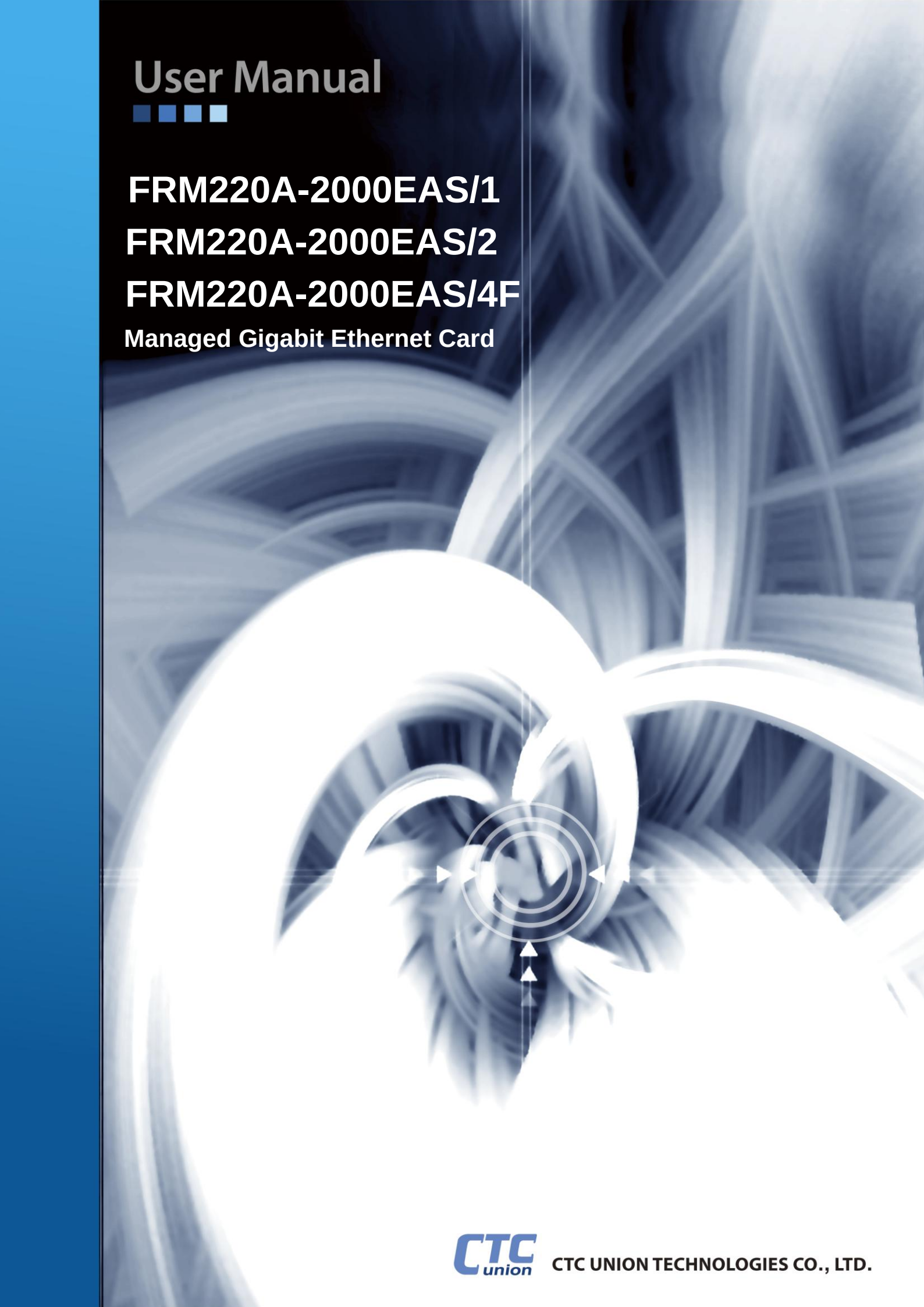
User Manual

FRM220A-2000EAS/1
FRM220A-2000EAS/2
FRM220A-2000EAS/4F

Managed Gigabit Ethernet Card



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.

User Manual
Version 0.9 (Preliminary) June 2021

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 this product from CTC Union. 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 introduce this series including features and specifications. Chapter 2 will describe the panels and LED indicators. All the models in this series utilize almost identical management interfaces, whether Console, Telnet, SSH, HTTP (Web GUI) or SNMP (Simple Network Management Protocol). Chapter 3 will cover the basic operation using Console or Telnet CLI. Chapter 4 will detail all of the configuration settings by using an easy to point and click Web GUI interface which can be accessed from any available web browser.

1.2 Product Description

FRM220A-2000EAS/1, /2 & /4F are Managed Gigabit Ethernet switch cards designed to make conversion between 10/100/1000Base-T RJ-45 and 100/1000Base-X fiber optics with SFP optical modules (FRM220A-2000EAS/1 & /2) or to simply transmist over SFP fiber optics (FRM220A-2000EAS/4F). Traditionally, transmission distance of Gigabit Ethernet over fiber interface can be extended from 550m to 100km using the flexibility of pluggable SFP modules.

FRM220A-2000EAS/1, /2 & /4F are 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 via 10/100/1000Base-T twisted pair to the RJ-45 ports of the switch cards (FRM220A-2000EAS/1 & FRM220A-2000EAS/2). No Ethernet crossover cables are required and link status can be easily monitored from the comprehensive LED display.

When FRM220A-2000EAS/1, /2 & /4F are deployed as stand-alone switches, they incorporate an easy-to-use Web user interface for operation, administration and maintenance both locally and remotely. All of the enabled Layer 2 features and functions can be configured and monitored via web interface and SNMP management.

1.3 Product Features

- 1 x 10/100/1000Base-T(X) RJ-45 with 1 x 100/1000Base-X SFP Fiber (FRM220A-2000EAS/1)
- 2 x 10/100/1000Base-T(X) RJ-45 with 2 x 100/1000Base-X SFP Fiber (FRM220A-2000EAS/2)
- 4 x 100/1000Base-X SFP Fiber (FRM220A-2000EAS/4F)
- Standalone IP Based, Web GUI, Telnet and SNMP management
- Supports dying gasp
- Supports Cisco® like CLI
- Online local / remote F/W upgrade
- Supports local / remote IEEE 802.3ah OAM / IP management
- Support advanced functions such as 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,Dynamic IEEE 802.3ad LACP Link Aggregation, Static Link Aggregation

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 802.1Q	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 802.1w	RSTP
Switch	VLAN Groups	up to 4096
	Data Processing	Store and Forward
	Flow Control	IEEE 802.3x for full duplex mode, back pressure for half duplex mode
	MTU	9600 Bytes (Jumbo Frames)
	MAC Table	8K
	Packet Buffer	4M bits
Connectors	LAN	FRM220A-2000EAS/1: 1 x RJ-45 10/100/1000BaseT(X) FRM220A-2000EAS/2: 2 x RJ-45 10/100/1000BaseT(X) Auto detect speed, auto negotiate duplex, auto MDI/MDI-X function, Full/Half duplex
	Fiber	FRM220A-2000EAS/1: 1 x 100/1000Base-X dual speed mode SFP slot, supporting DDMI FRM220A-2000EAS/2: 2 x 100/1000Base-X dual speed mode SFP slot, supporting DDMI FRM220A-2000EAS/4F: 4x 100/1000Base-X dual speed mode SFP slot, supporting DDMI
Ethernet	Network Cable	UTP/STP Cat.5e cable or above
	EIA/TIA-568	100-ohm (100m)
	Protocol	CSMA/CD
Power	Power Input	12VDC
Power Consumption		8W
Weight		130g
Dimensions		159.5mm (D) x 20.8mm (W) x 88mm (H)

CHAPTER 2. Panels, LED & Installation

2.1 Overview for Front Panel

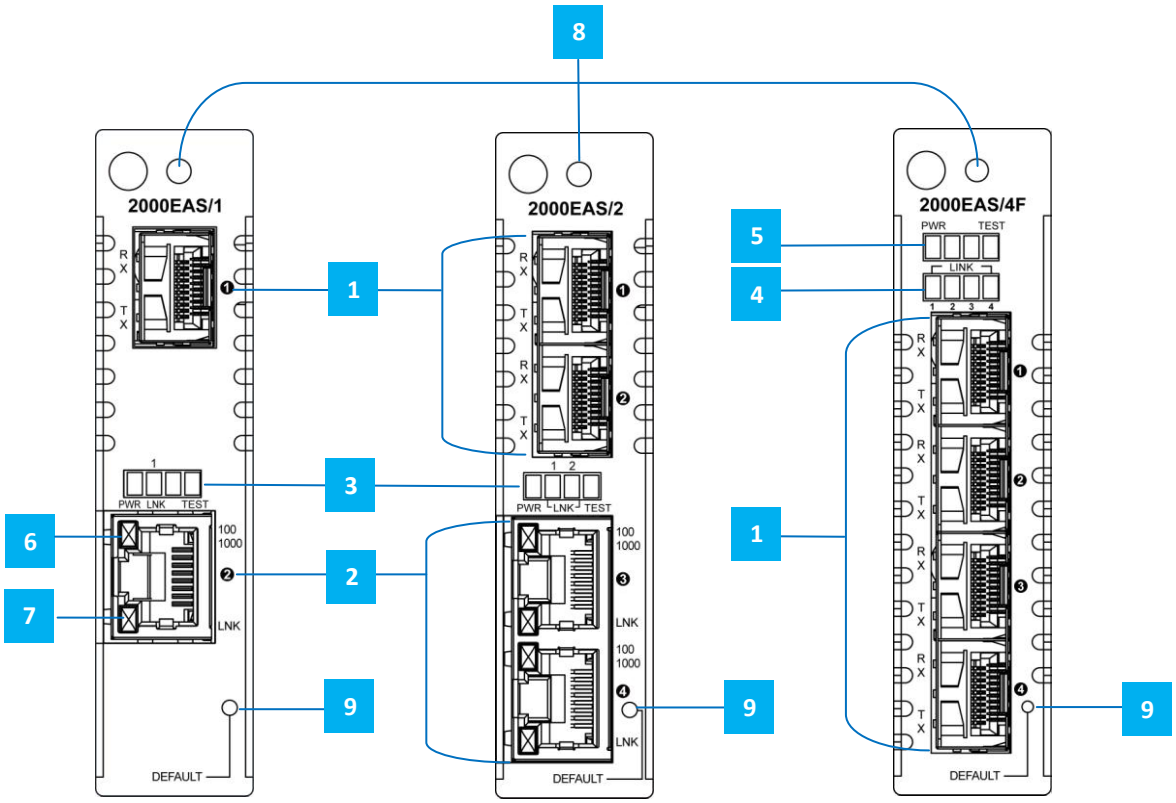


Figure 1. Front Panel of FRM220A-2000EAS/1

Figure 2. Front Panel of FRM220A-2000EAS/2

Figure 3. Front Panel of FRM220A-2000EAS/4F

1	SFP Slots	6	RJ-45 Speed LED indicators for FRM220A-2000EAS/1 & /2
2	RJ-45 LAN Ports	7	RJ-45 Link LED indicators for FRM220A-2000EAS/1 & /2
3	Power, Test, Fiber Link LED indicators for FRM220A-2000EAS/1 & /2	8	Thumb screw
4	Fiber Link LED indicators for FRM220A-2000EAS/4F	9	Reset-to-Default Push Button
5	Power & Test LED indicators for FRM220A-2000EAS/4F		

2.2 Chassis Option

FRM220A-2000EAS/1, /2 & /4F switch card can be placed in any **FRM220** & **FRM220A** series chassis, including the single slot CH-01M, two-slot CH02M or CH02-NMC or the full twenty slot CH-20 chassis. Chassis with built-in power are available with single AC (100~240VAC), single DC (18~72VDC), dual AC, dual DC or AC plus DC combo. The single slot chassis with external power adapter works with AC source voltage only with the provided 100~240VAC 12VDC@1A switching adapter.

