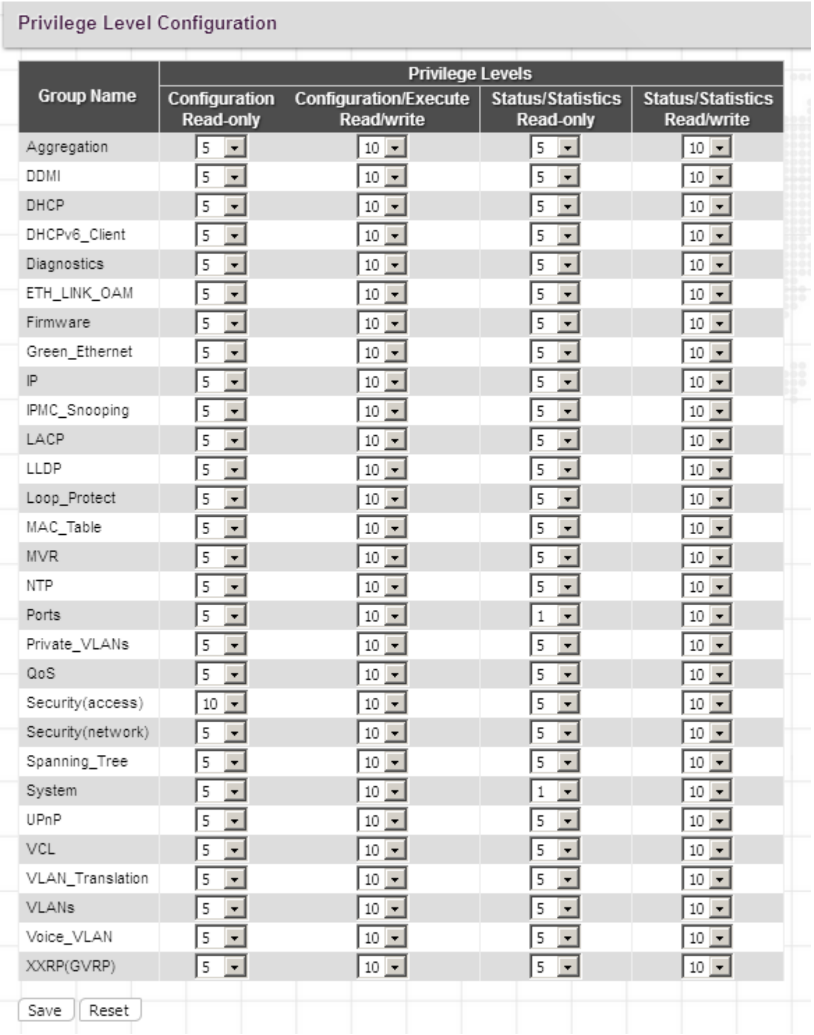
Password: Enter the password for this user account.

Password (again): Retype the password for this user account.

Privilege Level: Select the appropriate privilege level for this user account. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups' privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

4.8.1.2. Privilege Levels

This page provides an overview of the privilege levels.



Privilege Level Configuration

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
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
ETH_LINK_OAM	5	10	5	10
Firmware	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
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
MVR	5	10	5	10
NTP	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10
Security(access)	10	10	5	10
Security(network)	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
UPnP	5	10	5	10
VCL	5	10	5	10
VLAN_Translation	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10
XXRP(GVRP)	5	10	5	10

Group Name: This name identifies 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 contains more than one. The following description defines these privilege level groups in details:

System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.

Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, 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 Levels: Every group has an authorization Privilege level for the following sub groups:

configuration read-only

configuration/execute read-write

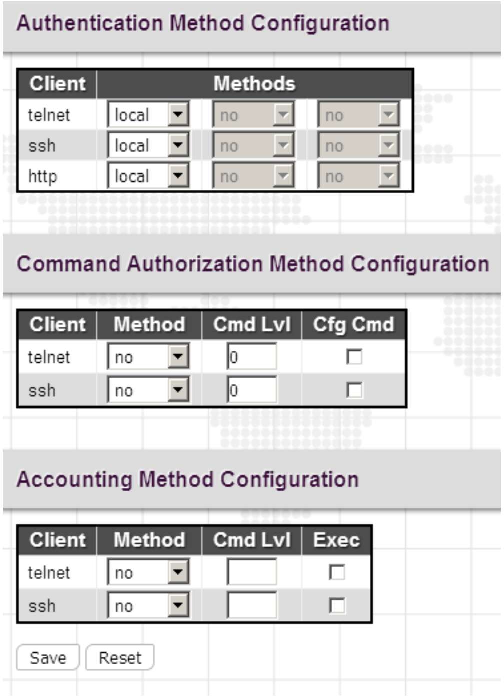
status/statistics read-only

status/statistics read-write (e.g. for clearing of statistics)

User Privilege should be the same or greater than the authorization Privilege level to have access to that group.

4.8.1.3. Auth Method

This page allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.



Authentication Method Configuration

Client	Methods		
telnet	local	no	no
ssh	local	no	no
http	local	no	no

Command Authorization Method Configuration

Client	Method	Cmd Lvl	Cfg Cmd
telnet	no	0	□
ssh	no	0	□

Accounting Method Configuration

Client	Method	Cmd Lvl	Exec
telnet	no		□
ssh	no		□

Accounting Method Configuration

Client: The management client for which the configuration below applies.

Methods: Method can be set to one of the following values:

no: Authentication is disabled and login is not possible.

local: Use the local user database on the switch for authentication.

radius: Use remote RADIUS server(s) for authentication.

tacacs: Use remote TACACS server(s) for authentication.

Note: *Methods that involve remote servers will time out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.*

Command Authentication Method Configuration

Client: The management client for which the configuration below applies.

Methods: Method can be set to one of the following values:

no: Authentication is disabled and login is not possible.

tacacs: Use remote TACACS+ server(s) for authentication.

Cmd Lvl: Authorize all commands with a privilege level higher than or equal to this level.

Cfg cmd: Authorize configuration commands.

Accounting Method Configuration

Client: The management client for which the configuration below applies.

Methods: Method can be set to one of the following values:

no: Authentication is disabled and login is not possible.

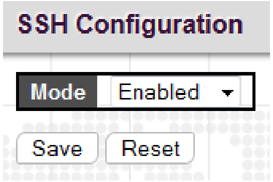
tacacs: Use remote TACACS server(s) for authentication.

Cmd Lvl: Authorize all commands with a privilege level higher than or equal to this level.

Exec: Enable Exec (login) accounting.

4.8.1.4. SSH

Configure SSH on this page.



SSH Configuration

Mode	Enabled

Mode: Indicates the SSH mode operation. Possible modes are:

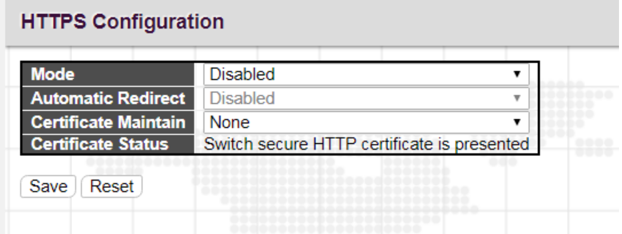
Enabled: Enable SSH mode operation. By default, it is enabled.

Disabled: Disable SSH mode operation.

***Note:** SSH is preferred to Telnet, unless the management network is trusted. Telnet passes authentication credentials in plain text, making those credentials susceptible to packet capture and analysis. SSH provides a secure authentication method. The SSH in this device uses version 2 of SSH protocol.*

4.8.1.5. HTTPS

Configure HTTPS on this page.



HTTPS Configuration

Mode	Disabled
Automatic Redirect	Disabled
Certificate Maintain	None
Certificate Status	Switch secure HTTP certificate is presented

Mode: Indicates the HTTPS operation mode. When the current connection is HTTPS and HTTPS mode operation is disabled, web browser will automatically redirect to an HTTP connection. Possible modes are:

Enabled: Enable HTTPS mode operation.

Disabled: Disable HTTPS mode operation.

Automatic Redirect: Indicates the HTTPS redirect mode operation. It applies only if HTTPS mode "Enabled" is selected. Automatically redirects HTTP of web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled. Possible modes are:

Enabled: Enable HTTPS redirect mode operation.

Disabled: Disable HTTPS redirect mode operation.

Certificate Maintain: Select a way to either upload or generate a certificate.

Certificate Pass Phrase: Configure private key pass phrase. The allowed string length is 0 to 60.

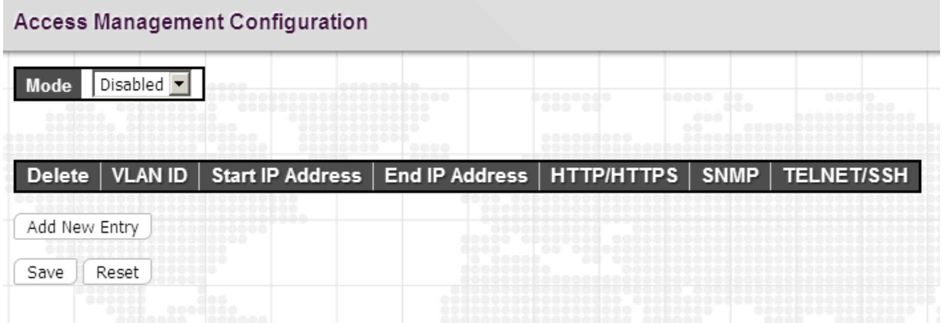
Certificate File: Indicates a way (either Web Browser or URL) to upload a certificate file.

Private Key File: Indicates a private key file for uploading.

4.8.1.6. Access Management

4.8.1.6.1. Configuration

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



Access Management Configuration

Mode: Disabled

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH

Mode: Indicates the access management mode operation. Possible modes are:

Enabled: Enable access management mode operation.

Disabled: Disable access management mode operation.

VLAN ID: Specify the VLAN ID to which this access management setting applies.

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: Checked indicates that the matched host can access the switch from HTTP/HTTPS interface.

SNMP: Checked indicates that the matched host can access the switch from SNMP.

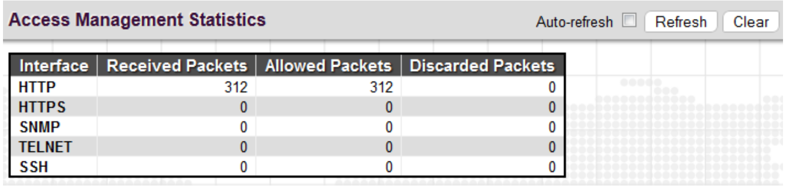
TELNET/SSH: Indicates that the matched host can access the switch from TELNET/SSH interface.

Click the “Add New Entry” button to add a new entry.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

4.8.1.6.2. Access Management Statistics

This page provides statistics for access management.



Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	312	312	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Interface: The interface type through which any remote host can access the switch.

Received Packets: The number of received packets from the interface when access management mode is enabled.

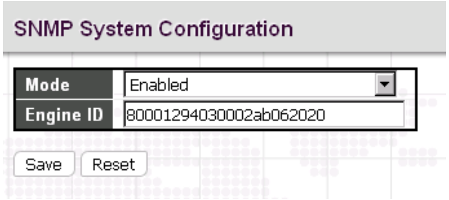
Allowed Packets: The number of allowed packets from the interface when access management mode is enabled.

Discarded Packets: The number of discarded packets from the interface when access management mode is enabled.

4.8.1.7. SNMP

4.8.1.7.1. System Configuration

Configure SNMP on this page.



SNMP System Configuration

Mode	Enabled
Engine ID	80001294030002ab062020

SNMP System Configuration

Mode: Indicates the SNMP mode operation. Possible modes are:

Enabled: Enable SNMP mode operation.

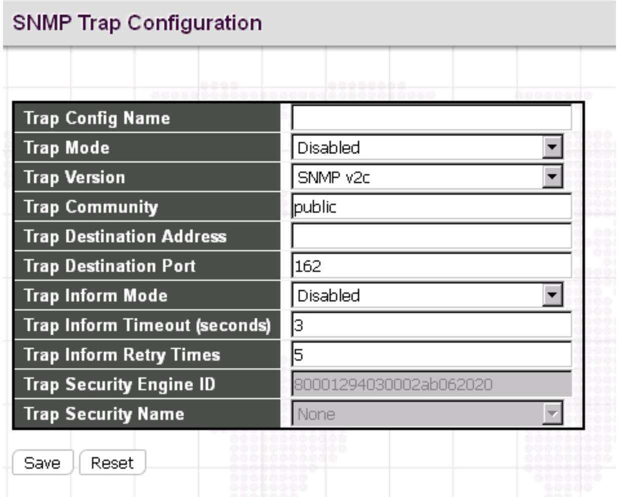
Disabled: Disable SNMP mode operation.

Engine ID: Indicates the SNMPv3 engine ID. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Changes to the Engine ID will clear all original local users.

4.8.1.7.2. SNMP Trap

4.8.1.7.2.1. Destination

Configure SNMP trap on this page.



SNMP Trap Configuration

Trap Config Name	
Trap Mode	Disabled
Trap Version	SNMP v2c
Trap Community	public
Trap Destination Address	
Trap Destination Port	162
Trap Inform Mode	Disabled
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Security Engine ID	80001294030002ab062020
Trap Security Name	None

Trap Config Name: Indicates a configuration name for this trap. The allowed string length is 1 to 32 and the allowed content is ASCII characters from 33 to 126.

Trap Mode: Indicates the SNMP trap mode operation. Possible modes are:

Enabled: Enable SNMP trap mode operation.

Disabled: Disable SNMP trap mode operation.

Trap Version: Indicates the SNMP trap supported version. Possible versions are:

SNMP v1: Set SNMP trap supported version 1.

SNMP v2c: Set SNMP trap supported version 2c.

SNMP v3: Set SNMP trap supported version 3.

Trap Community: Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 0x21 to 0x7E.

Trap Destination Address: Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). Also allowed is a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.) and dash (-). Spaces are not allowed. The first character must be an alpha character, and the first and last characters cannot be a dot or a dash.

Trap Destination IPv6 Address: Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol ' :: ' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Trap Destination Port: Indicates a SNMP destination port number. SNMP Agent will send SNMP message via this port. The port range is 1~65535.

Trap Inform Mode: Indicates the SNMP trap inform mode operation. Possible modes are:

Enabled: Enable SNMP trap inform mode operation.

Disabled: Disable SNMP trap inform mode operation.

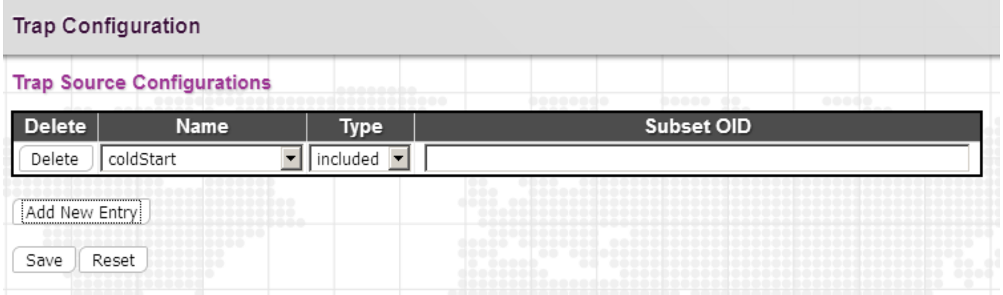
Trap Inform Timeout (seconds): Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.

Trap Inform Retry Times: Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.

Trap Security Engine ID: Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs use USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

Trap Security Name: Indicates the SNMP trap security name. SNMPv3 traps and informs use USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

4.8.1.7.2.2. Sources



Trap Configuration

Trap Source Configurations

Delete	Name	Type	Subset OID
Delete	coldStart	included	

Name: Indicate the trap source name of the entry.

Type: Indicates the trap source type that this entry should belong to. Possible view types are:

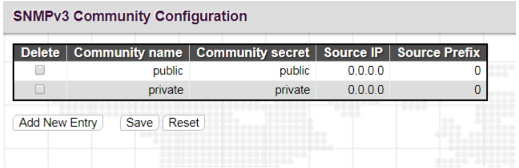
included: An optional flag to indicate a trap source is sent or the given trap source is matched.

excluded: An optional flag to indicate a trap source is not sent for the given trap source is matched.

Subset OID: Indicate the subset OID for the entry. The allowed OID length is 1 to 128. The allowed string content is digital number or an asterisk (*).

4.8.1.7.3. SNMPv3 Community Configuration

Configure SNMPv3 community table on this page. The entry index key is Community.



SNMPv3 Community Configuration

Delete	Community name	Community secret	Source IP	Source Prefix
□	public	public	0.0.0.0	0
□	private	private	0.0.0.0	0

Community name: Indicates the security name to map the community to the SNMP Groups information. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

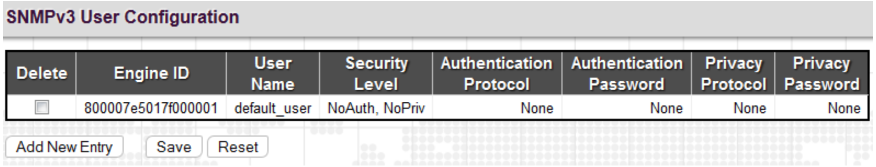
Community secret: Indicates the community access string to permit access using SNMPv1 and SNMPv2c to the SNMP agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. This string is case sensitive.

Source IP: Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.

Source Mask: Indicates the SNMP access source address mask.

4.8.1.7.4. SNMPv3 User Configuration

Configure SNMPv3 user table on this page. The entry index keys are Engine ID and User Name.



SNMPv3 User Configuration

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

Engine ID: An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it is a remote user.

User Name: A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Level: Indicates the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

Authentication Protocol: Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

None: No authentication protocol.

MD5: An optional flag to indicate that this user uses MD5 authentication protocol.

SHA: An optional flag to indicate that this user uses SHA authentication protocol.

The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

Authentication Password: A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32 characters. For SHA authentication protocol, the allowed string length is 8 to 40 characters. The allowed content is ASCII characters from 0x21 to 0x7E.

Privacy Protocol: Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

None: No privacy protocol.

DES: An optional flag to indicate that this user uses DES authentication protocol.

AES: An optional flag to indicate that this user uses AES authentication protocol.

Privacy Password: A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

Click the “Add New Entry” button to insert a new entry to the list.

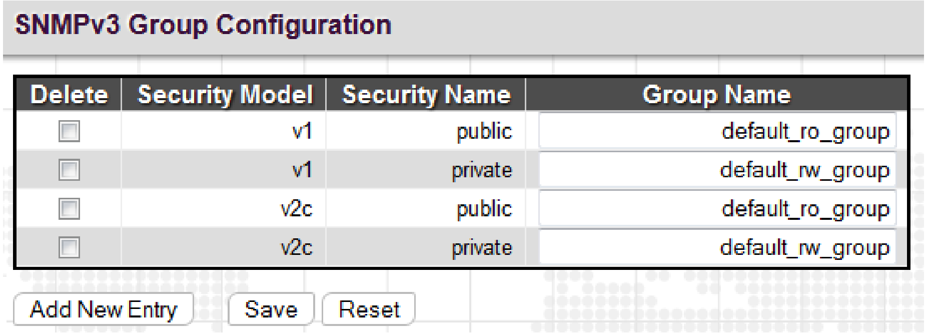
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.8.1.7.5. SNMPv3 Group Configuration

Configure SNMPv3 group table on this page. The entry index keys are Security Model and Security Name.



SNMPv3 Group Configuration

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

Security Model: Indicates the security model that this entry should belong to. Possible security models are:

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM) for SNMPv3.

Security Name: A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

Group Name: Identifies a string of the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

Click the “Add New Entry” button to add a new entry.

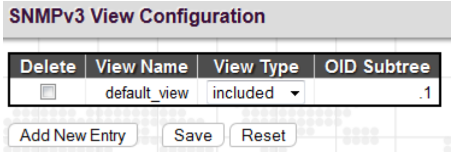
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.8.1.7.6. SNMPv3 View Configuration

Configure SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.



SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
☐	default_view	included	.1

View Name: A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

View Type: Indicates the view type that this entry should belong to. Possible view types are:

included: An optional flag to indicate that this view subtree should be included.

excluded: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and its OID subtree should overstep the 'excluded' view entry.

OID Subtree: The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or an asterisk (*).

Click the “Add New Entry” button to add a new entry.

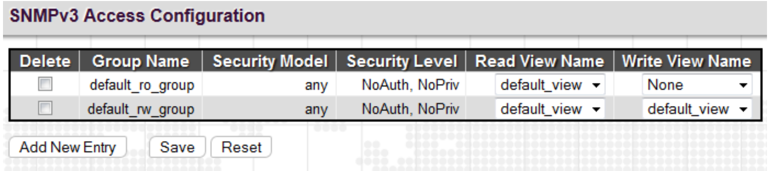
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.8.1.7.7. SNMPv3 Access Configuration

Configure SNMPv3 access table on this page. The entry index keys are Group Name, Security Model and Security Level.



SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	default_ro_group	any	NoAuth, NoPriv	default_view	None
□	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

Group Name: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

Security Model: Indicates the security model that this entry should belong to. Possible security models are:

any: Any security model accepted(v1|v2c|usm).

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM) for SNMPv3.

Security Level: Indicates the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

Read View Name: The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

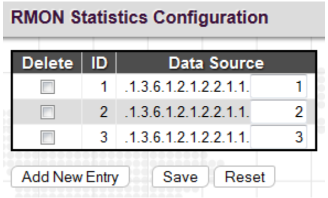
Write View Name: The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

4.8.1.8. RMON

4.8.1.8.1. RMON Statistics

4.8.1.8.1.1. Configuration

Remote monitoring is a standard specification that enables various network monitors to exchange network monitoring data. RMON provides the user with more freedom in selecting networking monitoring probes that meet their particular networking needs.



RMON Statistics Configuration

Delete	ID	Data Source
□	1	.1.3.6.1.2.1.2.2.1.1. 1
□	2	.1.3.6.1.2.1.2.2.1.1. 2
□	3	.1.3.6.1.2.1.2.2.1.1. 3

ID: Indicates the index of the entry. The range is from 1 to 65535.

Data Source: Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005.

Click the “Add New Entry” button to add a new entry.

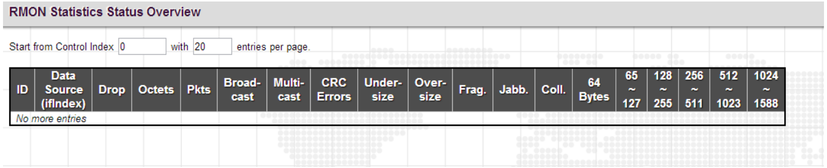
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.8.1.8.1.2. RMON Statistics Overview

This RMON statistics overview page shows interface statistics. All values displayed have been accumulated since the last system reboot and are shown as counts per second. The system will automatically refresh every 60 seconds by default.



RMON Statistics Status Overview

Start from Control Index 0 with 20 entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
No more entries																		

ID: Displays an ID index.

Data Source: Port ID to Monitor.

Drop: The total number of dropped packets due to lack of resources.

Octets: The total number of octets of data received.

Pkts: The total number of packets (including bad packets, broadcast packets) received.

Broadcast: The total number of good packets received that were directed to the broadcast address.

Multicast: The total number of good packets received that were directed to a multicast address.

CRC Errors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.

Undersize: The total number of packets received that were less than 64 octets.

Oversize: The total number of packets received that were longer than 1518 octets.

Frag.: The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.: The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.: The best estimate of the total number of collisions on this Ethernet segment.

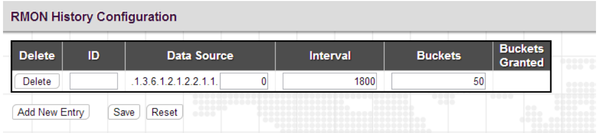
64 Bytes: The total number of packets (including bad packets) received that were 64 octets in length.

X~Y (65~127, 128~255, 256~511, 512~1023, 1024~1588): The total number packets received between X and Y octets in length.

4.8.1.8.2. RMON History

4.8.1.8.2.1. Configuration

RMON History Configuration is to collect statistics on a physical interface to monitor network utilization, packet types, and errors. A RMON historical record can also be used to monitor intermittent problems.



RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Delete		.1.3.6.1.2.1.2.2.1.1. 0	1800	50	

ID: Indicates the index of the entry. The range is from 1 to 65535.

Data Source: Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

Interval: Indicates the polling interval. By default, 1800 seconds is specified. The allowed range is 1~3600 seconds.

Buckets: The number of buckets requested for this entry. By default, 50 is specified. The allowed range is 1~3600.

Buckets Granted: The number of buckets granted.

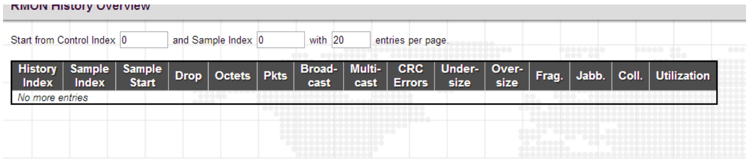
Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.8.1.8.2.2. RMON History Overview



RMON History Overview

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

History Index: Displays Index of History control entry.

Sample Index: Displays Index of the data entry associated with the control entry.

Sample Start: The time at which this sample started, expressed in seconds since the switch booted up.

Drop: The total number of dropped packets due to lack of resources.

Octets: The total number of octets of data received.

Pkts: The total number of packets (including bad packets, broadcast packets) received.

Broadcast: The total number of good packets received that were directed to the broadcast address.

Multicast: The total number of good packets received that were directed to a multicast address.

CRC Errors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.

Undersize: The total number of packets received that were less than 64 octets.

Oversize: The total number of packets received that were longer than 1518 octets.

Frag.: The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.: The number of frames which size is larger than 64 octets received with invalid CRC.

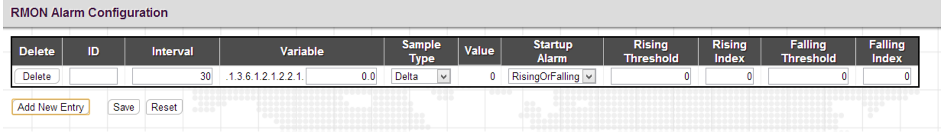
Coll.: The best estimate of the total number of collisions on this Ethernet segment.

Utilization: The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

4.8.1.8.3. Alarm

4.8.1.8.3.1. Configuration

RMON Alarm configuration defines specific criteria that will generate response events. It can be set to test data over any specified time interval and can monitor absolute or changing values. Alarms can also be set to respond to rising or falling thresholds.



RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
Delete		30	.1.3.6.1.2.1.2.2.1. 0.0	Delta	0	RisingOrFalling	0	0	0	0

ID: Indicates the index of the entry. The range is from 1 to 65535.

Interval: The polling interval for sampling and comparing the rising and falling threshold. The range is from 1to 2^31 seconds.

Variable: The object number of the MIB variable to be sampled. Only variables of the type ifEntry.n.n may be sampled. Possible variables are InOctets, InUcastPkts, InNUcastPkts, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPkts, OutNUcastPkts, OutDiscards, OutErrors, and OutQLen.

Sample Type: Test for absolute or relative change in the specified variable.

Absolute: The variable is compared to the thresholds at the end of the sampling period.

Delta: The last sample is subtracted from the current value and the difference is compared to the thresholds.

Value: The statistic value during the last sampling period.

Startup Alarm: Select a method that is used to sample the selected variable and calculate the value to be compared against the thresholds.

Rising or Falling: Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold.

Rising: Trigger alarm when the first value is larger than the rising threshold.

Falling: Trigger alarm when the first value is less than the falling threshold.

Rising Threshold: If the current value is greater than the rising threshold and the last sample value is less than this threshold, then an alarm will be triggered. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold. The threshold range is -2147483647 to 2147483647.

Rising Index: Indicates the rising index of an event. The range is 1~65535.

Falling Threshold: If the current value is less than the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the failing threshold. (Range: -2147483647 to 2147483647)

Falling Index: Indicates the falling index of an event. The range is 1~65535.

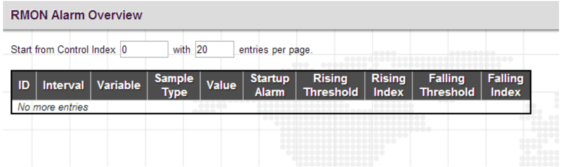
Click the "Add New Entry" button to insert a new entry to the list.

Click the "Delete" button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the "Save" button to save settings or changes.

Click the "Reset" button to restore changed settings to the default settings.

4.8.1.8.3.2. RMON Alarm Overview



RMON Alarm Overview

Start from Control Index 0 with 20 entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

ID: Display an alarm control index.

Interval: Interval in seconds for sampling and comparing the rising and falling threshold.

Variable: MIB object that is used to be sampled.

Sample Type: The method of sampling the selected variable and calculating the value to be compared against the thresholds.

Value: The value of the statistic during the last sampling period.

Startup Alarm: The alarm that may be triggered when this entry is first set to valid.

Rising Threshold: If the current value is greater than the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated.

Rising Index: The index of the event to use if an alarm is triggered by monitored variables crossing above the rising threshold.

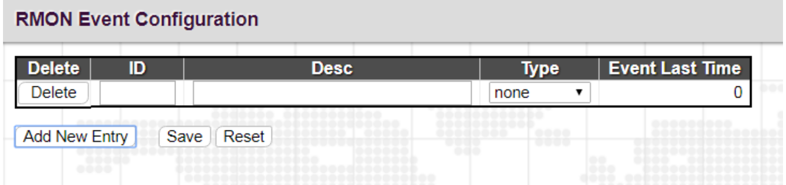
Falling Threshold: If the current value is less than the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated.

Falling Index: The index of the event to use if an alarm is triggered by monitored variables crossing below the falling threshold.

4.8.1.8.4. RMON Event

4.8.1.8.4.1. Configuration

RMON Event Configuration page is used to set an action taken when an alarm is triggered.



RMON Event Configuration

Delete	ID	Desc	Type	Event Last Time
Delete			none ▾	0

ID: Specifies an ID index. The range is 1~65535.

Desc: Enters a descriptive comment for this entry.

Type: Select an event type that will take when an alarm is triggered.

None: No event is generated.

Log: When the event is triggered, a RMON log entry will be generated.

snmptrap: Sends a trap message to all configured trap managers.

logandtrap: Logs an event and sends a trap message.

Event Last Time: The value of sysUpTime when an event was last generated for this entry.

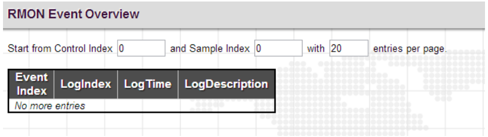
Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.8.1.8.4.2. RMON Event Overview



RMON Event Overview

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

Event Index	LogIndex	LogTime	LogDescription
No more entries			

Event Index: Display the event entry index.

Log Index: Display the log entry index.

Log Time: Display Event log time.

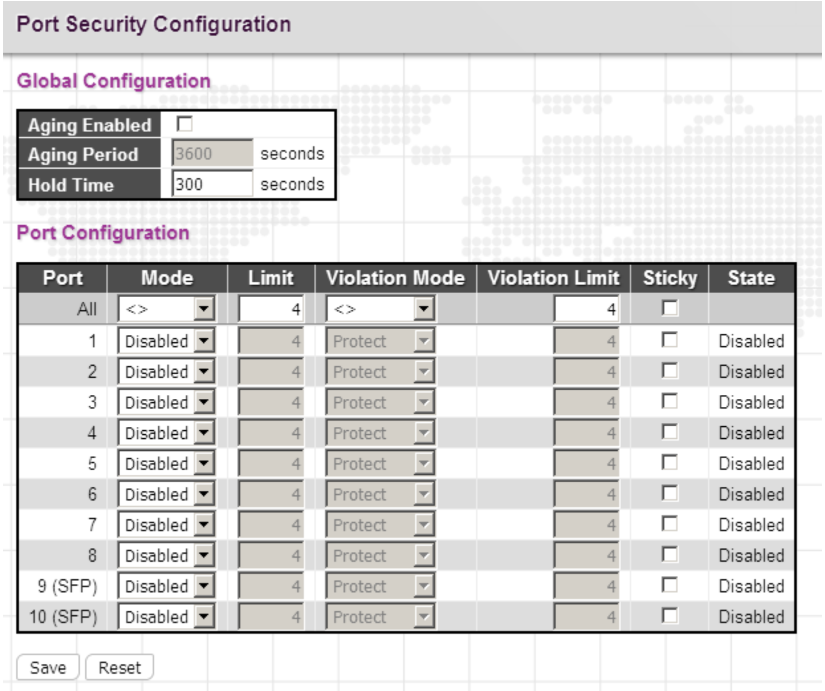
Log Description: Display Event description.

4.8.2. Network

4.8.2.1. Port Security

Port Security Limit Control can restrict the number of users that can access the switch based on users' MAC address and VLAN ID on a per port basis. Once the number of users that wants to access the switch exceeds the specified number, a selected action will be taken immediately.

4.8.2.1.1. Configuration



Port Security Configuration

Global Configuration

Aging Enabled	□	
Aging Period	3600	seconds
Hold Time	300	seconds

Port Configuration

Port	Mode	Limit	Violation Mode	Violation Limit	Sticky	State
All	<>	4	<>	4	□	
1	Disabled	4	Protect	4	□	Disabled
2	Disabled	4	Protect	4	□	Disabled
3	Disabled	4	Protect	4	□	Disabled
4	Disabled	4	Protect	4	□	Disabled
5	Disabled	4	Protect	4	□	Disabled
6	Disabled	4	Protect	4	□	Disabled
7	Disabled	4	Protect	4	□	Disabled
8	Disabled	4	Protect	4	□	Disabled
9 (SFP)	Disabled	4	Protect	4	□	Disabled
10 (SFP)	Disabled	4	Protect	4	□	Disabled

Global Configuration

Aging Enabled: If enabled, secured MAC addresses are subject to aging as discussed under Aging Period. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Aging Period: If Aging Enabled is checked, then the aging period can be set up with the desired value. By default, the aging period is set to 3600 seconds. The allowed range is 10 - 10,000,000 second.

Hold Time: Configure a desired hold time value in seconds. This value is used to determine how long a MAC address is held in the MAC table if it has been found to violate the limit. The default value 300 seconds but can be changed to the desired value from 10 to 10000000 seconds. The reason for holding a violating MAC address in MAC table is primarily to ensure that the same MAC address doesn't give rise to continuous notifications (if notifications on violation count is enabled).

Port Configuration

Port: Display the port number. “Port *” rules apply to all ports.

Mode: Enable or disable port security limit control on a per port basis. To make limit control function work, port security limit control needs to be enabled globally and on a port.

Limit: The maximum number of MAC addresses that can be secured on this port. The number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

Violation Mode: If the limit is exceeded, the selected action will take effect.

> **protect:** Do not allow more than the specified limit of MAC addresses to access on a port. No action is further taken.
>
> **restrict:** If Limit is reached, subsequent MAC addresses on the port will be counted and marked as violating. Such MAC addresses are removed from the MAC table when the hold time expires.
>
> **shutdown:** If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new addresses will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:
> * Boot the switch
> * Disable and re-enable Limit Control on the port or the switch
> * Click the “Reopen” button

Violation Limit: The maximum number of MAC addresses that can be marked as violating on the port. This number cannot exceed 1024. The default is 4. It is only used when Violation Mode is Restrict.

Sticky: Enable or disable sticky learning of MAC addresses on a port. When the port is in sticky mode, all MAC addresses that would otherwise have been learned as dynamic are learned as sticky.

Sticky MAC addresses are part of the running-config and can therefore be saved to startup-config. Sticky MAC addresses survive link changes (in contrast to Dynamic, which will have to be learned again). They also survive reboots if running-config is saved to startup-config.

State: Display the current state of the port from the port security limit control's point of view. The displayed state might be one of the following:

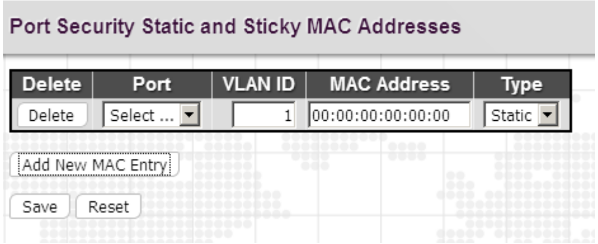
Disabled: Limit control is either globally disabled or disabled on a port.

Ready: The limit is not reached yet.

Limit Reached: The limit is reached on a port. This state can only be shown if Action is set to None or Trap.

Shutdown: The port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.

4.8.2.1.2. Static and Sticky MAC Addresses



Port Security Static and Sticky MAC Addresses

Delete	Port	VLAN ID	MAC Address	Type
Delete	Select ...	1	00:00:00:00:00:00	Static

Delete: Remove this entry from the list.

Port: Select the port to which this MAC address is bound.

VLAN ID: Specify the VLAN ID.

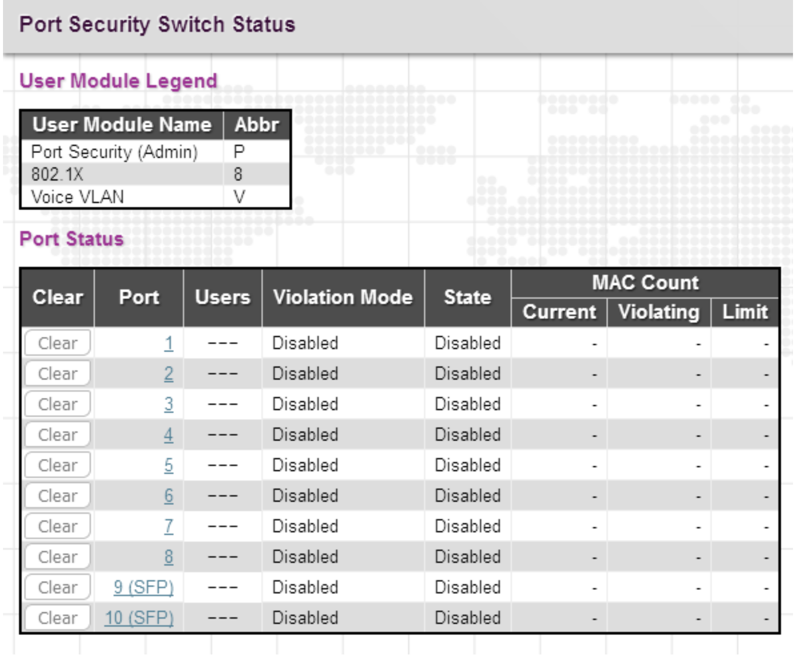
MAC Address: Specify the MAC address that bounds to the specified port.

Type: Select the type of the entry which could be Static or Sticky.

Static: A static MAC address is the address added by end-user. Static addresses are not subject to aging and will be added to MAC address table once Port Security gets enabled on the interface. Static entries are part of the running-config and will survive interface link state changes and reboots if saved to startup-config. Static entries can be added to the running-config at any time whether or not Port Security is enabled.

Sticky: When the interface is in Sticky mode, all entries would otherwise have learned as dynamic are learned as Sticky. Like static entries, sticky entries are part of the running-config and will survive interface link state changes and reboots if saved to startup-config. Though not the intention with the sticky entries, they can be added by management to the running-config at any time whether or not Port Security is enabled on the interface, as long as the interface is in Sticky mode. Sticky entries will disappear if the interface is taken out of Sticky mode.

4.8.2.1.3. Switch Status



Port Security Switch Status

User Module Legend

User Module Name	Abbr
Port Security (Admin)	P
802.1X	8
Voice VLAN	V

Port Status

Clear	Port	Users	Violation Mode	State	MAC Count		
					Current	Violating	Limit
Clear	1	---	Disabled	Disabled	-	-	-
Clear	2	---	Disabled	Disabled	-	-	-
Clear	3	---	Disabled	Disabled	-	-	-
Clear	4	---	Disabled	Disabled	-	-	-
Clear	5	---	Disabled	Disabled	-	-	-
Clear	6	---	Disabled	Disabled	-	-	-
Clear	7	---	Disabled	Disabled	-	-	-
Clear	8	---	Disabled	Disabled	-	-	-
Clear	9 (SFP)	---	Disabled	Disabled	-	-	-
Clear	10 (SFP)	---	Disabled	Disabled	-	-	-

<u>User Module Legend</u>

User Module Name: The full name of a module that may request Port Security services.

Abbr: This column is the abbreviation for the user module used in the “Users” column in the “Port Status”.

<u>Port Status</u>

Port: Port number. Click a particular port number to see its port status.

Users: Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter has enabled port security.

Violation Mode: This field displays the violation mode selected on this port.

State: This shows the current status of a port. It can be one of the following states:

Disabled: No user modules are currently using the Port Security service.

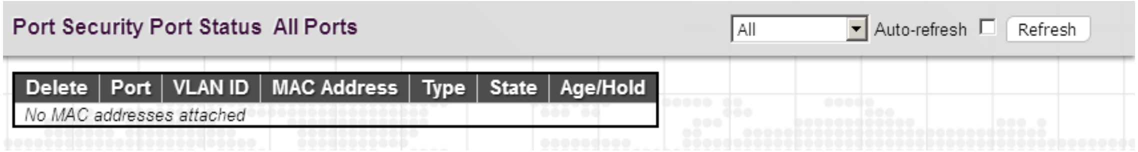
Ready: The Port Security service is in use by at least one user module and is awaiting frames from unknown MAC addresses to arrive.

Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached, and no more MAC addresses should be taken in.

Shutdown: The Port Security service is enabled by at least the Limit Control user module and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration page.

MAC Count (Current/Limit): The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

4.8.2.1.4. Details



Port Security Port Status All Ports

Delete	Port	VLAN ID	MAC Address	Type	State	Age/Hold
No MAC addresses attached						

This page shows MAC addresses learned on a particular port.

Port: This field shows the port that MAC address bounds to.

MAC Address: When "Port Security Limit Control" is enabled globally and on a port, MAC addresses learned on a port shows in here.

VLAN ID: Display VLAN ID that is seen on this port.

Type: This field shows one of the three values:

Dynamic: This is learned through frames coming to the Port Security module while the port is not in sticky mode.

Static: A static MAC address is the address added by end-user. Static addresses are not subject to aging and will be added to MAC address table once Port Security gets enabled on the interface. Static entries are part of the running-config and will survive interface link state changes and reboots if saved to startup-config. Static entries can be added to the running-config at any time whether or not Port Security is enabled.

Sticky: When the interface is in Sticky mode, all entries would otherwise have learned as dynamic are learned as Sticky. Like static entries, sticky entries are part of the running-config and will survive interface link state changes and reboots if saved to startup-config. Though not the intention with the sticky entries, they can be added by management to the running-config at any time whether or not Port Security is enabled on the interface, as long as the interface is in Sticky mode. Sticky entries will disappear if the interface is taken out of Sticky mode.

State: Display whether the corresponding MAC address is forwarding or blocked. In the blocked state, it will not be allowed to transmit or receive traffic.

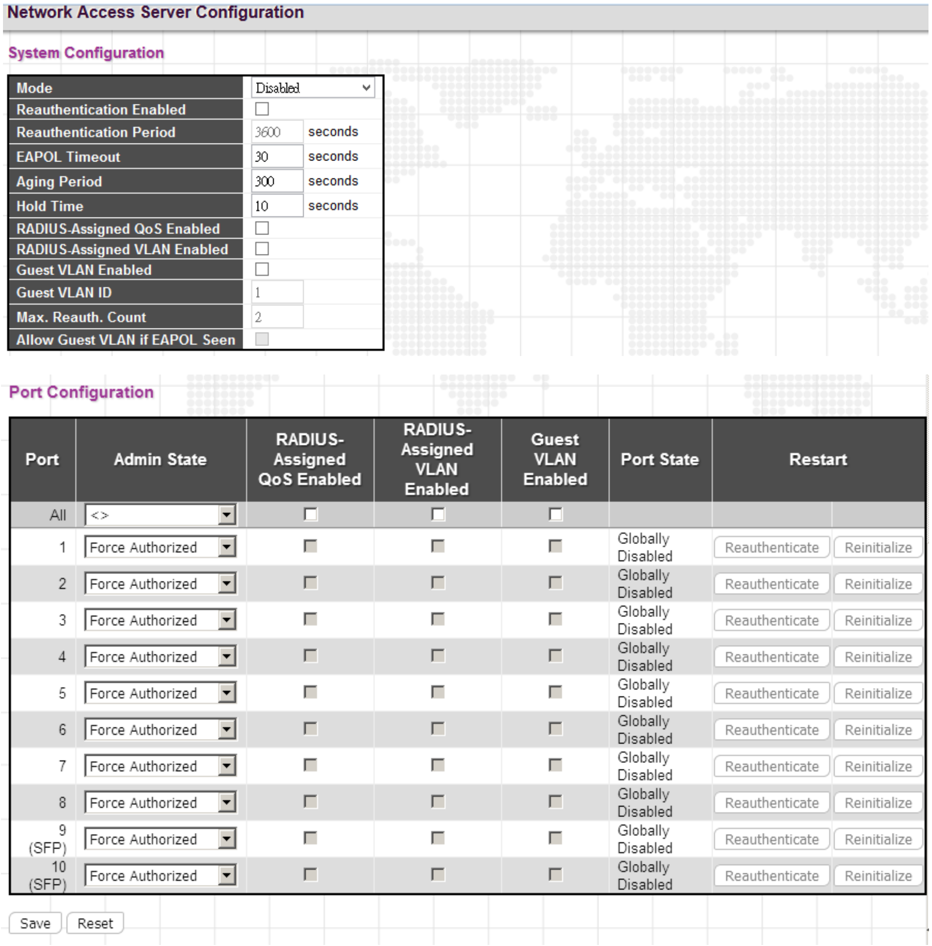
Age/Hold: If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address is still forwarding traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise, a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

4.8.2.2. NAS

Network Access Server configuration is useful to the networking environment that wants to authenticate clients (supplicants) before they can access resources on the protected network. To effectively control access to unknown clients, 802.1X defined by IEEE provides a port-based authentication procedure that can prevent unauthorized access to a network by requiring users to first submit credentials for authentication purposes.

A switch interconnecting clients and radius server usually acts as an authenticator and uses EAPOL (Extensible Authentication Protocol over LANs) to exchange authentication protocol messages with clients and a remote RADIUS authentication server to verify user identity and user's access right. This section is for setting up authenticator's configurations either on the system or on a per port basis. To configure backend server, please go to RADIUS configuration page.

4.8.2.2.1. Configuration



Network Access Server Configuration

System Configuration

Mode	Disabled
Reauthentication Enabled	□
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	□
RADIUS-Assigned VLAN Enabled	□
Guest VLAN Enabled	□
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	□

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
All	<>	□	□	□			
1	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
9 (SFP)	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
10 (SFP)	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize

System Configuration

Mode: Enable 802.1X and MAC-based authentication globally on the switch. If globally disabled, all ports are allowed to forward frames.

Reauthentication Enabled: Select the checkbox to set clients to be re-authenticated after an interval set in "Reauthentication Period" field. Re-authentication can be used to detect if a new device is attached to a switch port.

Reauthentication Period: Specify the time interval for a connected device to be re-authenticated. By default, the re-authenticated period is set to 3600 seconds. The allowed range is 1~3600 seconds.

EAPOL Timeout: Specify the time that the switch waits for a supplicant response during an authentication session before transmitting a Request Identify EAPOL packet. By default, it is set to 30 seconds. The allowed range is 1~255 seconds.

Aging Period: Specify the period that is used to age out a client's allowed access to the switch via 802.1X and MAC-based authentication. The default period is 300 seconds. The allowed range is 10~1000000 seconds.

Hold Time: The time after an EAP Failure indication or RADIUS timeout that a client is not allowed access. This setting applies to ports running Single 802.1X, Multi 802.1X, or MAC-based authentication. By default, hold time is set to 10 seconds. The allowed range is 10~1000000 seconds.

Radius-Assigned QoS Enabled: Select the checkbox to globally enable RADIUS assigned QoS.

Radius-Assigned VLAN Enabled: RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature.

The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

Guest VLAN Enabled: A Guest VLAN is a special VLAN typically with limited network access. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

Guest VLAN ID: This VLAN ID is functional only when Guest VLAN is enabled. This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. The range is 1~4095.

Max. Reauth. Count: The maximum number of times the switch transmits an EAPOL Request Identity frame without receiving a response before adding a port to the Guest VLAN. The value can only be changed when the Guest VLAN option is globally enabled. The range is 1~255.

Allow Guest VLAN if EAPOL Seen: The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.

Port Configuration

Port: Port number. “Port *” rules apply to all ports.

Admin State: Select the authentication mode on a port. This setting works only when NAS is globally enabled. The following modes are available:

> **Force Authorized:** In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.
>
> **Force Unauthorized:** In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.
>
> **Port-Based 802.1X:** This mode requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
>
> **Single 802.1X:** In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the “Port Security” module is used to secure a supplicant's MAC address once successfully authenticated.
>
> **Multi 802.1X:** In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the “Port Security” module.
>
> **MAC-based Auth.:** Unlike port-based 802.1X, MAC-based authentication do not transmit or receive EAPOL frames. In MAC-based authentication, 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.

RADIUS-Assigned QoS Enabled: Select the checkbox to enable RADIUS-Assigned QoS on a port.

Radius-Assigned VLAN Enabled: Select the checkbox to enable RADIUS-Assigned VLAN on a port.

Guest VLAN Enabled: Select the checkbox to enable Guest VLAN on a port.

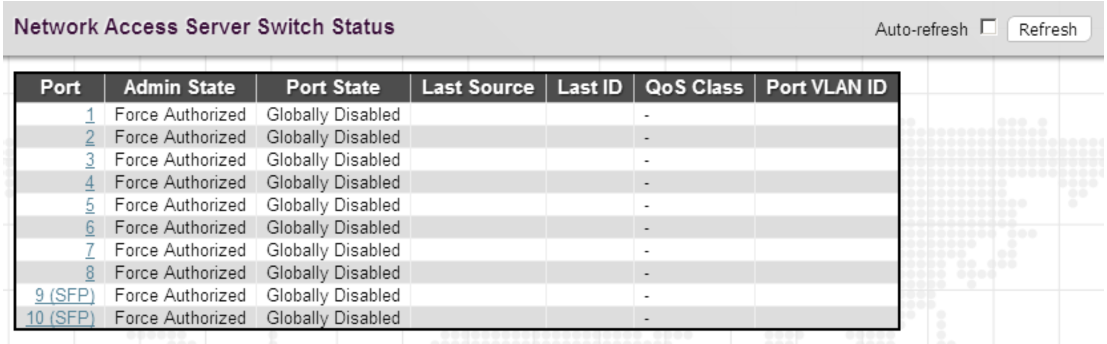
Port State: Display the current state of the port from 802.1X authentication point of view. The possible states are as follows:

> **Globally Disabled:** 802.1X and MAC-based authentication are globally disabled.
>
> **Link Down:** 802.1X and MAC-based authentication are enabled but there is no link on a port.
>
> **Authorized:** The port is forced in authorized mode and the supplicant is successfully authorized.
>
> **Unauthorized:** The port is forced in unauthorized mode and the supplicant is not successfully authorized by the RADIUS server.
>
> **X Auth/Y Unauth:** The port is in a multi-supplicant mode. X clients are authorized and Y are unauthorized.

Restart: Restart client authentication using one of the methods described below. Note that the restart buttons are only enabled when the switch’s authentication mode is globally enabled (under System Configuration) and the port's Admin State is an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect.

> **Reauthenticate:** Schedules reauthentication to whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.
>
> **Reinitialize**: This forces the reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

4.8.2.2.2. Switch Status



Network Access Server Switch Status

Auto-refresh □ Refresh

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 (SFP)	Force Authorized	Globally Disabled			-	
10 (SFP)	Force Authorized	Globally Disabled			-	

Port: Port number. Click a port to view the detailed NAS statistics.

Admin State: Display the port's current administrative state.

Port Status: Display the port state.

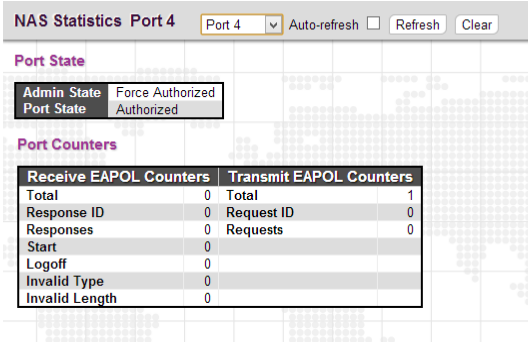
Last Source: The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication.

Last ID: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication.

QoS Class: Display the QoS class that NAS assigns to the port.   This field is left blank if QoS is not set by NAS.

Port VLAN ID: The VLAN ID of the port assigned by NAS. This field is left blank if VLAN ID is not set by NAS.

4.8.2.2.3. Port Statistics



NAS Statistics Port 4

Port State

Admin State	Force Authorized
Port State	Authorized

Port Counters

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	1
Response ID	0	Request ID	0
Responses	0	Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		

Port State

Admin State: Display the port’s current administrative state.

Port Status: Display the port state.

Port Counters

Total: The number of valid EAPOL frames of any type that have been received & transmitted by the switch.

Response ID: The number of valid EAPOL Response Identity frames that have been received & transmitted by the switch.

Responses: The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.

Requests: The number of valid EAPOL request frames (other than Request Identity frames) that have been transmitted by the switch.

Start: The number of EAPOL Start frames that have been received by the switch.

Logoff: The number of valid EAPOL Logoff frames that have been received by the switch.

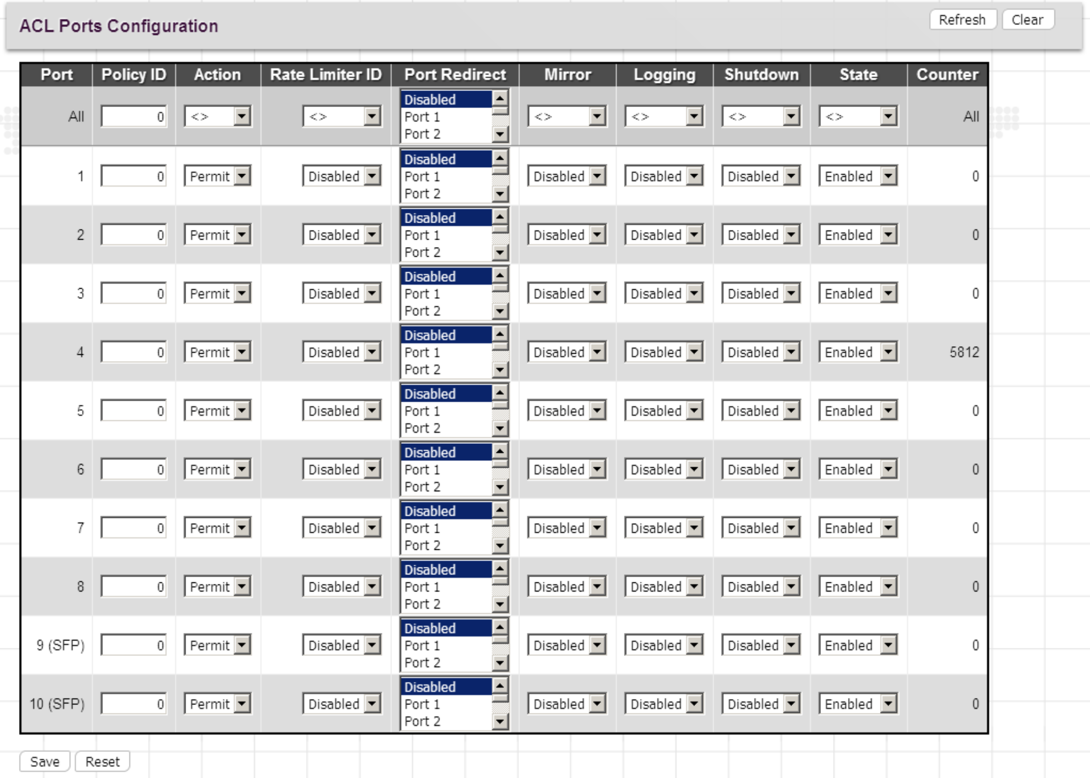
Invalid Type: The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.

Invalid Length: The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.

4.8.2.3. ACL

ACL is a sequential list established to allow or deny users to access information or perform tasks on the network. In this switch, users can establish rules applied to port numbers to permit or deny actions or restrict rate limit.

4.8.2.3.1. Ports



ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
All	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	All
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	5812
5	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
9 (SFP)	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
10 (SFP)	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

Port: The port number.

Policy Id: Assign an ACL policy ID to a particular port. A port can only use one policy ID; however, a policy ID can apply to many ports. The default ID is 0. The allowed range is 0~255.

Action: Permit or deny a frame based on whether it matches a rule defined in the assigned policy.

Rate Limiter ID: Select a rate limiter ID to apply to a port. Rate Limiter rule can be set up in "Rate Limiters" configuration page.

Port Redirect: Select a port to which matching frames are redirected.

Mirror: Enable or disable mirroring feature. When enabled, a copy of matched frames will be mirrored to the destination port specified in "Mirror" configuration page. ACL-based port mirroring set by this parameter and port mirroring set on the general Mirror Configuration page are implemented independently. To use ACL-based mirroring, enable the Mirror parameter on the ACL Ports Configuration page. Then open the Mirror Configuration page, set the “Port to mirror on” field to the required destination port, and leave the “Mode” field Disabled.

Logging: Enable logging of matched frames to the system log. To view log entries, go to System menu and then click the “System Log Information” option.

Shutdown: This field is to decide whether to shut down a port when matched frames are seen or not.

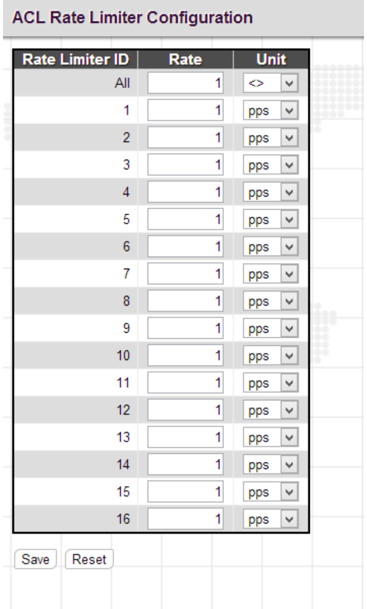
State: Select a port state.

Enabled: To re-open a port.

Disabled: To close a port.

Counters: The number of frames that have matched the rules defined in the selected policy.

4.8.2.3.2. Rate Limiters



ACL Rate Limiter Configuration

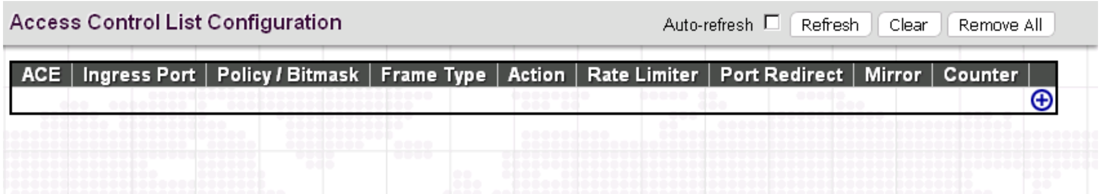
Rate Limiter ID	Rate	Unit
All	1	<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

Rate Limiter ID: Display every rate limiter ID.

Rate: Specify the threshold above which packets are dropped. The allowed values are 0~3276700 pps or 1, 100, 200, 300…1000000 kbps.

Unit: Select the unit of measure used in rate.

4.8.2.3.3. Access Control List



Access Control List Configuration

Auto-refresh □ Refresh Clear Remove All

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

Click on the ⊕ to insert a new ACE entry.

You can modify each ACE (Access Control Entry) in the table using the following buttons:

⊕: Inserts a new ACE before the current row.

ⓔ: Edits the ACE row.

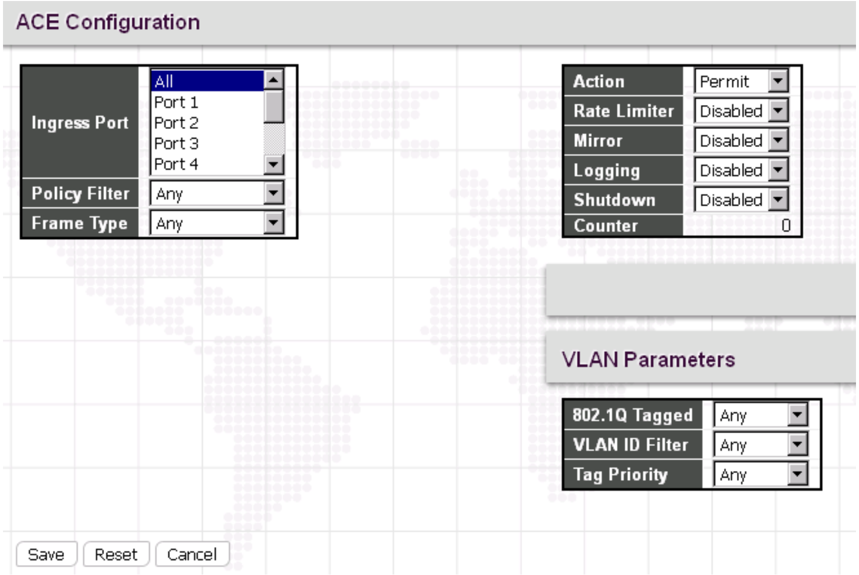
↑: Moves the ACE up the list.

↓: Moves the ACE down the list.

⊗: Deletes the ACE.

⊕: The lowest plus sign adds a new entry at the bottom of the ACE listings.

ACE Configuration



ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Any
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Save Reset Cancel

Ingress Port: Select the ingress port of the access control entry. Select “All” to apply an ACL rule to all ports or select a particular port.

Policy Filter: Select the policy filter type. “Any” means no policy filter is assigned to this rule (or don’t care). Select “Specific” to filter specific policy with this ACE.

Frame Type: Select a frame type to match. Available frame types include Any, Ethernet, ARP, IPv4. By default, any frame type is used.

Action: Select the action type, either to permit or deny.

Rate Limiter: Enable or disable the rate limiter when matched frames are found.

Mirror: Enable or disable mirror function.

Logging: Enable or disable logging when a frame is matched.

Shutdown: Enable or disable shutdown a port when a frame is matched.

Counter: Display the number of frames that have matched any of the rules defined for this ACL.

VLAN Parameters

802.1Q Tagged: Select whether or not the frames should be tagged.

VLAN ID Filter: Select the VLAN ID filter for this ACE.

> **Any:** No VLAN ID filter is specified. (Don’t care)
>
> **Specific:** Specify a VLAN ID. A frame with the specified VLAN ID matches this ACE rule.

Tag Priority: Select the User Priority value found in the VLAN tag to match this rule.

MAC Parameter

SMAC Filter: The type of source MAC address. Select "Any" to allow all types of source MAC addresses or select "Specific" to define a source MAC address. (This field is for ARP and Ethernet frame type only.)

DMAC Filter: The type of destination MAC address.

Any: To allow all types of destination MAC addresses

MC: Multicast MAC address

BC: Broadcast MAC address

UC: Unicast MAC address

Specific: Use this to self-define a destination MAC address. (This option is for Ethernet frame type only.)

Ethernet Type Parameter

Ether Type Filter: This option can only be used to filter Ethernet II formatted packets. Select "Specific" to define an Ether Type value.

ARP Parameter

ARP/RARP: Specify the type of ARP packet.

Any: No ARP/RARP opcode flag is specified

ARP: The frame must have ARP/RARP opcode set to ARP,

RARP: The frame must have ARP/RARP opcode set to RARP

Other: The frame has unknown ARP/RARP opcode flag

Request/Reply: Specify whether the packet is an ARP request, reply, or either type.

Any: No ARP/RARP opcode flag is specified

Request: The frame must have ARP Request or RARP Request opcode flag set.

Reply: The frame must have ARP Reply or RARP Reply opcode flag set.

Sender IP Filter: Specify the sender's IP address.

Any: No sender IP filter is specified.

Host: Specify the sender IP address.

Network: Specify the sender IP address and sender IP mask.

Target IP Filter: Specify the destination IP address.

Any: No target IP filter is specified.

Host: Specify the target IP address.

Network: Specify the target IP address and target IP mask.

ARP Sender SMAC Match: Select "0" to indicate that the SHA (Sender Hardware Address) field in the ARP/RARP frame is not equal to source MAC address. Select "1" to indicate that SHA field in the ARP/RARP frame is equal to source MAC address. Select "Any" to indicate a match and not a match.

RARP Target MAC Match: Select "0" to indicate that the THA (Target Hardware Address) field in the ARP/RARP frame is not equal to source MAC address. Select "1" to indicate that THA field in the ARP/RARP frame is equal to source MAC address. Select "Any" to indicate a match and not a match.

IP/Ethernet Length: Select "0" to indicate that HLN (Hardware Address Length) field in the ARP/RARP frame is not equal to Ethernet (0x6) and the Protocol Address Length field is not equal to IPv4 (0x4). Select "1" to indicate that HLN (Hardware Address Length) field in the ARP/RARP frame is equal to Ethernet (0x6) and the Protocol Address Length field is equal to IPv4 (0x4). Select "Any" to indicate a match and not a match.

IP: Select "0" to indicate that Protocol Address Space field in ARP/RARP frame is not equal to IP (0x800). Select "1" to indicate that Protocol Address Space is equal to IP (0x800). Select "Any" to indicate a match and not a match.

Ethernet: Select "0" to indicate that Hardware Address Space field in ARP/RARP frame is not equal to Ethernet (1). Select "1" to indicate that Hardware Address Space field is equal to Ethernet (1). Select "Any" to indicate a match and not a match.

IP Parameters

IP Protocol Filter: Select “Any”, “ICMP”, “UDP”, “TCP”, or “Other” protocol from the pull-down menu for IP Protocol filtering.

IP TTL: Select “Zero” to indicate that the TTL filed in IPv4 header is 0. If the value in TTL field is not 0, use “Non-Zero” to indicate that. You can also select “any” to denote the value which is either 0 or not 0.

IP Fragment: Select “Any” to allow any values. “Yes” denotes that IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must match this entry. “No” denotes that IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not match this entry.

IP Option: Specify the options flag setting for this rule. Select “Any” to allow any values. “Yes” denotes that IPv4 frames where the options flag is set must match this entry. “No” denotes that Pv4 frames where the options flag is set must not match this entry

SIP Filter: Select “Any”, “Host”, or “Network” for source IP filtering. If “Host” is selected, you need to indicate a specific host IP address. If “Network” is selected, you need to indicate both network address and subnet mask.

SIP Address: Specify a source IP address.

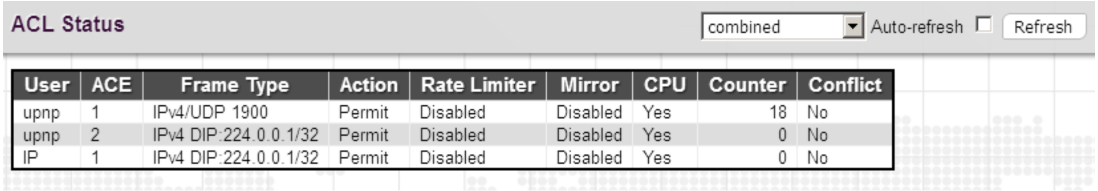
SIP Mask: Specify a source subnet mask.

DIP Filter: Select “Any”, “Host”, or “Network” for destination IP filtering. If “Host” is selected, you need to indicate a specific host IP address. If “Network” is selected, you need to indicate both network address and subnet mask.

DIP Address: Specify a destination IP address.

DIP Mask: Specify a destination subnet mask.

4.8.2.3.4. ACL Status



User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
upnp	1	IPv4/UDP 1900	Permit	Disabled	Disabled	Yes	18	No
upnp	2	IPv4 DIP:224.0.0.1/32	Permit	Disabled	Disabled	Yes	0	No
IP	1	IPv4 DIP:224.0.0.1/32	Permit	Disabled	Disabled	Yes	0	No

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

User: Display the ACL user.

ACE: Indicate the ACE number.

Frame Type: Display the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.

IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.

IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.

IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.

Action: Display the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE may be forwarded and learned.

Filtered: Frames matching the ACE are filtered.

Rate Limiter: Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Redirect: Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation 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".

CPU: Forward packet that matched the specific ACE to CPU.

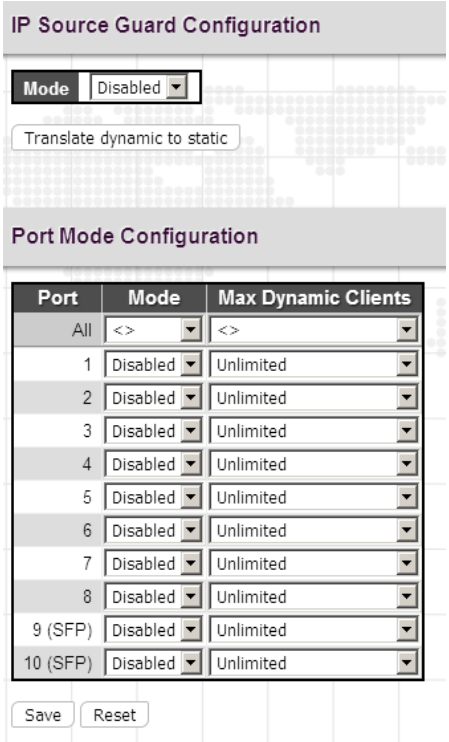
CPU Once: Forward first packet that matched the specific ACE to CPU.

Counter: The counter indicates the number of times the ACE was hit by a frame.

Conflict: Indicate the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

4.8.2.4. IP Source Guard

4.8.2.4.1. Configuration



IP Source Guard Configuration

Mode: Disabled

Port Mode Configuration

Port	Mode	Max Dynamic Clients
All	<>	<>
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 (SFP)	Disabled	Unlimited
10 (SFP)	Disabled	Unlimited

IP Source Guard Configuration

Mode: Enable or disable IP source guard globally.

Translate dynamic to static: Click this button to translate dynamic entries to static ones.

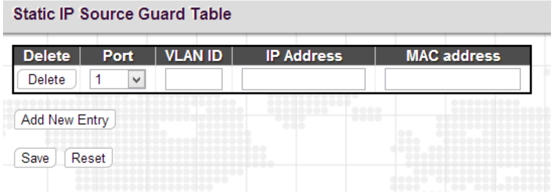
Port Mode Configuration

Port: The port number. “Port *” rules apply to all ports.

Mode: Enable or disable IP source guard on a port. Please note that to make IP source guard work, both global mode and port mode must be enabled.

Max Dynamic Clients: Select the maximum number of dynamic clients that can be learned on a port. The available options are 0, 1, 2, unlimited. If the port mode is enabled and the maximum number of dynamic clients is equal 0, the switch will only forward IP packets that are matched in static entries for a given port.

4.8.2.4.2. Static Table



Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address
Delete	1			

Port: Select a port to which a static entry is bound.

VLAN ID: Enter VLAN ID that has been configured.

IP Address: Enter a valid IP address.

MAC Address: Enter a valid MAC address.

Click the “Add New Entry” button to insert a new entry to the list.

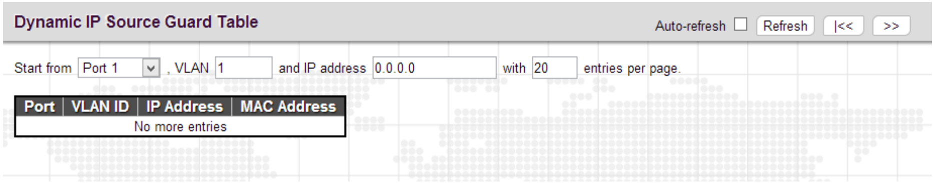
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.8.2.4.3. Dynamic Table

The Dynamic IP Source Guard table shows entries sorted by port, VLAN ID, IP address and MAC address. By default, each page displays 20 entries. However, it can display 999 entries by entering the number in “entries per page” input field.



Dynamic IP Source Guard Table

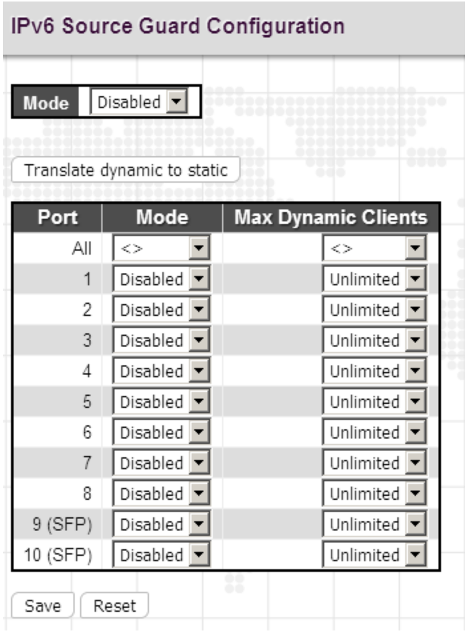
Auto-refresh □ Refresh |<< >>

Start from Port 1, VLAN 1 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	IP Address	MAC Address
No more entries			

4.8.2.5. IPv6 Source Guard

4.8.2.5.1. Configuration



IPv6 Source Guard Configuration

Mode	Disabled

Translate dynamic to static

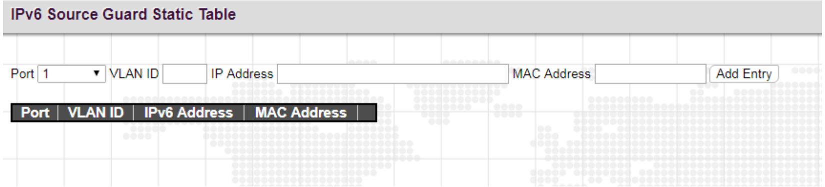
Port	Mode	Max Dynamic Clients
All	<>	<>
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited
9 (SFP)	Disabled	Unlimited
10 (SFP)	Disabled	Unlimited

Save Reset

Mode: Enable or disable the IPv6 Source Guard globally.

Max Dynamic Clients: Specify the maximum number of dynamic clients that can be learned on a given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, only IPv6 packets that are matched in static entries on the specific port are forwarded.

4.8.2.5.2. Static Table



IPv6 Source Guard Static Table

Port 1 VLAN ID IP Address MAC Address

Port	VLAN ID	IPv6 Address	MAC Address

This page shows the static IPv6 Source Guard entries. The maximum number of entries is 112 on the switch.

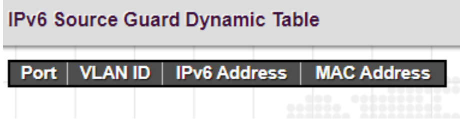
Port: The logical port the entry is bound to.

VLAN ID: The VLAN Id for the entry. If no VLAN Id is associated with the entry, this field shows 0.

IPv6 Address: Allowed Source IPv6 address.

MAC address: Allowed Source MAC address.

4.8.2.5.3. Dynamic Table



IPv6 Source Guard Dynamic Table

Port	VLAN ID	IPv6 Address	MAC Address

Port: Display the port number.

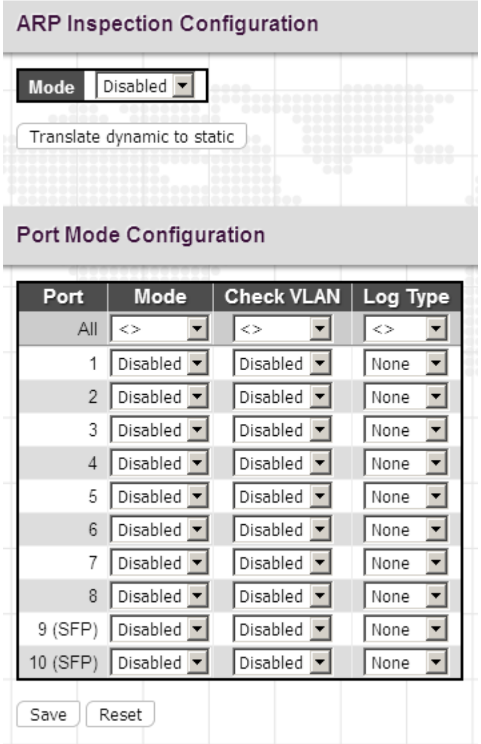
VLAN ID: Display the VLAN ID that traffic is permitted. "0" means no VLAN ID is associated with the entry.

IPv6 Address: Display source IPv6 address of the entry.

MAC Address: Source MAC address.

4.8.2.6. ARP Inspection

4.8.2.6.1. Configuration



ARP Inspection Configuration

Mode: Disabled

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
All	<>	<>	<>
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 (SFP)	Disabled	Disabled	None
10 (SFP)	Disabled	Disabled	None

ARP Inspection Configuration

Mode: Enable or disable ARP inspection function globally.

Port Mode Configuration

Port: The port number. “Port All” rules apply to all ports.

Mode: Enable or disable ARP Inspection on a port. Please note that to make ARP inspection work, both global mode and port mode must be enabled.

Check VLAN: Enable or disable Check VLAN inspection. If you want to inspect VLAN configurations, you need to enable this function. When disabled, the log type of ARP inspection will refer to the port setting. When enabled, the log type of ARP inspection will refer to the VLAN setting.