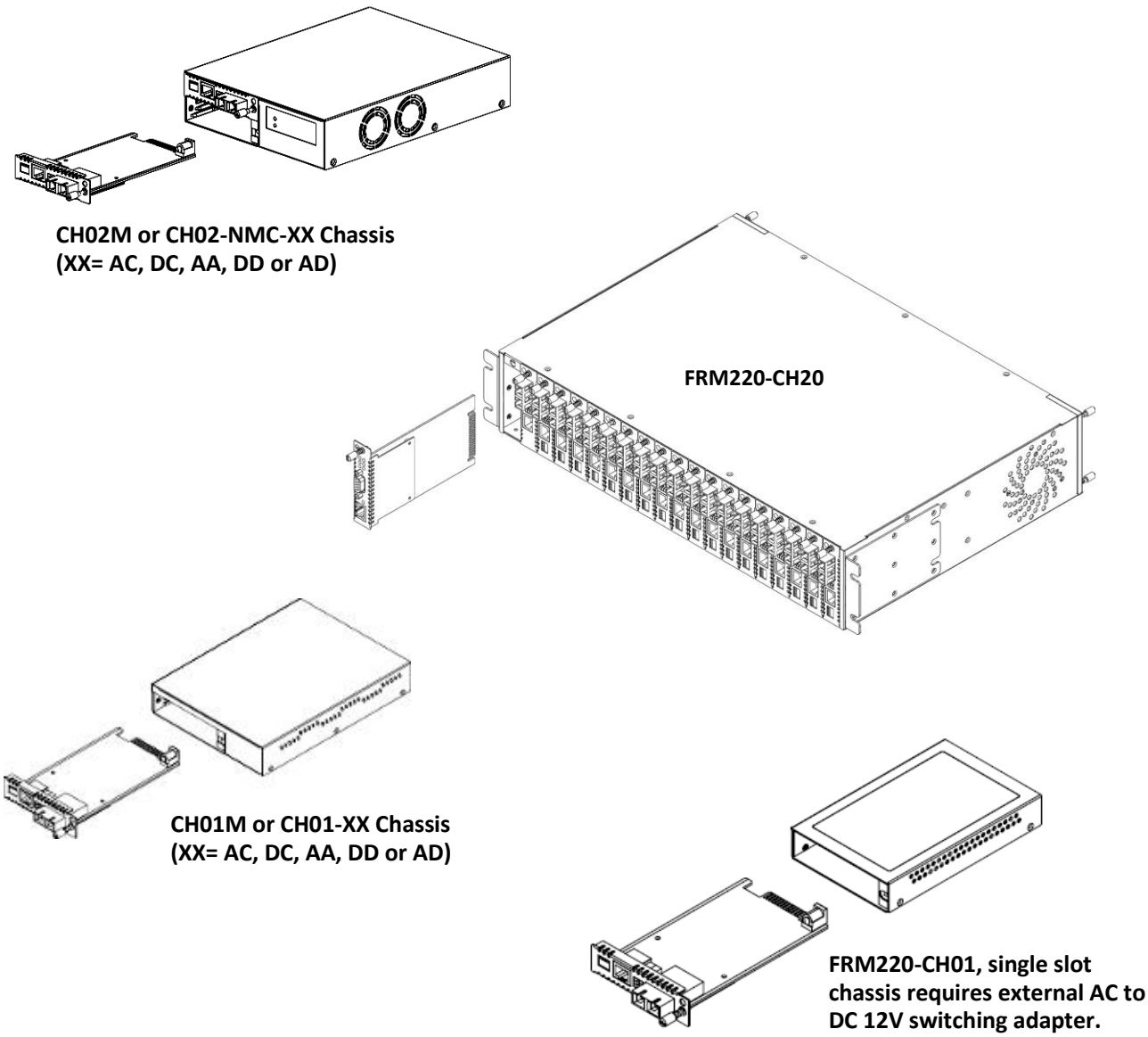


Figure 2. Chassis Options for FRM220A-2000EAS/1, /2 & /4F Card

2.3 Default Push-Button

Function	Press and hold for~	LED Status	Description
Reset to factory defaults	> 6 seconds	Test LED blinks	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.

2.4 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	Description
PWR	Green	On	The switch is receiving power.
		Off	The switch does not receive power or is in standby mode.
Fiber LNK 1 (FRM220A-2000EAS/1) or Fiber LNK 1 & 2 (FRM220A-2000EAS/2) or Fiber LNK 1~4 (FRM220A-2000EAS/4F)	Green	On	The fiber port link is up.
		Blinking	The fiber port is receiving and transmitting traffic.
		Off	The fiber port link is down.
RJ-45 1000/100 (FRM220A-2000EAS/1 and /2)	Green	On	When the LAN port is up and operating at 100Mbps.
		Off	The LAN port link is down.
	Amber	On	When the LAN port is up and operating at 1000Mbps.
		Off	The LAN port link is down.
RJ-45 LNK (FRM220A-2000EAS/1 and /2)	Green	Blinking	The LAN port is receiving and transmitting traffic.
Test	Red	On	1. Loopback function is enabled (set to Far-End or Near-End in Loopback menu). 2. Loopback operation is enabled (Link OAM menu). 3. Rest to default settings. Press Default push button for over 6 seconds, then the Test LED will blink once.
		Off	Normal operation.

Chapter 3 Command Line Interface (CLI) Provisioning

3.1 Introduction

This chapter will go into the details of the specific provisioning and operation of the FRM220A-2000EAS/1, /2 & /4F. Broken into two chapters, this chapter outlines the procedures and functions when using the telnet/SSH or local terminal console for configuration. The next chapter will outline the operation when using a network connection, including the Web-based GUI management.

All of the features and controls described in this chapter require the FRM220 chassis to have the switch card installed. This will allow remote network configuration to proceed from console, Telnet/SSH connection (remote console), web browser or any network management software after compiling the enterprise MIB-II compliant file for FRM220A-2000EAS/1, /2 and /4F. A MIB browser provides another simple platform for the user to setup using the SNMP protocol remotely.

3.2 Access Connection

3.2.1 Telnet Operation

To use Command Line Interface (CLI), you can choose to access the device through a Telnet/SSH connection via TCP/IP network over Ethernet ports. For initial operation, use the default TCP/IP settings (10.1.1.1) to login to the device. This device supports up to 16 simultaneous Telnet sessions. Each session will disconnect automatically after a period of idle time specified by exec-timeout command.

Default TCP/IP settings:

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

3.2.2 Console Operation

Install the card to FRM220 chassis with a CONSOLE port. Then, connect the "CONSOLE" port to the PC terminal communications port (DB9) using DB9 console cable. 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:
Login in progress...
Welcome to CCLI (v1.2).
Type 'help' or '?' to get help.
>
```

3.3 CLI Modes

The Command Line Interface (CLI) of this device 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, logout
Global Config Mode	(config)#	Enter "configure terminal" after "#"	End, exit, do logout
Config Interface Mode	(config-if)#	Specify interface, interface type and number after (config)#	End, exit, do logout

Apart from the basic and common modes mentioned above, there are other modes under Global Config Mode available that allow you to set up settings and profiles of advanced features.

Mode	Prompt	Enter Method	Exit Method
Config Interface VLAN mode	(config-if-vlan)#	(config)# interface vlan <vlist>	exit, end, do logout
Config Line mode	(config-line)#	(config)# line { <0~16> | console 0 | vty <0~15> }	exit, end, do logout
Config Aggregation mode	(config-stp-aggr)#	(config)# spanning-tree aggregation	exit, end, do logout
Config IPMC Profile Mode	(config-ipmc-profile)#	(config)# ipmc profile <profile_name>	exit, end, do logout

3.4 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.

3.5 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 uter curly bracket means that this is a must parameter. At leaset 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.

3.6 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 3.7, 3.8, 3.9.

3.6.1 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
Interface       Address                 Method   Status
--------------- ------------------------  ----------  ---------
VLAN 1          192.168.0.101/24    Manual   DOWN
```

3.6.2 Enter Config Interface Mode

- Enter Port 3's Config Interface mode.

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

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

- 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 1~2 & Port 4's Config Interface mode.

```
# config terminal
(config)# interface GigabitEthernet 1/1-2,4
(config-if)#
```

Note: 1/1-2,4 means Ethernet Interface 1, Port 1 to Port 2 and Port 4.

3.6.3 Save Configurations

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

3.6.4 Restart the Device

```
# reload cold
% Warm 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
```

3.6.5 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.
```

3.6.6 Show System and Software Information

```
#  show version

MEMORY          : Total=77679 KBytes, Free=51457 KBytes, Max=51417 KBytes
MAC Address     : 00-02-ab-00-00-01
Previous Restart : Cold

System Contact  :
System Name     :
System Location :
System Time     : 2017-01-01T00:28:35+00:00
System Uptime   : 00:28:39

Active Image
------------------
Image           :
Version         :
Date            : 2021-01-07T10:09:18+08:00

Alternative Image
------------------
Image           :
Version         :
Date            : 2021-01-07T10:09:18+08:00
```

```
------------------
Port Count          :5
Product             : CTCU 2000EAS/2 Switch
Software Version    : 1.002
Build Date          : 2021-01-07 T15:21:33+08:00
-------------------
#
```

3.6.7 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
```

3.6.8 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
```

3.6.9 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?'.)
```

3.6.10 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
```

3.7 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.

3.7.1 > clear ip arp

Syntax: > clear ip arp

Explanation: Clear ARP cache.

3.7.2 > clear statistics

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

<port_type>: Specify the interface type.

[<v_port_type_list>: Specify the ports that you want to clear.

Explanation: Clear statistics of the specified interfaces.

3.7.3 > enable

Syntax: > enable [<new_priv>]

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

Explanation: Enter the EXEC mode.

3.7.4 > exit

Syntax: > exit

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

3.7.5 > help

Syntax: > help

Explanation: Provide help messages.

3.7.6 > logout

Syntax: > logout

Explanation: Logout the Command Line Interface.

3.7.7 > ping ip

Syntax: > ping ip <v_ip_addr> [repeat <count>] [size <size>] [interval <seconds>]

<v_ip_addr>: Specify IPv4 address that you want to ping.

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

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

[interval <seconds>]: Timeout interval. The ping test is successful only when it receives echo reply from the destination IP or host within the time specified here.

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

3.7.8 > ping ipv6

Syntax: > ping ipv6 <v_ipv6_addr> [repeat <count>] [size <size>] [interval <seconds>] [interface vlan <v_vlan_id>]

<v_ipv6_addr>: Specify IPv6 address that you want to ping.

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

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

[interval <seconds>]: Timeout interval. The ping test is successful only when it receives echo reply from the destination IP or host within the time specified here.

[interface vlan <v_vlan_id>]:

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

3.7.9 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”.

3.8 Commands in EXEC Mode

3.8.1 # clear access management statistics

Syntax: # clear access management statistics

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

3.8.2 # clear access-list ace statistics

Syntax: # clear access-list ace statistics

Explanation: Clear access list entry statistics.

3.8.3 # clear ip arp

Syntax: # clear ip arp

Explanation: Clear ARP cache.

3.8.4 # 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.

3.8.5 # clear ipv6 neighbors

Syntax: # clear ipv6 neighbors

Explanation: Clear the table for IPv6 neighbors.

3.8.6 # 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.

3.8.7 # clear lacp statistics

Syntax: # clear lacp statistics

Explanation: Clear LACP statistics.

3.8.8 # clear logging

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

Explanation: Clear specific syslog events.

3.8.9 # clear mac address-table

Syntax: # clear mac address-table

Explanation: Clear MAC address table.

3.8.10 # 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.

3.8.11 # clear statistics

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

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

3.8.12 # config terminal

Syntax: # config terminal

Explanation: Enter the Global Config mode.

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

3.8.13 # 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.

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

Explanation: Save startup configurations to running 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.
```

3.8.14 # 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.
```

3.8.15 # 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 files, 3258 bytes total.
```

3.8.16 # disable & # enable

Explanation: Return to user mode or enter exec mode.

```
# disable
>
>
> enable
#
#
# enable 0
>
```