Log Type: There are four log types supported by this device:

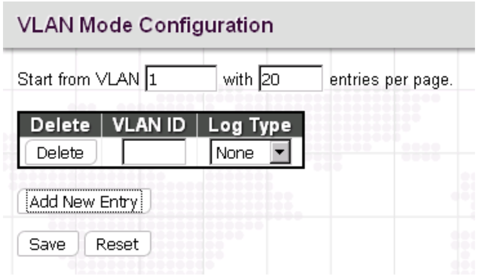
None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

All: Log all entries.

4.8.2.6.2. VLAN Mode Configuration



VLAN Mode Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Log Type
Delete		None

VLAN ID: Specify ARP Inspection is enabled on which VLANs.

Log Type: Select the log type.

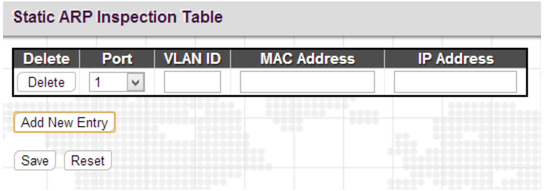
None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

All: Log all entries.

4.8.2.6.3. Static Table



Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1			

Port: Select a port to which a static entry is bound.

VLAN ID: Specify a configured VLAN ID.

MAC Address: Specify an allowed source MAC address in ARP request packets.

IP Address: Specify an allowed source IP address in ARP request packets.

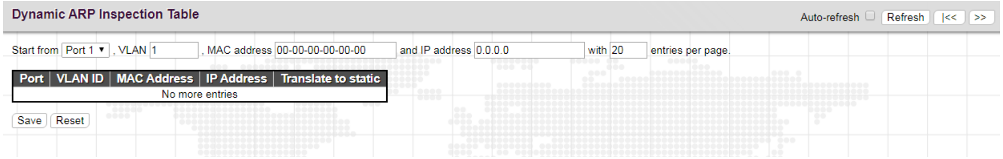
Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.8.2.6.4. Dynamic Table



Dynamic ARP Inspection Table

Start from Port 1 ▾ , VLAN 1 , MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	MAC Address	IP Address	Translate to static
No more entries				

Port: The port number of this entry.

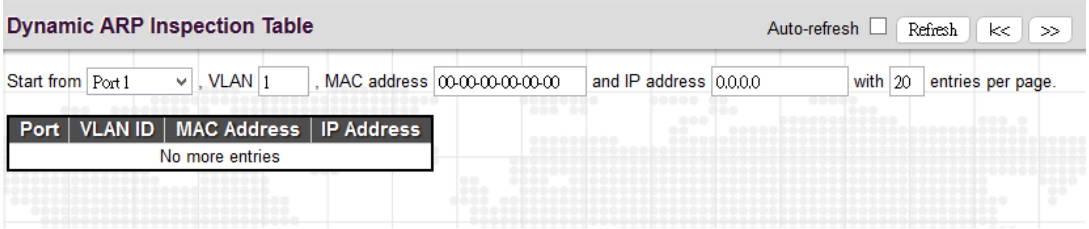
VLAN ID: VLAN ID in which the ARP traffic is permitted.

MAC Address: User MAC address of this entry.

IP Address: User IP address of this entry.

Translate to static: Translate the entry to the static one.

4.8.2.6.5. Dynamic ARP Inspection Table



Dynamic ARP Inspection Table

Start from Port 1 ▾ , VLAN 1 , MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	MAC Address	IP Address
No more entries			

Port: The port number of this entry.

VLAN ID: Displays VLAN ID in which the ARP traffic is permitted.

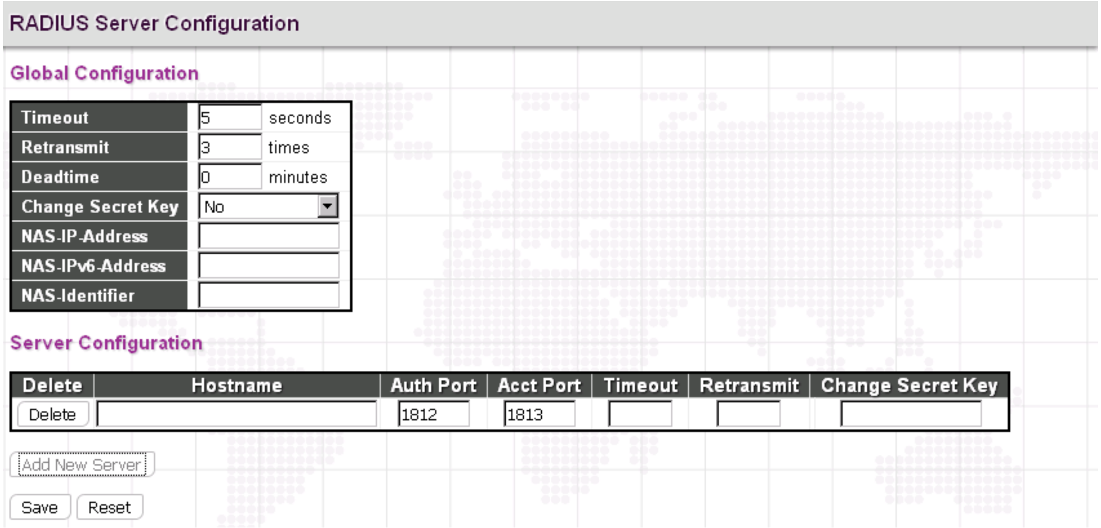
MAC Address: Displays User MAC address of this entry.

IP Address: Displays IP address of this entry.

4.8.3. AAA

4.8.3.1. RADIUS

4.8.3.1.1. Configuration



RADIUS Server Configuration

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Change Secret Key	No	
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Change Secret Key
Delete		1812	1813			

Global Configuration

Timeout: The time the switch waits for a reply from an authentication server before it retransmits the request.

Retransmit: This is the number of times (in the range 1 to 1000) that 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.

Deadtime: Deadtime 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 Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. The allowed deadtime range is between 0 to 1440minutes.

Change Secret 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 RADIUS server and the switch.

NAS-IP-Address (Attribute 4): The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-IPv6-Address (Attribute 95): 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.

NAS-Identifier (Attribute 32): The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

RADIUS Authentication Server Configuration

Hostname: The hostname or IPv4/IPv6 address for the RADIUS authentication server.

Auth Port: The UDP port to be used on the RADIUS server for authentication. Set to 0 to disable authentication.

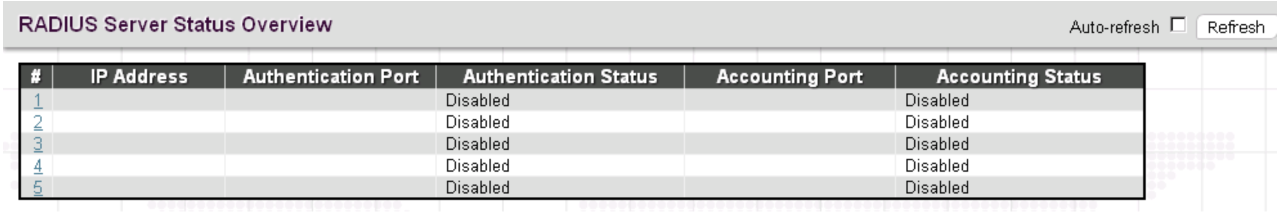
Acct Port: The UDP port to be used on the RADIUS server for accounting. Set to 0 to disable authentication.

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.

Change Secret Key: Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key.

4.8.3.1.2. Overview



RADIUS Server Status Overview

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1			Disabled		Disabled
2			Disabled		Disabled
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

RADIUS Server Status Overview

IP Address: The configured IP address of this server.

Authentication Port: UPD port number for authentication.

Authentication Status: The current state of RADIUS authentication server. Displayed states include the following:

Disabled: This server is disabled.

Not Ready: The server is ready but IP communication is not yet up and running.

Ready: The server is ready and IP communication is not yet up and running. The RADIUS server is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Accounting Port: UDP port number for accounting.

Accounting Status: The current status of the server. This field takes one of the following values:

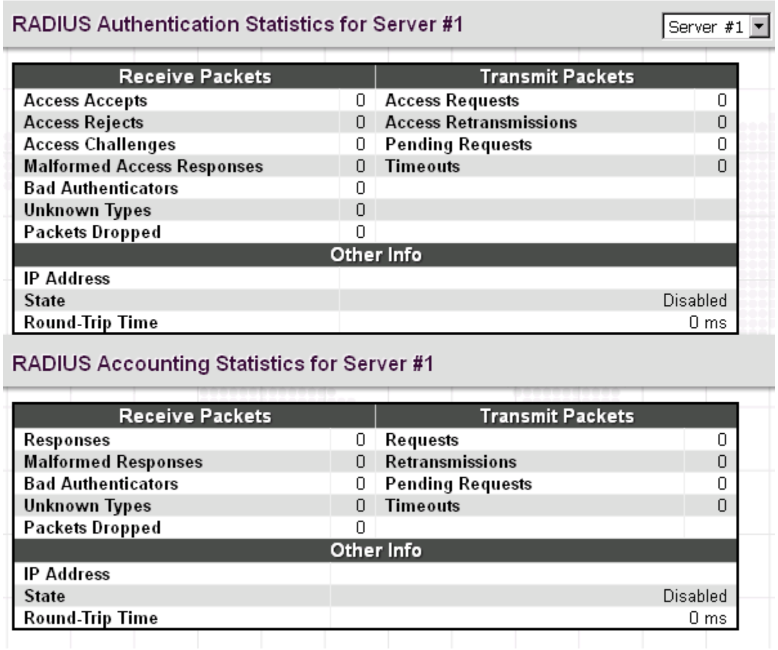
Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

4.8.3.1.3. RADIUS Details



RADIUS Authentication Statistics for Server #1

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

RADIUS Accounting Statistics for Server #1

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

RADIUS Authentication Statistics for Server

Access Accepts: The number of RADIUS Access-Accept packets (valid or invalid) received from the server.

Access Rejects: The number of RADIUS Access-Reject packets (valid or invalid) received from the server.

Access Challenges: The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.

Malformed Access Responses: The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.

Bad Authenticators: The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.

Unknown Types: The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.

Packets Dropped: The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.

Access Requests: The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.

Access Retransmissions: The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.

Pending Requests: The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

Timeouts: The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

IP Address: IP address and UDP port for the authentication server in question.

State: Shows the state of the server. It takes one of the following values:

Disabled: The selected server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time: The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics for Server

Responses: The number of RADIUS packets (valid or invalid) received from the server.

Malformed Responses: The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.

Bad Authenticators: The number of RADIUS packets containing invalid authenticators received from the server.

Unknown Types: The number of RADIUS packets of unknown types that were received from the server on the accounting port.

Packets Dropped: The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.

Requests: The number of RADIUS packets sent to the server. This does not include retransmissions.

Retransmissions: The number of RADIUS packets retransmitted to the RADIUS accounting server.

Pending Requests: The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.

Timeouts: The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

IP Address: IP address and UDP port for the accounting server in question.

State: Shows the state of the server. It takes one of the following values:

Disabled: The selected server is disabled.

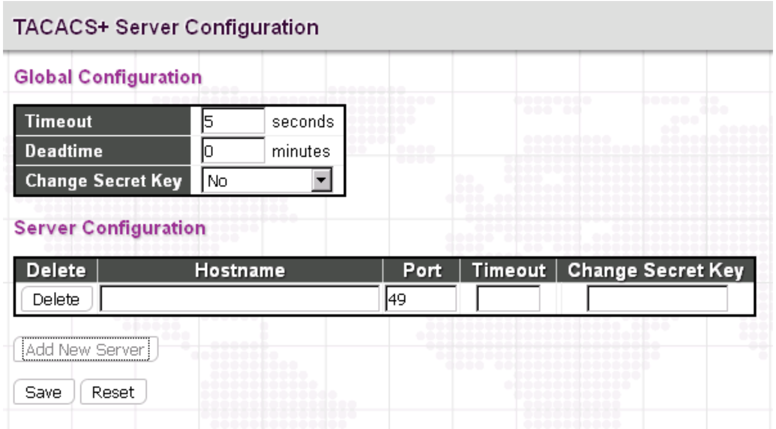
Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.

Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time: The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

4.8.3.2. TACACS+



TACACS+ Server Configuration

Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Change Secret Key	No	

Server Configuration

Delete	Hostname	Port	Timeout	Change Secret Key
Delete		49		

Global Configuration

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.

Deadtime: Deadtime, 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 Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Change Secret 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

Click "Adding a New Server" button to add a new server entry. Up to 5 servers are supported.

Hostname: The IPv4/IPv6 address or hostname of the TACACS+ server.

Port: The TCP port to use on the TACACS+ server for authentication.

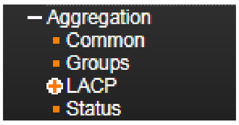
Timeout: This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Change Secret Key: Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key.

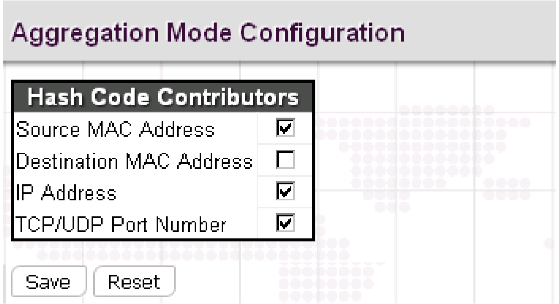
4.9. Aggregation

Compared with adding cost to install extra cables to increase the redundancy and link speed, link aggregation is a relatively inexpensive way to set up a high-speed backbone network that transfers much more data than any one single port or device can deliver. Link aggregation uses multiple ports in parallel to increase the link speed. And there are two types of aggregation that are available, namely “Static” and “LACP”.

Under the Aggregation heading are two major icons, static and LACP.



4.9.1. Common



Aggregation Mode Configuration

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

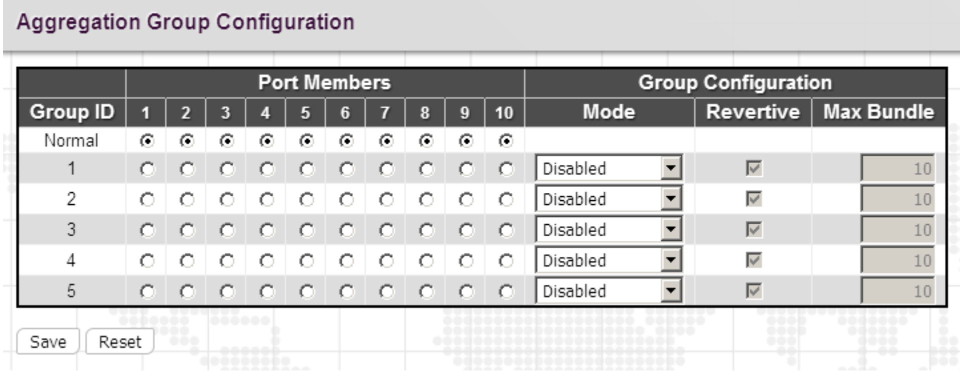
Source MAC Address: All traffic from the same Source MAC address is output on the same link in a trunk.

Destination MAC Address: All traffic with the same Destination MAC address is output on the same link in a trunk.

IP Address: All traffic with the same source and destination IP address is output on the same link in a trunk.

TCP/UDP Port Number: All traffic with the same source and destination TCP/UDP port number is output on the same link in a trunk.

4.9.2. Groups



Aggregation Group Configuration

	Port Members										Group Configuration		
Group ID	1	2	3	4	5	6	7	8	9	10	Mode	Revertive	Max Bundle
Normal	●	●	●	●	●	●	●	●	●	●			
1	○	○	○	○	○	○	○	○	○	○	Disabled	☑	10
2	○	○	○	○	○	○	○	○	○	○	Disabled	☑	10
3	○	○	○	○	○	○	○	○	○	○	Disabled	☑	10
4	○	○	○	○	○	○	○	○	○	○	Disabled	☑	10
5	○	○	○	○	○	○	○	○	○	○	Disabled	☑	10

Group ID: Trunk ID number. “Normal” means that no aggregation is used. Five aggregation groups are available for use. Each group contains at least 2 to 10 links (ports). Please note that each port can only be used once in Group ID 1~5.

Port Members: Select ports to belong to a certain trunk.

Mode: Determines the mode for the aggregation group.

Disabled: The group is disabled.

Static: The group operate in static aggregation mode.

LACP (Active): The group operates in LACP active aggregation mode.

LACP (Passive): The group operates in LACP passive aggregation mode.

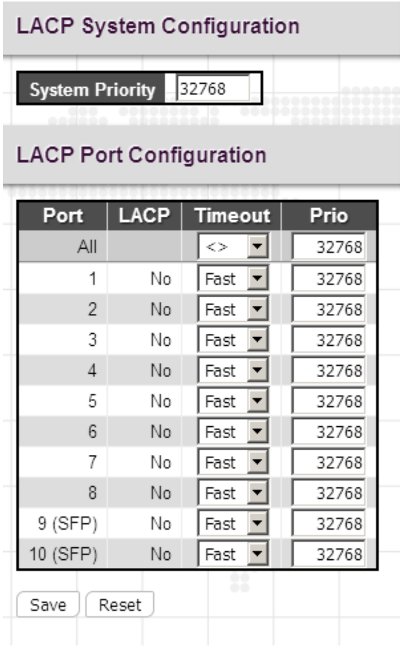
Revertive: This setting only applies to LACP-enabled ports. If the checkbox is selected, the group will perform automatic link re-calculation when links with higher priority become available.

Max Bundle: This setting only applies to LACP-enabled ports. It determines the maximum number of active bundled LACP ports allowed in an aggregation group.

4.9.3. LACP

The Switch supports dynamic Link Aggregation Control Protocol (LACP) which is specified in IEEE 802.3ad. Static trunks have to be manually configured at both ends of the link. In other words, LACP configured ports can automatically negotiate a trunked link with LACP configured ports on another devices. You can configure any number of ports on the Switch as LACP, as long as they are not already configured as part of a static trunk. If ports on other devices are also configured as LACP, the Switch and the other devices will negotiate a trunk link between them.

4.9.3.1. Port Configuration



LACP System Configuration

System Priority: 32768

LACP Port Configuration

Port	LACP	Timeout	Prio
All		<>	32768
1	No	Fast	32768
2	No	Fast	32768
3	No	Fast	32768
4	No	Fast	32768
5	No	Fast	32768
6	No	Fast	32768
7	No	Fast	32768
8	No	Fast	32768
9 (SFP)	No	Fast	32768
10 (SFP)	No	Fast	32768

System Priority: A LACP system priority is configured on each device running LACP. The system priority can be configured through the user interface. For priority setting, the range is 1 to 65535. The default priority is 32768. The lower the value, the higher the system priority

LACP Port Configuration

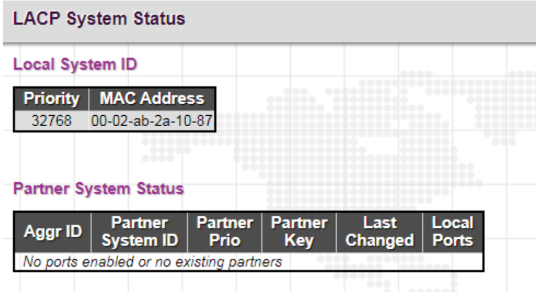
Port: The port number. “Port All” settings apply to all ports.

LACP: This shows whether LACP is currently enabled on a port or not.

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 priority of the port. The lower number means greater priority. This priority value controls which ports will be active and which ones will be in a backup role.

4.9.3.2. System Status



LACP System Status

Local System ID

Priority	MAC Address
32768	00-02-ab-2a-10-87

Partner System Status

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

Local System ID

This table displays system priority and MAC address.

Partner System Status

Aggr ID: Display the aggregation ID associated with the Link Aggregation Group (LAG).

Partner System ID: LAG's partner system ID (MAC address).

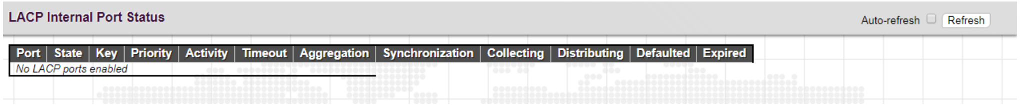
Partner Prio: The priority value of the partner.

Partner Key: The partner key assigned to this LAG.

Last Changed: The time since this LAG changed.

Local Ports: The local ports that are a port of this LAG.

4.9.3.3. Internal Status



LACP Internal Port Status

Port	State	Key	Priority	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
No LACP ports enabled											

Port: Display the switch port number.

State: Display the current port state.

Down: The port is not active.

Active: The port is in active state.

Standby: The port is in standby state.

Key: The key assigned to this port. Only ports with the same key can aggregate together.

Priority: The priority assigned to this aggregation group.

Activity: The LACP mode of the group (Active or Passive).

Timeout: The timeout mode configured for the port (Fast or Slow).

Aggregation: Show whether the system considers this link is able to be "aggregated" or not; i.e., a potential candidate for aggregation.

Synchronization: Show whether the system considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.

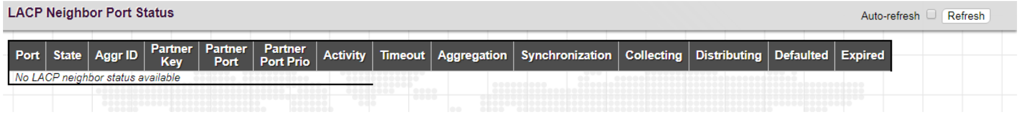
Collecting: Show if collection of incoming frames on this link is enabled.

Distributing: Show if distribution of outgoing frames on this link is enabled.

Defaulted: Show if the Actor's Receive machine is using Defaulted operational Partner information.

Expired: Show if that the Actor's Receive machine is in the EXPIRED state.

4.9.3.4. Neighbor Status



LACP Neighbor Port Status

Port	State	Aggr ID	Partner Key	Partner Port	Partner Port Prio	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
No LACP neighbor status available													

Port: Display the switch port number.

State: Display the current port state.

Down: The port is not active.

Active: The port is in active state.

Standby: The port is in standby state.

Aggr ID: The aggregation group ID which the port is assigned to.

Partner Key: The key assigned to this port by the partner.

Partner Port: The partner port number associated with this link.

Partner Port Priority: The priority assigned to this partner port.

Activity: The LACP mode of the group (Active or Passive).

Timeout: The timeout mode configured for the partner port (Fast or Slow).

Aggregation: Show whether the partner considers this link is able to be "aggregated" to not; i.e., a potential candidate for aggregation.

Synchronization: Show whether the partner considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.

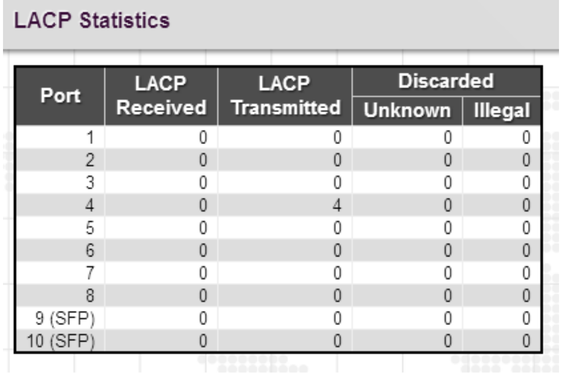
Collecting: Show if collection of incoming frames on this link is enabled.

Distributing: Show if distribution of outgoing frames on this link is enabled.

Defaulted: Show if the partners Receive machine is using Defaulted operational Partner information.

Expired: Show if that the partners Receive machine is in the EXPIRED state.

4.9.3.5. Port Statistics



LACP Statistics

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

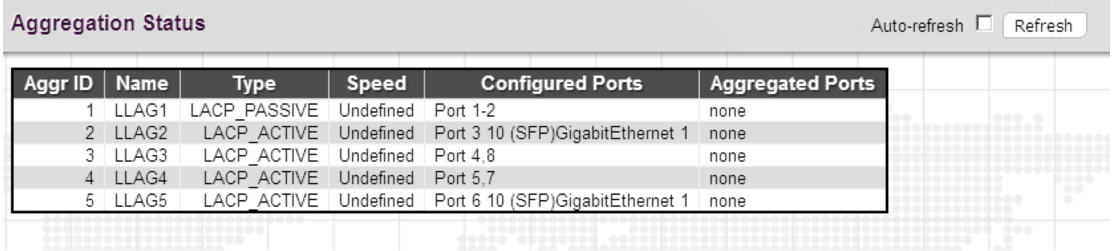
Port: The port number.

LACP Received: The number of LACP packets received on a port.

LACP Transmitted: The number of LACP packets transmitted by a port

Discarded: The number of unknown and illegal packets that have been discarded on a port.

4.9.4. Aggregation Status



Aggregation Status

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports
1	LLAG1	LACP_PASSIVE	Undefined	Port 1-2	none
2	LLAG2	LACP_ACTIVE	Undefined	Port 3 10 (SFP)GigabitEthernet 1	none
3	LLAG3	LACP_ACTIVE	Undefined	Port 4,8	none
4	LLAG4	LACP_ACTIVE	Undefined	Port 5,7	none
5	LLAG5	LACP_ACTIVE	Undefined	Port 6 10 (SFP)GigabitEthernet 1	none

Aggr ID: Display the aggregation ID associated with this aggregation instance.

Name: Display the name of the group ID.

Type: Display the type of aggregation group (Static or LACP).

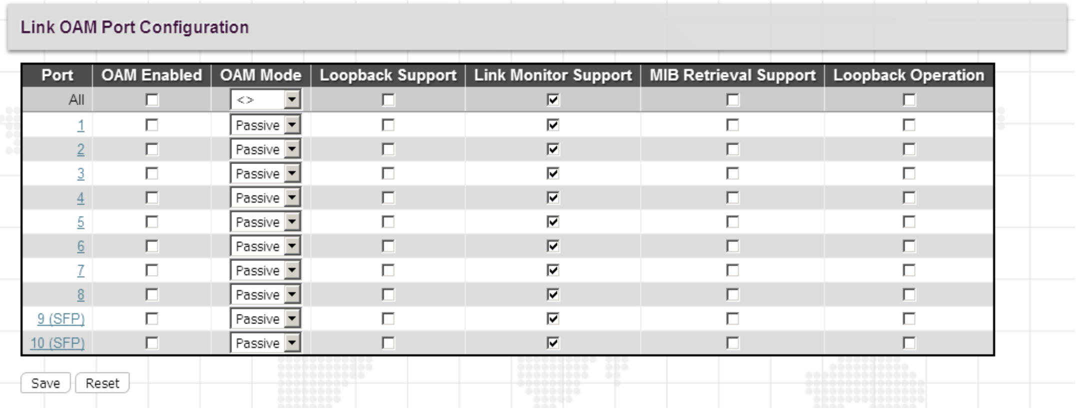
Speed: Display the speed of the aggregation group.

Configured Ports: The configured ports of the aggregation group.

Aggregated Ports: Aggregated member ports of the aggregation group.

4.10. Link OAM

4.10.1. Port Settings



Link OAM Port Configuration

Port	OAM Enabled	OAM Mode	Loopback Support	Link Monitor Support	MIB Retrieval Support	Loopback Operation
All	□	<>	□	☑	□	□
1	□	Passive	□	☑	□	□
2	□	Passive	□	☑	□	□
3	□	Passive	□	☑	□	□
4	□	Passive	□	☑	□	□
5	□	Passive	□	☑	□	□
6	□	Passive	□	☑	□	□
7	□	Passive	□	☑	□	□
8	□	Passive	□	☑	□	□
9 (SFP)	□	Passive	□	☑	□	□
10 (SFP)	□	Passive	□	☑	□	□

Port: The port number. Click on the port to view its OAM status details.

OAM Enabled: Select the checkbox to enable OAM function on a port. Clear the checkbox to disable OAM.

OAM Mode: Select the OAM mode on a per port basis. The default mode is “Passive”.

> **Active:** The device set in Active mode initiates the exchange of Information OAMPDUs
>
> **Passive:** The device in Passive mode does not initiate the Discovery process but reacts to the initiation of the Discovery process by the remote 802.3ah-enabled device.

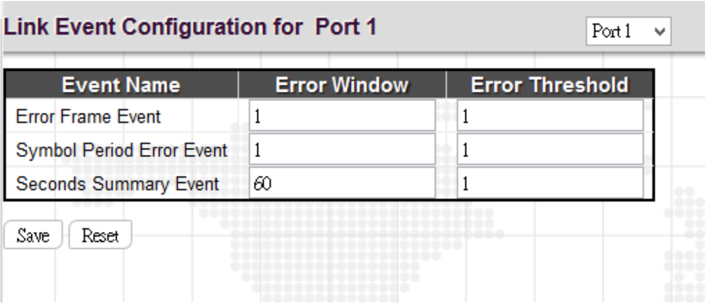
Loopback Support: Select the checkbox to enable loopback support on a port. Link OAM remote loopback support can be used for fault localization and link performance testing. Enabling the loopback support will allow the DTE to execute the remote loopback command that helps in the fault detection.

Link Monitor Support: Select the checkbox to enable link monitor support. Once enabled, the DTE supports event notification that permits the inclusion of diagnostic information.

MIB Retrieval Support: Select the checkbox to enable MIB retrieval support. Once enabled, the DTE supports polling of various link OAM based MIB variables’ contents.

Loopback Operation: If the “Loopback Support” is enabled, selecting the “Loopback Operation” checkbox will start a loopback operation for the port.

4.10.2. Event Settings



Link Event Configuration for Port 1

Event Name	Error Window	Error Threshold
Error Frame Event	1	1
Symbol Period Error Event	1	1
Seconds Summary Event	60	1

Link Event can be configured on a per-port basis. Select the desire port number from the pull-down menu to configure its Link Event settings.

Event Name: Ethernet OAM entities monitor link status by exchanging Event Notification OAMPDUs. When one of the events listed here is detected, an OAM entity sends an Event Notification OAMPDU to its peer OAM entity.

Error Frame Event: The Errored Frame Event counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 1 sec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Error Frame Event' must be an integer value between 1~60 and its default value is '1'. Whereas Error Threshold must be between 0-0xffffffff and its default value is '0'.

Symbol Period Error Event: The Errored Symbol Period Event counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period. Error Window for 'Symbol Period Error Event' must be an integer value between 1~60 and its default value is '1'. Whereas Error Threshold must be between 0-0xffffffff and its default value is '0'.

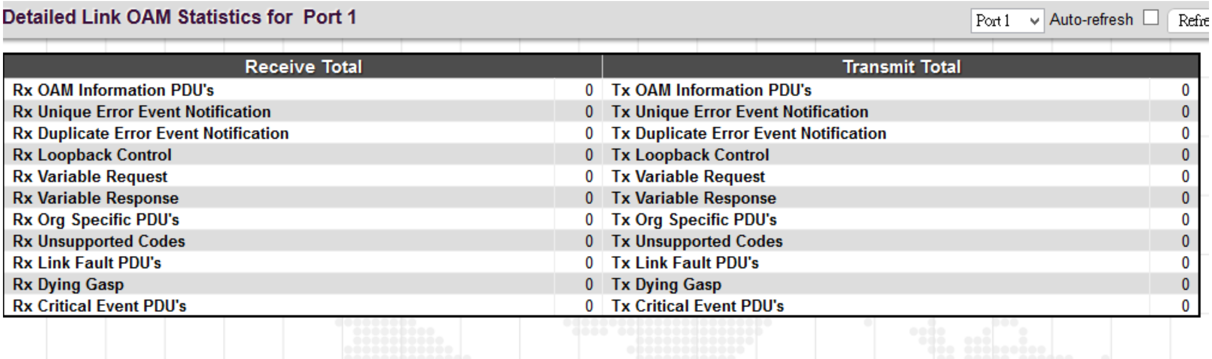
Seconds Summary Event: The Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Seconds Summary Event' must be an integer value between 10~900 and its default value is '60'. Whereas Error Threshold must be between 0-0xffff and its default value is '1'.

Error Window: Specify the window period in the order of 1 sec for the observation of various link events.

Error Threshold: Specify the error threshold value for the window period for the appropriate Link event so as to notify the peer of this error.

4.10.3. Statistics

This page provides Link OAM statistics for the selected port. Use the pull-down menu to select the port that you want to view detailed statistics.



Detailed Link OAM Statistics for Port 1

Receive Total		Transmit Total	
Rx OAM Information PDU's	0	Tx OAM Information PDU's	0
Rx Unique Error Event Notification	0	Tx Unique Error Event Notification	0
Rx Duplicate Error Event Notification	0	Tx Duplicate Error Event Notification	0
Rx Loopback Control	0	Tx Loopback Control	0
Rx Variable Request	0	Tx Variable Request	0
Rx Variable Response	0	Tx Variable Response	0
Rx Org Specific PDU's	0	Tx Org Specific PDU's	0
Rx Unsupported Codes	0	Tx Unsupported Codes	0
Rx Link Fault PDU's	0	Tx Link Fault PDU's	0
Rx Dying Gasp	0	Tx Dying Gasp	0
Rx Critical Event PDU's	0	Tx Critical Event PDU's	0

Rx & Tx OAM Information PDU’s: The number of received and transmitted OAM Information PDU's. Discontinuities of this counter can occur at re-initialization of the management system.

Rx & Tx Unique Error Event Notification: A count of the number of unique Event OAMPDUs received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.

Rx & Tx Duplicate Error Event Notification: A count of the number of duplicate Event OAMPDUs received and transmitted on this interface. Event Notification OAMPDUs may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.

Rx & Tx Loopback Control: The number of Loopback Control OAMPDUs received and transmitted on this interface.

Rx & Tx Variable Request: The number of Variable Request OAMPDUs received and transmitted on this interface.

Rx & Tx Variable Response: The number of Variable Response OAMPDUs received and transmitted on this interface.

Rx & Tx Org Specific PDU’s: The number of Organization Specific OAMPDUs transmitted on this interface.

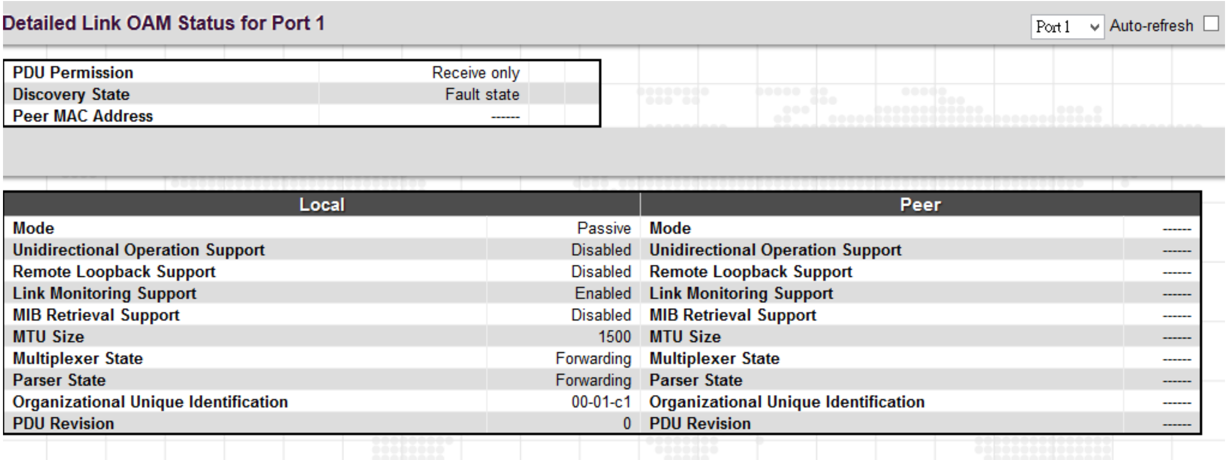
Rx & Tx Unsupported Codes: The number of OAMPDUs transmitted on this interface with an unsupported op-code.

Rx & Tx Link fault PDU’s: The number of Link fault PDU's received and transmitted on this interface.

Rx & Tx Dying Gasp: The number of Dying Gasp events received and transmitted on this interface.

Rx & Tx Critical Event PDU's: The number of Critical event PDU's received and transmitted on this interface.

4.10.4. Port Status



Detailed Link OAM Status for Port 1

PDU Permission	Receive only
Discovery State	Fault state
Peer MAC Address	------

Local		Peer	
Mode	Passive	Mode	------
Unidirectional Operation Support	Disabled	Unidirectional Operation Support	------
Remote Loopback Support	Disabled	Remote Loopback Support	------
Link Monitoring Support	Enabled	Link Monitoring Support	------
MIB Retrieval Support	Disabled	MIB Retrieval Support	------
MTU Size	1500	MTU Size	------
Multiplexer State	Forwarding	Multiplexer State	------
Parser State	Forwarding	Parser State	------
Organizational Unique Identification	00-01-c1	Organizational Unique Identification	------
PDU Revision	0	PDU Revision	------

Detailed Link OAM Status

PDU Permission: Displays the current permission rules set for the local DTE. Possible values are "Link fault", "Receive only", "Information exchange only", "ANY".

Discovery State: Displays the current state of the discovery process. Possible states are Fault state, Active state, Passive state, SEND_LOCAL_REMOTE_STATE, SEND_LOCAL_REMOTE_OK_STATE, SEND_ANY_STATE.

Peer MAC Address: Displays the MAC address of the peer device.

Local & Peer

Mode: This field shows the Mode in which the Link OAM is operating, Active or Passive.

Unidirectional Operation Support: This feature is not available to be configured by the user. The status of this configuration is retrieved from the PHY.

Remote Loopback Support: If status is enabled, the device is capable of OAM remote loopback mode.

Link Monitoring Support: If status is enabled, the device supports interpreting Link Events.

MIB Retrieval Support: If status is enabled, the device supports sending Variable Response OAMPDUs.

MTU Size: It represents the largest OAMPDU, in octets, supported by the device. This value is compared to the remotes Maximum PDU Size and the smaller of the two is used.

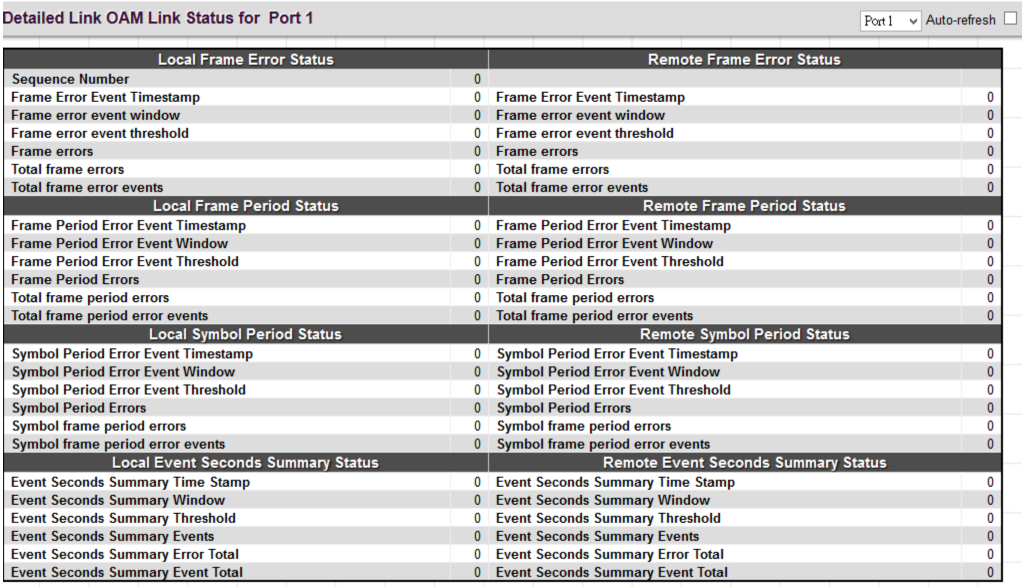
Multiplexer State: When in forwarding state, the device is forwarding non-OAMPDUs to the lower sub-layer. In case of discarding, the device discards all the non-OAMPDU's.