3.8.17 # firmware swap

Syntax: # firmware swap

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

3.8.18 # firmware upgrade

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

<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
```

3.8.19 # ip dhcp retry interface vlan

Syntax: # ip dhcp retry interface vlan <vlan_id>

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

Explanation: Restart the DHCP query process.

3.8.20 # ipv6 dhcp-client restart

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

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

Explanation: Restart the IPv6 client service.

3.8.21 # more

Syntax: # more <path>

<path>: Specify the filename.

Explanation: Display file in Flash or in TFTP server.

3.8.22 # ping ip

Syntax: # ping ip <v_ip_addr> [repeat <count>] [size <size>] [interval <seconds>]

Explanation: Ping the specified IP.

Parameters:

<addr>: Specify the IPv4 address for ping test.

3.8.23 # ping ipv6

Syntax: #ping ipv6 <v_ipv6_addr> [repeat <count>] [size <size>] [interval <seconds>] [interface vlan <v_vlan_id>]

< v_ipv6_addr >: Specify the IPv6 address for ping test.

Explanation: Ping the specified IPv6 address.

Parameters:

[repeat <count>]: The number of echo packets will be sent.

[size <size>]: The size or length of echo packets.

[interval <seconds>]: The time interval between each ping request.

[interface vlan <v_vlan_id>]: Specify the VLAN ID.

3.8.24 # reload cold

Syntax: # reload cold

Explanation: Perform a warm restart on the system.

3.8.25 # reload defaults

Syntax: # reload defaults [keep-ip]

Parameters:

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

Explanation: Restore the device to factory default settings.

3.8.26 # 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.

3.8.27 # terminal editing

Syntax: # terminal editing

Explanation: Enable command line editing.

Show: > show terminal
show terminal

Negation: # no terminal editing

3.8.28 # 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

3.8.29 # 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

3.8.30 # 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

3.8.31 # 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

3.8.32 # no port-security shutdown

Syntax: # no port-security shutdown [interface (<port_type>[<v_port_type_list>])]

Explanation: Reopen ports that are shutdown or disabled by Port Security function.

Parameters:

[interface (<port_type>[<v_port_type_list>])]: Specify the port type and port numbers that you want to reopen.

3.8.33 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”.

3.9 Commands in Config Mode

3.9.1 (config)# aaa

3.9.1.1 (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

3.9.1.2 (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

3.9.1.3 (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

3.9.2 (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

3.9.3 (config)# access-list

3.9.3.1 (config)# access-list ace

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

1. Frame Type : Any

(config)# access-list ace [update] <ace_id> [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 **any** [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 [update] <ace_id> [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 [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. Frmae Type: IPv4/ipv4-icmp/ipv4-udp/ipv4-tcp

access-list ace [update] <ace_id> [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

access-list ace [update] <ace_id> [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:

<AceId : 1-128>: 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 : 1-256>|last}]: Insert the current ACE ID before the next ACE ID or put the ACE ID to the last one.

[policy <PolicyId : 0-63>]: 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>]]

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

Clear: # clear access-list ace statistics

3.9.3.2 (config)# access-list rate-limiter

Syntax: (config)# access-list rate-limiter [<rate_limiter_list>] { pps <pps_rate> | 100pps <pps100_rate> | kpps <kpps_rate> | 100kbps <kpbs100_rate> }

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

Parameters:

[<rate_limiter_list>]: Specify the “rate limit ID”, “100kbps” or “pps” . The allowed rate limit ID range is from1~16.

{ pps <pps_rate> | 100pps <pps100_rate> | kpps <kpps_rate> | 100kbps <kpbs100_rate> }: Specify the rate limit rate.

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

3.9.3.3 (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>])]]

3.9.3.4 (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

3.9.3.5 (config-if)# access-list mirror

Syntax: (config-if)# access-list mirror

Explanation: Enable a specific port's mirroring function on a ACL-based. 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

3.9.3.6 (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

3.9.3.7 (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

3.9.3.8 (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

3.9.3.9 (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

3.9.3.10 (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 this port's frames to the specified port.

Negation: (config-if)# no access-list redirect

3.9.4 (config)# aggregation

3.9.4.1 (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]

3.9.4.2 (config-if)# aggregation group

Syntax: (config-if)# aggregation group <unit>

Explanation: Add this specific interface to the specified aggregation group.

Parameters:

<unit>: Specify the aggregation group ID.

Negation: (config-if)# no aggregation group

Show: # show aggregation [mode]

3.9.5 (config)# banner

3.9.5.1 (config)# banner [motd] <banner>

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

Parameters:

[motd]: Type in the message of the day.

Explanation: Configure the message of the day.

Negation: (config)# no banner [motd]

3.9.5.2 (config)# banner exec <banner>

Syntax: (config)# banner exec <banner>

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

Negation: (config)# no banner exec

3.9.5.3 (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

3.9.6 (config)# clock

3.9.6.1 (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

3.9.6.2 (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

3.9.6.3 (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

3.9.7 (config)# default

3.9.7.1 (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
```

3.9.7.2 (config)# default snmp-server community v2c { ro | rw }

Syntax: (config)# default snmp-server community v2c { ro | rw }

Explanation: To default the SNMP server community setting.

Parameters:

{ ro | rw }: Specify "ro" Read only or "rw" Read write level.

3.9.8 (config)# enable

3.9.8.1 (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>]

3.9.8.2 (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>]

3.9.9 (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

3.9.10 (config-if)# flowcontrol { on | off }

Syntax: (config-if)# flowcontrol { on | off }

Explanation: Enable or disable flow confrol 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

3.9.11 (config-if)# frame-length-check

Syntax: (config-if)# frame-length-check

Explanation: 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.

Negation: (config-if)# no frame-length-check

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

3.9.12 (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
AccessSW(Config)#
```

Negation: (config)# no hostname

Show: > show version
show version

3.9.13 (config)# interface

3.9.13.1 (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>]) }

3.9.13.2 (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)#
```

3.9.14 (config)# ip

3.9.14.1 (config)# ip dns proxy

Syntax: (config)# ip dns proxy

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

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

Negation: (config)# no ip dns proxy

3.9.14.2 (config)# ip domain name

Syntax: (config)# ip domain name { <v_domain_name> | <dhcp [ipv4 | ipv6] | [interface <v_vlan_id_dhcp>] }

Explanation: Configure a domain name for this device.

Parameters:

{ <v_domain_name> | <dhcp [ipv4 | ipv6] | [interface <v_vlan_id_dhcp>] }: Specify a domain name manually, or by DHCP or by indicating an interface.

3.9.14.3 (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

3.9.14.4 (config)# ip http secure-certificate

Syntax: (config)# ip http secure-certificate { upload <url_file> [pass-phrase <pass_phrase>] | delete | generate }

Explanation: Upload or generate HTTPs certificate.

Parameters:

{ upload <url_file> [pass-phrase <pass_phrase>] | delete | generate }: Upload a certicate via URL link and protected by a passphrass if necessary. You can also delete or generate a certificate by issuing "delete" or "generate" command.

Show: # show ip http server secure status

3.9.14.5 (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

3.9.14.6 (config)# ip name-server

Syntax: (config)# ip name-server [<order: 0-3>] { <v_ipv4_ucast> | { <v_ipv6_ucast> [interface vlan <v_vlan_id_static>] } | dhcp [ipv4 | ipv6] [interface vlan <v_vlan_id_dhcp>] }

Explanation: Set up DNS IP address manually (IPv4 or IPv6) or obtain DNS IP address via specific VLAN DHCP server.

Parameters:

[<order>]: Specify the number of this name server. The allowed number is 0 through 3.

{ <v_ipv4_ucast> | { <v_ipv6_ucast> [interface vlan <v_vlan_id_static>] } | dhcp [ipv4 | ipv6] [interface vlan <v_vlan_id_dhcp>] }: Specify IPv4, IPv6 or DHCP interface.

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

{ <v_ipv6_ucast> [interface vlan <v_vlan_id_static>] }: Manually specify IPv6 name server address.

dhcp [ipv4 | ipv6] [interface vlan <v_vlan_id_dhcp>]: Configure DNS IP address via specific VLAN DHCP server.

Negation: (config)# no ip name-server <order: 0-3>

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

3.9.14.7 (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

3.9.14.8 (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.*

3.9.14.9 (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

3.9.14.10 (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 }]

3.9.14.11 (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 }]

3.9.14.12 (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>]

3.9.15 (config)# lacp

3.9.15.1 (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.

Example: Enable IPv6 MLD proxy.

```
# 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 }

3.9.15.2 (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

3.9.15.3 (config-if)# lacp key

Syntax: (config-if)# lacp key { <v_1_to_65535> | auto }

Explanation: Configure a LACP key for this interface.

Parameters:

{ <v_1_to_65535> | auto }: Specify a LACP key for this interface. The “auto” setting sets the key as appropriate by the physical link speed. If you want a user-defined key value, enter a value between 1 and 65535. Ports in an aggregated link group must have the same LACP port Key. In order to allow a port to join an aggregated group, the port Key must be set to the same value.

Negation: (config-if)# no lacp key { <v_1_to_65535> | auto }

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

3.9.15.4 (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 }

3.9.15.5 (config-if)# lacp role { active | passive }

Syntax: (config-if)# lacp role { active | passive }

Explanation: Configure LACP role for this interface.

Parameters:

{ active | passive }: Specify either "Active" or "Passive" role depending on the device's capability of negotiating and sending LACP control packets. Ports that are designated as "Active" are able to process and send LACP control frames. Hence, this allows LACP compliant devices to negotiate the aggregated like so that the group may be changed dynamically as required. In order to add or remove ports from the group, at least one of the participating devices must set to "Active" LACP ports.

Negation: (config-if)# no lacp role { active | passive }

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

3.9.15.6 (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 }

3.9.16 (config)# line

3.9.16.1 (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]

3.9.16.2 (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)#
```

3.9.16.3 (config-line)# editing

Syntax: (config-line)# editing

Explanation: Enable command line editing.

Negation: (config-line)# no editing

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

3.9.16.4 (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
#
```

3.9.16.5 (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]

3.9.16.6 (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]

3.9.16.7 (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)#
```

3.9.16.8 (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?'.)
```

3.9.16.9 (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]

3.9.16.10 (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]

3.9.16.11 (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]

3.9.16.12 (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]

3.9.16.13 (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]

3.9.16.14 (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]

3.9.17 (config)# logging

3.9.17.1 (config)# logging on

Syntax: (config)# logging on <id>

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:

<id>: Specify the syslog server ID number. The available ID range is 1~3.

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>]

3.9.17.2 (config)# logging host

Syntax: (config)# logging host <id> { <ipv4_addr> | <domain_name> }

Parameters:

<id>: 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]

3.9.17.3 (config)# logging level

Syntax: (config)# logging level <id> { informational | notice | warning | error }

Explanation: Configure what kind of messages will send to syslog server.

Parameters:

<id>: Specify the log server ID (1~3)

{ 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]

3.9.18 (config)# loop-protect

3.9.18.1 (config)# loop-protect

Syntax: (config)# loop-protect

Explanation: Enable loop protection function.

Example: Enable loop protection function.

```
# config t
(config)# loop-protect
```

Negation: (config)# no loop-protect

Show: # show loop-protect [interface (<port_type> [<plist>])]

3.9.18.2 (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>])]

3.9.18.3 (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>])]

3.9.18.4 (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>])]

3.9.18.5 (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>])]

3.9.18.6 (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>])]

3.9.19 (config)# mac

3.9.19.1 (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

3.9.19.2 (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 1/1-10
```

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

3.9.19.3 (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

3.9.20 (config-if)# mtu

Syntax: (config-if)# mtu <max_length>

Explanation: Configure the maximum transmission unit for this specific interface.

Parameters:

<max_length: 1518-9600>}: Specify the MTU. The range is 1518 to 9600 bytes.

Negation: (config-if)# no mtu

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

3.9.21 (config)# monitor

3.9.21.1 (config)# monitor destination interface

Syntax: (config)# monitor destination interface <port_type> <in_port_type>

Explanation: Configure which port traffic should be mirrored to.

Parameters:

<port_type>: Specify the interface type.

<in_port_type>: Specify the port number.