Parser State: When in forwarding state, the device is forwarding non-OAMPDUs to higher sub-layer. When in loopback, the device is looping back non-OAMPDUs to the lower sub-layer. When in discarding state, the device is discarding non-OAMPDUs.

Organizational Unique Identification: 24-bit Organizationally Unique Identifier of the vendor.

PDU Revision: It indicates the current revision of the Information TLV. The value of this field shall start at zero and be incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV doesn't need to be parsed as nothing in it has changed).

4.10.5. Event Status



Detailed Link OAM Link Status for Port 1

Local Frame Error Status		Remote Frame Error Status	
Sequence Number	0		
Frame Error Event Timestamp	0	Frame Error Event Timestamp	0
Frame error event window	0	Frame error event window	0
Frame error event threshold	0	Frame error event threshold	0
Frame errors	0	Frame errors	0
Total frame errors	0	Total frame errors	0
Total frame error events	0	Total frame error events	0
Local Frame Period Status		**Remote Frame Period Status**	
Frame Period Error Event Timestamp	0	Frame Period Error Event Timestamp	0
Frame Period Error Event Window	0	Frame Period Error Event Window	0
Frame Period Error Event Threshold	0	Frame Period Error Event Threshold	0
Frame Period Errors	0	Frame Period Errors	0
Total frame period errors	0	Total frame period errors	0
Total frame period error events	0	Total frame period error events	0
Local Symbol Period Status		**Remote Symbol Period Status**	
Symbol Period Error Event Timestamp	0	Symbol Period Error Event Timestamp	0
Symbol Period Error Event Window	0	Symbol Period Error Event Window	0
Symbol Period Error Event Threshold	0	Symbol Period Error Event Threshold	0
Symbol Period Errors	0	Symbol Period Errors	0
Symbol frame period errors	0	Symbol frame period errors	0
Symbol frame period error events	0	Symbol frame period error events	0
Local Event Seconds Summary Status		**Remote Event Seconds Summary Status**	
Event Seconds Summary Time Stamp	0	Event Seconds Summary Time Stamp	0
Event Seconds Summary Window	0	Event Seconds Summary Window	0
Event Seconds Summary Threshold	0	Event Seconds Summary Threshold	0
Event Seconds Summary Events	0	Event Seconds Summary Events	0
Event Seconds Summary Error Total	0	Event Seconds Summary Error Total	0
Event Seconds Summary Event Total	0	Event Seconds Summary Event Total	0

Local & Remote Frame Error Status

Sequence Number: This two-octet field indicates the total number of events occurred at the remote end.

Frame Error Event Timestamp: This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Frame error event window: This two-octet field indicates the duration of the period in terms of 100 ms intervals. 1) The default value is one second. 2) The lower bound is one second. 3) The upper bound is one minute.

Frame error event threshold: This four-octet field indicates the number of detected errored frames in the period is required to be equal to or greater than in order for the event to be generated. 1) The default value is one frame error. 2) The lower bound is zero frame errors. 3) The upper bound is unspecified.

Frame errors: This four-octet field indicates the number of detected errored frames in the period.

Total frame errors: This eight-octet field indicates the sum of errored frames that have been detected since the OAM sub-layer was reset.

Total frame error events: This four-octet field indicates the number of Errored Frame Event TLVs that have been generated since the OAM sublayer was reset.

Local & Remote Frame Period Status

Frame Period Error Event Timestamp: This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Frame Period Error Event Window: This four-octet field indicates the duration of period in terms of frames.

Frame Period Error Event Threshold: This four-octet field indicates the number of errored frames in the period is required to be equal to or greater than in order for the event to be generated.

Frame Period Errors: This four-octet field indicates the number of frame errors in the period.

Total frame period errors: This eight-octet field indicates the sum of frame errors that have been detected since the OAM sub-layer was reset.

Total frame period error events: This four-octet field indicates the number of Errored Frame Period Event TLVs that have been generated since the OAM sub-layer was reset.

Local & Remote Symbol Period Status

Symbol Period Error Event Timestamp: This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Symbol Period Error Event Window: This eight-octet field indicates the number of symbols in the period.

Symbol Period Error Event Threshold: This eight-octet field indicates the number of errored symbols in the period is required to be equal to or greater than in order for the event to be generated.

Symbol Period Errors: This eight-octet field indicates the number of symbol errors in the period.

Symbol frame period errors: This eight-octet field indicates the sum of symbol errors since the OAM sub-layer was reset.

Symbol frame period error events: This four-octet field indicates the number of Errored Symbol Period Event TLVs that have been generated since the OAM sub-layer was reset.

Local & Remote Event Seconds Summary Status

Event Seconds Summary Time Stamp: This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

Event Seconds Summary Window: This two-octet field indicates the duration of the period in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

Event Seconds Summary Threshold: This two-octet field indicates the number of errored frame seconds in the period is required to be equal to or greater than in order for the event to be generated, encoded as a 16-bit unsigned integer.

Event Seconds Summary Events: This two-octet field indicates the number of errored frame seconds in the period, encoded as a 16-bit unsigned integer.

Event Seconds Summary Error Total: This four-octet field indicates the sum of errored frame seconds that have been detected since the OAM sub-layer was reset.

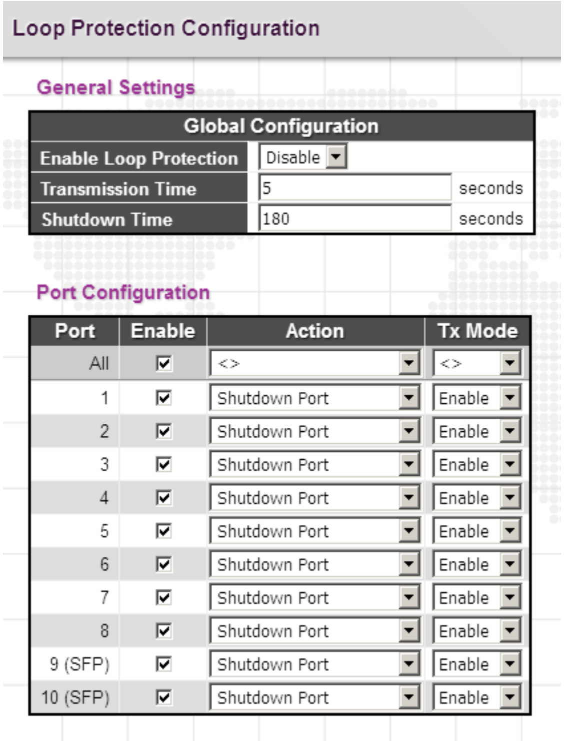
Event Seconds Summary Event Total: This four-octet field indicates the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sub-layer was reset, encoded as a 32bit unsigned integer.

4.11. Loop Protection

Loops sometimes occur in a network due to improper connecting, hardware problem or faulty protocol settings. When loops are seen in a switched network, they consume switch resources and thus downgrade switch performance. Loop Protection feature is provided in this switch and can be enabled globally or on a per port basis. Using loop protection enables the switch to automatically detect loops on a network. Once loops are detected, ports received the loop protection packet form the switch can be shut down or loopped events can be logged.

In Loop Protection menu, you can select Configuration or Status.

4.11.1. Configuration



Loop Protection Configuration

General Settings

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

Port Configuration

Port	Enable	Action	Tx Mode
All	☑	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
3	☑	Shutdown Port	Enable
4	☑	Shutdown Port	Enable
5	☑	Shutdown Port	Enable
6	☑	Shutdown Port	Enable
7	☑	Shutdown Port	Enable
8	☑	Shutdown Port	Enable
9 (SFP)	☑	Shutdown Port	Enable
10 (SFP)	☑	Shutdown Port	Enable

General Settings

Enable Loop Protection: Enable or disable loop protection function.

Transmission Time: The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.

Shutdown Time: The period for which a port will be kept disabled. Valid values are 0 to 604800 seconds. 0 means that a port is kept disabled until next device restart.

Port Configuration

Port: List the number of each port. “All” settings apply to all ports.

Enable: Enable or disable the selected ports’ loop protection function.

Action: When a loop is detected on a port, the loop protection will immediately take appropriate actions. Actions will be taken include “Shutdown Port”, “Shutdown Port and Log” or “Log Only”.

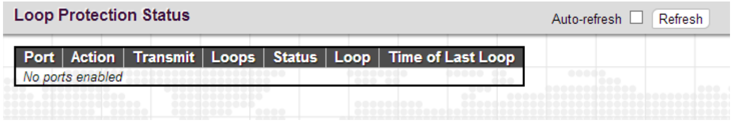
Shutdown Port: A loop-detected port is shutdown for a period of time configured in “Shutdown Time”.

Shutdown Port and Log: A loop-detected port is shutdown for a period of time configured in “Shutdown Time” and the event is logged.

Log Only: The event is logged and the port remains enable.

Tx Mode: Enable or disable a port to actively generate loop protection PDUs or to passively look for looped PDUs.

4.11.2. 4.11.2 Status



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

Port: The port number.

Action: Display the configured action that the switch will react when loops occur.

Transmit: Display the configured transmit (Tx) mode.

Loops: The number of loops detected on a port.

Status: The current loop status detected on a port.

Loop: Loops detected on a port or not.

Time of Last Loop: The time of the last loop event detected.

4.12. Spanning Tree

For some networking services, always-on connections are required to ensure that end users' online related activities are not interrupted due to unexpected disconnections. In these circumstances, multiple active paths between network nodes are established to prevent disconnections from happening. However, multiple paths interconnected with each other have a high tendency to cause bridge loops that make networks unstable and in worst cases make networks unusable. For example, the MAC address table used by the switch or bridge can fail, since the same MAC addresses (and hence the same network hosts) are seen on multiple ports. Second, a broadcast storm occurs. This is caused by broadcast packets being forwarded in an endless loop between switches. A broadcast storm can consume all available CPU resources and bandwidth.

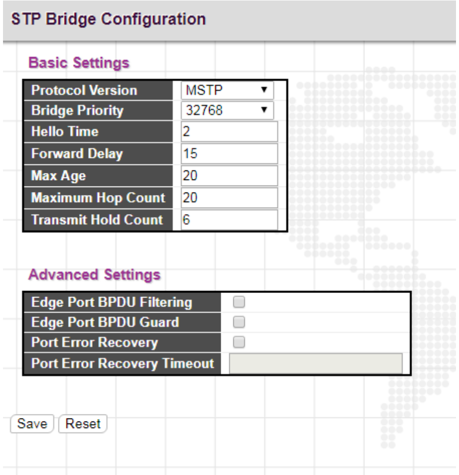
To solve problems causing by bridge loops, spanning tree allows a network design to include redundant links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manually enabling/disabling these backup links.

The Spanning Tree Protocol (STP), defined in the IEEE Standard 802.1s, can create a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches) and disable the links which are not part of that tree, leaving a single active path between any two network nodes.

To provide faster spanning tree convergence after a topology change, an evolution of the Spanning Tree Protocol "Rapid Spanning Tree Protocol (RSTP)", is introduced by IEEE 802.1w. RSTP is a refinement of STP; therefore, it shares most of its basic operation characteristics. This essentially creates a cascading effect away from the root bridge where each designated bridge proposes to its neighbors to determine if it can make a rapid transition. This is one of the major elements which allows RSTP to achieve faster convergence times than STP.

The other extension of RSTP is IEEE 802.1s Multiple Spanning Tree protocol (MSTP) that allows different VLANs to travel along separate instances of spanning tree. Unlike STP and RSTP, MSTP eliminates the needs for having different STP for each VLAN. Therefore, in a large networking environment that employs many VLANs, MSTP can be more useful than legacy STP.

4.12.1. Bridge Settings



STP Bridge Configuration

Basic Settings

Protocol Version	MSTP ▾
Bridge Priority	32768 ▾
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	□
Edge Port BPDU Guard	□
Port Error Recovery	□
Port Error Recovery Timeout	

Basic Settings

Protocol Version: Select the appropriate spanning tree protocol. Protocol versions provided include "STP", "RSTP", and "MSTP".

Bridge Priority: Each switch has a relative priority and cost that is used to decide what the shortest path is to forward a packet. The lowest cost path (lowest numeric value) has a higher priority and is always used unless it is down. If you have multiple bridges and interfaces then you need to adjust the priorities to achieve optimized performance. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Forward Delay: Fort STP bridges, the Forward Delay is the time spent in each Listening and Learning state before the Forwarding state is entered. This delay occurs when a new bridge comes onto a network. Valid values are 4-30 seconds.

Max Age: If another switch in the spanning tree does not send out a hello packet for a period of time, it is considered to be disconnected. Valid values are 6 to 40 seconds, and Max Age values must be smaller than or equal to (Forward Delay-1)*2.

Maximum Hop Count: The maximum number of hops allowed for MST region before a BPDU is discarded. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the BPDU is discarded. The default hop count is 20. The allowed range is 6-40.

Transmit Hold Count: The number of BPDU sent by a bridge port per second. When exceeded, transmission of the next BPDU will be delayed. By default, it is set to 6. The allowed transmit hold count is 1 to 10. Please note that increasing this value might have a significant impact on CPU utilization and decreasing this value might slow down convergence. It is recommended to remain Transmit Hold Count to the default setting.

Advanced Settings

Edge Port BPDU Filtering: The purpose of Port BPDU Filtering is to prevent the switch from sending BPDU frames on ports that are connected to end devices.

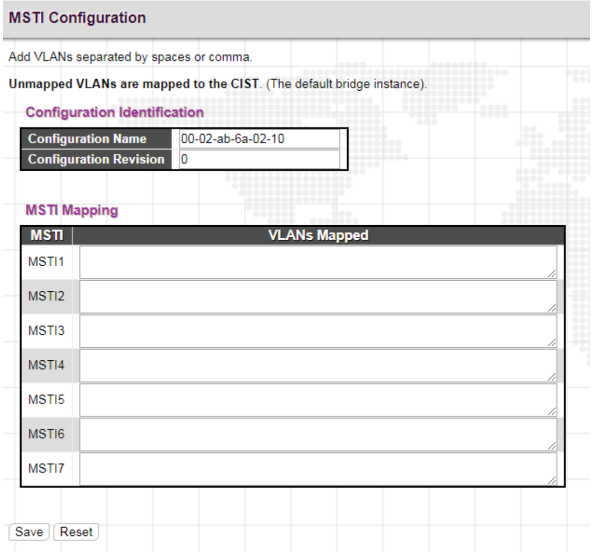
Edge Port BPDU Guard: Edge ports generally connect directly to PC, file servers or printers. Therefore, edge ports are configured to allow rapid transition. Under normal situations, edge ports should not receive configuration BPDUs. However, if they do, this probably is due to malicious attacks or mis-settings. When edge ports receive configuration BPDUs, they will be automatically set to non-edge ports and start a new spanning tree calculation process.

BPDU Guard is therefore used to prevent the device from suffering malicious attacks. With this function enabled, when edge ports receive configuration BPDUs, STP disables those affected edge ports. After a period of recovery time, those disabled ports are re-activated.

Port Error Recovery: When enabled, a port that is in the error-disabled state can automatically be enabled after a certain time.

Port Error Recovery Timeout: The time that has to pass before a port in the error-disabled state can be enabled. The allowed range is 30~86400 seconds.

4.12.2. MSTI Mapping



MSTI Configuration

Add VLANs separated by spaces or comma.

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

Configuration Identification

Configuration Name	00-02-ab-6a-02-10
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

<u>Configuration Identification</u>

Configuration Name: The name for this MSTI. By default, the switch's MAC address is used. The maximum length is 32 characters. In order to share spanning trees for MSTI, bridges must have the same configuration name and revision value.

Configuration Revision: The revision number for this MSTI. The allowed range is 0~65535.

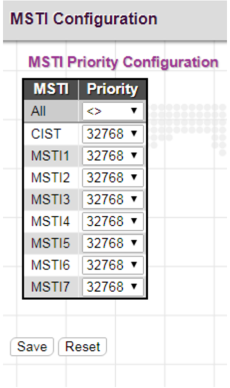
<u>MSTI Mapping</u>

MSTI: MSTI instance number.

VLAN Mapped: Specify VLANs mapped to a certain MSTI. Both a single VLAN and a range of VLANs are allowed. Separate

VLANs with a comma and use hyphen to denote a range of VLANs. (Example: 2,5,20-40) Leave the field empty for unused MSTI.

4.12.3. MSTI Priorities



MSTI Configuration

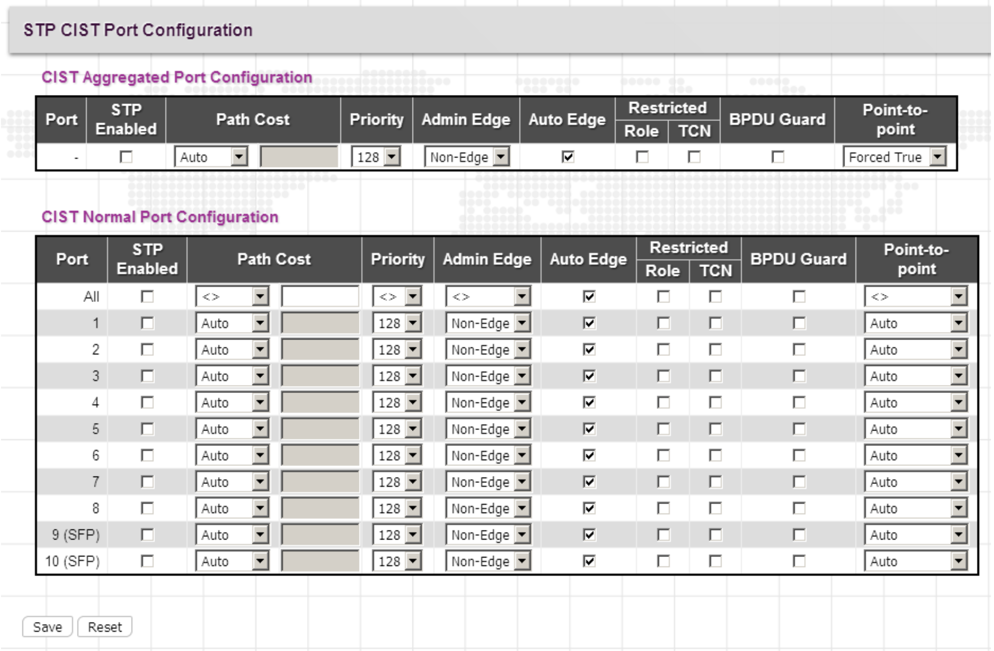
MSTI Priority Configuration

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

MSTI: Display MSTI instance number. “MSTI All” priority rule applies to all ports.

Priority: Select an appropriate priority for each MSTI instance. Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Note that lower numeric values indicate higher priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

4.12.4. CIST Ports



STP CIST Port Configuration

CIST Aggregated Port Configuration

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

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
All	☐	<>		<>	<>	☑	☐	☐	☐	<>
1	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
2	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
3	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
4	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
5	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
6	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
7	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
8	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
9 (SFP)	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
10 (SFP)	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto

<u>CIST Aggregated & Normal Port Configuration</u>

Port: The port number.

STP Enabled: Enable STP function

Path Cost: Path cost is used to determine the best path between devices. If “Auto” mode is selected, the system automatically detects the speed and duplex mode to decide the path cost. Select “Specific”, if you want to use user-defined value. Valid values are 1 to 200000000. Please note that path cost takes precedence over port priority.

Priority: Select port priority.

Admin Edge: If an interface is attached to end nodes, you can set it to “Edge”.

Auto Edge: Select the checkbox to enable this feature. When enabled, a port is automatically determined to be at the edge of the network when it receives no BPDUs.

Restricted Role: If enabled, this causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority.

Restricted TCN: If enabled, this causes the port not to propagate received topology change notifications and topology changes to other ports.

BPDU Guard: This feature protects ports from receiving BPDUs. It can prevent loops by shutting down a port when a BPDU is received instead of putting it into the spanning tree discarding state. If enabled, the port will disable itself upon receiving valid BPDU's.

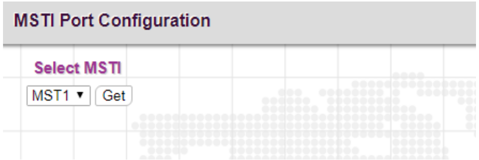
Point-to-Point: Select the link type attached to an interface.

Auto: The switch automatically determines whether the interface is attached to a point-to-point link or shared medium.

Forced True: It is a point-to-point connection.

Forced False: It is a shared medium connection.

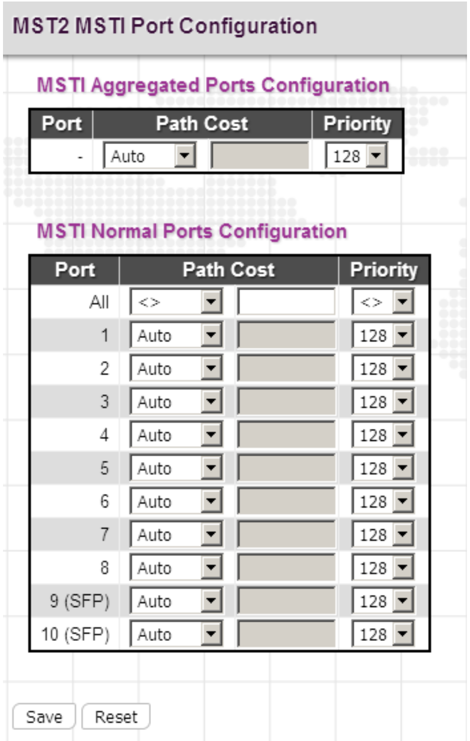
4.12.5. MSTI Ports



MSTI Port Configuration

Select MSTI

MST1 ▾ Get



MST2 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost		Priority
-	Auto		128

MSTI Normal Ports Configuration

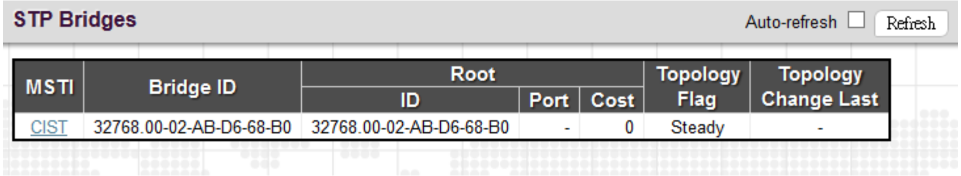
Port	Path Cost		Priority
All	<>		<>
1	Auto		128
2	Auto		128
3	Auto		128
4	Auto		128
5	Auto		128
6	Auto		128
7	Auto		128
8	Auto		128
9 (SFP)	Auto		128
10 (SFP)	Auto		128

Port: The port number.

Path Cost: Path cost is used to determine the best path between devices. If "Auto" mode is selected, the system automatically detects the speed and duplex mode to decide the path cost. Select "Specific", if you want to use user-defined value. Valid values are 1 to 200000000. Please note that path cost take precedence over port priority.

Priority: Select port priority.

4.12.6. Bridge Status



STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-02-AB-D6-68-B0	32768.00-02-AB-D6-68-B0	-	0	Steady	-

STP Bridge

MSTI: The bridge instance. Click this instance to view STP detailed bridge status.

Bridge ID: The unique bridge ID for this instance consisting a priority value and MAC address of the bridge switch.

Root ID: Display the root device's priority value and MAC address.

Root Port: The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.

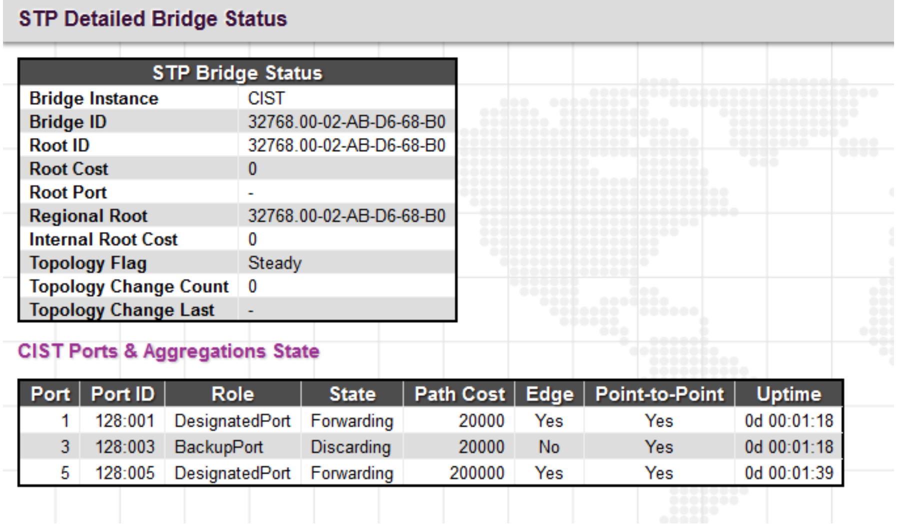
Root Cost: The path cost from the root port on the switch to the root device. For the root bridge this is zero. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge.

Topology Flag: The current state of the Topology Change Notification flag for this bridge instance.

Topology Change Last: The time since this spanning tree was last configured.

STP Detailed Bridge Status

Click the MSTI instance to view STP detailed bridge status.



STP Detailed Bridge Status

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.00-02-AB-D6-68-B0
Root ID	32768.00-02-AB-D6-68-B0
Root Cost	0
Root Port	-
Regional Root	32768.00-02-AB-D6-68-B0
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
1	128:001	DesignatedPort	Forwarding	20000	Yes	Yes	0d 00:01:18
3	128:003	BackupPort	Discarding	20000	No	Yes	0d 00:01:18
5	128:005	DesignatedPort	Forwarding	200000	Yes	Yes	0d 00:01:39

Bridge Instance: The bridge instance.

Bridge ID: The unique bridge ID for this instance consisting a priority value and MAC address of the bridge switch.

Root ID: Display the root device’s priority value and MAC address.

Root Cost: The path cost from the root port on the switch to the root device. For the root bridge this is zero. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge.

Root Port: The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.

Regional Root: The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (This parameter only applies to the CIST instance.)

Internal Root Cost: The Regional Root Path Cost. For the Regional Root Bridge the cost is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (This parameter only applies to the CIST instance.)

Topology Flag: The current state of the Topology Change Notification flag for this bridge instance.

Topology Change Last: The time since this spanning tree was last configured.

CIST Ports & Aggregations State

Port: Display the port number.

Port ID: The port identifier used by the RSTP protocol. This port ID contains the priority and the port number.

Role: The role assigned by Spanning Tree Algorithm. Roles can be "Designated Port", "Backup Port", "Root Port".

State: Display the current state of a port.

Blocking: Ports only receive BPDU messages but do not forward them.

Learning: Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses

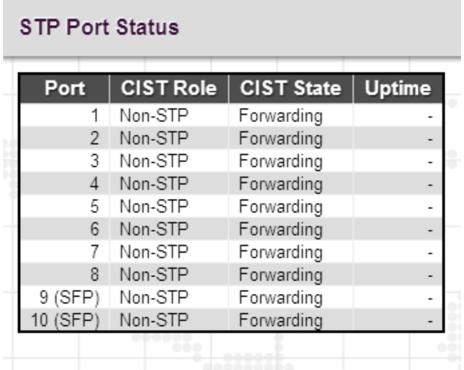
Forwarding: Ports forward packets and continue to learn addresses.

Edge: Display whether this port is an edge port or not.

Point-to-Point: Display whether this point is in point-to-point connection or not. This can be both automatically and manually configured.

Uptime: The time since the bridge port was last initialized.

4.12.7. Port Status



STP Port Status

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9 (SFP)	Non-STP	Forwarding	-
10 (SFP)	Non-STP	Forwarding	-

Port: The port number.

CIST Role: The role assigned by Spanning Tree Algorithm. Roles can be “Designated Port”, “Backup Port”, “Root Port” or “Non-STP”.

CIST State: Display the current state of a port. The CIST state must be one of the following:

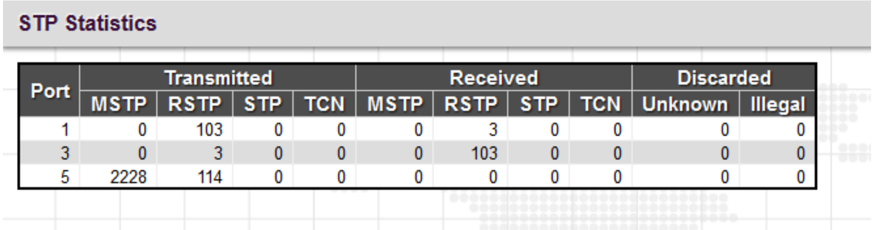
Discarding: Ports only receive BPDU messages but do not forward them.

Learning: Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses

Forwarding: Ports forward packets and continue to learn addresses.

Uptime: The time since the bridge port was last initialized.

4.12.8. Port Statistics



STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	0	103	0	0	0	3	0	0	0	0
3	0	3	0	0	0	103	0	0	0	0
5	2228	114	0	0	0	0	0	0	0	0

Port: Display the port number.

Transmitted & Received MSTP/RSTP/STP: The number of MSTP/RSTP/STP configuration BPDU messages transmitted and received on a port.

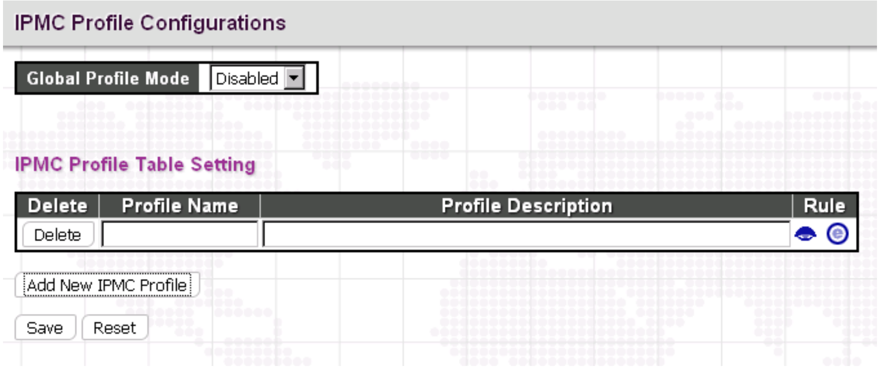
Transmitted & Received TCN: The number of TCN messages transmitted and received on a port.

Discarded Unknown/Illegal: The number of unknown and illegal packets discarded on a port.

4.13. IP Multicast

4.13.1. IPMC Profile

4.13.1.1. Profile Table



IPMC Profile Configurations

Global Profile Mode	Disabled

IPMC Profile Table Setting

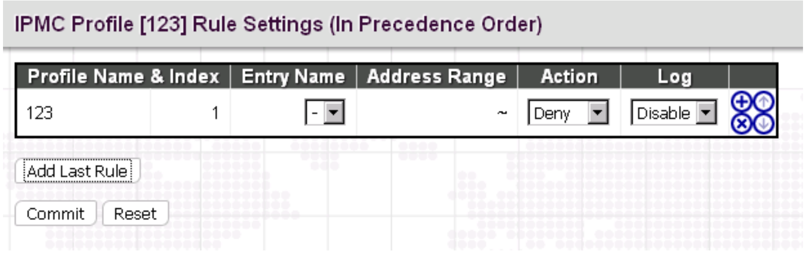
Delete	Profile Name	Profile Description	Rule
Delete			

Global Profile Mode: Enable or Disable the Global IPMC Profile. System starts to do filtering based on profile settings only when the global profile mode is enabled.

<u>IPMC Profile Table Setting</u>

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.



IPMC Profile [123] Rule Settings (In Precedence Order)

Profile Name & Index		Entry Name	Address Range	Action	Log	
123	1	-	~	Deny	Disable	

Profile Name: The name of the designated profile to be associated. This field is not editable.

Entry Name: The name used in specifying the address range used for this rule. Only the existing profile address entries will be chosen in the selected box. This field is not allowed to be selected as none ("-") while the Rule Settings Table is committed.

Address Range: The corresponding address range of the selected profile entry. This field is not editable and will be adjusted automatically according to the selected profile entry.

Action: Indicates the learning action upon receiving the Join/Report frame that has the group address matches the address range of the rule.

Permit: Group address matches the range specified in the rule will be learned.

Deny: Group address matches the range specified in the rule will be dropped.

Log: Indicates the logging preference upon receiving the Join/Report frame that has the group address matches the address range of the rule.

Enable: Corresponding information of the group address, that matches the range specified in the rule, will be logged.

Disable: Corresponding information of the group address, that matches the range specified in the rule, will not be logged.

Rule Management Buttons: You can manage rules and the corresponding precedence order by using the following buttons:

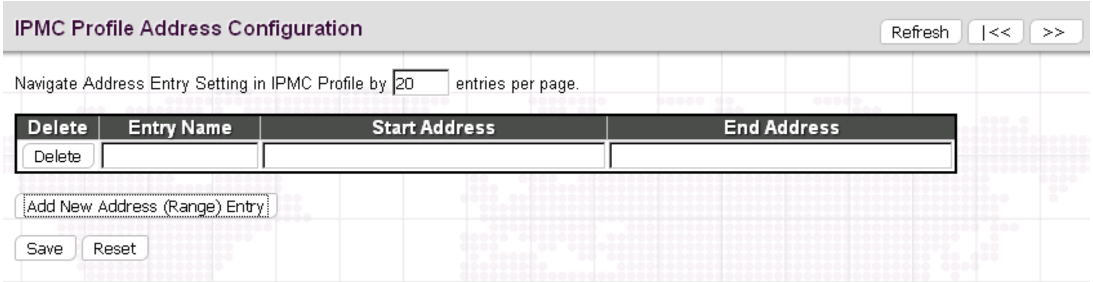
⊕: Insert a new rule before the current entry of rule.

⊗: Delete the current entry of rule.

↑: Moves the current entry of rule up in the list.

↓: Moves the current entry of rule down in the list.

4.13.1.2. Address Entry



IPMC Profile Address Configuration

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

Delete	Entry Name	Start Address	End Address
Delete			

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.

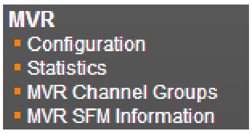
End Address: The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

4.13.2. MVR

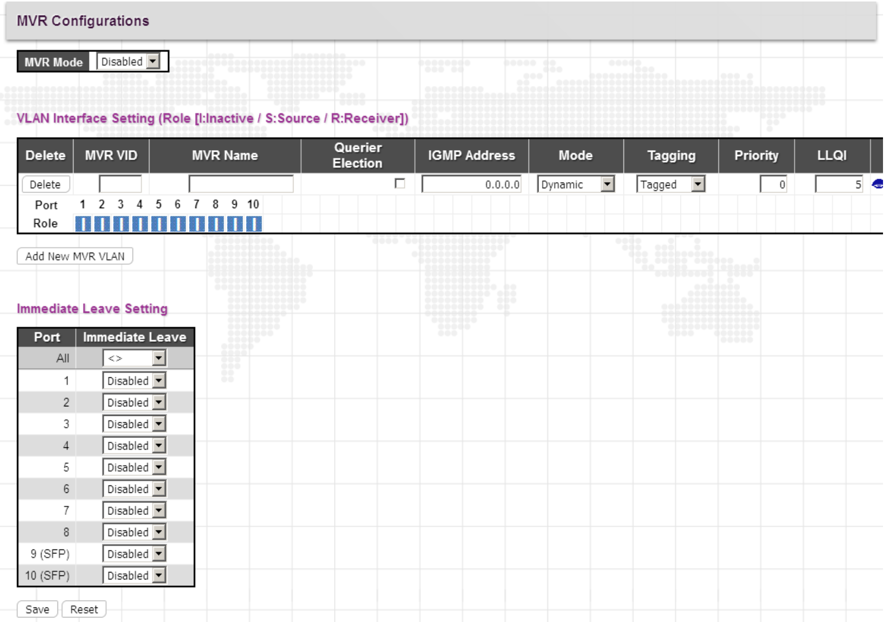
Multicast VLAN Registration protocol (MVR) allows a media server to transmit multicast stream in a single multicast VLAN when clients receiving multicast VLAN stream can reside in different VLANs. Clients in different VLANs intend to join or leave the multicast group simply by sending the IGMP Join or Leave message to a receiver port. The receiver port that belongs to one of the multicast groups can receive multicast stream from the media server.

MVR further isolates users who are not intended to receive multicast traffic and hence provide data security by VLAN segregation that allows only multicast traffic into other VLANs to which the subscribers belong. Even though common multicast streams are passed onto different VLAN groups from the MVR VLAN, users in different IEEE 802.1Q or private VLANs cannot exchange any information (except through upper-level routing services).

The “MVR” menu contains the following sub menus.



4.13.2.1. Configuration


MVR Configurations

MVR Mode: Disabled

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete	MVR VID	MVR Name	Querier Election	IGMP Address	Mode	Tagging	Priority	LLQI
Delete			□	0.0.0.0	Dynamic	Tagged	0	5

Port	1	2	3	4	5	6	7	8	9	10
Role	I	I	I	I	I	I	I	I	I	I

Add New MVR VLAN

Immediate Leave Setting

Port	Immediate Leave
All	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9 (SFP)	Disabled
10 (SFP)	Disabled

Save Reset

MVR Configurations

MVR Mode: Enable or disable MVR feature globally on this device. Any multicast data from source ports will be sent to associated receiver ports registered in the table. By default, MVR feature is turned off.

VLAN Interface Setting

MVR ID: Specify multicast VLAN ID. Please note that MVR source ports are not recommended to be used as management VLAN ports. MVR source ports should be configured as members of the MVR VLAN, but MVR receiver ports should not be manually configured as members of this VLAN.

MVR Name: Optionally specify a user-defined name for this multicast VLAN. The maximum length of the MVR name string is 32. Both alphabets and numbers are allowed for use.

Mode: Two MVR operation modes are provided.

Dynamic: MVR allows dynamic MVR membership reports on source ports. (This is the default mode.)

Compatible: MVR membership reports are forbidden on source ports.