Example: Set the traffic to be mirrored to Gigabit Ethernet port 3.

```
# config t
(config)# monitor destination interface gigabitethernet 1/3
```

Negation: (config)# no monitor destination

3.9.21.2 (config)# monitor source

Syntax: (config)# monitor source { { interface (<port_type> [<v_port_type_list>]) } | { cpu [<cpu_switch_range>] } } { both | rx | tx }

Explanation: Configure which source ports' RX or TX traffic should be mirrored to the destination port.

Parameters:

{ { interface (<port_type> [<v_port_type_list>]) }: Specify the interface type. * means all interfaces.

{ both | rx | tx }: Specify which direction of traffic should be mirrored to the destination port. "both" means both received and transmitted traffic. "rx" means received traffic. "tx" means transmitted traffic.

Example: Set port 1 to 5's RX traffic to be mirrored to the destination port.

```
# config t
(config)# monitor source interface GigabitEthernet 1/1-5 rx
```

Negation: (config)# no monitor source { { interface (<port_type> [<v_port_type_list>]) } | { cpu [<cpu_switch_range>] } }

3.9.22 (config)# ntp

3.9.22.1 (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

3.9.22.2 (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

3.9.23 (config)# privilege

Syntax: (config)# privilege { exec | configure | config-vlan | line | interface | if-vlan | snmps-host | stp-aggr } 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 | snmps-host | stp-aggr }: 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 that start with the letter "v"

```
# config t
(config)# privilege exec level 15 host
```

Negation: (config)# no privilege { exec | configure | config-vlan | line | interface | if-vlan | snmps-host | stp-aggr } level <0-15> <cmd>

Show: > show privilege
show privilege

3.9.24 (config-if)# pvlan

3.9.24.1 (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>

3.9.24.2 (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>])]

3.9.25 (config)# qos

3.9.25.1 (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>] }]

3.9.25.2 (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 } }

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).

Explanation: Configure the DSCP Ingress classification.

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>] }]

3.9.25.3 (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>] }]

3.9.25.4 (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>] }]

3.9.25.5 (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>] }]

3.9.25.6 (config)# qos qce refresh

Syntax: (config)# qos qce refresh

Explanation: To refresh QCE.

Example: Refresh QCE.

```
# config t
(config)# qos qce refresh
```

3.9.25.7 (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>] }]

3.9.25.8 (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.

```
# config t
(config)# qos storm broadcast 1024 kfps
```

Negation: (config)# no qos storm { unicast | multicast | broadcast }

Show: # show qos storm

3.9.25.9 (config-if)# qos cos

Syntax: (config-if)# qos cos <cos>

Explanation: Configure CoS value on this selecte infterface.

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>] }]

3.9.25.10 (config-if)# qos dei

Syntax: (config-if)# qos dei <dei>

Explanation: Configure DEI (Drop Eligible Indicator) value on this selecte infterface.

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>] }]

3.9.25.11 (config-if)# qos dpl

Syntax: (config-if)# qos dpl <dpl>

Explanation: Configure DPL value on this selecte infterface.

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>] }]

3.9.25.12 (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>] }]

3.9.25.13 (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>] }]

3.9.25.14 (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>] }]

3.9.25.15 (config-if)# qos map cos-tag cos <cos> dpl <dpl> pcp <pcp> dei <dei>

Syntax: (config-if)# qos map cos-tag cos <cos> dpl <dpl> pcp <pcp> dei <dei>

Explanation: Configure (CoS, DPL) to (PCP, DEI level) 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>] }]

3.9.25.16 (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>] }]

3.9.25.17 (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>] }]

3.9.25.18 (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>] }]

3.9.25.19 (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: 1-3276700>: Specify Policer rate in kbps.

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>] }]

3.9.25.20 (config-if)# qos queue-shaper queue

Syntax: (config-if)# qos queue-shaper queue <queue> <rate> [kbps | mbps] [excess] [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: 1-3281943>: Specify Policer rate and rate unit (kbps or mbps).

[excess]: Allow all excess bandwidth.

[rate-type { line | data}]: Specify the rate type. It could be "line" or "data" type.

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>] }]

3.9.25.21 (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: 1-3281943>: Specify Policer rate and rate unit.

[rate-type { line | data }]: Specify the rate type. It could be "line" or "data" type.

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>] }]

3.9.25.22 (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>] }]

3.9.25.23 (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>] }]

3.9.25.24 (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>] }]

3.9.25.25 (config-if)# qos wrr

Syntax: (config-if)# qos wrr <w0> <w1> <w2> <w3> <w4> <w5>

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.

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>] }]

3.9.26 (config)# radius-server

3.9.26.1 (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]

3.9.26.2 (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]

3.9.26.3 (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]

3.9.26.4 (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]

3.9.26.5 (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]

3.9.26.6 (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

3.9.26.7 (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]

3.9.26.8 (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]

3.9.27 (config)# rmon

3.9.27.1 (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 1 to 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>]

3.9.27.2 (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>]

3.9.27.3 (config-if)# rmon collection history

Syntax: (config-if)# rmon collection history <id> [buckets <buckets>] [interval <interval>]

Explanation: RMON History Configuration is to collect statistics on a physical interface to monitor network utilization, packet types, and errors. A RMON historical record can be used to monitor intermittent problems.

Parameters:

<id>: Specify an ID index. The range is 1~65535.

[buckets <buckets>]: The number of buckets requested for this entry. The allowed range is 1~65535.

[interval <interval>]: Indicates the polling interval. By default, 1800 seconds is specified. The allowed range is 1~3600 seconds.

Negation: (config-if)# no rmon collection history <id>

Show: # show rmon history [<id_list>]

3.9.27.4 (config-if)# rmon collection stats

Syntax: (config-if)# rmon collection stats <id>

Explanation: Configure RMON Statistics table using this command.

Parameters:

<id>: Specify an ID index. The range is 1~65535.

Negation: (config-if)# no rmon collection stats <id>

Show: # show rmon statistics [<id_list>]

3.9.28 (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

3.9.29 (config)# snmp-server

3.9.29.1 (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

3.9.29.2 (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 }]

3.9.29.3 (config)# snmp-server community v2c

Syntax: (config)# snmp-server community v2c <comm> [ro | rw]

Explanation: Configure Read or Write community string.

Parameters:

<comm >: Indicate a community read or write access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 0x21 to 0x7E.

[ro | rw]: Indicates whether the specified community applies to read only access string or read & write access string.

Example: Set Write community access string to private123.

```
# config t
(config)# snmp-server community v2c private124 rw
```

Negation: (config)# no snmp-server community v2c

Show: # show snmp

3.9.29.4 (config)# snmp-server community v3

Syntax: (config)# snmp-server community v3 <v3_comm> [<v_ipv4_addr> <v_ipv4_netmask>]

Explanation: Configure SNMP server community v3 value.

Parameters:

<v3_comm>: Specify SNMPv3 community string.

[<v_ipv4_addr> <v_ipv4_netmask>]: Specify IPv4 address and subnet mask address.

Negation: (config)# no snmp-server community v3 <word127>

Show: # show snmp
show snmp community v3

3.9.29.5 (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

3.9.29.6 (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 engined-id local

Show: # show snmp

3.9.29.7 (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
```

Negation: (config)# snmp-server host <conf_name>

Show: # show snmp host [<conf_name>] [system] [switch] [power] [interface] [aaa]

3.9.29.8 (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

3.9.29.9 (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>]

3.9.29.10 (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

3.9.29.11 (config)# snmp-server user

Syntax: (configt)# snmp-server user <username> engine-id <engineID> [{ md5 <md5_passwd> | sha <sha_passwd> } [priv { des | aes } <priv_passwd>]]

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> | sha <sha_passwd> }: 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.

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.

[priv { des | aes } <priv_passwd>]]: 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.

Negation: (config)# no snmp-server user <username> engine-id <engineID>

Show: #show snmp user [<username> <engineID>]

3.9.29.12 (config)# snmp-server version

Syntax: (config)# snmp-server version { v1 | v2c | v3 }

Explanation: Configure SNMP server version.

Parameters:

{ v1 | v2c | v3 }: Specify which SNMP server version you want to use.

Example: Set SNMP server version to v3.

```
# config t
(config)# snmp-server version v3
```

Negation: (config)# no snmp-server version

Show: # show snmp

3.9.29.13 (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>]

3.9.38.14 (config-if)# snmp-server host <conf_name> traps

Syntax: (config-if)# snmp-server host <conf_name> traps [linkup] [linkdown] [lldp]

Explanation: Configure SNMP trap events for the selected interface.

Parameters:

<conf_name: word 32>: Specify the name of the trap.

traps [linkup] [linkdown] [lldp]: Enable the selected interfaces' trap events.

[linkup]: Port link up trap.

[linkdown]: Port link down trap.

[lldp]: LLDP (Link Layer Discovery Protocol) trap.

Negation: (config-if)# no snmp-server host <conf_name> traps

3.9.29.15 (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

3.9.29.16 (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

3.9.29.17 (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

3.9.29.18 (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

3.9.29.19 (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

3.9.29.20 (config-snmps-host)# traps

Syntax: (config-snmps-host)# traps [authentication snmp-auth-fail] [system [coldstart] [warmstart]] [switch [stp] [rmon]]

Explanation: Configure SNMP trap events.

Parameters:

[authentication]: A trap will be issued at any SNMP authentication failure.

[system [coldstart] [warmstart]]: The system trap events include the following.

coldstart: The switch has booted from a powered off or due to power cycling (power failure).

warmstart: The switch has been rebooted from an already powered on state.

[switch [stp] [rmon]]: Indicates the Switch group's traps. Possible traps are:

stp: Enable STP trap.

rmon: Enable RMON trap.

Example: Send a trap notice when any authentication fails.

```
# config t
(config-snmps-host)# traps authentication snmp-auth-fail
```

Negation: (config-snmps-host)# no traps

Show: # show snmp host [<conf_name>] [system] [switch] [interface] [aaa]

3.9.30 (config)# spanning-tree

3.9.30.1 (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

3.9.30.2 (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

3.9.30.3 (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

3.9.30.4 (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

3.9.30.5 (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

3.9.30.6 (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

3.9.30.7 (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

3.9.30.8 (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

3.9.30.9 (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

3.9.30.10 (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

3.9.30.11 (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

3.9.30.12 (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

3.9.30.13 (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

3.9.30.14 (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

3.9.30.15 (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

3.9.30.16 (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

3.9.30.17 (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

3.9.30.18 (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

3.9.30.19 (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

3.9.30.20 (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

3.9.30.21 (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

3.9.30.22 (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

3.9.30.23 (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

3.9.30.24 (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

3.9.30.25 (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

3.9.30.26 (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

3.9.30.27 (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

3.9.30.28 (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

3.9.30.29 (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

3.9.30.30 (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

3.9.31(config-if)# speed

Syntax: (config-if)# speed { 1000 | 100 | 10 | auto { [10] [100] [1000] } }

Explanation: Configure port speed for this specific interface.

Negation: (config-if)# no speed

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

3.9.32 (config-if)# switchport

3.9.32.1 (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

3.9.32.2 (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> }]

3.9.32.3 (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

3.9.32.4 (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

3.9.32.5 (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

3.9.32.6 (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

3.9.32.7 (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

3.9.32.8 (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, 1. If the tagged frame with TPID=0x8100, it becomes a double-tag frame and is forwarded. 2. 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, 1. If a tagged frame with TIPID=0x8100, it is forwarded. 2. 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, 1. If a tagged frame with TPID=0x88A8, it is forwarded. 2. 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, 1. If a tagged frame with TPID=0x88A8, it is forwarded. 2. 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

3.9.32.9 (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

3.9.32.10 (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

3.9.321.11 (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

3.9.32.12 (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

3.9.32.13 (config-if)# switchport vlan ip-subnet id

Syntax: (config-if)# switchport vlan ip-subnet id <1-128> <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:

<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>]

3.9.32.14 (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 does 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>]

3.9.32.15 (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>]

3.9.33 (config)# tacacs-server

3.9.33.1 (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

3.9.33.2 (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

3.9.33.3 (config)# tacacs-server key

Syntax: (config)# tacacs-server key <key>

Explanation: Specify the secret key up to 63 characters. This is shared between a TACACS+ sever and the switch.

Parameters:

<key:1-63>: Specify a shared secret key value.

Negation: (config)# no tacacs-server key

Show: # show tacacs-server

3.9.33.4 (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

3.9.34 (config)# upnp

3.9.34.1 (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

3.9.34.2 (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

3.9.34.3 (config)# upnp ttl

Syntax: (config)# upnp ttl <v_1_to_255>

Parameters:

<v_1_to_255>: Specify the ttl (time to live) value. The allowed range is 1 to 255.

Explanation: TTL (Time to live) is used to configure how many steps an UPnP advertisement can travel before it disappears.

Example: Set the upnp ttl value to 10.