Tagging: Specify whether IGMP/MLD control frames will be sent tagged with MVR VID or untagged.

Priority: Specify the priority for transmitting IGMP/MLD control frames. By default, priority is set to 0. Allowed priority values is 0~7.

LLQI: LLQI stands for Last Listener Query Interval and is to configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. By default, LLQI is set to 5 tenths of a second (0.5 second). The allowed range is 0~31744 tenths of a second.

Interface Channel Profile: Click the “Save” button before editing its Interface Channel Profile. Once “Save” is clicked, you are allowed to edit MVR channels of the selected IPMC profile settings by clicking the ✎ button.

Port Role: Click the Port Role symbol to change the role status.

Inactive (I): By default, all ports are set to inactive. Inactive ports do not participate in MVR operations.

Source (S): Set a port (uplink ports) to source port. Source ports will receive and send multicast data. Subscribers can not directly be connected to source ports. Please also note that source ports cannot be management ports at the same time.

Receiver (R): Set a port to receiver port. Client or subscriber ports are configured to receiver ports so that they can issue IGMP/MLD messages to receive multicast data.

Immediate Leave Setting

Port: The port number.

Immediate Leave: Enable for disable immediate leave function. When enabled, the device immediately removes a port from a multicast stream as soon as it receives leave message for that group. This option only applies to an interface configured as MVR receivers.

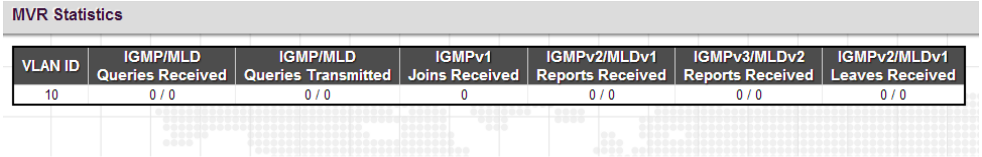
Click the "Add New MVR VLAN" button to insert a new entry to the list.

Click the "Delete" button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the "Save" button to save settings or changes.

Click the "Reset" button to restore changed settings to the default settings.

4.13.2.2. Statistics



MVR Statistics

VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
10	0 / 0	0 / 0	0	0 / 0	0 / 0	0 / 0

This page displays MVR statistics information on queries, joins, reports and leaves messages.

VLAN ID: Display VLAN ID that is used for processing multicast traffic.

IGMP/MLD Queries Received: The number of received queries for IGMP and MLD.

IGMP/MLD Queries Transmitted: The number of transmitted queries for IGMP/MLD.

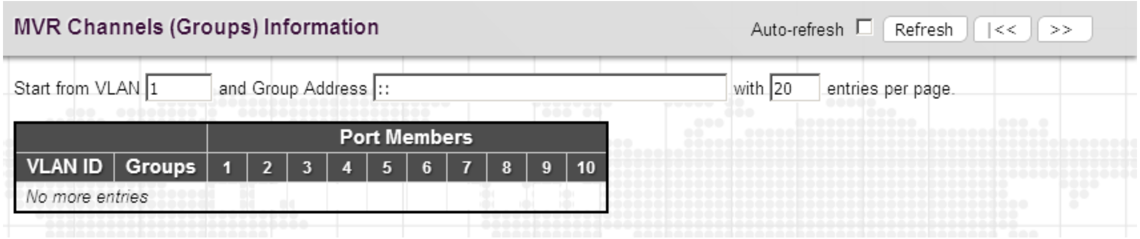
IGMPv1 Joins Received: The number of IGMPv1 received joins

IGMPv2/MLDv1 Reports Received: The number of IGMPv2 and MLDv1 received reports.

IGMPv3/MLDv2 Reports Received: The number of IGMPv3 and MLDv2 received reports.

IGMPv2/MLDv1 Leaves Received: The number of IGMPv2 and MLDv1 received leaves.

4.13.2.3. MVR Channel Groups



MVR Channels (Groups) Information

Auto-refresh □ Refresh |<< >>

Start from VLAN 1 and Group Address :: with 20 entries per page.

		Port Members									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10
No more entries											

Start from VLAN ____ and Group Address _______ with 20 entries per page.

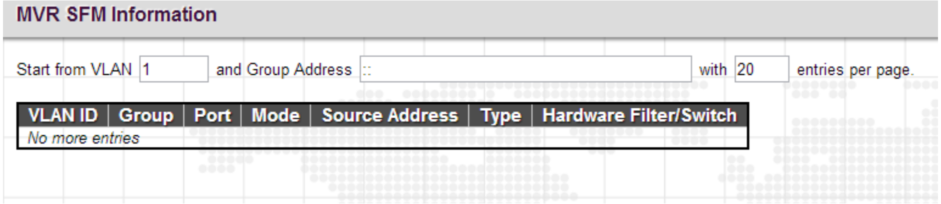
This table displays MVR channels (groups) information and is sorted by VLAN ID.

VLAN ID: VLAN ID of the group.

Groups: Group ID

Port Members: Ports that belong to this group.

4.13.2.4. MVR SFM Information



MVR SFM Information

Start from VLAN 1 and Group Address :: with 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

VLAN ID: VLAN ID of the group.

Group: The group address.

Port: Switch port number.

Mode: Indicate the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address: The source IP Address. Currently, the system limits the total number of source IP addresses for filtering to be 128. When there is no source filtering address, "None" is shown in the Source Address field.

Type: Indicate the Type. It can be either Allow or Deny.

Hardware Filter/Switch: Indicate whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

4.13.3. IPMC

The "IPMC" menu includes IGMP Snooping and MLD Snooping sub menu. Select the appropriate menu to set up detailed configurations.

4.13.3.1. IGMP Snooping

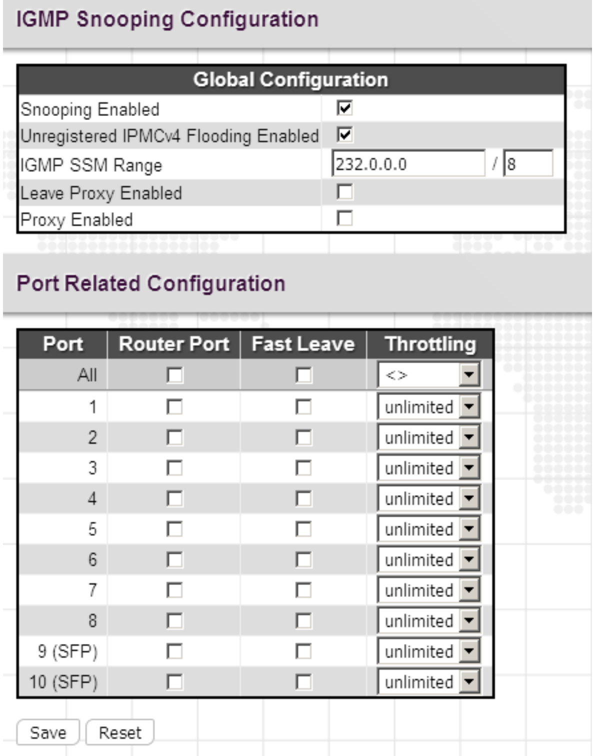
The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It can be used more efficiently when supporting activities, such as, online streaming video and gaming.

IGMP Snooping is the process of listening to IGMP traffic. IGMP snooping, as implied by the name, is a feature that allows the switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer 3 packets that IGMP packets sent in a multicast network.

When IGMP snooping is enabled in a switch, it analyses all the IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch receives an IGMP report for a given multicast group from a host, the switch adds the host's port number to the multicast list for that group. When the switch hears an IGMP Leave, it removes the host's port from the table entry.

IGMP snooping can reduce multicast traffic from streaming and other bandwidth intensive IP applications more effectively. A switch using IGMP snooping will only forward multicast traffic to the hosts in that traffic. This reduction of multicast traffic reduces the packet processing at the switch (at the cost of needing additional memory to handle the multicast tables) and also decreases the workload at the end hosts since their network cards (or operating system) will not receive and filter all the multicast traffic generated in the network.

4.13.3.1.1. Basic Configuration



IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	☑
Unregistered IPMCv4 Flooding Enabled	☑
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	□
Proxy Enabled	□

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
All	□	□	<>
1	□	□	unlimited
2	□	□	unlimited
3	□	□	unlimited
4	□	□	unlimited
5	□	□	unlimited
6	□	□	unlimited
7	□	□	unlimited
8	□	□	unlimited
9 (SFP)	□	□	unlimited
10 (SFP)	□	□	unlimited

IGMP Snooping Configuration: Global Configuration

Snooping Enabled: Select the checkbox to globally enable IGMP Snooping feature. When enabled, this device will monitor network traffic and determine which hosts will receive multicast traffic. The switch can passively monitor or snoop on IGMP Query and Report packets transferred between IP multicast routers and IP multicast service subscribers to identify the multicast group members. The switch simply monitors the IGMP packets passing through it, picks out the group registration information and configures the multicast filters accordingly.

Unregistered IPMCv4 Flooding Enabled: Set forwarding mode for unregistered (not-joined) IP multicast traffic. Select the checkbox to flood traffic.

IGMP 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 Enabled: Suppresses leave messages unless received from the last member port in the group. IGMP leave proxy suppresses all unnecessary IGMP leave messages so that a non-querier switch forwards an IGMP leave packet only when the last dynamic member port leaves a multicast group.

Proxy Enabled: When enabled, the switch performs like "IGMP Snooping with Proxy Reporting" (as defined in DSL Forum TR-101, April 2006).

Port Related Configuration

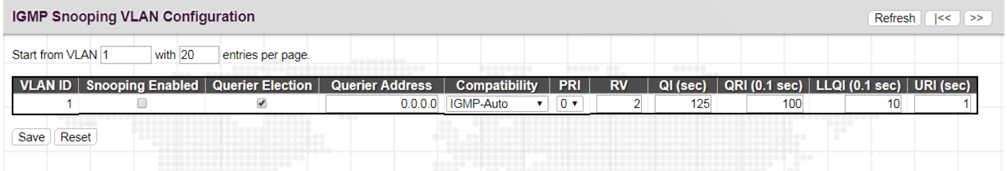
Port: The port number. “All” rules apply to all ports.

Router Port: Select the checkbox on a given port to assign it as a router port. If IGMP snooping cannot locate the IGMP querier, you can manually designate a port which is connected to a known IGMP querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Fast Leave: Enable fast leave function if the checkbox is ticked. When a leave packet is received, the switch immediately removes it from a multicast service without sending an IGMP group-specific (GS) query to that interface.

Throttling: This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new IGMP join reports will be dropped. By default, unlimited is selected. Other allowed options are 1~10

4.13.3.1.2. VLAN Configuration



IGMP Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	□	☑	0.0.0.0	IGMP-Auto ▾	0 ▾	2	125	100	10	1

This page is used to configure IGMP Snooping for an interface.

VLAN ID: Specify VLAN ID for IGMP snooping.

Snooping Enabled: Select the checkbox to enable snooping feature on an interface basis. When enabled, the switch will monitor network traffic on the specified interface to determine which hosts want to receive multicast services. If IGMP snooping is enabled globally and an interface’s IGMP snooping is enabled on an interface, IGMP snooping on an interface will take precedence. When disabled, snooping can still be configured on an interface. However, settings will only take effect until IGMP snooping is enabled globally.

Querier Election: Enable to join querier election in the VLAN. When disabled, it will act as an IGMP non-querier.

Querier Address: Specify the IPv4 source address used in IP header for IGMP querier election. When the field is not specified, the switch uses the first available IPv4 management address of the IP interface associated with this VLAN.

Compatibility: This configures how hosts and routers take actions within a network depending on IGMP version selected. Available options are “IGMP-Auto”, “Forced IGMPv1”, “Forced IGMPv2”, “Forced IGMPv3”. By default, IGMP-Auto is used.

PRI: Select the priority of interface. It indicates the IGMP control priority level generated by the system. These values can be used to prioritize classes of traffic.

RV: The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2.

QI (sec): The Query Interval is the interval between IGMP General Query messages sent by the Querier. The default Querier Interval is 125 seconds.

QRI: The Query Response Interval is the maximum amount of time that the IGMP router waits to receive a response to a General Query message. The QRI applies when the switch is acting as the querier and is used to inform other devices of the maximum time this system waits for a response to general queries. By default, RQI is set to 10 seconds. The allowed range is 10~31744 tenths of a second.

LLQI: The Last Listener Query Interval sets the interval that waits for a response to a group-specific or group-and-source specific query message.

URI: The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. By default, URI is set to 1 second. The allowed range for URI is 0~31744 seconds.

Click the “Add New IGMP VLAN” button to add a new entry.

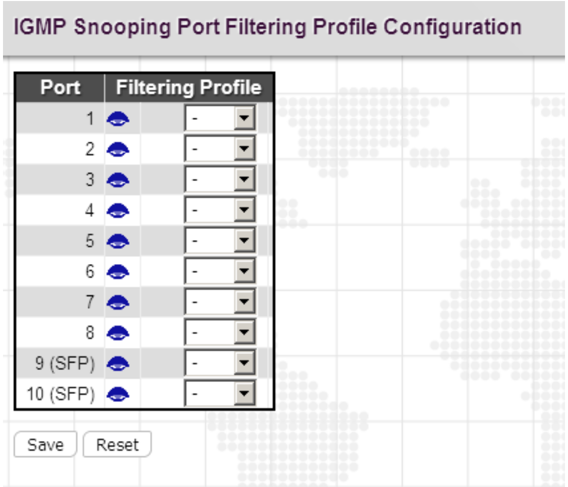
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.13.3.1.3. Port Group Filtering

The Port Filtering Configuration page is to filter specific multicast traffic on a per port basis. Before you select a filtering profile for filtering purposes, you must set up profiles in IPMC Profile page.



IGMP Snooping Port Filtering Profile Configuration

Port	Filtering Profile
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9 (SFP)	-
10 (SFP)	-

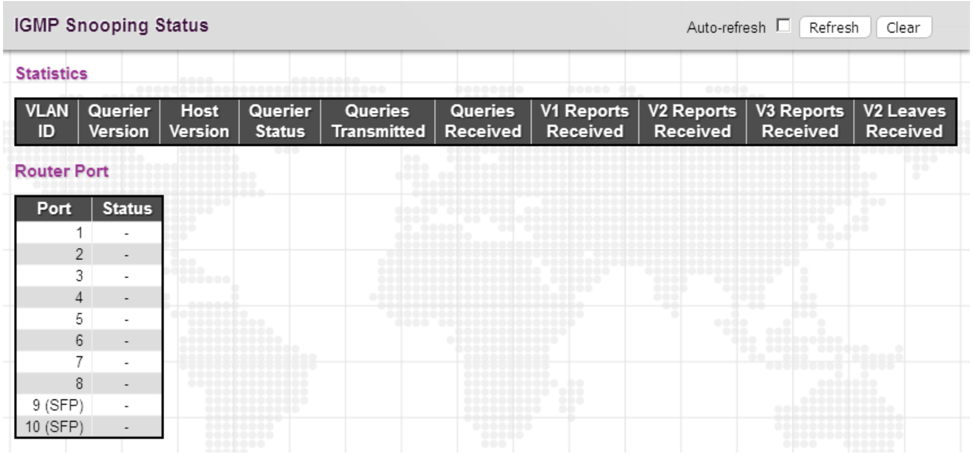
Port: The port number.

Filtering Profile: Enter multicast group address for filtering on a port. When a certain multicast group is specified on a port, IGMP join reports received on a port will be dropped.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.13.3.1.4. Status



IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9 (SFP)	-
10 (SFP)	-

Statistics

VLAN ID: The VLAN ID of this entry.

Querier Version: The current working Querier version.

Host Version: The current host version.

Querier Status: Show the Querier status that is either "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted: The number of queries transmitted.

Queries Received: The number of queries received.

V1 Reports Received: The number of Received V1 Reports.

V2 Reports Received: The number of Received V2 Reports.

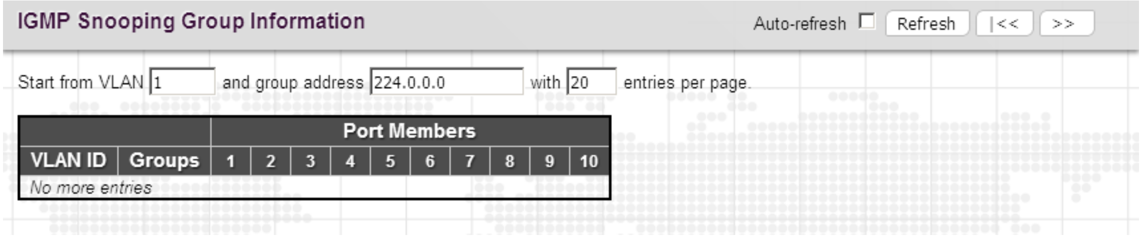
V2 Leaves Received: The number of Received V2 Leaves.

Router Port

Port: The port number.

Status: Indicate whether a specific port is a router port or not.

4.13.3.1.5. Groups Information



IGMP Snooping Group Information

Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page.

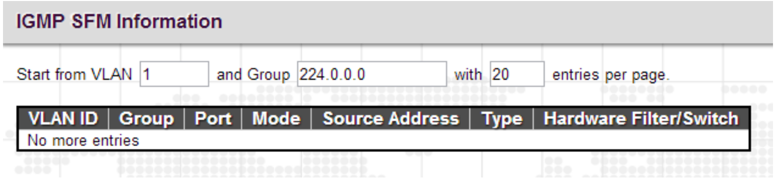
		Port Members									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10
No more entries											

VLAN ID: Display the VLAN ID of the group.

Groups: Display the group address.

Port Members: Ports that belong to this group.

4.13.3.1.6. IPv4 SFM Information



IGMP SFM Information

Start from VLAN 1 and Group 224.0.0.0 with 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

VLAN ID: Display the VLAN ID of the group.

Groups: Display the IP address of a multicast group.

Port: The switch port number.

Mode: The filtering mode maintained per VLAN ID, port number and group address.

Source Address: The source IP address available for filtering.

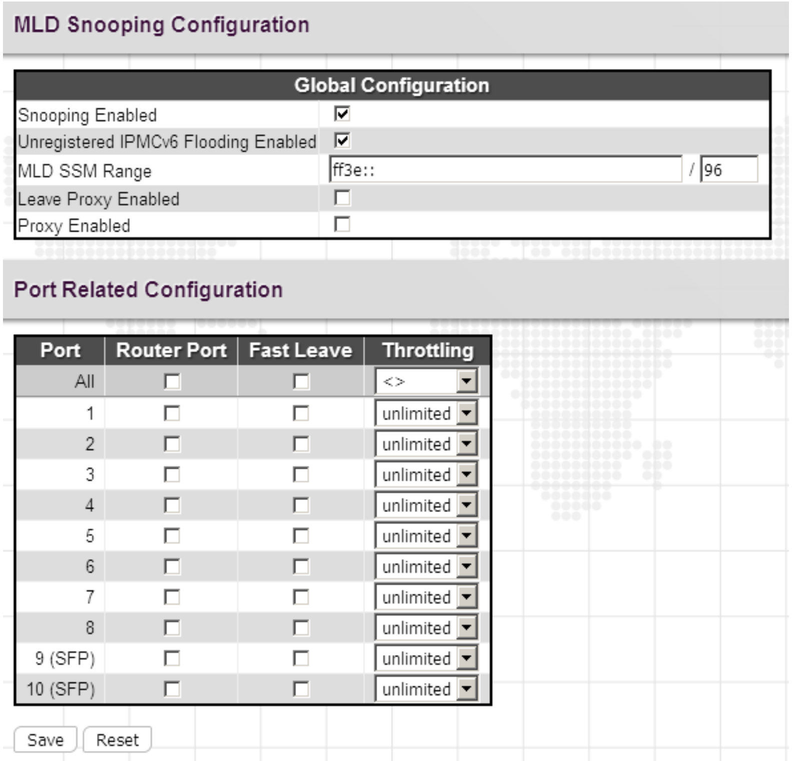
Type: Display either Allow or Deny type.

Hardware Filter/Switch: Indicates whether the data plane destined to the specific group address from the source IPv4 address can be handled by the chip or not.

4.13.3.2. MLD Snooping

Multicast Listener Discovery (MLD) snooping, similar to IGMP snooping for IPv4, operates on IPv6 for multicast traffic. In other words, MLD snooping configures ports to limit or control IPv6 multicast traffic so that multicast traffic is forwarded to ports (or users) who want to receive it. In this way, MLD snooping can reduce the flooding of IPV6 multicast packets in the specified VLANs. Please note that IGMP Snooping and MLD Snooping are independent of each other. They can both be enabled and function at the same time.

4.13.3.2.1. 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
All	□	□	<>
1	□	□	unlimited
2	□	□	unlimited
3	□	□	unlimited
4	□	□	unlimited
5	□	□	unlimited
6	□	□	unlimited
7	□	□	unlimited
8	□	□	unlimited
9 (SFP)	□	□	unlimited
10 (SFP)	□	□	unlimited

<u>Global Configuration</u>

Snooping Enabled: Select the checkbox to globally enable MLD Snooping feature. When enabled, this device will monitor network traffic and determine which hosts would like to receive multicast traffic. The switch can passively monitor or snoop on MLD Listener Query and Report packets transferred between IP multicast routers and IP multicast service subscribers to identify the multicast group members. The switch simply monitors the IGMP packets passing through it, picks out the group registration information and configures the multicast filters accordingly.

Unregistered IPMCv6 Flooding Enabled: Set forwarding mode for unregistered (not-joined) IP multicast traffic. Select the checkbox to flood traffic.

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 Enabled: To prevent multicast router from becoming overloaded with leave messages, MLD snooping suppresses leave messages unless received from the last member port in the group. When the switch acts as the querier, the leave proxy feature will not function.

Proxy Enabled: When MLD proxy is enabled, the switch exchanges MLD messages with the router on its upstream interface, and performs the host portion of the MLD task on the upstream interface as follows:

- When queried, it sends multicast listener reports to the group.
- When a host joins a multicast group to which no other host belongs, it sends unsolicited multicast listener reports to that group.
- When the last host in a particular multicast group leaves, it sends an unsolicited multicast listener done report to the all-routers address (FF02::2) for MLDv1.

<u>Port Related Configuration</u>

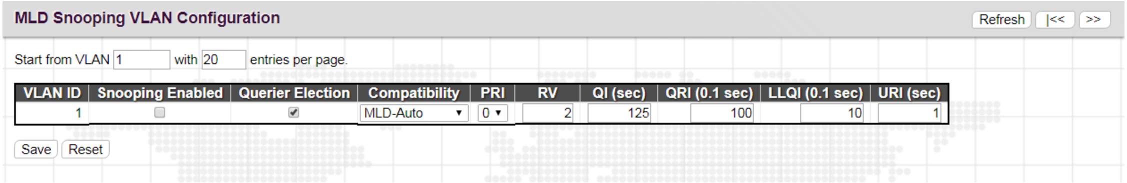
Port: List each port number. "All" rules apply to all ports.

Router Port: Select the checkbox on a given port to assign it as a router port. If MLD snooping cannot locate the MLD querier, you can manually designate a port which is connected to a known MLD querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Fast Leave: Enable fast leave function if the checkbox is ticked. When a leave packet is received, the switch immediately removes it from a multicast service without sending a MLD group-specific (GS) query to that interface.

Throttling: This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new MLD join reports will be dropped. By default, unlimited is selected. Other allowed options are 1~10.

4.13.3.2.2. VLAN Configuration



MLD Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

VLAN ID	Snooping Enabled	Querier Election	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	☐	☑	MLD-Auto	0	2	125	100	10	1

This page is used to configure MLD Snooping for an interface.

VLAN ID: Specify VLAN ID for MLD snooping.

Snooping Enabled: Select the checkbox to enable snooping feature on an interface basis. When enabled, the switch will monitor network traffic on the specified interface to determine which hosts want to receive multicast services.

MLD Querier: Enable to join querier election in the VLAN. When enabled, the switch can serve as the MLDv2 querier in the bidding process with other competing multicast routers or switches. Once it becomes querier, it will be responsible for asking hosts periodically if they want to receive multicast traffic. When disabled, it will act as an IGMP non-querier.

Compatibility: This configures how hosts and routers take actions within a network depending on MLD version selected. Available options are “MLD-Auto”, “Forced MLDv1”and “Forced MLDv2”. By default, MLD-Auto is used.

PRI: Select the priority of interface. It indicates the IGMP control priority level generated by the system. These values can be used to prioritize classes of traffic.

RV: The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2. The allowed range is 1~255.

QI (sec): The Query Interval is the interval between IGMP General Query messages sent by the Querier. The default Querier Interval is 125 seconds. The allowed interval range is 1~255 seconds.

QRI: The Query Response Interval is the maximum amount of time that the IGMP router waits to receive a response to a General Query message. The QRI applies when the switch is acting as the querier and is used to inform other devices of the maximum time this system waits for a response to general queries. By default, RQI is set to 10 seconds. The allowed range is 10~31744 tenths of a second.

LLQI: The Last Listener Query Interval sets the interval that waits for a response to a group-specific or group-and-source specific query message.

URI: The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. By default, URI is set to 1 second. The allowed range for URI is 0~31744 seconds.

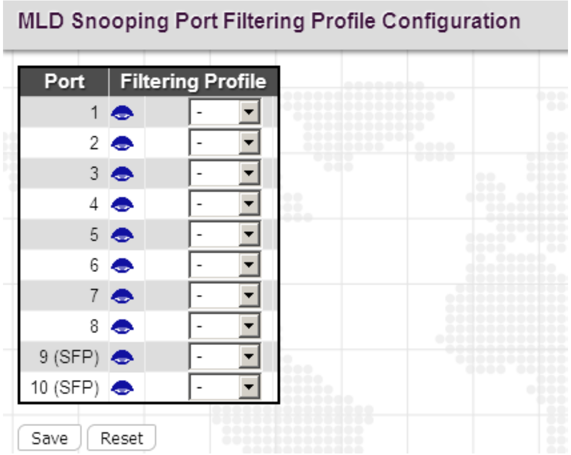
Click the "Add New MLD VLAN" button to add a new entry.

Click the "Delete" button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the "Save" button to save settings or changes.

Click the "Reset" button to restore changed settings to the default settings.

4.13.3.2.3. Port Group Filtering



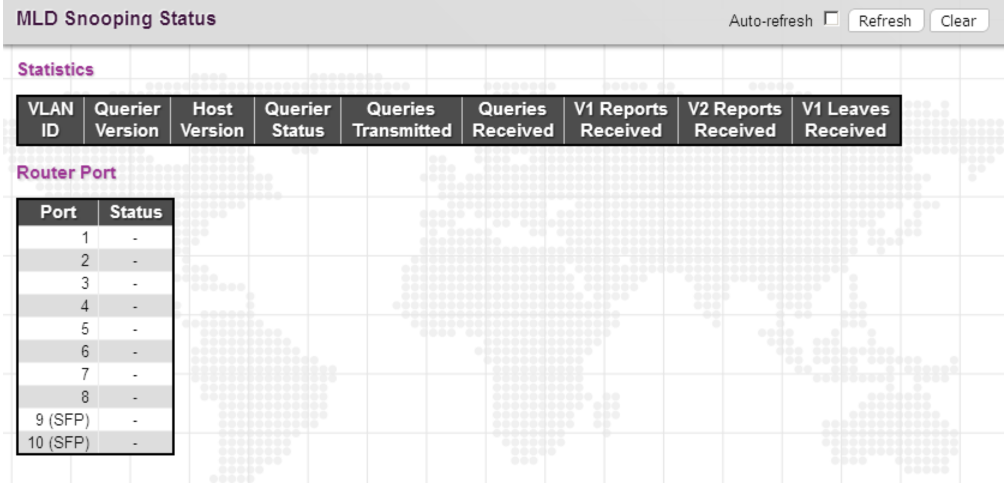
MLD Snooping Port Filtering Profile Configuration

Port	Filtering Profile
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9 (SFP)	-
10 (SFP)	-

Port: Select a port number to be used for this rule.

Filtering Profile: Enter multicast group address for filtering on a port. When a certain multicast group is specified on a port, MLD join reports received on a port will be dropped.

4.13.3.2.4. Status



MLD Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9 (SFP)	-
10 (SFP)	-

<u>Statistics</u>

VLAN ID: The VLAN ID of this entry.

Querier Version: The current working Querier version.

Host Version: The current host version.

Querier Status: Show the Querier status that is either "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted: The number of queries transmitted.

Queries Received: The number of queries received.

V1 Reports Received: The number of Received V1 Reports.

V2 Reports Received: The number of Received V2 Reports.

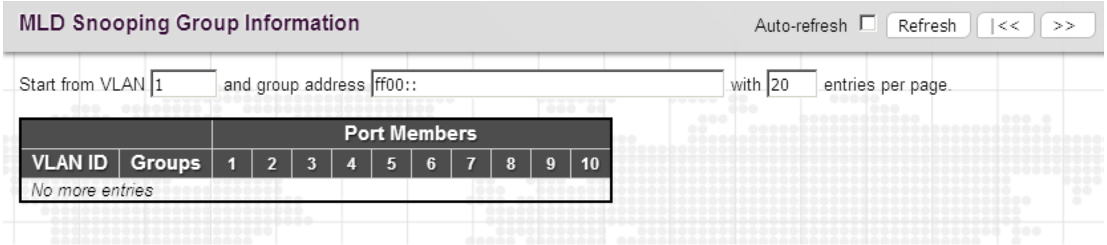
V1 Leaves Received: The number of Received V1 Leaves.

<u>Router Port</u>

Port: The port number.

Status: Indicate whether a specific port is a router port or not.

4.13.3.2.5. Groups Information



MLD Snooping Group Information

Start from VLAN 1 and group address ff00:: with 20 entries per page.

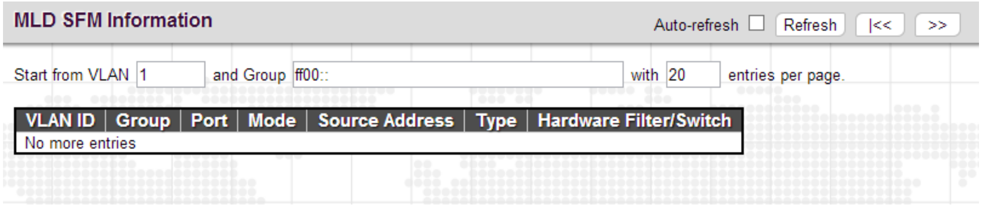
		Port Members									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10
No more entries											

VLAN ID: Display the VLAN ID of the group.

Groups: Display the group address.

Port Members: Ports that belong to this group.

4.13.3.2.6. IPv6 SFM Information



MLD SFM Information

Start from VLAN 1 and Group ff00:: with 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

VLAN ID: Display the VLAN ID of the group.

Group: Display the IP address of a multicast group.

Port: The switch port number.

Mode: The filtering mode maintained per VLAN ID, port number and group address.

Source Address: The source IP address available for filtering.

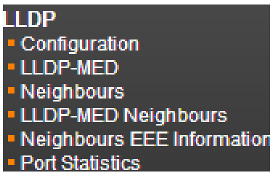
Type: Display either Allow or Deny type.

Hardware Filter/Switch: Indicates whether the data plane destined to the specific group address from the source IPv4 address can be handled by the chip or not.

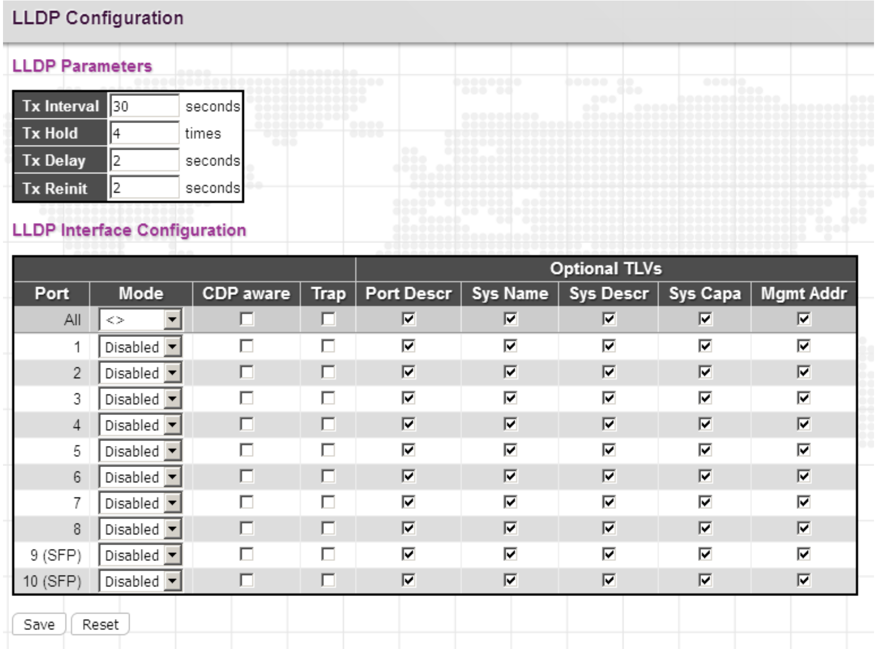
4.14. LLDP

LLDP (Link Layer Discovery Protocol) runs over data link layer which is used for network devices to send information about themselves to other directly connected devices on the network. By using LLDP, two devices running different network layer protocols can learn information about each other. A set of attributes referred to TLVs are used to discover neighbor devices. Details such as port description, system name, system description, system capabilities, and management address can be sent and received on this device.

The "LLDP" menu contains the following sub menus. Select the appropriate menu to set up detailed configurations.



4.14.1. Configuration



LLDP Configuration

LLDP Parameters

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

LLDP Interface Configuration

				Optional TLVs				
Port	Mode	CDP aware	Trap	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
All	<>	□	□	☑	☑	☑	☑	☑
1	Disabled	□	□	☑	☑	☑	☑	☑
2	Disabled	□	□	☑	☑	☑	☑	☑
3	Disabled	□	□	☑	☑	☑	☑	☑
4	Disabled	□	□	☑	☑	☑	☑	☑
5	Disabled	□	□	☑	☑	☑	☑	☑
6	Disabled	□	□	☑	☑	☑	☑	☑
7	Disabled	□	□	☑	☑	☑	☑	☑
8	Disabled	□	□	☑	☑	☑	☑	☑
9 (SFP)	Disabled	□	□	☑	☑	☑	☑	☑
10 (SFP)	Disabled	□	□	☑	☑	☑	☑	☑

LLDP Parameters

Tx Interval: Specify the interval between LLDP frames are sent to its neighbours for updated discovery information. The valid values are 5~32768 seconds. The default is 30 seconds.

Tx Hold: This setting defines how long LLDP frames are considered valid and is used to compute the TTL. Valid range is 2~10 times. The default is 4.

Tx Delay: Specify a delay between the LLDP frames that contain changed configurations. Tx Delay cannot be larger than 1/4 of the Tx interval value. The valid values are 1 - 8192 seconds.

Tx Reinit: Specify a delay between the shutdown frame and a new LLDP initialization. The valid values are 1~10 seconds.

LLDP Port Configuration

Port: The port number. "All" settings apply to all ports.

Mode: Select the appropriate LLDP mode.

Disabled: LLDP information will not be sent and LLDP information received from neighbours will be dropped.

Enabled: LLDP information will be sent and LLDP information received from neighbours will be analyzed.

Rx Only: The switch will analyze LLDP information received from neighbours.

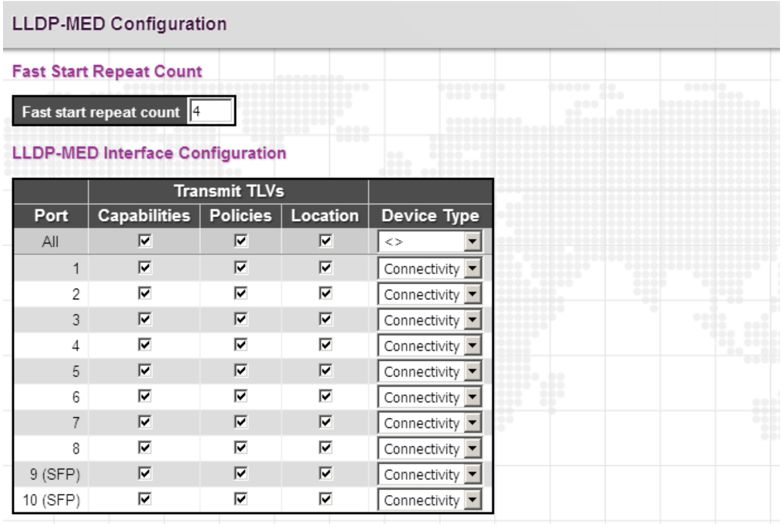
Tx Only: The switch will send out LLDP information but will drop LLDP information received from neighbours.

CDP Aware: CDP aware operation is used to decode incoming CDP (Cisco Discovery Protocol) frames. If enabled, CDP TLVs that can be mapped into a corresponding field in the LLDP neighbors table are decoded, all others are discarded. CDP TLVs are mapped into LLDP neighbors table as shown below:

Optional TLVs: LLDP uses several attributes to discover neighbour devices. These attributes contains type, length, and value descriptions and are referred to TLVs. Details such as port description, system name, system description, system capabilities, management address can be sent from this device. Uncheck the boxes if they are not appropriate to be known by other neighbour devices.

4.14.2. LLDP-MED

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices such as IP phones and network devices such as switches. It specifically provides support for voice over IP (VoIP) applications and provides additional TLVs for capabilities discovery, network policy, Power over Ethernet, inventory management and location information.



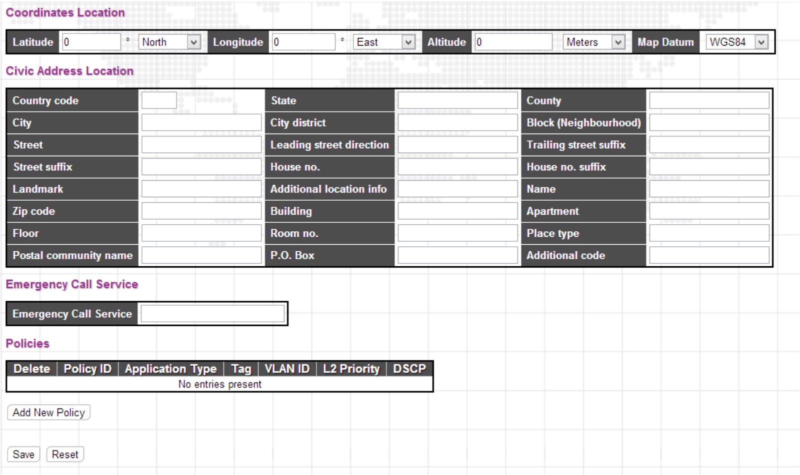
LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count	4

LLDP-MED Interface Configuration

	Transmit TLVs			
Port	Capabilities	Policies	Location	Device Type
All	☑	☑	☑	<>
1	☑	☑	☑	Connectivity
2	☑	☑	☑	Connectivity
3	☑	☑	☑	Connectivity
4	☑	☑	☑	Connectivity
5	☑	☑	☑	Connectivity
6	☑	☑	☑	Connectivity
7	☑	☑	☑	Connectivity
8	☑	☑	☑	Connectivity
9 (SFP)	☑	☑	☑	Connectivity
10 (SFP)	☑	☑	☑	Connectivity



Coordinates Location

Latitude	0 °	North	Longitude	0 °	East	Altitude	0	Meters	Map Datum WGS84

Civic Address Location

Country code		State		County	
City		City district		Block (Neighbourhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

Emergency Call Service

Emergency Call Service	

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No entries present						

Fast Start Repeat Count: Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy. With this in mind, LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. With Fast start repeat count it is possible to specify the number of times the fast start transmission is repeated. The recommended value is 4 times, giving that 4 LLDP frames with a 1 second interval will be transmitted, when a LLDP frame with new information is received. It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including between Network Connectivity Devices, or to other types of links.