```
# config t
(config)# upnp ttl 10
```

Negation: (config)# no upnp ttl

Show: # show upnp

3.9.35 (config)# username

3.9.35.1 (config)# username<username>privilege<priv>password encrypted

Syntax: (config)# username <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 <username: word31>: 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

3.9.35.2 (config)# username<username>privilege<priv>password none

Syntax: (config)# username <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 <username: word31>: 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 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

3.9.35.3 (config)# username<username>privilege<priv>password unencrypted

Syntax: (config)# username <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 <username: word31>: 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 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

3.9.36 (config)# vlan

3.9.36.1 (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> }

3.9.36.2 (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> }

3.9.36.3 (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>]

3.9.37 (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  10   5  10
Debug                             15  15  15  15
DHCP                               5  10   5  10
DHCPv6_Client                      5  10   5  10
Diagnostics                        5  10   5  10
ETH_LINK_OAM                       5  10   5  10
IP                                 5  10   5  10
LACP                               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
NTP                                5  10   5  10
Ports                              5  10   1  10
Private_VLANs                      5  10   5  10
QoS                                5  10   5  10
RS485                              5  10   5  10
Security                           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
VLANs                              5  10   5  10
```

Negation: (config)# no web privilege group <group_name> level

Show: > show web privilege group <group_name> level
show web privilege group <group_name> level

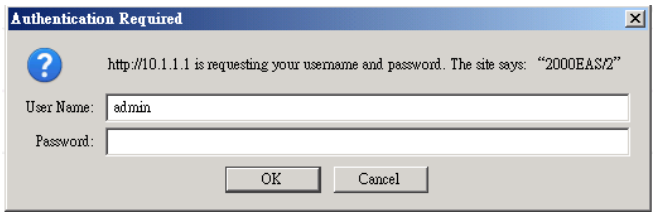
CHAPTER 4. WEB OPERATION & CONFIGURATION

4.1 Home Page

Using your favorite web browser, enter the IP address of the FRM220A-2000EAS/1, /2 or /4F in the browser's location bar. The factory default address is 10.1.1.1.

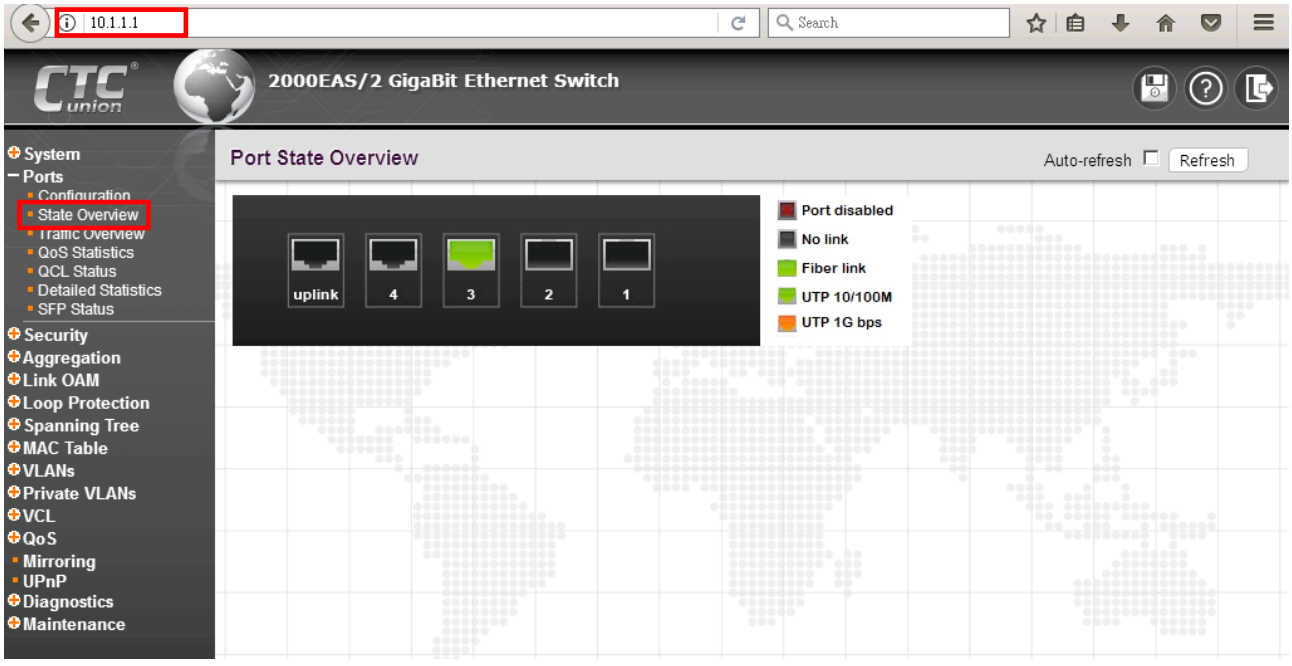
4.1.1 Login

A standard login prompt will appear depending on the type of browser used. The example below is with Firefox browser.



The FRM220A-EAS/1, /2, /4F factory default is username '**admin**' with **no password**.

NOTE: FRM220A-EAS/1, FRM220A-EAS/2 and, FRM220A-EAS/4F *switch cards have the same software functions despite of the difference in the number of ports. In this user manual, we use* FRM220A-EAS/2 *switch card to demonstrate software functions. Therefore, if you purchase devices other than* FRM220A-EAS/2*, the Port State page and other pages involved with port configurations will be slightly different from the demonstrative screenshots provided in this manual.*



Note: *Each FRM220A-2000EAS switch card has one more port shown in "Port State Overview" or port settings than it actually has. This added port is used to connect to the FRM220A-GSW/SNMP(n) management card when it is placed in FRM220A chassis. In the figure provided above, the last port (Uplink or Port 5) is used for this purpose. If the FRM220A-2000EAS switch card is used as a stand-alone device, the settings of this port (Uplink or Port 5 in this example) are ignored.*

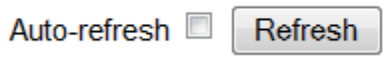
4.1.2 Port Status

The initial page, when logged in, displays a graphical overview of the port status for the electrical and optical ports. The "Green" LAN port indicates a LAN connection with a speed of 10M or 100M. The "Orange" colored LAN port indicates a connection speed of 1000M. When the fiber link is up, it shows green colored ports.

The status display can be reached by using the left side menu, and return 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" checkbox may be selected. The screen will be auto refreshed every 3 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 Save

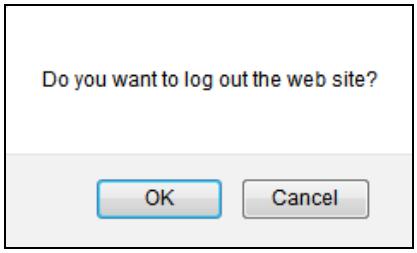
After completing configuration, you must save all your configurations before logging out of the web GUI. This is easily accomplished by clicking the Save icon. The other way to save configurations is to meun tab on the left pane and go to **Maintenance > Configuration > Save startup-config**.

Note: *If you do not save configurations before logging out or restarting the device, all configurations that you have changed will be lost.*

4.1.6 Logout

After completing configuration, we recommend logging out of the web GUI. This is easily accomplished by clicking the logout icon.

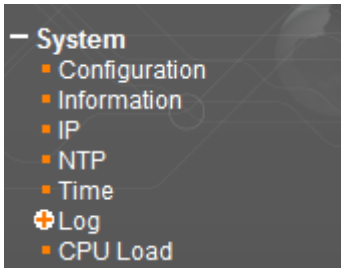
After clicking the logout icon, a confirmation screen will be displayed. Click "OK" to finish logging out or click "Cancel" to return to the web configuration GUI.



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.

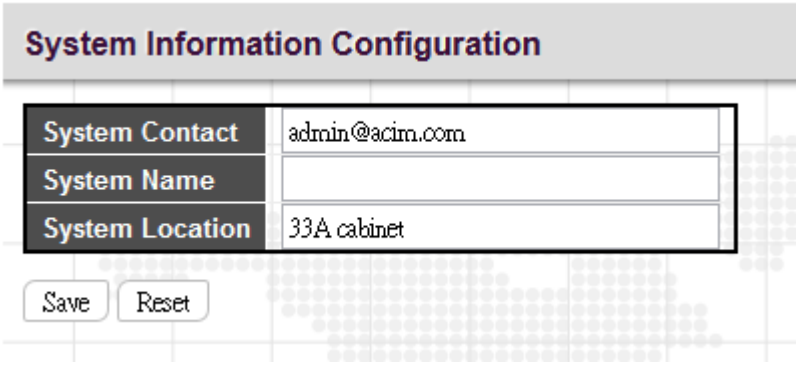
4.2 System

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.



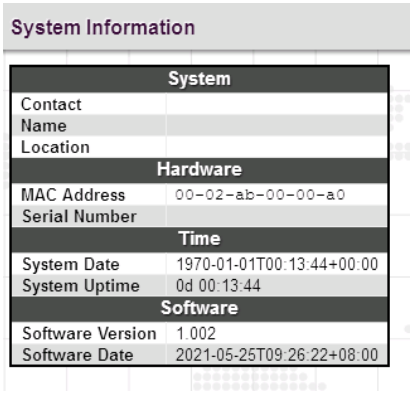
System Contact: Indicate the descriptive contact information. This could be a person's name, email address or other descriptions. The allowed string length is 0~255 and the allowed content is the ASCII characters from 32~126.

System Name: 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.

System Location: Indicate the location of this device. The allowed string length is 0~255.

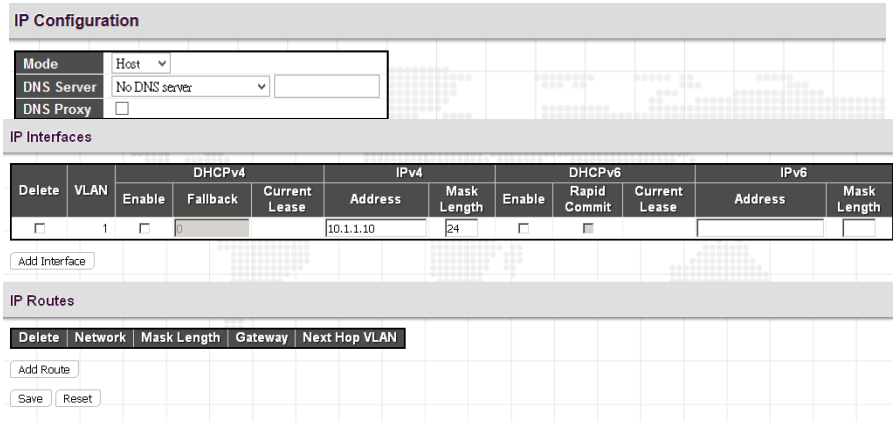
4.2.2 System Information

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.



4.2.3 System IP

Setup the IP configuration, interface and routes.



IP Configuration

Mode: The "Mode" pull-down 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.

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.

No DNS server: No DNS server will be used.

Configured IPv4 or IPv6: Explicitly provide the IP address of the DNS Server in dotted decimal notation.

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. Valid value is from 0 to 4294967295.

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.

IPv4 Mask: 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 DHCPv6 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

Route 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.