Coordinates Location

Latitude: Latitude should be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.

Longitude: Longitude should be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

Altitude: Altitude should be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters).

> **Meters:** Representing meters of Altitude defined by the vertical datum specified.
>
> **Floors:** Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

Map Datum: The Map Datum is used for the coordinates given in these options:

> **WGS84:** (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.
>
> **NAD83/NAVD88:** North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; the associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).
>
> **NAD83/MLLW:** North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; the associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

Country Code: The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

State: National subdivisions (state, canton, region, province, prefecture).

County: County, parish, gun (Japan), district.

City: City, township, shi (Japan) - Example: Copenhagen.

City District: City division, borough, city district, ward, chou (Japan).

Block (Neighbourhood): Neighbourhood, block.

Street: Street - Example: Poppelvej.

Leading street direction: Example: N.

Trailing street suffix: Example: SW.

Street suffix: Example: Ave, Platz.

House no.: Example: 21.

House no. suffix: Example: A, 1/2.

Landmark: Landmark or vanity address - Example: Columbia University.

Additional location info: Example: South Wing.

Name: Name (residence and office occupant): Example: Flemming Jahn.

Zip code: Postal/zip code - Example: 2791.

Building: Building (structure). Example: Low Library.

Apartment: Unit (Apartment, suite). Example: Apt 42.

Floor: Example: 4.

Room no.: Room number - Example: 450F.

Place type: Example: Office.

Postal community name: Example: Leonia.

P.O. Box: Example: 12345.

Additional code: Example: 1320300003.

Emergency Call Service

Emergency Call Service: Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Policies

Policy ID: Specify the ID for this policy.

Application Type: The application types include "Voice", "Voice Signaling", "Guest Voice", "Guest Voice Signaling", "Softphone Voice", "Video Conferencing", "Streaming", "Video Signaling".

Tag: Tag indicating whether the specified application type is using a "tagged" or an "untagged" VLAN.

VLAN ID: Specify the VLAN ID for the port.

L2 Priority: Specify one of eight priority levels (0-7) as defined by 802.1D-2004.

DSCP: Specify one of 64 code point values (0-63) as defined in IETF RFC 2474.

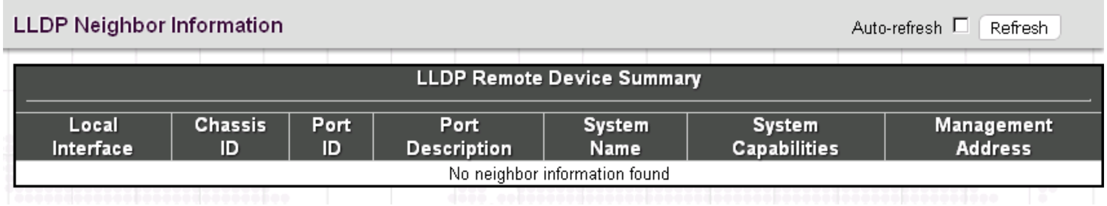
Click the "Add New Policy" button to insert a new policy to the list.

Click the "Delete" button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the "Save" button to save settings or changes.

Click the "Reset" button to restore changed settings to the default settings.

4.14.3. Neighbours



LLDP Neighbor Information

LLDP Remote Device Summary

Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
No neighbor information found						

Local Port: The local port that a remote LLDP-capable device is attached.

Chassis ID: An ID indicating the particular chassis in this system.

Port ID: A port ID is the identification of the neighbor port.

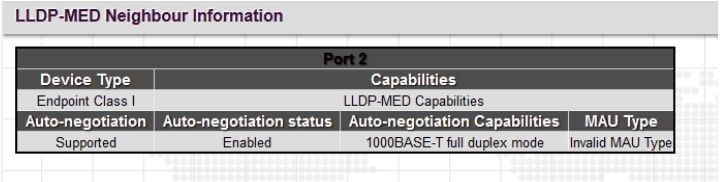
Port Description: A remote port's description.

System Name: The system name assigned to the remote system.

System Capabilities: This shows the neighbour unit's capabilities. When a capability is enabled, the capability is followed by (+). If disabled, the capability is followed by (-).

Management Address: The IPv4 address of the remote device. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. If the neighbor device allows management access, clicking on an entry in this field will re-direct the web browser to the neighbor's management interface.

4.14.4. LLDP-MED Neighbours

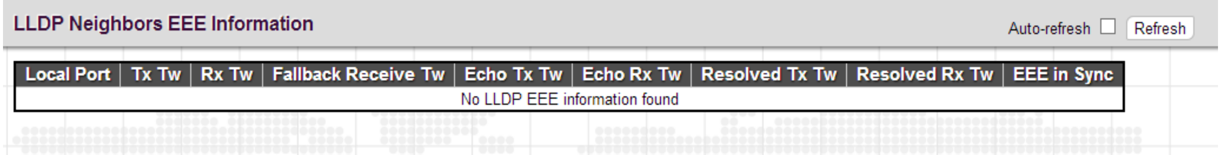


LLDP-MED Neighbour Information

Port 2			
Device Type	Capabilities		
Endpoint Class I	LLDP-MED Capabilities		
Auto-negotiation	Auto-negotiation status	Auto-negotiation Capabilities	MAU Type
Supported	Enabled	1000BASE-T full duplex mode	Invalid MAU Type

This page displays information about LLDP-MED neighbours detected on the network.

4.14.5. Neighbours EEE Information



LLDP Neighbors EEE Information

Auto-refresh □ Refresh

Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
No LLDP EEE information found								

Local Port: The port for this switch on which the LLDP frame was received.

Tx Tw: The link partner's maximum time that transmit path can hold-off sending data after de-assertion of LPI.

Rx Tw: The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.

Fallback Receive Tw: The link partner's fallback receive Tw.

Echo Tx Tw: The link partner's Echo Tx Tw value. The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.

Echo Rx Tw: The link partner's Echo Rx Tw value.

Resolved Tx Tw: The resolved Tx Tw for this link.

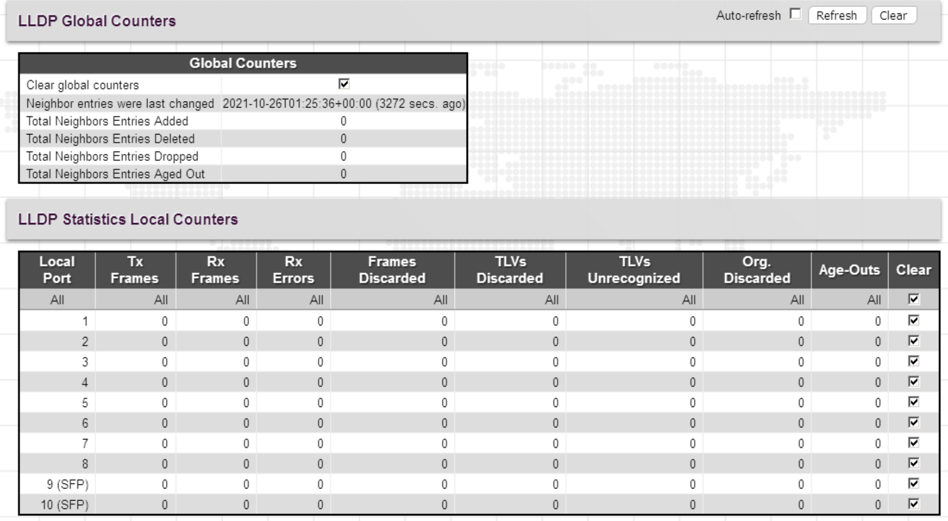
Resolved Rx Tw: The resolved Rx Tw for this link.

EEE in Sync: This shows whether the switch and the link partner have agreed on wake times.

Red: Switch and link partner have not agreed on wakeup times.

Green: Switch and link partner have agreed on wakeup times.

4.14.6. Port Statistics



LLDP Global Counters

Global Counters	
Clear global counters	☑
Neighbor entries were last changed	2021-10-26T01:25:36+00:00 (3272 secs. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	Clear
All	All	All	All	All	All	All	All	All	☑
1	0	0	0	0	0	0	0	0	☑
2	0	0	0	0	0	0	0	0	☑
3	0	0	0	0	0	0	0	0	☑
4	0	0	0	0	0	0	0	0	☑
5	0	0	0	0	0	0	0	0	☑
6	0	0	0	0	0	0	0	0	☑
7	0	0	0	0	0	0	0	0	☑
8	0	0	0	0	0	0	0	0	☑
9 (SFP)	0	0	0	0	0	0	0	0	☑
10 (SFP)	0	0	0	0	0	0	0	0	☑

<u>Global Counters</u>

Total Neighbours Entries Added: Shows the number of new entries added since the switch was rebooted, and for which the remote TTL has not yet expired.

Total Neighbors Entries Deleted: The number of LLDP neighbors which have been removed from the LLDP remote systems MIB for any reason.

Total Neighbors Entries Dropped: The number of times which the remote database on this switch dropped an LLDPDU because the entry table was full.

Total Neighbors Entries Aged Out: The number of times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

LLDP Statistics Local Counters

Local Port: The port number.

Tx Frames: The number of LLDP PDUs transmitted.

Rx Frames: The number of LLDP PDUs received.

Rx Errors: The number of received LLDP frames with some kind of error.

Frames Discarded: The number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular Type Length Value (TLV).

TLVs Discarded: Each LLDP frame can contain multiple pieces of information, known as TLVs. If a TLV is malformed, it is counted and discarded.

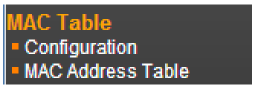
TLVs Unrecognized: The number of well-formed TLVs, but with an unknown type value.

Org. Discarded: The number of organizational TLVs discarded.

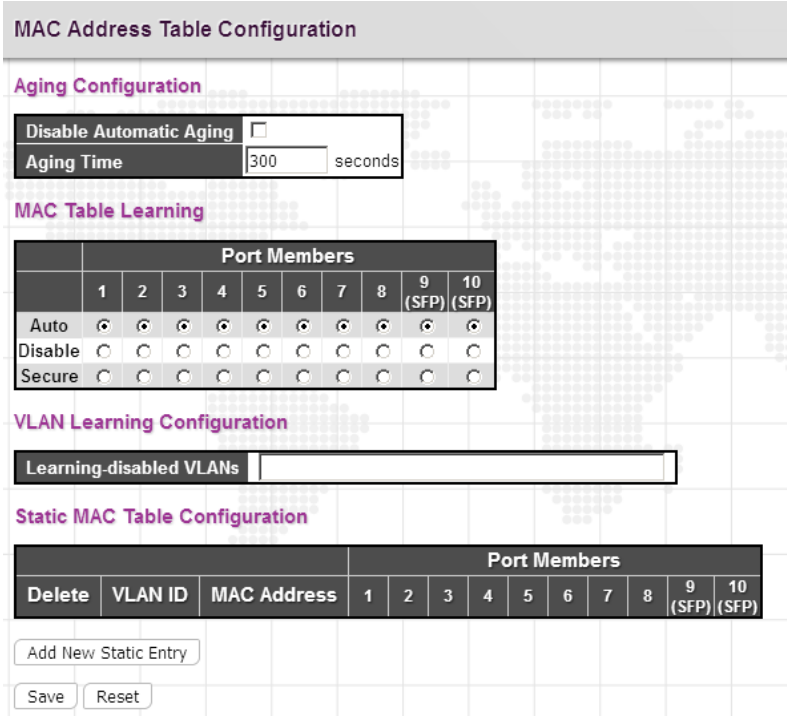
Age-Outs: Each LLDP frame contains information about how long the LLDP information is valid (age-out time). If no new LLDP frame is received within the age-out time, the LLDP information is removed, and the Age-Out counter is incremented.

4.15. MAC Table

The “MAC Table” menu contains configuration and status sub menu. Select the configuration page to set up detailed configuration



4.15.1. Configuration



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

MAC Table Learning

	Port Members									
	1	2	3	4	5	6	7	8	9 (SFP)	10 (SFP)
Auto	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○

VLAN Learning Configuration

Learning-disabled VLANs	

Static MAC Table Configuration

			Port Members									
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9 (SFP)	10 (SFP)

Disable Automatic Aging: Learned MAC addresses will appear in the table permanently.

Aging Time: Set up the aging time for a learned MAC to be appeared in MAC learning table. The allowed range is 10 to 1000000 seconds.

MAC Learning Table: Three options are available on each port.

Auto: On a given port, learning is automatically done once unknown SMAC is received.

Disable: Disable MAC learning function.

Secure: Only static MAC entries listed in “Static MAC Table Configuration” are learned. Others will be dropped.

***Note:** Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.*

Learning-disabled VLANs: This field shows the Learning-disabled VLANs. When a new MAC arrives into a learning-disabled VLAN, the MAC will not be learnt. By default, the field is empty. More VLANs can be created into the list.

Static MAC Table Configuration: This table is used to manually set up static MAC entries. The total entries that can be entered are 64.

VLAN ID: Specify the VLAN ID for this entry.

MAC Address: Specify the MAC address for this entry.

Port Members: Check or uncheck the ports. If the incoming packet has the same destination MAC address as the one specified in VID, it will be forwarded to the checked port directly.

Click the “Add New Static Entry” button to insert a new entry to the list.

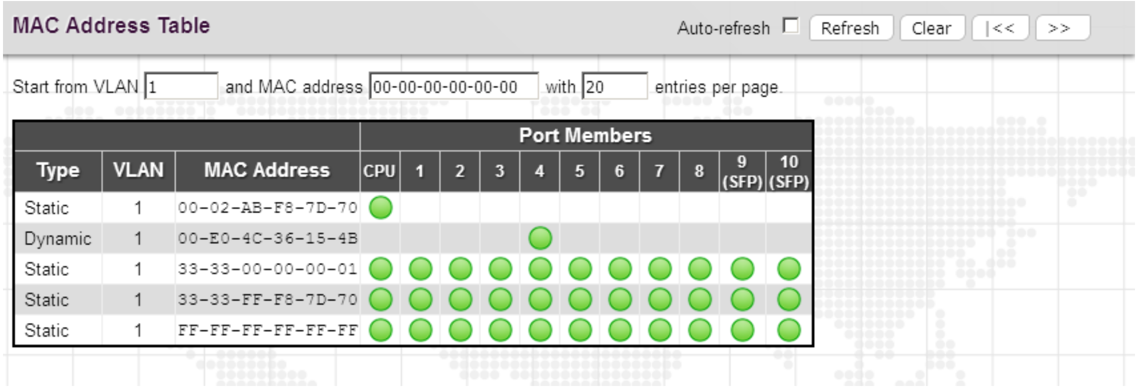
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.15.2. MAC Address Table

The MAC Address Table shows both static and dynamic MAC addresses learned from CPU or switch ports. You can enter the starting VLAN ID and MAC addresses to view the desired entries.



MAC Address Table

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

Type	VLAN	MAC Address	Port Members										
			CPU	1	2	3	4	5	6	7	8	9 (SFP)	10 (SFP)
Static	1	00-02-AB-F8-7D-70	●										
Dynamic	1	00-E0-4C-36-15-4B					●						
Static	1	33-33-00-00-00-01	●	●	●	●	●	●	●	●	●	●	●
Static	1	33-33-FF-F8-7D-70	●	●	●	●	●	●	●	●	●	●	●
Static	1	FF-FF-FF-FF-FF-FF	●	●	●	●	●	●	●	●	●	●	●

Type: Display whether the learned MAC address is static or dynamic.

VLAN ID: The VLAN ID associated with this entry.

MAC Address: The MAC address learned on CPU or certain ports.

Port Members: Ports associated with this entry.

4.16. VLANs

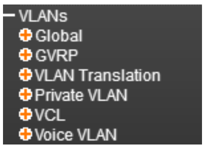
IEEE 802.1Q VLAN (Virtual Local Area Network) is a popular and cost-effective way to segment your networking deployment by logically grouping devices with similar attributes irrespective of their physical connections. VLANs also segment the network into different broadcast domains so that packets are forwarded to ports within the VLAN that they belong. Using VLANs provides the following main benefits:

VLANs provide extra security: Devices that frequently communicate with each other are grouped into the same VLAN. If devices in a VLAN want to communicate with devices in a different VLAN, the traffic must go through a routing device or Layer 3 switching device.

VLANs help control traffic: Traditionally, when networks are not segmented into VLANs, congestion can be easily caused by broadcast traffic that is directed to all devices. To minimize the possibility of broadcast traffic damaging the entire network, VLANs can help group devices that communicate frequently with other in the same VLAN so as to divide the entire network into several broadcast domains.

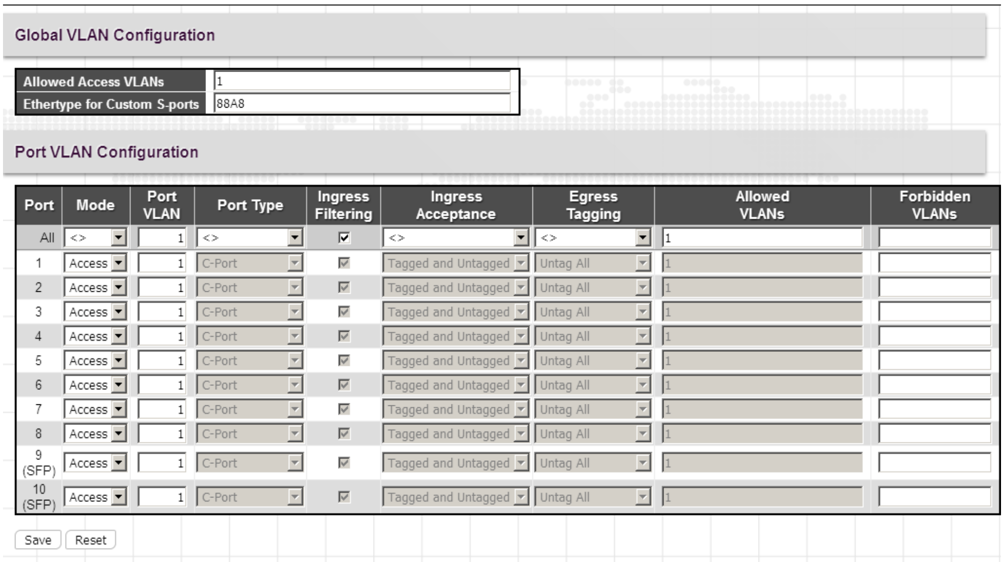
VLANs make changes of devices or relocation more easily: In traditional networks, when moving a device geographically to a new location (for example, move a device in floor 2 to floor 4), the network administrator may need to change the IP or even subnet of the network or require re-cabling. However, by using VLANs, the original IP settings can remain the same and re-cabling can be reduced to minimal.

The “VLAN” menu contains the following sub menus. Select the appropriate one to set up the detailed configurations.



4.16.1. Global

4.16.1.1. VLAN Configuration



Global VLAN Configuration

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

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
All	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9 (SFP)	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10 (SFP)	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

<u>Global VLAN Configuration</u>

Allowed Access VLANs: This shows the allowed access VLANs. This setting only affects ports set in “Access” mode. Ports in other modes are members of all VLANs specified in “Allowed VLANs” field. By default, only VLAN 1 is specified. More allowed access VLANs can be entered by specifying the individual VLAN ID separated by comma. If you want to specify a range, separate it by a dash. For example, 1, 5, 10, 12-15, 100

Ethertype for Custom S-ports: Specify ether type used for customer s-ports (such as 88A8, 9100).

Port VLAN Configuration

Port: List the number of each port. “Port *” settings apply to all ports.

Mode: The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied.

Access: Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:

- Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1.
- Accepts untagged and C-tagged frames.
- Discards all frames that are not classified to the Access VLAN.
- On egress all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged.

Trunk: Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:

- By default, a trunk port is member of all VLANs (1-4095).
- 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.

Hybrid: Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:

- 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: Configures the VLAN identifier for the port. The allowed values are from 1 through 4095. The default value is 1.

The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

Port Type: When you select "Hybrid" mode, the Port Type field becomes selectable. There are four port types available. Each port type's ingress and egress action is described in the following table.

Action Port Type	Ingress Action	Egress Action
Unaware	When a tagged frame is received on a port, ● If the tagged frame with TPID=0x8100, it becomes a double-tag frame and is forwarded. ● If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by Unaware port will be set to 0x8100. The final status of the frame after egressing are also affected by egress rule.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
C-port	When a tagged frame is received on a port, ● If a tagged frame with TIPID=0x8100, it is forwarded. ● If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by C-port will be set to 0x8100.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
S-port	When a tagged frame is received on a port, ● If a tagged frame with TPID=0x88A8, it is forwarded. ● If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded.	The TPID of frame transmitted by S-port will be set to 0x88A8
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
S-custom port	When a tagged frame is received on a port, ● If a tagged frame with TPID=0x88A8, it is forwarded. ● If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded.	The TIPID of frame transmitted by S-custom-port will be set to a self-customized value, which can be set by the user using the column of Ethertype for Custom S-ports.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	

Ingress Filtering: If Ingress Filtering is enabled and the ingress port is not a member of a VLAN, the frame from the ingress port is discarded. By default, ingress filtering is disabled.

Ingress Acceptance: Select the acceptable ingress traffic type on a port.

Tagged and Untagged: Both tagged and untagged ingress packets are acceptable on a port.

Tagged Only: Only tagged ingress packets are acceptable on a port. Untagged packets will be dropped.

Untagged Only: Only untagged ingress packets are acceptable on a port. Tagged packets will be dropped.

Egress Tagging: The action taken when packets are sent out from a port.

Untag Port VLAN: Frames that carry PVID will be removed when leaving from a port. Frames with tags other than PVID will be transmitted with the carried tags.

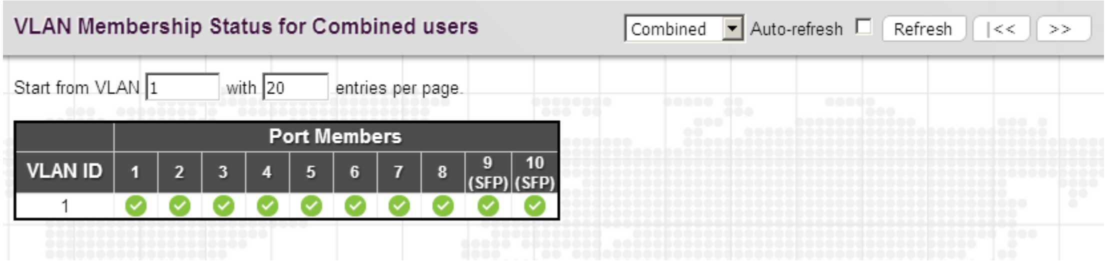
Tag All: Frames are transmitted with a tag.

Untag All: Frames are transmitted without a tag. This option is only available for ports in Hybrid mode.

Allowed VLAN: 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. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4095.

Forbidden VLAN: A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. By default, the field is left blank, which means that the port may become a member of all possible VLANs.

4.16.1.2. VLAN Membership



VLAN Membership Status for Combined users

Start from VLAN 1 with 20 entries per page.

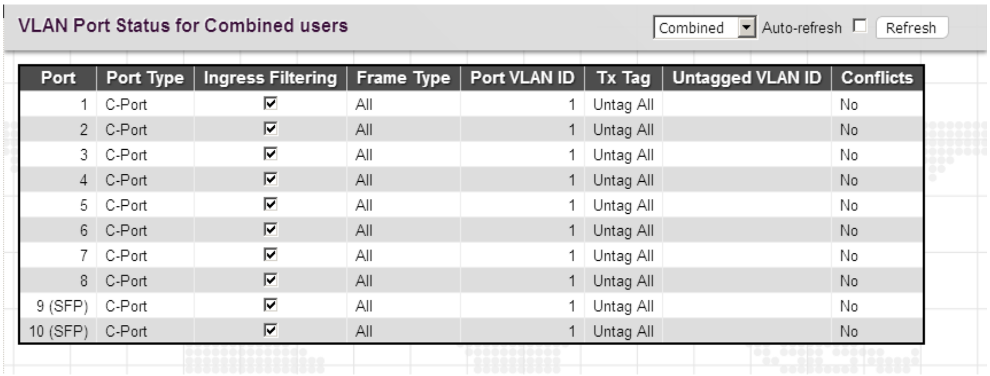
VLAN ID	Port Members									
	1	2	3	4	5	6	7	8	9 (SFP)	10 (SFP)
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

This page shows the current VLAN membership saved on the Switch.

VLAN ID: VLANs that are already created.

Port members: Display member ports on the configured VLANs.

4.16.1.3. Port Status



VLAN Port Status for Combined users

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

This page shows the current VLAN settings on a per-port basis saved on the Switch.

Port: The port number.

PVID: The port VLAN ID assigned to a port.

Port Type: Display the selected port type on a port.

Ingress Filtering: Display whether Ingress Filtering is enabled or disabled.

Frame Type: Display the accepted frame type on a port.

Tx Tag: Display the Egress action on a port.

UVID: Display the untagged VLAN ID. A port's UVID determines the packet's behavior at the egress side. If the VID of

Ethernet frames leaving a port match the UVID, these frames will be sent untagged.

Conflicts: Display whether conflicts exist or not. When a software module requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

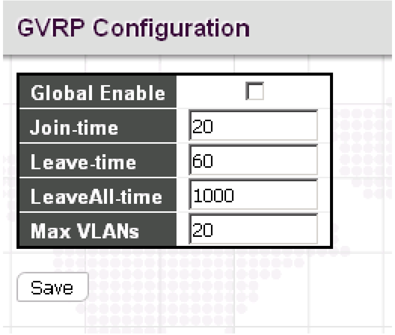
*Functional conflicts between features.
*Conflicts due to hardware limitations.
*Direct conflicts between user modules.

4.16.2. GVRP

GVRP (GVRP VLAN Registration Protocol) is defined in the IEEE 802.1Q standard and enables the switch to dynamically create IEEE 802.1Q compliant VLANs between GVRP-enabled devices. With GVRP, VLAN information can be automatically propagated from device to device so as to reduce errors when creating VLANs manually and provide VIDs consistency across network.

This section provides configuration pages for users to set up GVRP timers and enable GVRP on a per-port basis.

4.16.2.1. Global Config



GVRP Configuration

Global Enable	□
Join-time	20
Leave-time	60
LeaveAll-time	1000
Max VLANs	20

Global Enable: Select the checkbox to globally enable GVRP function.

Join-time: Specify the amount of time in units of centi-seconds that PDUs are transmitted. The default value is 20 centi-seconds. The valid value is 1~20.

Note: *The “Leave-time” parameter must be three times greater than or equal to Join time.*

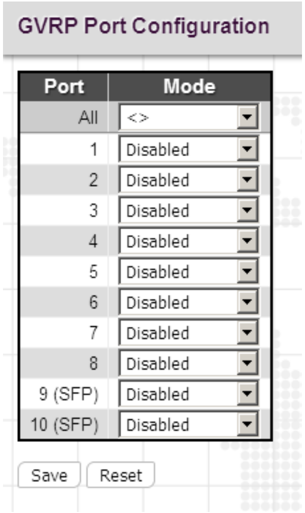
Leave-time: Specify the amount of time in units of centi-seconds that the device waits before deleting the associated entry. The leave time is activated by a “Leave All-time” message sent/received and cancelled by the Join message. The default value is 60 centi-seconds.

LeaveAll-time: Specify the amount of time that "LeaveAll" PDUs are created. A LeaveAll PDU indicates that all registrations are shortly de-registered. Participants will need to rejoin in order to maintain registration. The valid value is 1000 to 5000 centi-seconds. The factory default 1000 centi-seconds.

NOTE: *The "LeaveAll-time" parameter must be greater than the "Leave-time" parameter.*

Max VLANs: The maximum number of VLANs can be learned via GVRP.

4.16.2.2. Port Configuration



GVRP Port Configuration

Port	Mode
All	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9 (SFP)	Disabled
10 (SFP)	Disabled

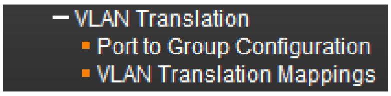
Port: The port number.

Mode: Enable GVRP on a per port basis.

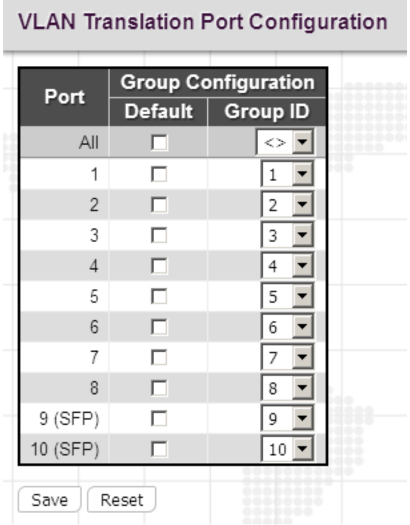
4.16.3. VLAN Translation

VLAN Translation is especially useful for users who want to translate the original VLAN ID to a new VLAN ID so as to exchange data across different VLANs and improve VLAN scaling. VLAN translation replaces an incoming C-VLAN tag with an S-VLAN tag instead of adding an additional tag. When configuring VLAN Translation, both ends of the link normally must be able to replace tags appropriately. In other words, both ends must be configured to translate the C-VLAN tag to S-VLAN tag and S-VLAN tag to C-VLAN tag appropriately in a network. Note that only access ports support VLAN translation. It is not recommended to configure VLAN Translation on trunk ports.

The "VLAN Translation" menu contains the following sub menus. Select the appropriate one to configure settings or view its status.



4.16.3.1. Port to Group Configuration



VLAN Translation Port Configuration

Port	Group Configuration	
	Default	Group ID
All	□	<>
1	□	1
2	□	2
3	□	3
4	□	4
5	□	5
6	□	6
7	□	7
8	□	8
9 (SFP)	□	9
10 (SFP)	□	10

Port Number: List of ports available for VLAN Translation mapping.

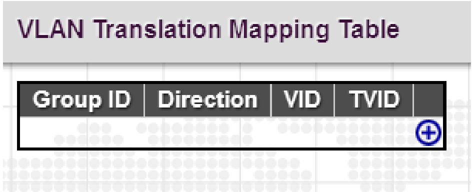
Group Configuration

Default: Click the appropriate radio button to include a port into a default VLAN translation group.

Group ID: The VLAN Translation mappings are organized into Groups, identified by the Group ID. In this way, a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 53.

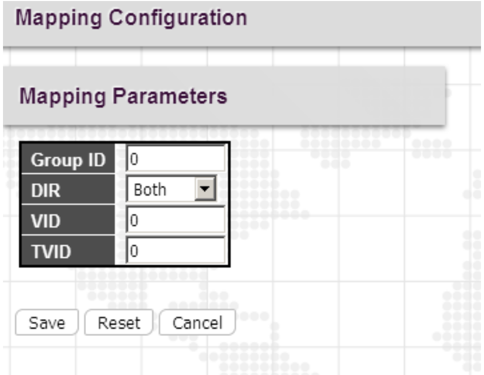
NOTE: *By default, each port is mapped to a group with a group ID equal to the port number. For example, port 2 is mapped to the group with ID is 2.*

4.16.3.2. VID Translation Mapping



VLAN Translation Mapping Table

Group ID	Direction	VID	TVID
			⊕



Mapping Configuration

Mapping Parameters

Group ID	0
DIR	Both
VID	0
TVID	0

Group ID: Indicate the Group ID that applies to this translation rule.

Direction: Select the direction of the VLAN Translation. The direction can be 'Ingress', where the translation takes place on the VLAN ID of frames entering the switch port, 'Egress', where the translation takes place on the VLAN ID of frames exiting the switch port, or 'Both', where the translation takes place on both of the above directions.

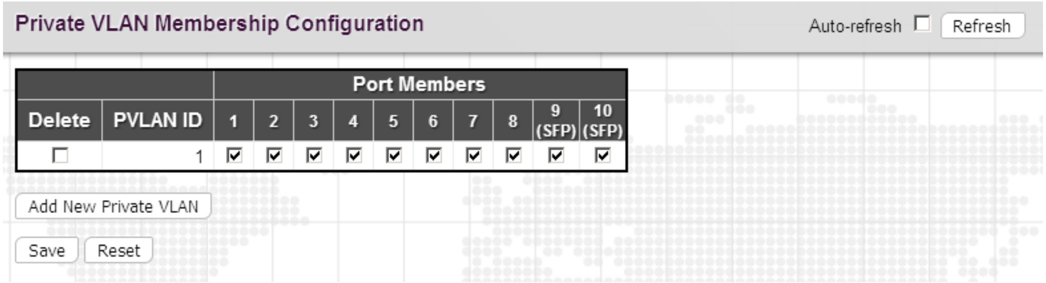
VLAN ID: Indicate the VLAN ID that will be mapped to a new VID.

Translated to VID: Indicate the new VID to which VID of ingress frames will be changed.

Click the "Add New Entry" button once to add a new VLAN Translation entry.

4.16.4. Private VLANs

4.16.4.1. PVLAN Membership



Private VLAN Membership Configuration

		Port Members									
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9 (SFP)	10 (SFP)
□	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

This page is used to configure private VLANs. New Private VLANs can be added here and existing VLANs can be modified. Private VLANs are based on the source port mask and there are no connections to VLANs which means that VLAN IDs and Private VLAN IDs can be identical. A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

PVLAN ID: Specify the PVLAN ID. Valid values are 1 to 4095.

Port Members: Select the checkbox, if you would like a port to belong to a certain Private VLAN. Uncheck the checkbox to remove a port from a Private VLAN.

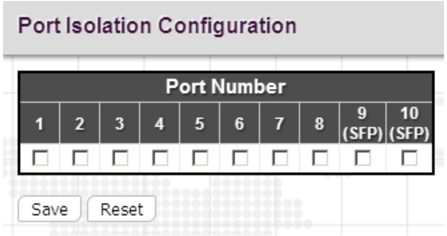
Click the “Add New Private VLAN” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.16.4.2. Port Isolation



Port Isolation Configuration

Port Number									
1	2	3	4	5	6	7	8	9 (SFP)	10 (SFP)
□	□	□	□	□	□	□	□	□	□

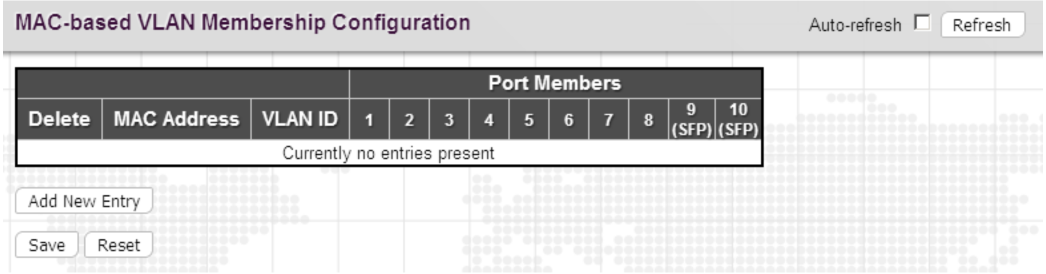
Private VLAN is used to group ports together so as to prevent communications within PVLAN. Port Isolation is used to prevent communications between customer ports in a same Private VLAN. The port that is isolated from others cannot forward any unicast, multicast or broadcast traffic to any other ports in the same PVLAN.

Port Number: Select the checkbox if you want a port or ports to be isolated from other ports.

4.16.5. VCL

4.16.5.1. MAC-based VLAN

MAC-based VLAN configuration page is to set up VLANs based on source MAC addresses. When ingress untagged frames are received by a port, source MAC address is processed to decide which VLAN these untagged frames belong. When source MAC addresses do not match the rules created, untagged frames are assigned to the receiving port's native VLAN ID (PVID).



MAC-based VLAN Membership Configuration

Auto-refresh □

			Port Members									
Delete	MAC Address	VLAN ID	1	2	3	4	5	6	7	8	9 (SFP)	10 (SFP)
Currently no entries present												

MAC Address: Indicate the source MAC address. Please note that the source MAC address can only map to one VLAN ID.

VLAN ID: Map this MAC address to the associated VLAN ID.

Port Members: Ports that belong to this VLAN.

Click the "Add New Entry" button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

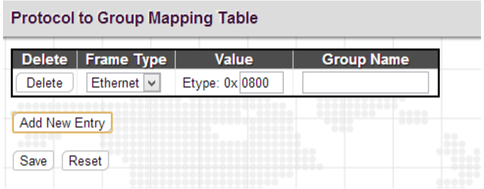
Click the “Reset” button to restore changed settings to the default settings.

4.16.5.2. Protocol-based VLAN

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

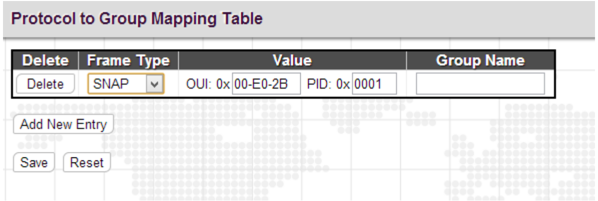
To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

4.16.5.2.1. Protocol to Group



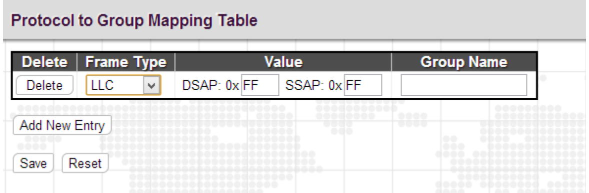
Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
Delete	Ethernet	Etype: 0x 0800	



Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
Delete	SNAP	OUI: 0x 00-E0-2B PID: 0x 0001	



Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
Delete	LLC	DSAP: 0x FF SSAP: 0x FF	

Frame Type: There are three frame types available for selection; these are “Ethernet”, “SNAP”, and “LLC”. The value field will change accordingly.