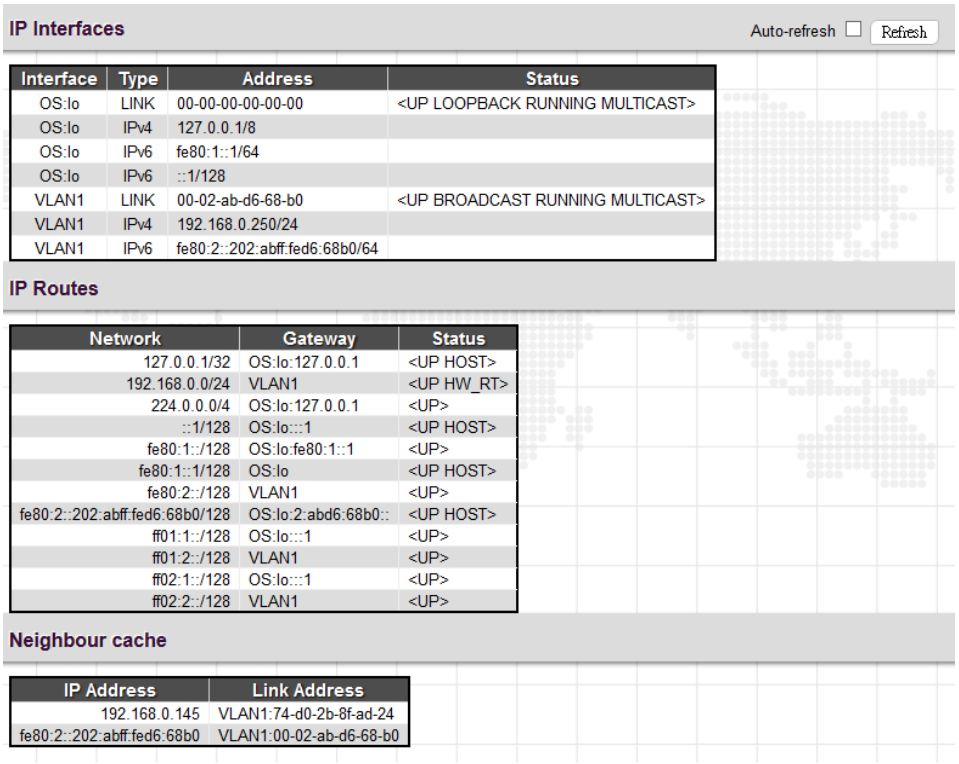
Mask Length: The route mask is a destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have 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.

4.2.4 System IP Status

Display the status of IP interfaces and routes.



IP Interfaces

Auto-refresh Refresh

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80:1::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-02-ab-d6-68-b0	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.250/24	
VLAN1	IPv6	fe80:2::202:abff:fed6:68b0/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	OS:lo:127.0.0.1	<UP HOST>
192.168.0.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	OS:lo:127.0.0.1	<UP>
::1/128	OS:lo:::1	<UP HOST>
fe80:1::/128	OS:lo:fe80:1::1	<UP>
fe80:1::1/128	OS:lo	<UP HOST>
fe80:2::/128	VLAN1	<UP>
fe80:2::202:abff:fed6:68b0/128	OS:lo:2:abd6:68b0::	<UP HOST>
ff01:1::/128	OS:lo:::1	<UP>
ff01:2::/128	VLAN1	<UP>
ff02:1::/128	OS:lo:::1	<UP>
ff02:2::/128	VLAN1	<UP>

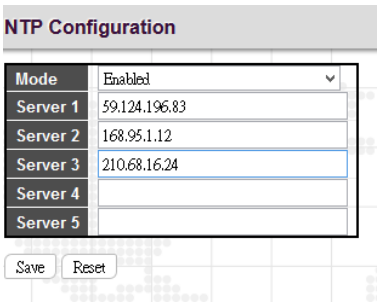
Neighbour cache

IP Address	Link Address
192.168.0.145	VLAN1:74-d0-2b-8f-ad-24
fe80:2::202:abff:fed6:68b0	VLAN1:00-02-ab-d6-68-b0

Please refer to “System IP” for the configuration of the interfaces and routes. This page is informational only.

4.2.5 System NTP

Setup the Network Time Protocol configuration, to synchronize the device’s clock to network time.



NTP Configuration

Mode	Enabled
Server 1	59.124.196.83
Server 2	168.95.1.12
Server 3	210.68.16.24
Server 4	
Server 5	

Save Reset

Mode: Configure the NTP mode operation. Possible modes are:

Enabled: Enable NTP client mode operation.

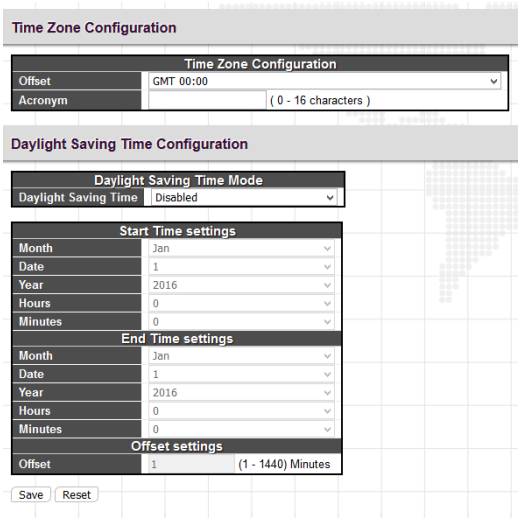
Disabled: Disable NTP client mode operation.

Server #: Enter the IPv4 or IPv6 address of an 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. NTP servers can also be represented by a legally valid IPv4 address. For example,

'::192.1.2.34'. The NTP servers are tried in numeric order. If 'Server 1' is unavailable, the NTP client will try to contact 'Server 2'.

4.2.6 System Time

Setup the device time.



Time Zone Configuration

Time Zone: Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set.

Acronym: Set the acronym of the time zone.

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.

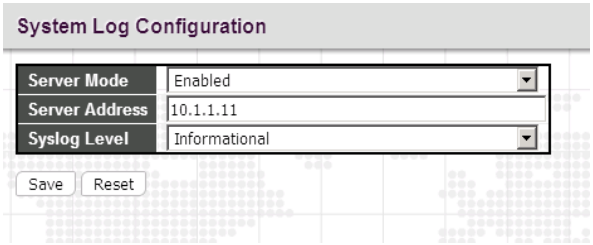
End time settings: Select he ending week, day, month, year, hours, and minutes.

Offset settings: Enter the number of minutes to add during Daylight Saving Time. The allowed range is 1 to 1440.

4.2.7 Log

4.2.7.1 Configuration

Configure System Log on this page.



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:

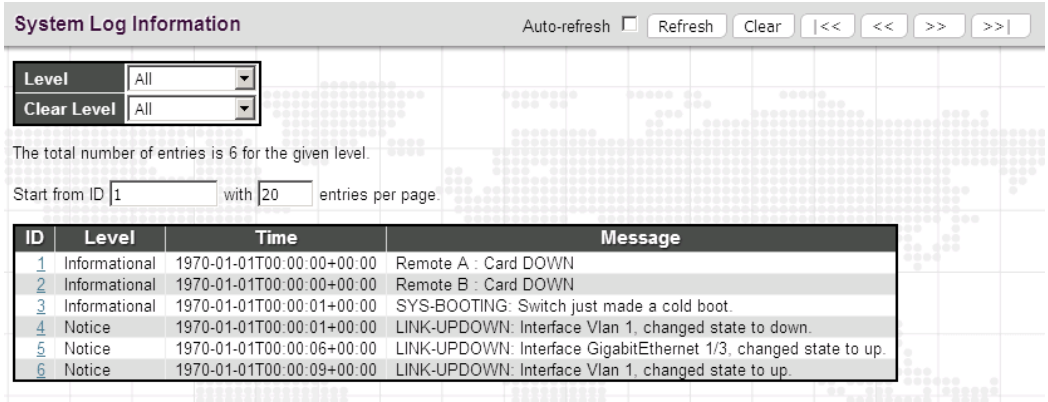
Info: Send information, warnings and errors.

Warning: Send warnings and errors.

Error: Send errors only.

4.2.8 System Log Information

Displays the collected log information.



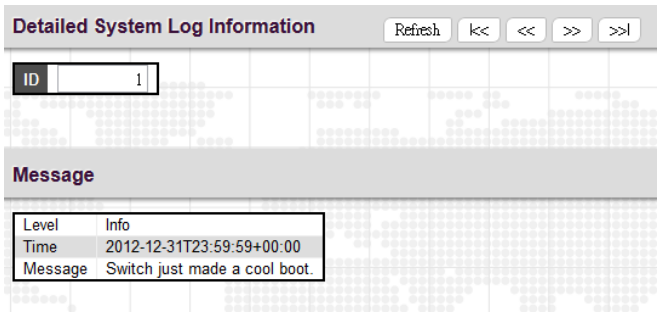
Level: Use this pull down to display all messages or messages of type info, warning or error.

Clear Level: Use this pull down to clear selected message types from the log.

Browsing buttons: Use these buttons to quickly go to the beginning or end of the log or to page through the log.

4.2.9 System Detailed Log

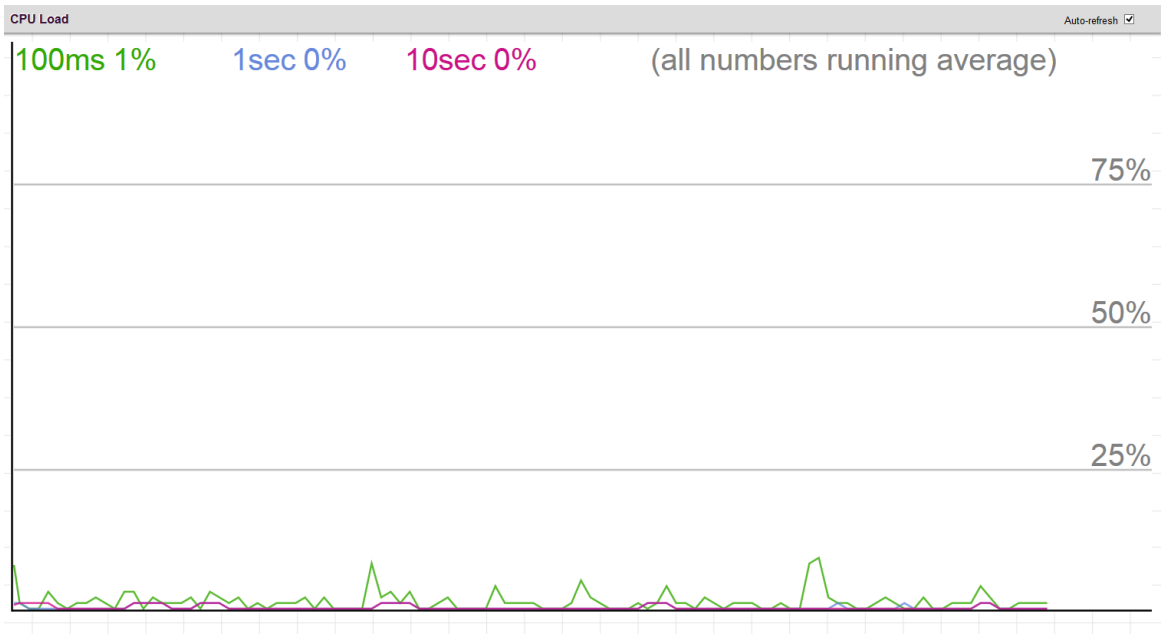
Displays individual log records.



View each log, by ID number.

4.2.10 System CPU Load

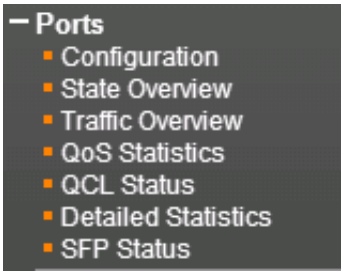
This page displays the CPU load, using an SVG graph.



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.