Value: This field specifically indicates the protocol type. This value field varies depending on the frame type you selected.

Ethernet: Ether Type (etype) value. By default, it is set to 0x0800. The range allowed is 0x0600 to 0xffff.

SNAP: This includes OUI (Organizationally Unique Identifier) and PID (Protocol ID) values.

OUI: A value in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value in the ranges of 0x00-0xff.

PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type field value for the protocol running on top of SNAP. If the OUI is that of a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI is other than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.

LLC (Logical Link Control): This includes DSAP (Destination Service Access Point) and SSAP (Source Service Access Point) values. By default, the value is 0xff. Valid range is 0x00 to 0xff.

Group Name: Indicate the descriptive name for this entry. This field only allows 16 alphabet characters (a-z; A-Z) or integers (0-9).

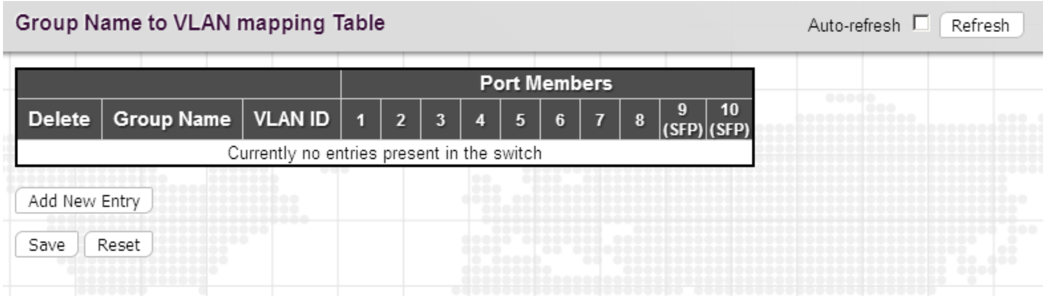
Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.16.5.2.2. Group to VLAN



			Port Members									
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8	9 (SFP)	10 (SFP)
Currently no entries present in the switch												

Group Name: Indicate the descriptive name for this entry. This field only allows 16 alphabet characters (a-z; A-Z) or integers (0-9).

VLAN ID: Indicate the VLAN ID.

Port Members: Assign ports to this rule.

Click the “Add New Entry” button to insert a new entry to the list.

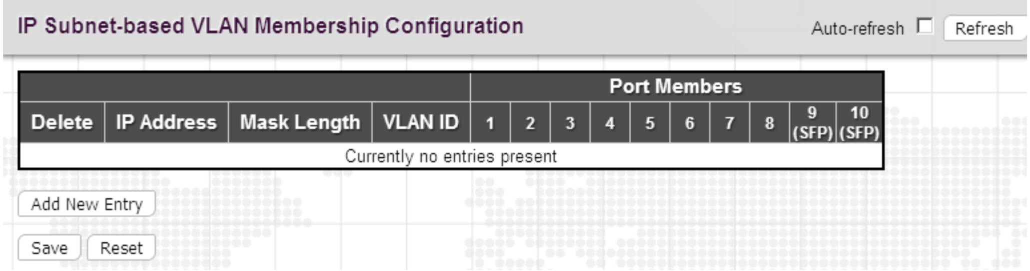
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.16.5.3. IP Subnet-based VLAN

IP Subnet-based VLAN configuration is to map untagged ingress frames to a specific VLAN if the source address is found in the IP subnet-to-VLAN mapping table. When IP subnet-based VLAN classification is enabled, the source address of untagged ingress frame is checked against the IP subnet-to-VLAN mapping table. If an entry is found for that subnet, these frames are assigned to the VLAN indicated in the entry. If no IP subnet is matched, the untagged frames are classified as belonging to the receiving port’s VLAN ID (PVID).



				Port Members									
Delete	IP Address	Mask Length	VLAN ID	1	2	3	4	5	6	7	8	9 (SFP)	10 (SFP)
Currently no entries present													

VCE ID: Index of the entry. Valid range is 0-256.

IP Address: Indicate the IP address for this rule.

Mask Length: Indicate the network mask length.

VLAN ID: Indicate the VLAN ID

Port Members: Assign ports to this rule.

Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

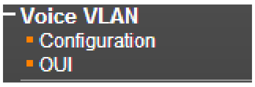
Click the “Reset” button to restore changed settings to the default settings.

4.16.6. Voice VLAN

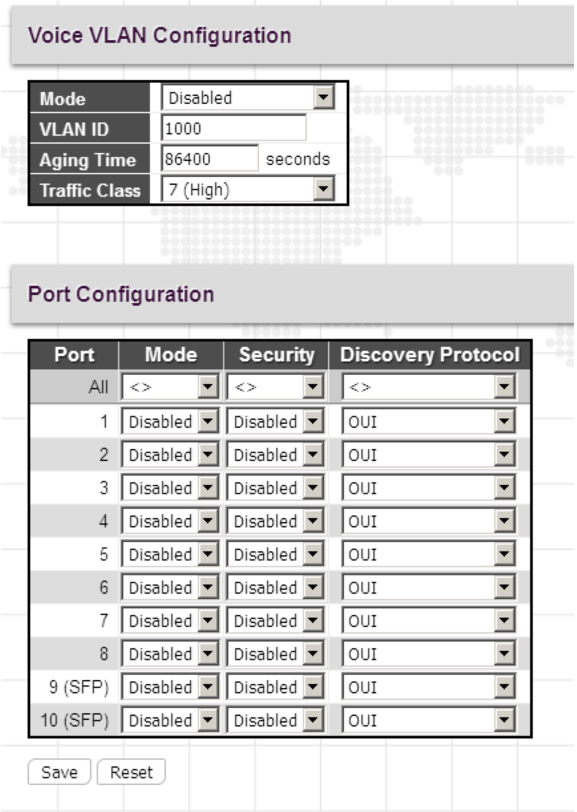
Nowadays, in the enterprise network, VoIP devices are commonly deployed to save operational cost due to its easy-to-setup feature and convenience. However, while deploying VoIP devices, it is recommended that VoIP traffic is separated from data traffic. By isolating traffic, VoIP traffic can be assigned to have the highest priority while forwarding so that higher voice quality can be achieved without encountering situations like excessive packet delays, packet loss, and jitters. Moreover,

This switch provides Voice VLAN feature that enables voice traffic to be forwarded on the voice VLAN. The user can also overwrite traffic priority by assigning higher traffic class value to voice traffic. Voice traffic can be detected on a port by using LLDP (IEEE 802.1ab) to discover VoIP devices attached to the switch or from devices’ OUI (Organizationally Unique Identifier). When voice packets are detected on a port, the switch automatically assigns the port as a tagged member of the Voice VLAN and forward packets based on configurations set in Voice VLAN configuration page.

The Voice VLAN section provides that following two sub menus:



4.16.6.1. Configuration



Voice VLAN Configuration

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

Port Configuration

Port	Mode	Security	Discovery Protocol
All	<>	<>	<>
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI
7	Disabled	Disabled	OUI
8	Disabled	Disabled	OUI
9 (SFP)	Disabled	Disabled	OUI
10 (SFP)	Disabled	Disabled	OUI

Voice VLAN Configuration

Mode: Enable or disable Voice VLAN function on this switch.

VLAN ID: Assign a VLAN ID to this Voice VLAN. Only one Voice VLAN is supported on the switch. By default, VLAN 1000 is set. The allowed range is 1~4095.

Note:

1. *The Voice VLAN cannot be the same as management VLAN, MVR VLAN, or the native VLAN assigned to any port.*
2. *MSTP must be disabled before the Voice VLAN is enabled or the Voice VLAN port mode is set to Auto or Forced. This prevents the spanning tree's ingress filter from dropping VoIP traffic tagged for the Voice VLAN.*

Aging Time: The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port. By default, the aging time is set to 86400 seconds. The allowed aging time is 10 – 10,000,000 seconds.

Traffic Class: Select the traffic class value which defines a service priority for traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new traffic class when the Voice VLAN feature is active on a port. By default, 7 (Highest priority) is used. The allowed range is 0 (Lowest) – 7 (Highest).

Port Configuration

Port: The port number. “All” rules apply to all ports.

Mode: Select whether a particular is enabled with Voice VLAN feature or not. There are three options available:

Disabled: Disable Voice VLAN feature on a particular port.

Auto: Enable the Voice VLAN auto detection mode. When voice (VoIP) traffic is detected on a port, the port will be added as a tagged member to the Voice VLAN. When Auto mode is selected, you need to further decide a method for detecting voice traffic in “Discovery Protocol” field, either OUI or LLDP (802.1ab).

Forced: Enable Voice VLAN feature on a particular port.

Security: Enable or disable security filtering feature on a per port basis. When enabled, any non-VoIP packets received on a port with Voice VLAN ID will be discarded. VoIP traffic is identified by source MAC addresses configured in the telephony OUI list or through LLDP which is used to discover VoIP devices attached to the switch.

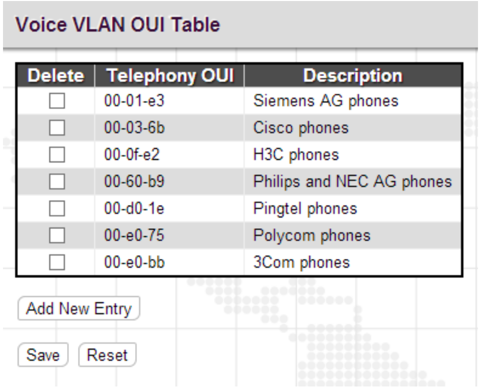
Discovery Protocol: Select a method for detecting VoIP traffic. By default, OUI is used.

OUI: Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address. OUI numbers are assigned to manufacturers and form the first three octets of a device MAC address. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.

LLDP: Use LLDP (IEEE 802.1ab) to discover VoIP devices attached to a port. LLDP checks that the “telephone bit” in the system capability TLV is turned on or not.

Both: Use both OUI table and LLDP to detect VoIP traffic on a port.

4.16.6.2. OUI



Voice VLAN OUI Table

Delete	Telephony OUI	Description
□	00-01-e3	Siemens AG phones
□	00-03-6b	Cisco phones
□	00-0f-e2	H3C phones
□	00-60-b9	Philips and NEC AG phones
□	00-d0-1e	Pingtel phones
□	00-e0-75	Polycom phones
□	00-e0-bb	3Com phones

Telephony OUI: Specify your VoIP device's OUI. It must be 6 characters long and the input format is "xx-xx-xx" (x is hexadecimal digit)

Description: Specify a descriptive comments or information to this entry.

Click the "Add New Entry" button to insert a new entry to the list.

Click the "Delete" button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the "Save" button to save settings or changes.

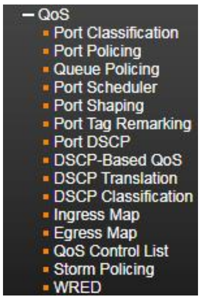
Click the "Reset" button to restore changed settings to the default settings.

4.17. QoS

Network traffic is always unpredictable and the only basic assurance that can be offered is the best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria and receives preferential treatments.

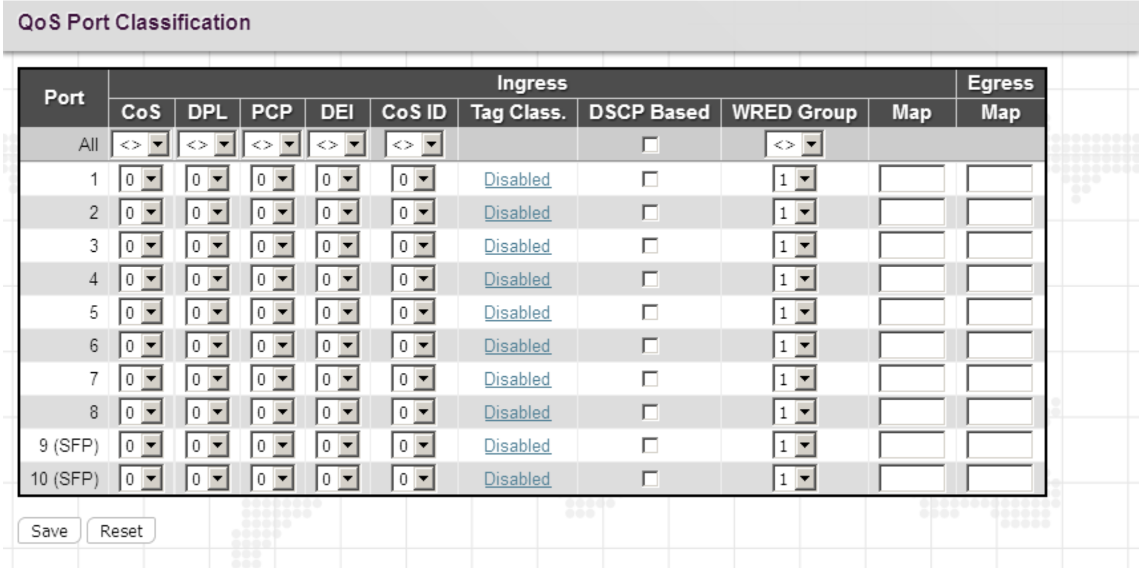
QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic. To set up the priority of packets in this switch, go to "Port Classification" page.

The "QoS" menu contains the following sub menus.



- QoS
  - Port Classification
  - Port Policing
  - Queue Policing
  - Port Scheduler
  - Port Shaping
  - Port Tag Remarking
  - Port DSCP
  - DSCP-Based QoS
  - DSCP Translation
  - DSCP Classification
  - Ingress Map
  - Egress Map
  - QoS Control List
  - Storm Policing
  - WRED

4.17.1. Port Classification



QoS Port Classification

Port	Ingress									Egress
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	WRED Group	Map	Map
All	<>	<>	<>	<>	<>		□	<>		
1	0	0	0	0	0	Disabled	□	1		
2	0	0	0	0	0	Disabled	□	1		
3	0	0	0	0	0	Disabled	□	1		
4	0	0	0	0	0	Disabled	□	1		
5	0	0	0	0	0	Disabled	□	1		
6	0	0	0	0	0	Disabled	□	1		
7	0	0	0	0	0	Disabled	□	1		
8	0	0	0	0	0	Disabled	□	1		
9 (SFP)	0	0	0	0	0	Disabled	□	1		
10 (SFP)	0	0	0	0	0	Disabled	□	1		

Port: The port number. "All" rules will apply to all ports.

QoS class: Indicate the default QoS class. A QoS class of 0 has the lowest priority. By Default, 0 is used.

DP Level: Select the default Drop Precedence Level.

PCP: Select the appropriate value for the default Priority Code Point (or User Priority) for untagged frames.

DEI: Select the appropriate value for the default Drop Eligible Indicator for untagged frames.

Tag Class: This field displays classification mode for tagged frames on this port:

Disabled: Use the default QoS class and DP level for tagged frames.

Enabled: Use the mapped versions of PCP and DEI for tagged frames.

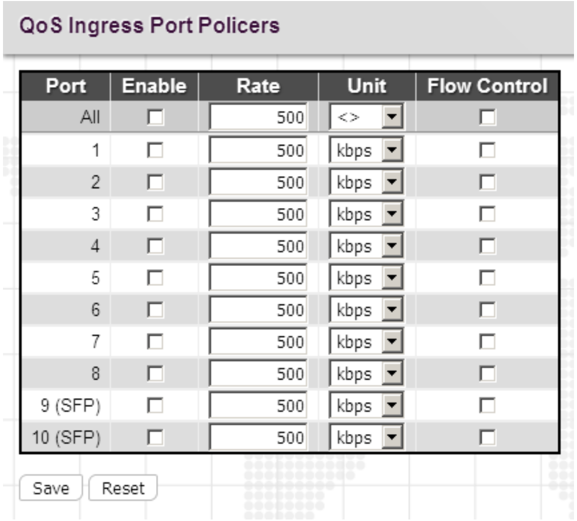
DSCP Based: Select the checkbox to enable DSCP based QoS (Ingress Port).

WRED Group: Specify the WRED group used for a specific port.

Ingress Map: Specify the ingress map ID.

Egress Map: Specify the egress map ID.

4.17.2. Port Policing



QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
All	□	500	<>	□
1	□	500	kbps	□
2	□	500	kbps	□
3	□	500	kbps	□
4	□	500	kbps	□
5	□	500	kbps	□
6	□	500	kbps	□
7	□	500	kbps	□
8	□	500	kbps	□
9 (SFP)	□	500	kbps	□
10 (SFP)	□	500	kbps	□

This page allows users to set each port’s allowed bandwidth.

Port: The port number. “All” settings apply to all ports.

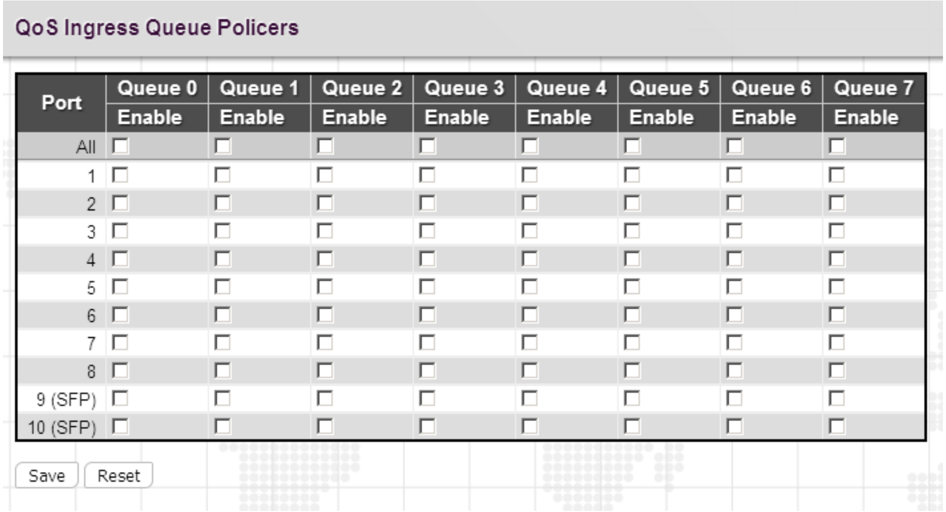
Enabled: Select the checkbox to enable port policing function on a port.

Rate: Indicate the rate for the policer. By default, 500kbps is used. The allowed range for kbps and fps is 100 to 1000000. The allowed range for Mbps and kfps is 1 to 3300Mbps.

Unit: Select the unit of measure for the policer.

Flow Control: If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

4.17.3. Port Policers



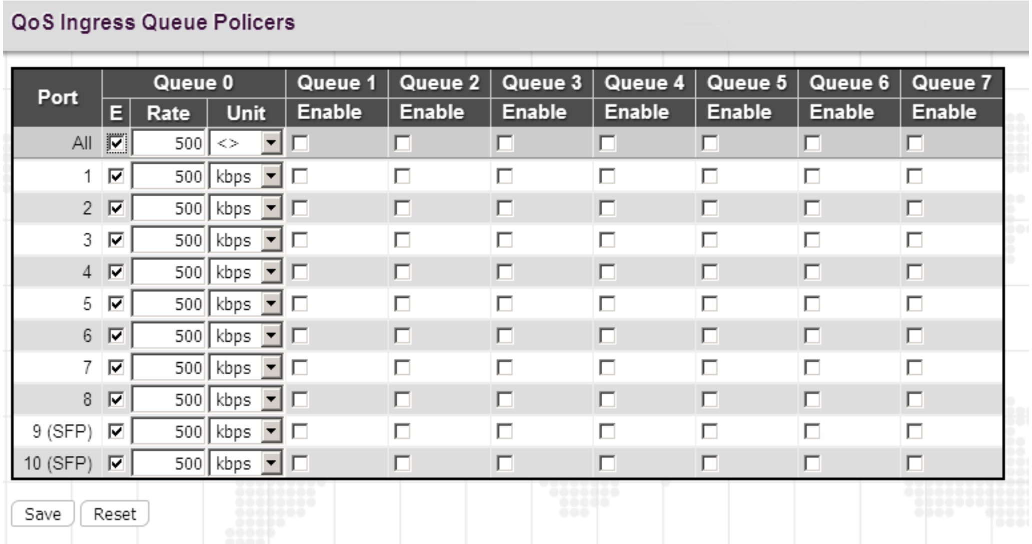
QoS Ingress Queue Policers

Port	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable
All	□	□	□	□	□	□	□	□
1	□	□	□	□	□	□	□	□
2	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□
4	□	□	□	□	□	□	□	□
5	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	□
7	□	□	□	□	□	□	□	□
8	□	□	□	□	□	□	□	□
9 (SFP)	□	□	□	□	□	□	□	□
10 (SFP)	□	□	□	□	□	□	□	□

Port: The port number. “Port *” settings apply to all ports.

Queue 0~7 Enable: Select the appropriate checkboxes to enable queue policing function on switch ports.

When enabled, the following image will appear:



QoS Ingress Queue Policers

Port	Queue 0			Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	E	Rate	Unit	Enable	Enable	Enable	Enable	Enable	Enable	Enable
All	☑	500	<>	□	□	□	□	□	□	□
1	☑	500	kbps	□	□	□	□	□	□	□
2	☑	500	kbps	□	□	□	□	□	□	□
3	☑	500	kbps	□	□	□	□	□	□	□
4	☑	500	kbps	□	□	□	□	□	□	□
5	☑	500	kbps	□	□	□	□	□	□	□
6	☑	500	kbps	□	□	□	□	□	□	□
7	☑	500	kbps	□	□	□	□	□	□	□
8	☑	500	kbps	□	□	□	□	□	□	□
9 (SFP)	☑	500	kbps	□	□	□	□	□	□	□
10 (SFP)	☑	500	kbps	□	□	□	□	□	□	□

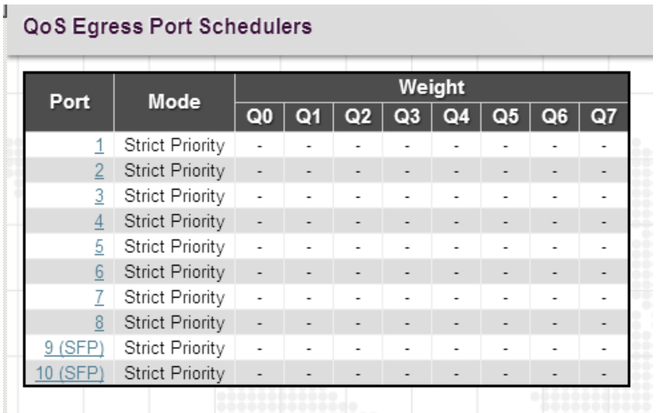
Rate: Indicate the rate for the ingress queue policer. By default, 500kbps is used. Allowed range for kbps is 100 to 1000000. Allowed range for Mbps is 1 to 3300Mbps.

Unit: Select he unit of measure for the ingress queue policer.

Save: Save the current running configurations to memory.

Reset: Clear all selected settings.

4.17.4. Port Scheduler



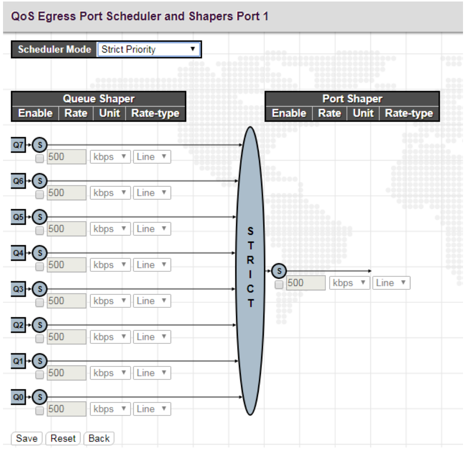
QoS Egress Port Schedulers

Port	Mode	Weight							
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
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 (SFP)	Strict Priority	-	-	-	-	-	-	-	-
10 (SFP)	Strict Priority	-	-	-	-	-	-	-	-

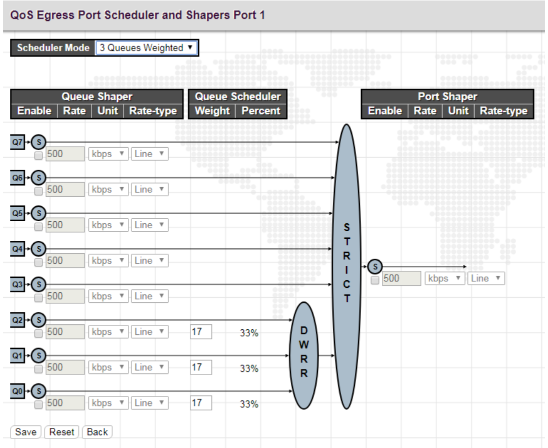
Port: Click the port to set up detailed settings for port scheduler.

Mode: Display scheduler mode selected.

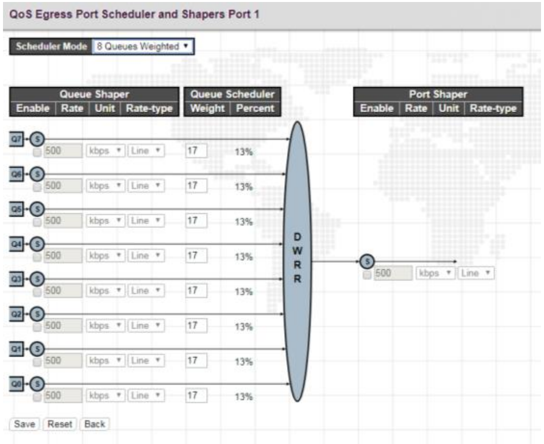
Weight: Display the weight in percentage assigned to Q0~Q7.


QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority


QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: 3 Queues Weighted


QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: 8 Queues Weighted

This page allows you to set up the Schedulers and Shapers for a specific port.

Scheduler Mode: The device offers two modes to handle queues.

Strict mode: This gives egress queues with higher priority to be transmitted first before lower priority queues are serviced.

Weight mode: Deficit Weighted Round-Robin (DWRR) queuing which specifies a scheduling weight for each queue. (Options: Strict, Weighted; Default: Strict) DWRR services the queues in a manner similar to WRR, but the next queue is serviced only when the queue's Deficit Counter becomes smaller than the packet size to be transmitted.

Queue Shaper/Port Shaper/Queue Shaper

Enable: Select the checkbox to enable queue shaper on a certain queue for this selected port.

Rate: Indicate the rate for the queue shaper. By default, 500kbps is used. Allowed range for kbps is 100 to 1000000. Allowed range for Mbps is 1 to 3300Mbps.

Unit: Select he unit of measure for the queue shaper.

Excess: Select the checkbox to allow excess bandwidth.

<u>Queue Schedule</u>

Queue Scheduler: When Scheduler Mode is set to Weighted, the user needs to indicate a relative weight for each queue. DWRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Weight: Assign a weight to each queue. This weight sets the frequency at which each queue is polled for service and subsequently affects the response time software applications assigned a specific priority value.

Percent: The weight as a percentage for this queue.

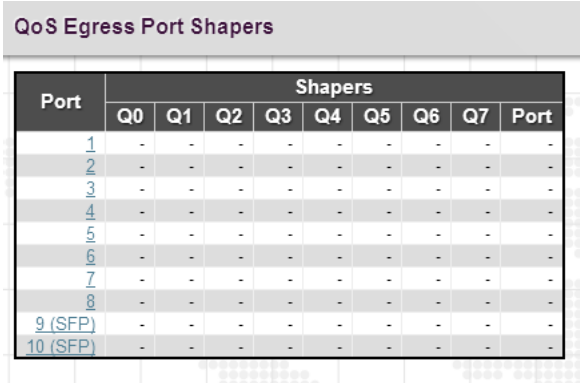
Port Shaper: Set the rate at which traffic can egress this queue.

Enable: Select the checkbox to enable Port shaper.

Rate: Indicate the rate for Port Shaper. By default, 500kbps is used. Allowed range for kbps is 100 to 1000000. Allowed range for Mbps is 1 to 3300Mbps.

Unit: Select the rate of measure

4.17.5. Port Shaping



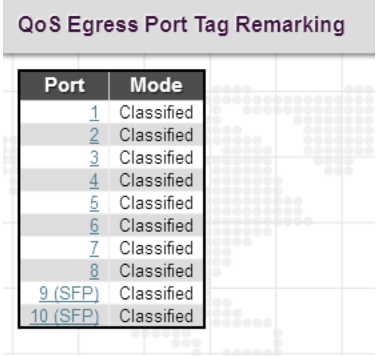
QoS Egress Port Shapers

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

This displays each port’s queue shaper and port shaper’s rate.

Click the port number to modify or reset queue shaper and port shaper’s rates. See “Port Scheduler” for detailed explanation on each configuration option.

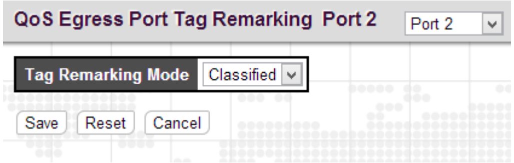
4.17.6. Port Tag Remarking



QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9 (SFP)	Classified
10 (SFP)	Classified

Click the port number that you want change settings.



QoS Egress Port Tag Remarking Port 2

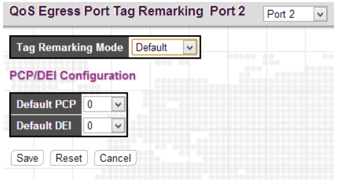
Tag Remarking Mode: Classified

Tag Remarking Mode: Select the appropriate remarking mode used by this port.

Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values (Default PCP:0; Default DEI:0).

Mapped: Use the mapping of the classified QoS class values and DP levels to PCP/DEI values.

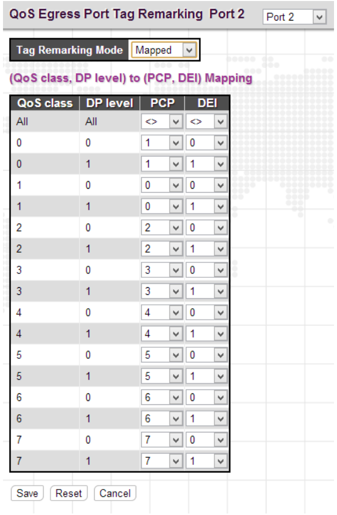


QoS Egress Port Tag Remarking Port 2 | Port 2

Tag Remarking Mode: Default

PCP/DEI Configuration

Default PCP: 0
Default DEI: 0



QoS Egress Port Tag Remarking Port 2 | Port 2

Tag Remarking Mode: Mapped

(QoS class, DP level) to (PCP, DEI) Mapping

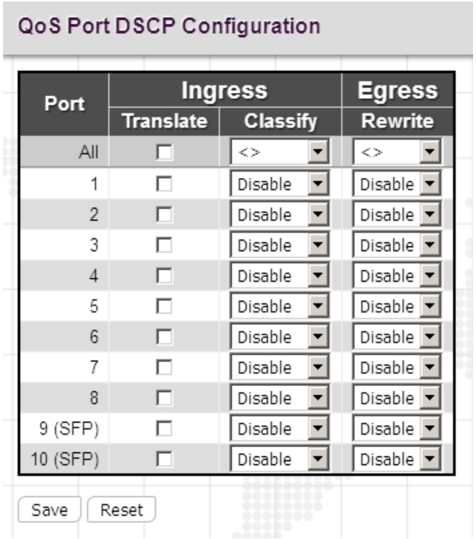
QoS class	DP level	PCP	DEI
All	All	<>	<>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

QoS class/DP level: Show the mapping options for QoS class values and DP levels (drop precedence).

PCP: Remarks matching egress frames with the specified Priority Code Point (or User Priority) value. (Range: 0-7; Default: 0)

DEI: Remarks matching egress frames with the specified Drop Eligible Indicator. (Range: 0-1; Default: 0)

4.17.7. Port DSCP



QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
All	□	<>	<>
1	□	Disable	Disable
2	□	Disable	Disable
3	□	Disable	Disable
4	□	Disable	Disable
5	□	Disable	Disable
6	□	Disable	Disable
7	□	Disable	Disable
8	□	Disable	Disable
9 (SFP)	□	Disable	Disable
10 (SFP)	□	Disable	Disable

Port: List the number of each. “All” settings apply to all ports.

Ingress Translate: Select the checkbox to enable ingress translation of DSCP values based on the selected classification method.

Ingress Classify: Select the appropriate classification method:

Disable: No ingress DSCP classification is performed.

DSCP=0: Classify if incoming DSCP is 0.

Selected: Classify only selected DSCP for which classification is enabled in DSCP Translation table

All: Classify all DSCP.

Egress Rewrite: Configure port egress rewriting of DSCP values.

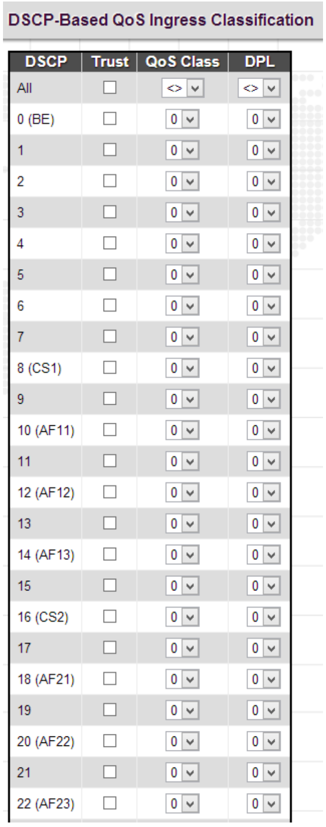
Disable: Egress rewriting is disabled.

Enable: Enable egress rewriting is enabled but with remapping.

Remap DP aware: Frame with DSCP from analyzer is remapped and remarked with the remapped DSCP value. Depending on the frame’s DP level, the remapped DSCP value is either taken from the DSCP Translation table, Egress Remap DP0 or DP1 field.

Remap DP unaware: Frame with DSCP from analyzer is remapped and remarked with the remapped DSCP value. The remapped DSCP value is always taken from the DSCP Translation table, Egress Remap DP0 field.

4.17.8. DSCP-Based QoS



DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
All	□	<>	<>
0 (BE)	□	0	0
1	□	0	0
2	□	0	0
3	□	0	0
4	□	0	0
5	□	0	0
6	□	0	0
7	□	0	0
8 (CS1)	□	0	0
9	□	0	0
10 (AF11)	□	0	0
11	□	0	0
12 (AF12)	□	0	0
13	□	0	0
14 (AF13)	□	0	0
15	□	0	0
16 (CS2)	□	0	0
17	□	0	0
18 (AF21)	□	0	0
19	□	0	0
20 (AF22)	□	0	0
21	□	0	0
22 (AF23)	□	0	0

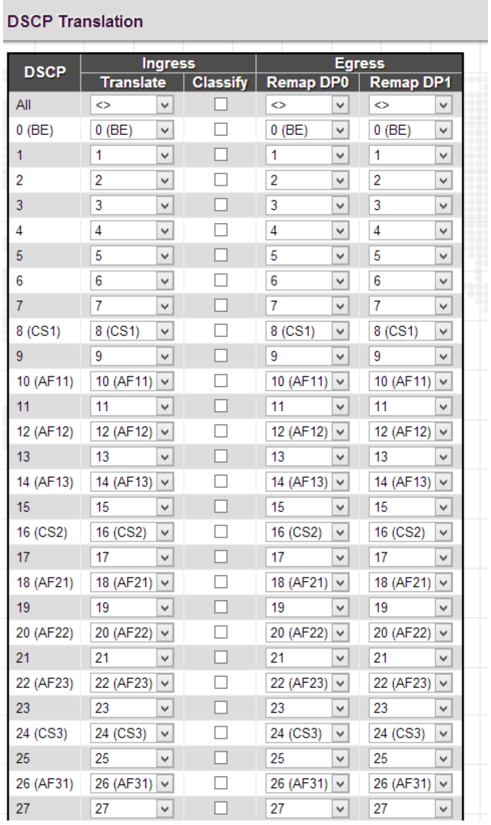
DSCP: DSCP value in ingress packet. DSCP range is from 0 to 63.

Trust: Select the checkbox to indicate that DSCP value is trusted. Only trusted DSCP values are mapped to a specific QoS class and drop precedence level (DPL). Frames with untrusted DSCP values are treated as non-IP frames.

QoS Class: Select the QoS class to the corresponding DSCP value for ingress processing. By default, 0 is used. Allowed range is 0 to 7.

DPL: Select the drop precedence level to the corresponding DSCP value for ingress processing. By default, 0 is used. The value “1” has the higher drop priority.

4.17.9. DSCP Translation



DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
All	<>	□	<>	<>
0 (BE)	0 (BE)	□	0 (BE)	0 (BE)
1	1	□	1	1
2	2	□	2	2
3	3	□	3	3
4	4	□	4	4
5	5	□	5	5
6	6	□	6	6
7	7	□	7	7
8 (CS1)	8 (CS1)	□	8 (CS1)	8 (CS1)
9	9	□	9	9
10 (AF11)	10 (AF11)	□	10 (AF11)	10 (AF11)
11	11	□	11	11
12 (AF12)	12 (AF12)	□	12 (AF12)	12 (AF12)
13	13	□	13	13
14 (AF13)	14 (AF13)	□	14 (AF13)	14 (AF13)
15	15	□	15	15
16 (CS2)	16 (CS2)	□	16 (CS2)	16 (CS2)
17	17	□	17	17
18 (AF21)	18 (AF21)	□	18 (AF21)	18 (AF21)
19	19	□	19	19
20 (AF22)	20 (AF22)	□	20 (AF22)	20 (AF22)
21	21	□	21	21
22 (AF23)	22 (AF23)	□	22 (AF23)	22 (AF23)
23	23	□	23	23
24 (CS3)	24 (CS3)	□	24 (CS3)	24 (CS3)
25	25	□	25	25
26 (AF31)	26 (AF31)	□	26 (AF31)	26 (AF31)
27	27	□	27	27

DSCP: DSCP value in ingress packet. DSCP range is from 0 to 63.

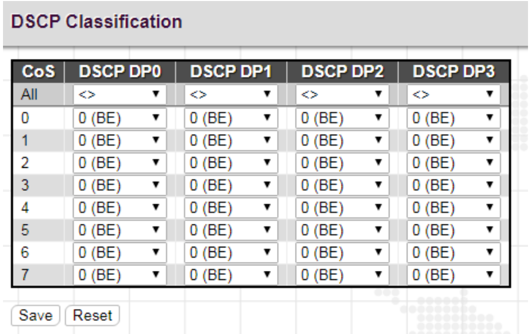
Ingress Translate: Enable Ingress Translation of DSCP values based on the specified classification method.

Ingress Classify: Enable classification at ingress side as defined in the QoS port DSCP Configuration Table.

Egress Remap DP0: Remap DP0 value to the selected DSCP value. DP0 indicates a drop precedence with a low priority.

Egress Remap DP1: Remap DP1 value to the selected DSCP value. DP1 indicates a drop precedence with a high priority.