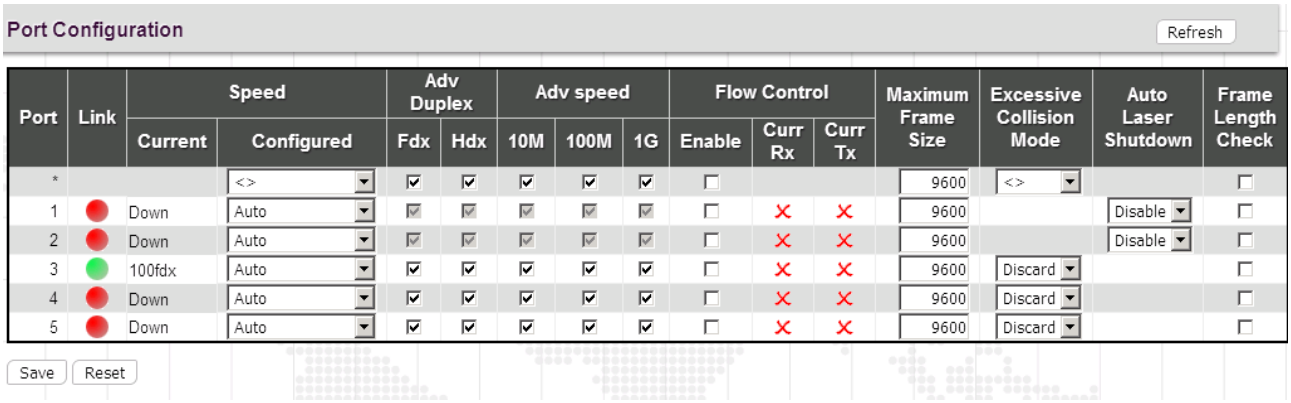
4.3 Ports

Configurations related to the fiber and electrical ports are performed under the Ports menu.



4.3.1 Ports Configuration

This page displays current port configurations and allows some configuration here.



Port: FRM220A-2000EAS/2 is a managed Gigabit switch card with 2 electrical LAN ports and 2 fiber ports (as shown above); while FRM220A-2000EAS/1 is a managed Gigabit switch card with 1 electrical LAN port and 1 fiber port. FRM220A-2000EAS/4F is a managed Gigabit switch card with 4 fiber ports. Each logical port number is displayed in a row. The "All" settings will apply actions on all ports.

Note: *Each FRM220A-2000EAS switch card has one more port shown in port settings than it actually has. This added port is used to connect to the FRM220A-GSW/SNMP(n) management card when it is placed in FRM220A chassis. In the figure provided above, the last port (Port 5) is used for this purpose. If the FRM220A-2000EAS switch card is used as a stand-alone device, the settings of this port (Port 5 in this example) are ignored.*

Link: The current link state for each port is displayed graphically. Green 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) 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 - Port auto negotiating speed with the link partner, selecting the highest speed that is compatible with the link partner.
100Mbps FDX - Forces the fiber port to 100Mbps full duplex mode.
1Gbps FDX - Forces the fiber port to 1Gbps full duplex mode.

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.

Maximum Frame Size: Enter the maximum frame size allowed for the switch port, including FCS. This switch supports up to 9600 byte packets.

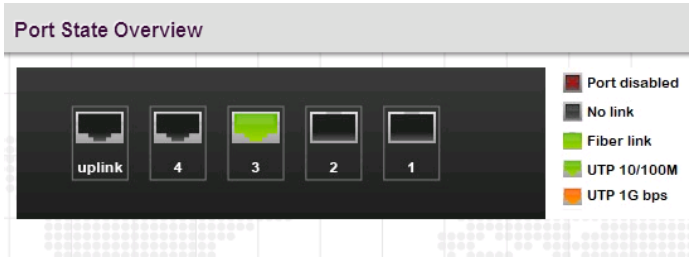
Excessive Collision Mode: This setting configures the port transmit collision behavior to either "Discard" (Discard frame after 16 collisions - default) or to "Restart" (Restart backoff algorithm after 16 collisions).

Auto Laser Shutdown: Enable or disable the laser module of the transceiver shutdown automatically.

Frame Length Check: 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). When "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. When "frame length check" is disabled, frames are not dropped due to frame length mismatch.

4.3.2 Ports State

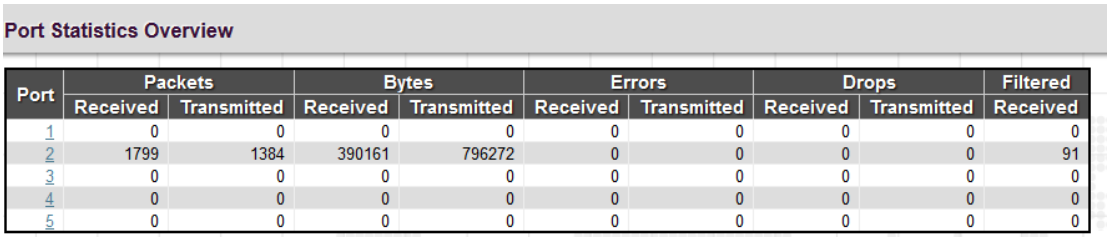
Display an overview graphic of the switch.



This is the same graphic overview shown when first logging into the switch for management. "Green" colored ports indicate a 10M or 100M linked state, while "Orange" colored ports indicate a 1000M linked state. When the fiber link is up, it shows green colored ports. "Grey" ports have no link. 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.

4.3.3 Ports Traffic Overview

Displays a comprehensive overview of traffic on all ports.



Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	1799	1384	390161	796272	0	0	0	0	91
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0

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.

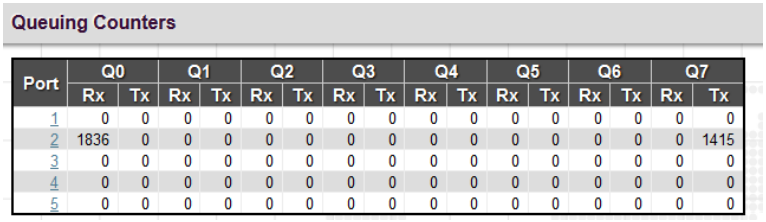
Drops: The number of frames discarded due to ingress or egress congestion.

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.

4.3.4 Ports QoS Statistics

This page provides statistics for the different queues for all switch ports.



Queuing Counters

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1836	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1415
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

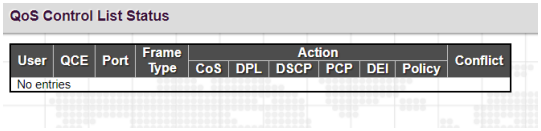
Port: The logical port for the settings contained in the same row.

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.

4.3.5 Ports QCL Status

This page shows the QCL status by different QCL users.



QoS Control List Status

User	QCE	Port	Frame Type	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	
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.

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.

Port: Indicates the list of ports configured with the QCE.

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.

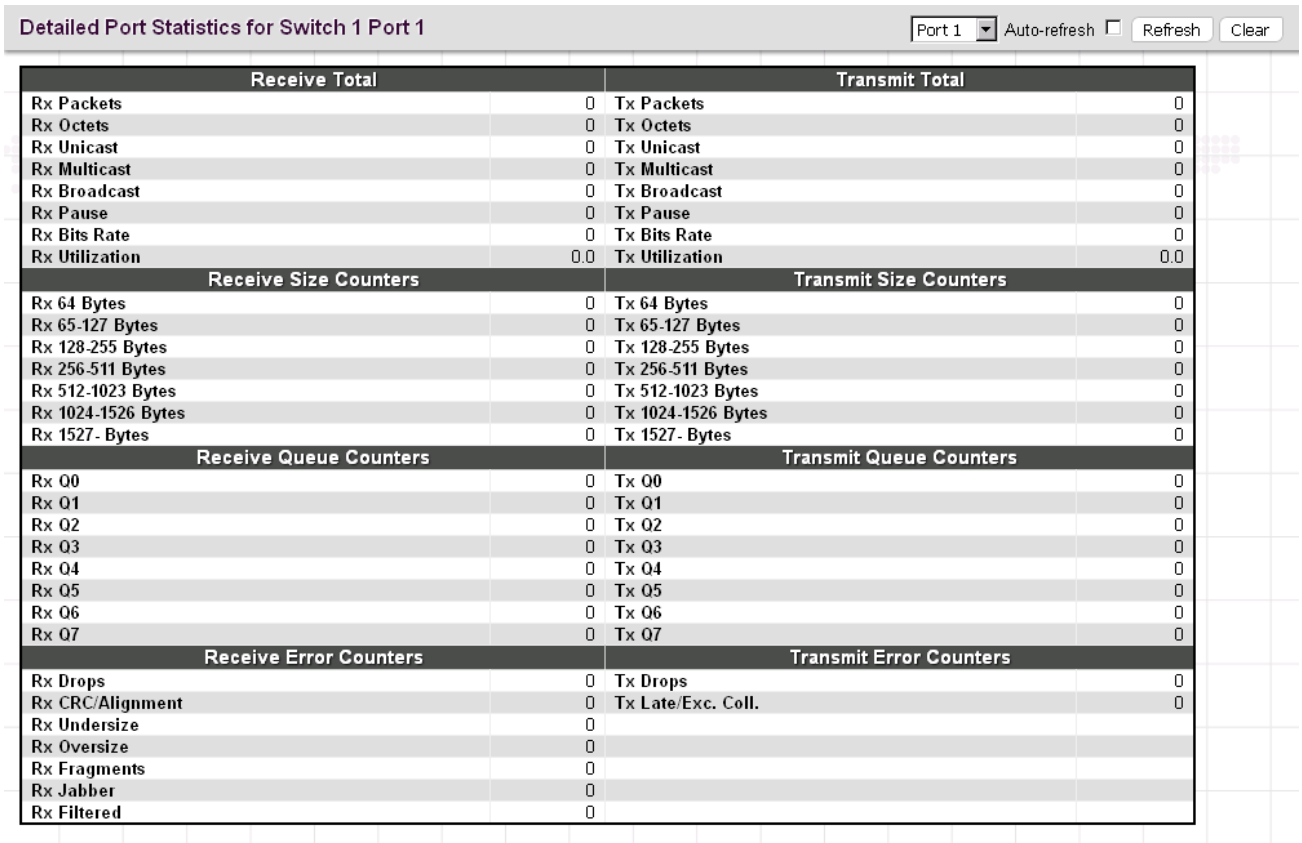
DEI: If a frame matches the QCE then DEI will be classified with the value displayed under DEI column.

Policy: ACL polic number.

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.

4.3.6 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.



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		

Receive Total and Transmit Total

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.

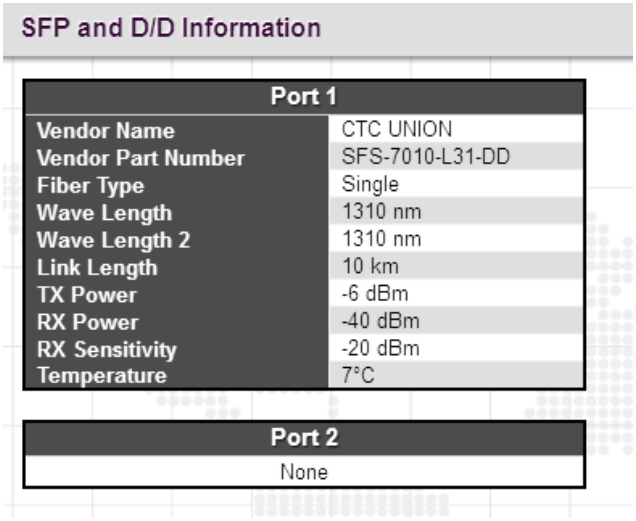
Transmit Error Counters

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.

4.3.7 Ports SFP

This page provides status of SFP.



Vendor Name: The SFP vendor's (company) name.

Vendor Part Number: The part number provided by SFP vendor.

Fiber Type: The type of fiber channel transmission media (multi-mode or single mode).

Wave Length: The wavelength of the transceiver.

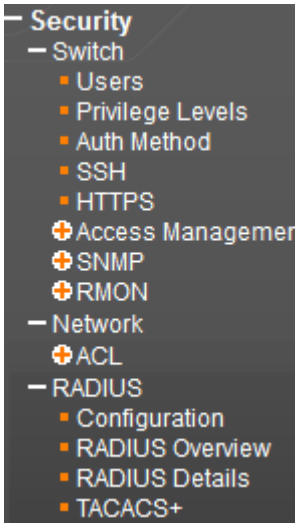
Link Length: The link length supported by the transceiver.

TX Power: The laser diode transmit power is reported by the SFP that support DDI (Digital Diagnostic monitoring Interface).