4.17.10. DSCP Classification



DSCP Classification

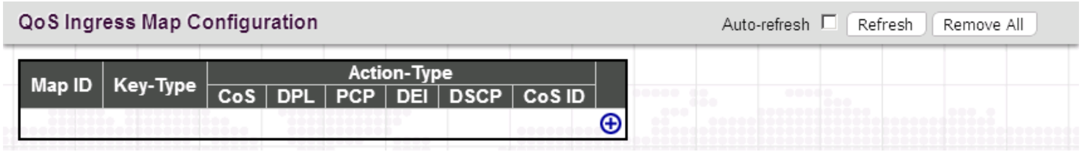
CoS	DSCP DP0	DSCP DP1	DSCP DP2	DSCP DP3
All	<>	<>	<>	<>
0	0 (BE)	0 (BE)	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)	0 (BE)	0 (BE)
5	0 (BE)	0 (BE)	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)	0 (BE)	0 (BE)

Map DSCP values to QoS class and DPL value.

QoS Class: List of actual QoS class values.

DSCP DP0~3: Select the DSCP value to map QoS class and DPL value. DSCP value selected for "*" will map to all QoS class and DPL value.

4.17.11. QoS Ingress Map Configuration

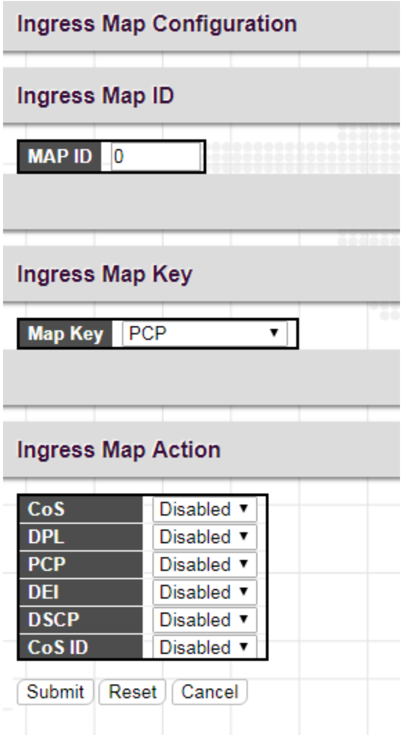


QoS Ingress Map Configuration

Map ID	Key-Type	Action-Type					
		CoS	DPL	PCP	DEI	DSCP	CoS ID
							⊕

This page allows to edit or to create a single QoS Ingress Map entry at a time. Each entry has a key and an action. The key indicates which fields of the frame will be mapped to the fields specified by and according to the action. Each Map can hold a number of map rules, or mappings between possible keys and actions. Which of those rules will be applied depends on the selection of (Key-Type, Action-Type).

Click ⊕ to create a new Ingress Map entry.



Ingress Map Configuration

Ingress Map ID

MAP ID	0

Ingress Map Key

Map Key	PCP

Ingress Map Action

CoS	Disabled
DPL	Disabled
PCP	Disabled
DEI	Disabled
DSCP	Disabled
CoS ID	Disabled

Map ID: Indicates the Map (unique) ID. The allowed range is 0 to 255. When in edit mode, this is non-configurable. However, it is possible to overwrite an existing mapping through the create mode.

Map Key: Indicates the Key type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various keys and this is to make a select set of them. Possible Key types are:

PCP: Use PCP as key for tagged frames and none for the rest.

PCP - DEI: Use PCP/DEI as key for tagged frames and none for the rest.

DSCP: Use DSCP as key for IP frames and none for the rest.

DSCP - PCP - DEI: Use DSCP as key for IP frames, PCP/DEI for tagged frames and none for the rest.

Map Action: Indicates the Action type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various actions available and this is to make a select set of them. Possible Action types are:

CoS: Class of Service.

DPL: Drop Precedence Level.

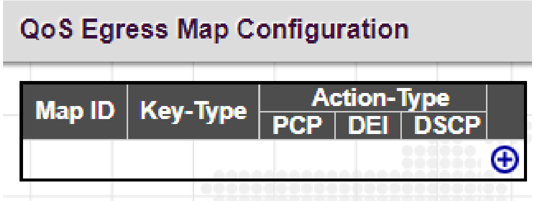
PCP: Priority Code Point.

DEI: Drop Eligible Indicator.

DSCP: Differentiated Services Code Point.

CoS ID: CoS ID.

4.17.12. Egress Map Configuration

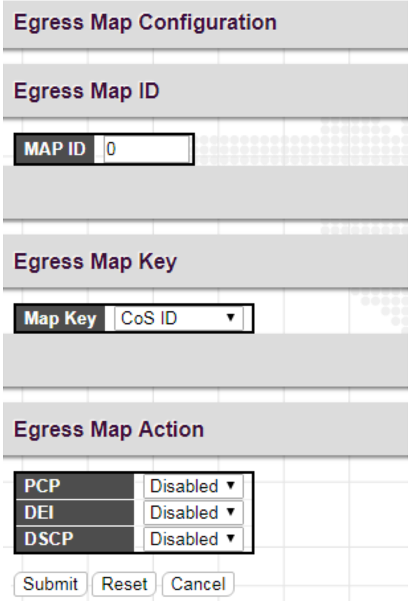


QoS Egress Map Configuration

Map ID	Key-Type	Action-Type		
		PCP	DEI	DSCP

This page allows to edit or create a single QoS Egress Map entry at a time. Each entry has a key and an action. The key indicates which fields of the frame will be mapped to the fields specified by and according to the action. Each Map can hold a number of map rules, or mappings between possible keys and actions. Which of those rules will be applied depends on the selection of (Key-Type, Action-Type).

Click ⊕ to create a new Egress Map instance.



Egress Map Configuration

Egress Map ID

MAP ID	0

Egress Map Key

Map Key	CoS ID

Egress Map Action

PCP	Disabled
DEI	Disabled
DSCP	Disabled

Map ID: Indicates the Map (unique) ID. The allowed range is 0 to 511. When in edit mode, this is non-configurable. However, it is possible to overwrite an existing mapping through the create mode.

Map Key: Indicates the Key type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various keys and this is to make a select set of them. Possible Key types are:

CoS ID: Use classified COS ID as key.

CoS ID - DPL:Use classified COS ID and DPL as key.

DSCP: Use classified DSCP as key.

DSCP - DPL: Use classified DSCP and DPL as key.

Map Action: Indicates the Action type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various actions available and this is to make a select set of them. Possible Action types are:

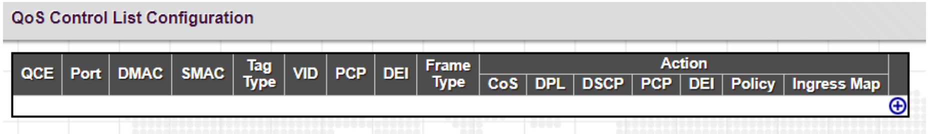
PCP: Priority Code Point.

DEI: Drop Eligible Indicator.

DSCP: Differentiated Services Code Point.

4.17.13. QoS Control List

Quality of Service control list is used to establish policies for handling ingress packets based on frame type, MAC address, VID, PCP, DEI values. Once a QCE is mapped to a port, traffic matching the first entry in the QoS Control List is assigned to the QoS class, drop precedence level, and DSCP value defined by that entry. Traffic not matching any of the QCEs are classified to the default QoS Class for the port.



QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action							
									CoS	DPL	DSCP	PCP	DEI	Policy	Ingress Map	
																⊕

This page displays rules created in QoS control list (QCL) only. The maximum number of QCL is 256 on this device.

QCE#: Display Quality Control Entry index.

Port: Display the port number that uses this QCL.

Frame Type: Display the frame type to look for in incoming frames. Possible frame types are Any, Ethernet, LLC SNAP, IPv4, IPv6.

SMAC: Source MAC address.

DMAC: Destination MAC address. Possible values are Any, Broadcast, Multicast, Unicast.

VID: Display VLAN ID (1~4095)

PCP: Display PCP value.

DEI: Display DEI value.

Action: Display the classification action taken on ingress frames when the configured parameters are matched in the frame’s content. If a frame matches the QCL, the following actions will be taken.

Class: If a frame matches the QCL, it will be put in the queue corresponding to the specified QoS class.

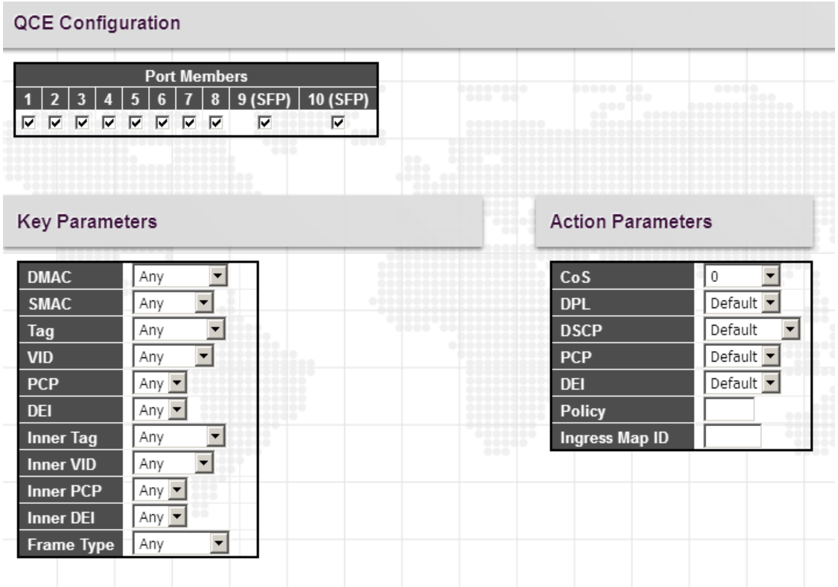
DPL: The drop precedence level will be set to the specified value.

DSCP: The DSCP value will be set to the specified value.

You can modify each QCE (QoS Control Entry) in the table using the following buttons:

⊕: Inserts a new QCE before the current row.
ⓔ: Edits the QCE row.
↑: Moves the QCE up the list.
↓: Moves the QCE down the list.
⊗: Deletes the QCE.
⊕: The lowest plus sign adds a new entry at the bottom of the QCE listings.

Once ⊕ is clicked in display page, the following page will appear.



QCE Configuration

Port Members									
1	2	3	4	5	6	7	8	9 (SFP)	10 (SFP)
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Key Parameters

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

Action Parameters

CoS	0
DPL	Default
DSCP	Default
PCP	Default
DEI	Default
Policy	
Ingress Map ID	

QCE Configuration

Port Members: Select ports that use this rule.

Key Parameters

Tag: Select VLAN tag type (Tag or Untag). By default, any type is used.

VID: Select VID preference. By default, any VID is used. Select "Specific", if you would like to designate a VID to this QCL entry. Or Select "Range", if you would like to map a range of VIDs to this QCL entry.

PCP: Select a PCP value (either specific value or a range of values are provided). By default, any is used.

DEI: Select a DEI value. By default, any is used.

SMAC: Select source MAC address type. By default, any is used. Select "Specific" to specify a source MAC (first three bytes of the MAC address or OUI).

DMAC Type: Select destination MAC address type. By default, any is used. Other options available are "UC" for unicast, "MC" for multicast, and "BC" for broadcast.

Frame Type: The frame types can be selected are listed below.

Any: By default, any is used which means that all types of frames are allowed.

Ethernet: This option can only be used to filter Ethernet II formatted packets. (Options: Any, Specific – 600-ffff hex; Default: ffff). Note that 800 (IPv4) and 86DD (IPv6) are excluded. A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).

LLC: LLC refers to Link Logical Control and further provides three options.

SSAP: SSAP stands for Source Service Access Point address. By default, any is used. Select specific to indicate a value (0x00 - 0xFF).

DSAP: DSAP stands for Destination Service Access Point address. By default, any is used. Select specific to indicate a value (0x00 to 0xFF).

Control: Control field may contain command, response, or sequence information depending on whether the LLC frame type is Unnumbered, Supervisory, or Information. By default, any is used. Select specific to indicate a value (0x00 to 0xFF).

SNAP: SubNetwork Access Protocol can be distinguished by an OUI and a Protocol ID. (Options for PID: Any, Specific (0x00-0xffff); Default: Any) If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP. If the OUI is that of a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI isother than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.

IPv4:

Protocol: IPv4 frame type includes Any, TCP, UDP, Other. If "TCP" or "UDP" is selected, you might further define Sport (Source port number) and Dport (Destination port number).

Source IP: Select source IP type. By default, any is used. Select "Specific" to indicate self-defined source IP and submask format. The address and mask must be in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When the 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

IP Fragment: By default, any is used. Datagrams sometimes may be fragmented to ensure they can pass through a network device that uses a maximum transfer unit smaller than the original packet's size.

DSCP: By default, any is used. Select "Specific" to indicate a DSCP value. Select "Range" to indicate a range of DSCP value.

IPv6:

Protocol: IPv6 protocol includes Any, TCP, UDP, Other. If "TCP" or "UDP" is selected, you may need to further define Sport (Source port number) and Dport (Destination port number).

Source IP: Select source IP type. By default, any is used. Select "Specific" to indicate self-defined source IP and submask format.

DSCP: By default, any is used. Select "Specific" to indicate a DSCP value. Select "Range" to indicate a range of DSCP value.

Action Parameters

Specify the classification action taken on ingress frame if the parameters match the frame's content. The actions taken include the following:

Class: If a frame matches the QCE, it will be put in the queue corresponding to the specified QoS class or placed in a queue based on basic classification rules.

DPL: If a frame matches the QCE, the drop precedence level will be set to the selected value or left unchanged.

DSCP: If a frame matches the QCE, the DSCP value will be set to the selected one.

PCP: If a frame matches the QCE, the PCP value will be set to the selected one.

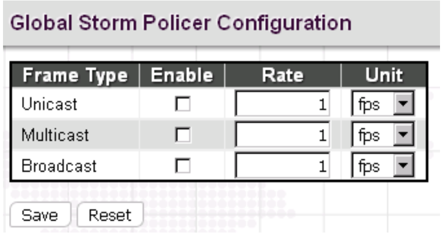
DEI: If a frame matches the QCE, the DEI value will be set to the selected one.

Policy: If a frame matches the QCE, the policy ID specified will be applied.

Ingress Map ID: If a frame matches the QCE, the ingress map ID specified will be applied.

4.17.14. Storm Policing

Storm Policing is used to keep a network from downgraded performance or a complete halt by setting up a threshold for traffic like broadcast, unicast and multicast. When a device on the network is malfunctioning or application programs are not well designed or properly configured, storms may occur and will degrade network performance or even cause a complete halt. The network can be protected from storms by setting a threshold for specified traffic on the device. Any specified packets exceeding the specified threshold will then be dropped.



Global Storm Policer Configuration

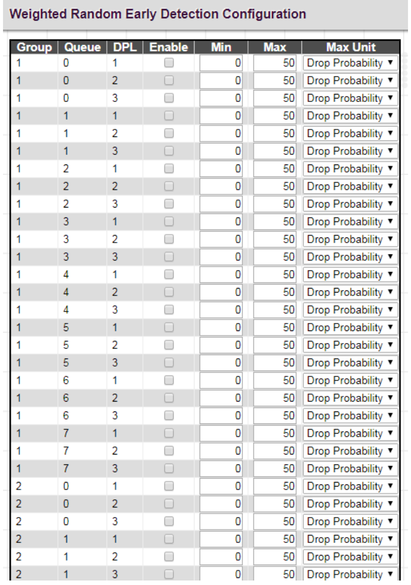
Frame Type	Enable	Rate	Unit
Unicast	□	1	fps
Multicast	□	1	fps
Broadcast	□	1	fps

Enable: Enable Unicast storm, Multicast storm or Broadcast storm protection.

Rate (pps): Select the packet threshold. The packets received exceed the selected value will be dropped.

Unit: Select the unit for each frame type.

4.17.15. WRED



Weighted Random Early Detection Configuration

Group	Queue	DPL	Enable	Min	Max	Max Unit
1	0	1	□	0	50	Drop Probability
1	0	2	□	0	50	Drop Probability
1	0	3	□	0	50	Drop Probability
1	1	1	□	0	50	Drop Probability
1	1	2	□	0	50	Drop Probability
1	1	3	□	0	50	Drop Probability
1	2	1	□	0	50	Drop Probability
1	2	2	□	0	50	Drop Probability
1	2	3	□	0	50	Drop Probability
1	3	1	□	0	50	Drop Probability
1	3	2	□	0	50	Drop Probability
1	3	3	□	0	50	Drop Probability
1	4	1	□	0	50	Drop Probability
1	4	2	□	0	50	Drop Probability
1	4	3	□	0	50	Drop Probability
1	5	1	□	0	50	Drop Probability
1	5	2	□	0	50	Drop Probability
1	5	3	□	0	50	Drop Probability
1	6	1	□	0	50	Drop Probability
1	6	2	□	0	50	Drop Probability
1	6	3	□	0	50	Drop Probability
1	7	1	□	0	50	Drop Probability
1	7	2	□	0	50	Drop Probability
1	7	3	□	0	50	Drop Probability
2	0	1	□	0	50	Drop Probability
2	0	2	□	0	50	Drop Probability
2	0	3	□	0	50	Drop Probability
2	1	1	□	0	50	Drop Probability
2	1	2	□	0	50	Drop Probability
2	1	3	□	0	50	Drop Probability

Group: This column shows the group number. There are three groups for WRED configuration.

Queue: The queue number.

DPL: The Drop Precedence level the selected group and queue.

Enable: Select the checkbox to enable RED on a particular queue.

Min. threshold: Specify the lowest RED threshold. If the average queue filling level is below this threshold, the drop probability is zero. This valid value for this field is 0~100.

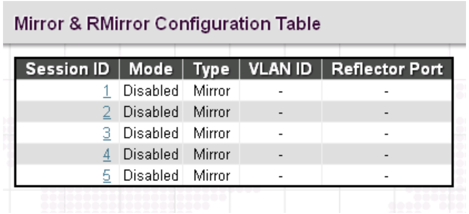
Max. DP 1: Controls the drop probability for the frames when the average queue filling level is 100%. The valid value is 1~100.

Max Unit: Select the item for Max. Unit. Possible values are:

Drop Probability: Max controls the drop probability just below 100% fill level.

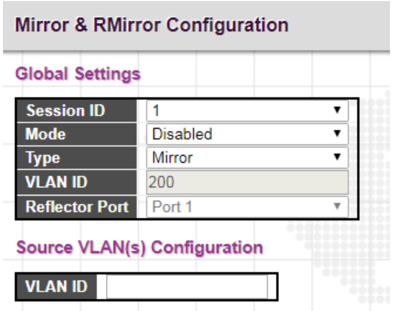
Fill Level: Max controls the fill level where drop probability reaches 100%.

4.18. Mirroring



Mirror & RMirror Configuration Table

Session ID	Mode	Type	VLAN ID	Reflector Port
1	Disabled	Mirror	-	-
2	Disabled	Mirror	-	-
3	Disabled	Mirror	-	-
4	Disabled	Mirror	-	-
5	Disabled	Mirror	-	-



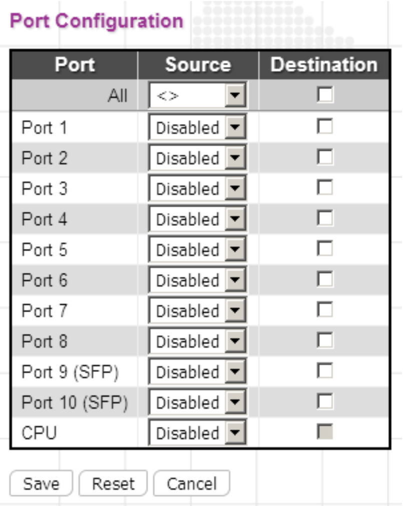
Mirror & RMirror Configuration

Global Settings

Session ID	1 ▾
Mode	Disabled ▾
Type	Mirror ▾
VLAN ID	200
Reflector Port	Port 1 ▾

Source VLAN(s) Configuration

VLAN ID	



Port Configuration

Port	Source	Destination
All	<>	□
Port 1	Disabled	□
Port 2	Disabled	□
Port 3	Disabled	□
Port 4	Disabled	□
Port 5	Disabled	□
Port 6	Disabled	□
Port 7	Disabled	□
Port 8	Disabled	□
Port 9 (SFP)	Disabled	□
Port 10 (SFP)	Disabled	□
CPU	Disabled	□

Mirroring is a feature for switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

Remote Mirroring is an extend function of Mirroring. It can extend the destination port in other switch. So the administrator can analyze the network traffic on the other switches.

If you want to get the tagged mirrored traffic, you have to set VLAN egress tagging as "Tag All" on the reflector port. On the other hand, if you want to get untagged mirrored traffic, you have to set VLAN egress tagging as "Untag ALL" on the reflector port.

Session ID: Select session id to configure.

Mode: Enable or disable the mirror or Remote Mirroring function.

Type: Select switch type.

> **Mirror:** The switch is running on mirror mode. The source port(s) and destination port are located on this switch.
>
> **RMirror source:** The switch is a source node for monitor flow. The source port(s), reflector port are located on this switch.
>
> **RMirror destination:** The switch is an end node for monitor flow. The destination port(s) is located on this switch.

VLAN ID: The VLAN ID points out where the monitor packet will copy to. The default VLAN ID is 200.

Reflector Port: The reflector port is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled.

If you shut down a port, it cannot be a candidate for reflector port.
If you shut down the port which is a reflector port, the remote mirror function cannot work.

Note1: The reflector port needs to select only on Source switch type.

Note2: The reflector port needs to disable MAC Table learning and STP.

Note3: The reflector port only supports on pure copper ports.

Port Configuration

Port: The logical port for the settings contained in the same row.

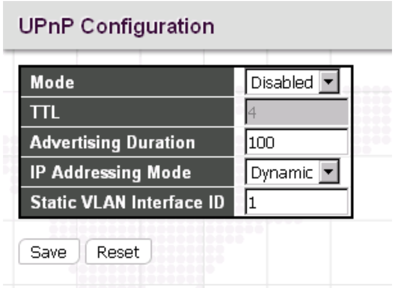
Source: Select mirror mode.

> **Disabled:** Neither frames transmitted nor frames received are mirrored.
>
> **Both:** Frames received and frames transmitted are mirrored on the Destination port.
>
> **Rx only:** Frames received on this port are mirrored on the Destination port. Frames transmitted are not mirrored.
>
> **Tx only:** Frames transmitted on this port are mirrored on the Destination port. Frames received are not mirrored.

Destination: Select destination port. This checkbox is designed for mirror or Remote Mirroring. The destination port is a switched port that you receive a copy of traffic from the source port.

> Note1: On mirror mode, the device only supports one destination port.
>
> Note2: The destination port needs to disable MAC Table learning.

4.19. UPnP



UPnP Configuration

Mode	Disabled
TTL	4
Advertising Duration	100
IP Addressing Mode	Dynamic
Static VLAN Interface ID	1

Mode: Enable or disable UPnP operation.

TTL: TTL (Time to live) is used to configure how many steps an UPnP advertisement can travel before it disappears.

Advertising Duration: This defines how often an UPnP advertisement is sent. The duration is carried in Simple Service Discover Protocol (SSDP) packets which informs a control point how often it should receive a SSDP advertisement message from the switch. By default, the advertising duration is set to 100 seconds. However, due to the unreliable nature of UDP, it is recommended to set to the shorter duration since the shorter the duration, the fresher is UPnP status.

IP Addressing Mode: IP addressing mode provides two ways to determine IP address assignment:

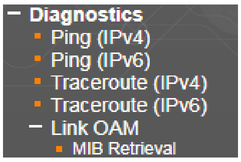
> **Dynamic:** Default selection for UPnP. UPnP module helps users choosing the IP address of the switch device. It

finds the first available system IP address.

Static: User specifies the IP interface VLAN for choosing the IP address of the switch device.

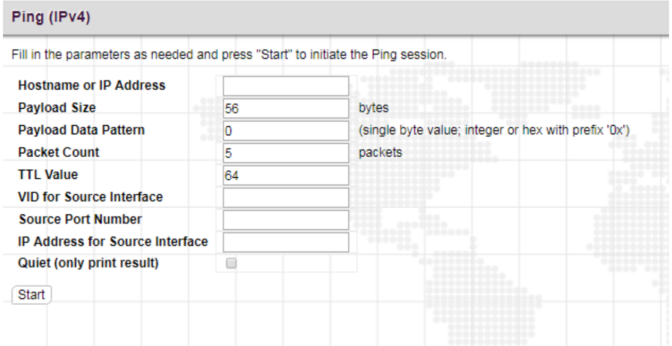
Static VLAN Interface ID: The index of the specific IP VLAN interface. It will only be applied when IP Addressing Mode is static. Valid configurable values range from 1 to 4095. Default value is 1.

4.20. Diagnostics



4.20.1. Ping (IPv4)

This Ping function is for ICMPv4 packets.



Ping (IPv4)

Fill in the parameters as needed and press "Start" to initiate the Ping session.

Hostname or IP Address		
Payload Size	56	bytes
Payload Data Pattern	0	(single byte value; integer or hex with prefix '0x')
Packet Count	5	packets
TTL Value	64	
VID for Source Interface		
Source Port Number		
IP Address for Source Interface		
Quiet (only print result)	□	

Start

Hostname or IP Address: Enter the destination hostname or IP address that you wish to ping.

Payload Size: Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.

Payload Data Pattern: Determines the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

Packet Count: Determines the number of PING requests sent. The default value is 5. The valid range is 1-60.

TTL Value: Determines the Time-To-Live (TTL) field value in the IPv4 header. The default value is 64. The valid range is 1-255.

VID for Source Interface: This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

Source Port Number: This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the Source Port Number or the IP Address for the source interface.

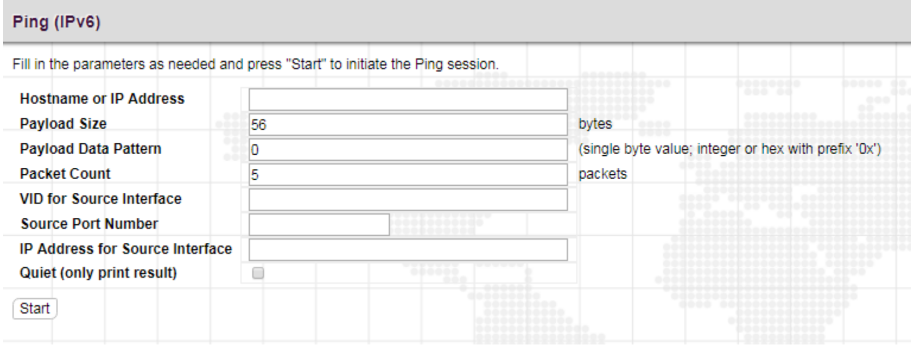
IP Address for Source Interface: This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

Quiet (only print result): Checking this option will not print the result of each ping request but will only show the final result.

After you press Start button , ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

4.20.2. Ping (IPv6)



Ping (IPv6)

Fill in the parameters as needed and press "Start" to initiate the Ping session.

Hostname or IP Address		
Payload Size	56	bytes
Payload Data Pattern	0	(single byte value; integer or hex with prefix '0x')
Packet Count	5	packets
VID for Source Interface		
Source Port Number		
IP Address for Source Interface		
Quiet (only print result)	□	

Hostname or IP Address: Enter the destination hostname or IP address that you wish to ping.

Payload Size: Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.

Payload Data Pattern: Determines the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

Packet Count: Determines the number of PING requests sent. The default value is 5. The valid range is 1-60.

VID for Source Interface: This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

Source Port Number: This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the Source Port Number or the IP Address for the source interface.

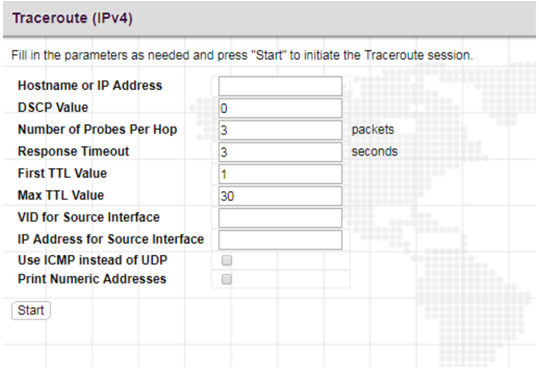
IP Address for Source Interface: This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

Quiet (only print result): Checking this option will not print the result of each ping request but will only show the final result.

After you press Start button , ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

4.20.3. Traceroute (IPv4)



Traceroute (IPv4)

Fill in the parameters as needed and press "Start" to initiate the Traceroute session.

Hostname or IP Address		
DSCP Value	0	
Number of Probes Per Hop	3	packets
Response Timeout	3	seconds
First TTL Value	1	
Max TTL Value	30	
VID for Source Interface		
IP Address for Source Interface		
Use ICMP instead of UDP	□	
Print Numeric Addresses	□	

This page allows you to perform a traceroute test over IPv4 towards a remote host. traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network.

Hostname or IP Address: The destination IP Address.

DSCP Value: This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-63.

Number of Probes Per Hop: Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

Response Timeout: Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.

First TTL Value: Determines the value of the Time-To-Live (TTL) field in the IPv4 header in the first packet sent. The default number is 1. The valid range is 1-30.

Max TTL Value: Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.

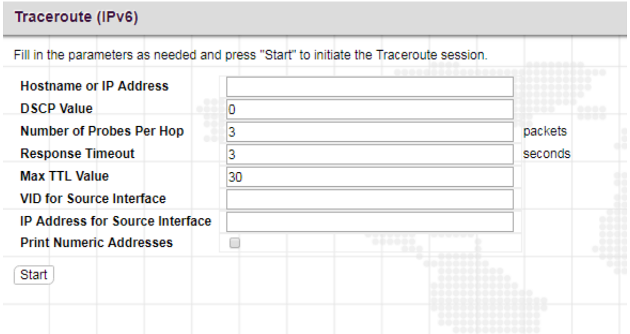
VID for Source Interface: This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

IP Address for Source Interface: This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

Use ICMP instead of UDP: By default, the traceroute command will use UDP datagrams. Selecting this option forces it to use ICMP ECHO packets instead.

Print Numeric Addresses: By default the traceroute command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

4.20.4. Traceroute (IPv6)



Traceroute (IPv6)

Fill in the parameters as needed and press "Start" to initiate the Traceroute session.

Hostname or IP Address		
DSCP Value	0	
Number of Probes Per Hop	3	packets
Response Timeout	3	seconds
Max TTL Value	30	
VID for Source Interface		
IP Address for Source Interface		
Print Numeric Addresses	□	

This page allows you to perform a traceroute test over IPv4 towards a remote host. traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network.

Hostname or IP Address: The destination IPv6 Address.

DSCP Value: This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-63.

Number of Probes Per Hop: Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

Response Timeout: Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.

Max TTL Value: Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.

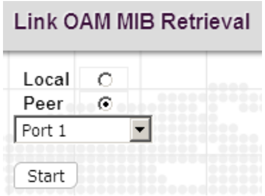
VID for Source Interface: This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

IP Address for Source Interface: This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.

Print Numeric Addresses: By default the traceroute command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

4.20.5. Link OAM

4.20.5.1. MIB Retrieval



Link OAM MIB Retrieval

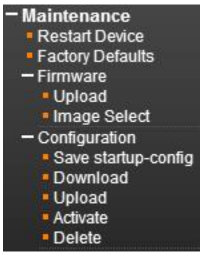
Local ○
Peer ●
Port 1

Local or Peer: Click on the radio button to select the location of MIB to be polled.

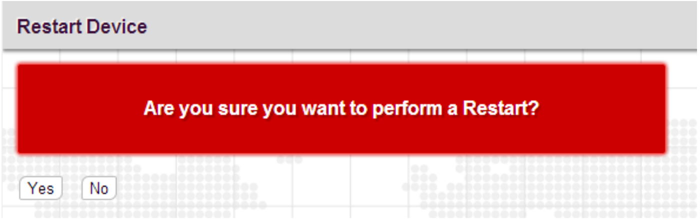
Port: The port on the device that is used for OAM MIB retrieval.

4.21. Maintenance

The “Maintenance” menu contains several sub menus. Select the appropriate sub menu to restart the device, set the device to the factory default or upgrade firmware image.



4.21.1. Restart Device

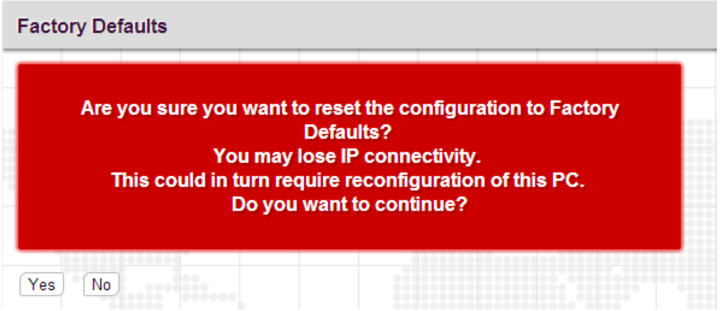


Restart Device

Are you sure you want to perform a Restart?

Click “Yes” button to reboot the switch.

4.21.2. Factory Defaults



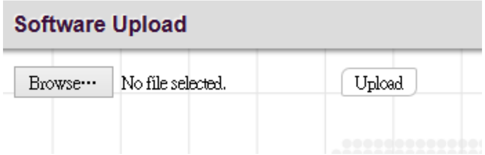
Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?
You may lose IP connectivity.
This could in turn require reconfiguration of this PC.
Do you want to continue?

Click “Yes” button to reset your device to factory defaults settings. Please note that all changed settings will be lost. It is recommended that a copy of the current configuration is saved to your local device.

4.21.3. Firmware

4.21.3.1. Upload



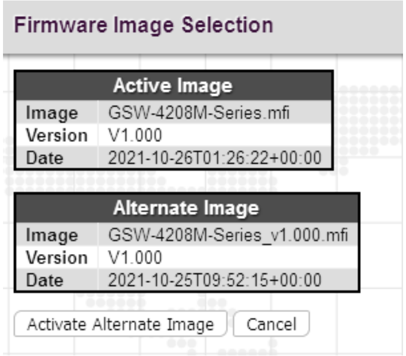
Software Upload

No file selected.

Update the latest Firmware file.

Select a Firmware file from your local device and then click “Upload” to start updating.

4.21.3.2. Image Select



Firmware Image Selection

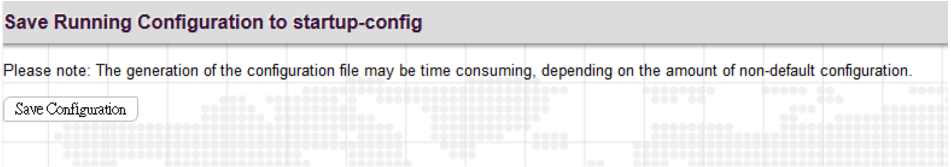
Active Image	
Image	GSW-4208M-Series.mfi
Version	V1.000
Date	2021-10-26T01:26:22+00:00

Alternate Image	
Image	GSW-4208M-Series_v1.000.mfi
Version	V1.000
Date	2021-10-25T09:52:15+00:00

Select the image file to be used in this device.

4.21.4. Configuration

4.21.4.1. Save

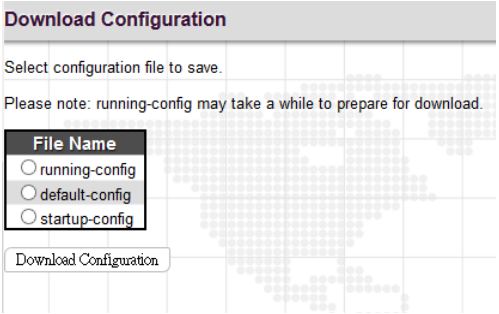


Save Running Configuration to startup-config

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

Click on the “Save Configuration” button to save current running configurations to startup configurations.

4.21.4.2. Download



Download Configuration

Select configuration file to save.

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

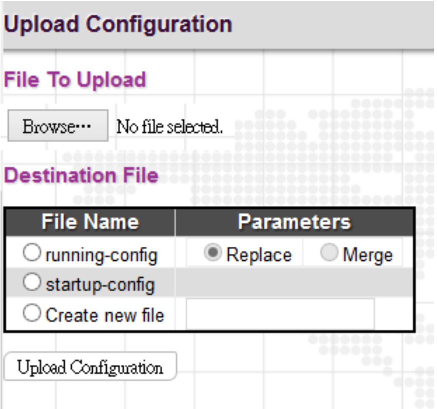
File Name
○ running-config
○ default-config
○ startup-config

running-config: Download a copy of the current running configurations to your local device.

default-config: Download a copy of the factory default configurations to your local device.

startup-config: Download a copy of startup configurations to your local device.

4.21.4.3. Upload



Upload Configuration

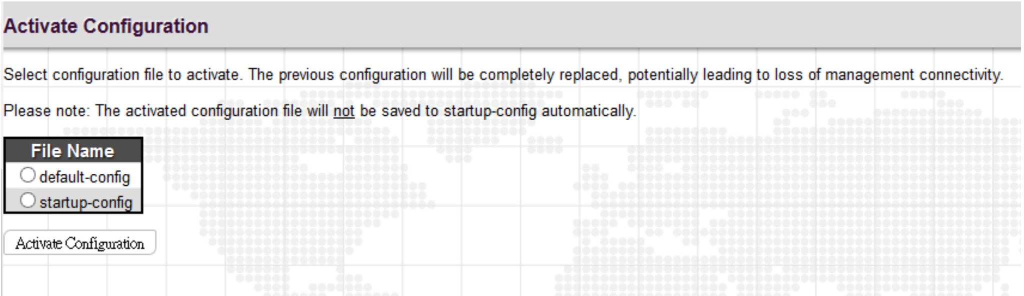
File To Upload

Destination File

File Name	Parameters	
○ running-config	● Replace	○ Merge
○ startup-config		
○ Create new file		

Select a file and then click “Upload Configuration” to start uploading the file.

4.21.4.4. Activate



Activate Configuration

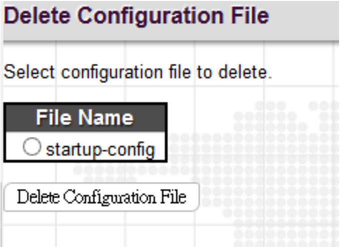
Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

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

File Name
○ default-config
○ startup-config

Select the file that you would like to use. Click on the “Activate Configuration” to replace configurations to the selected one.

4.21.4.5. Delete



Delete Configuration File

Select configuration file to delete.

File Name
○ startup-config

Select the file that you would like to delete. Click on the “Delete Configuration File” to remove the file from the device.

This page is intentionally left blank.

www.ctcu.com

T +886-2 2659-1021 **F** +886-2 2659-0237 **E** sales@ctcu.com