RX Power: The laser diode receive power is reported by the SFP that support DDI (Digital Diagnostic monitoring Interface).

4.4 Security

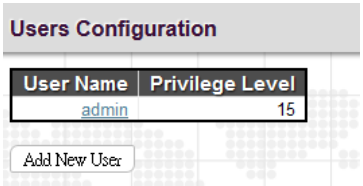
Under the security heading are three major icons, switch, network and RADIUS.



4.4.1 Switch

4.4.1.1 Users

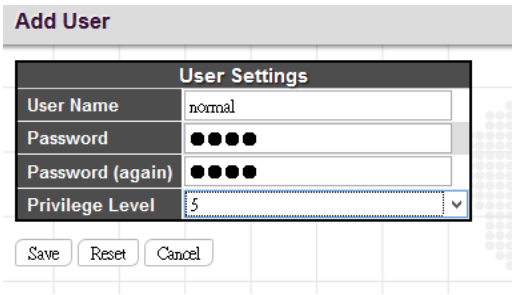
This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.



By default, there is only one user, 'admin', assigned the highest privilege level of 15.

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.

Add User



User Name: Enter the new user name.

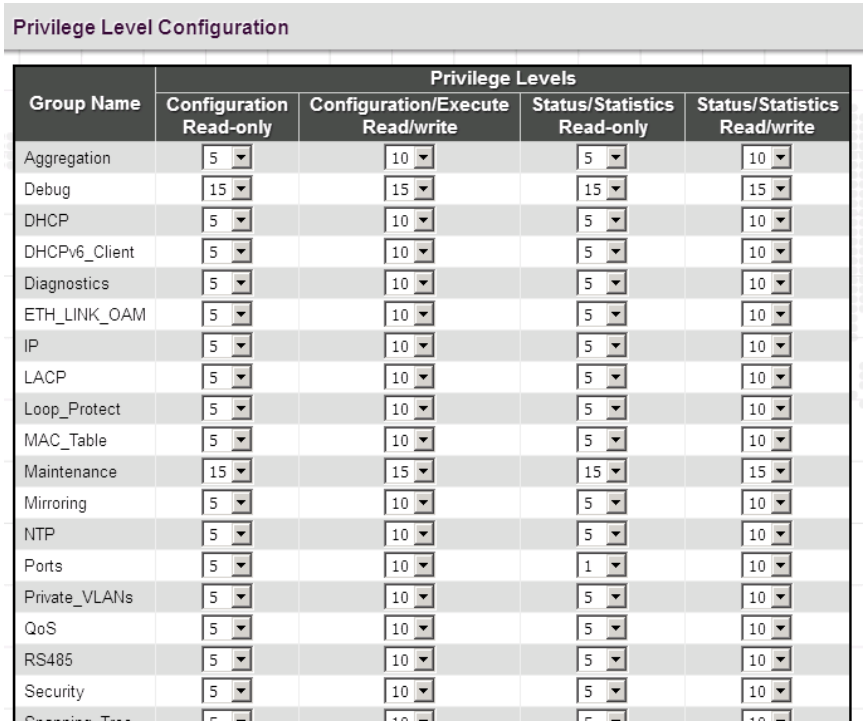
Password: Enter the password for this user account.

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.

4.4.1.2 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
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
ETH_LINK_OAM	5	10	5	10
IP	5	10	5	10
LACP	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
NTP	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10
RS485	5	10	5	10
Security	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.

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

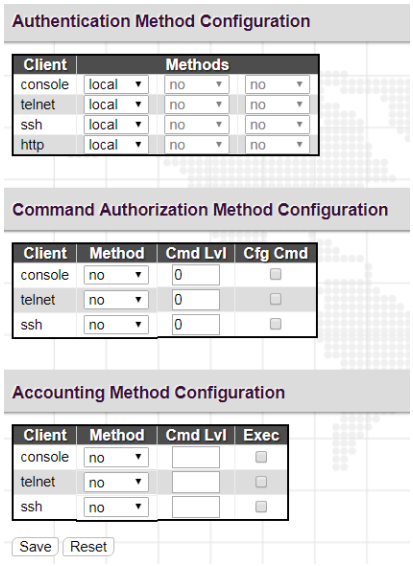
status/statistics read-only

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.

4.4.1.3 Auth Method

This page allows you to configure how users are authenticated when they log into the switch via one of the management client interfaces.



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.

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.

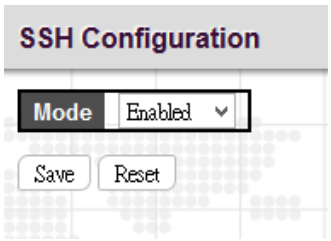
tacacs: Use remote TACACS+ server(s) for authentication.

Cmd Lvl: Authorize all commands with a privilege level higher than or equal to this level.

Exec: Enable Exec (login) accounting.

4.4.1.4 SSH

Configure SSH on this page.



Mode: Indicates the SSH mode operation. Possible modes are:

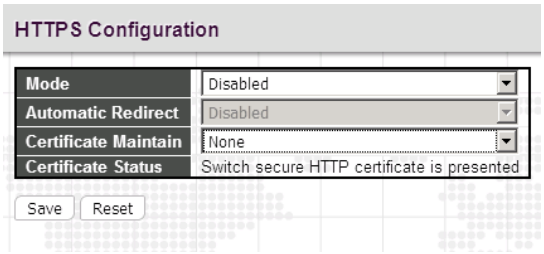
Enabled: Enable SSH mode operation. By default, SSH mode operation is enabled.

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.*

4.4.1.5 HTTPS

Configure HTTPS on this page.



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.

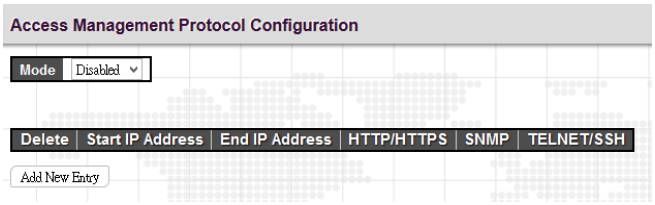
Disabled: Disable HTTPS redirect mode operation.

Certificate Maintain: Select a way to either upload or generate a certificate file.

4.4.1.6 Access Management

4.4.1.6.1 Access Management 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 Protocol Configuration

Mode: Indicates the access management mode operation. Possible modes are:

Enabled: Enable access management mode operation.

Disabled: Disable access management mode operation.

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.

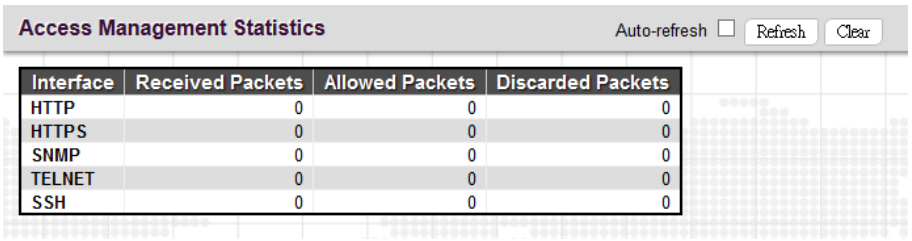
TELNET/SSH: Indicates that the matched host can access the switch from TELNET/SSH interface.

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.

4.4.1.6.2 Access Management Statistics

This page provides statistics for access management.



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.

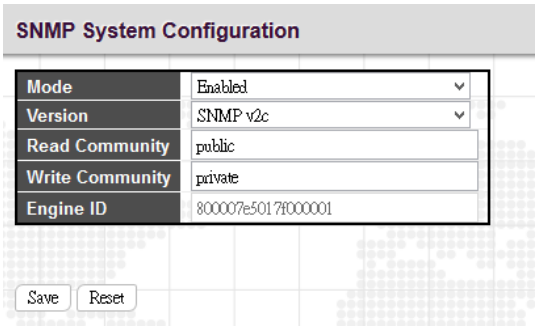
Allowed Packets: The number of allowed packets from the interface when access management mode is enabled.

Discarded Packets: The number of discarded packets from the interface when access management mode is enabled.

4.4.1.7 SNMP

4.4.1.7.1 SNMP System Configuration

Configure SNMP on this page.



Mode: Indicates the SNMP mode operation. Possible modes are:

Enabled: Enable SNMP mode operation.

Disabled: Disable SNMP mode operation.

Version: Indicates the SNMP supported version. Possible versions are:

SNMP v1: Set SNMP supported version 1.

SNMP v2c: Set SNMP supported version 2c.

SNMP v3: Set SNMP supported version 3.

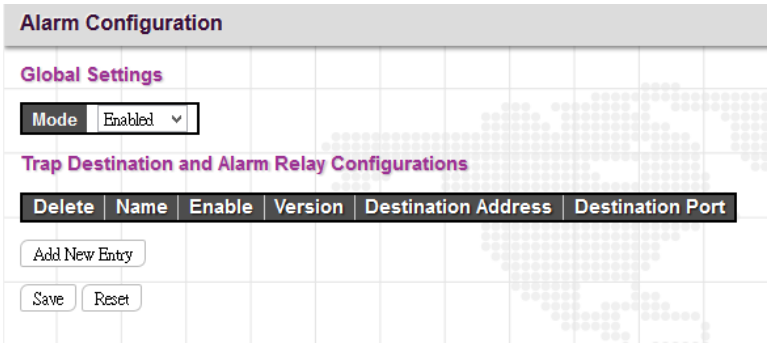
Read Community: Indicates the community read access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 0x21 to 0x7E.

Write Community: Indicates the community write access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 0x21 to 0x7E. These two fields are applicable only for SNMP version v1 or v2c. If SNMP version is v3, the community string will be associated with SNMPv3 communities table. SNMPv3 provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

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.

4.4.1.7.2 Trap Configuration

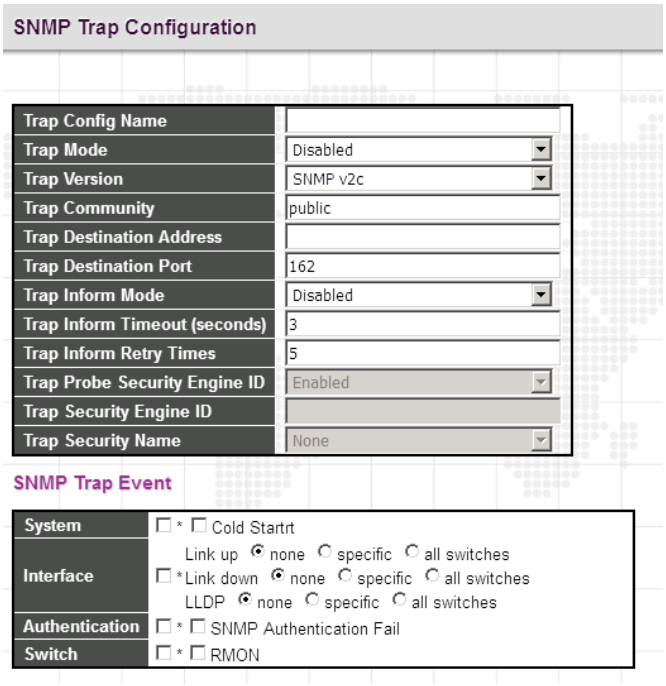
Configure SNMP trap on this page.



Global Settings

Mode: Globally enable or disable trap function.

Click the “Add New Entry” to insert a SNMP trap entry.



SNMP Trap Configuration

Trap Config Name: Indicates a descriptive name for this SNMP trap entry.

Trap Mode: Indicates the SNMP trap mode operation.

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-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.

Trap Destination 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.

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 Probe Security Engine ID: Indicates the SNMP trap probe security engine ID mode of operation. Possible values are:

Enabled: Enable SNMP trap probe security engine ID mode of operation.

Disabled: Disable SNMP trap probe security engine ID mode of operation.

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.

SNMP Trap Event

System: The system trap events include the following.

Warm Start: The switch has been rebooted from an already powered on state.

Cold Start: The switch has booted from a powered off or due to power cycling (power failure).

Dying Gasp: A SNMP trap will be issued immediately when the remote device encounters power failure.

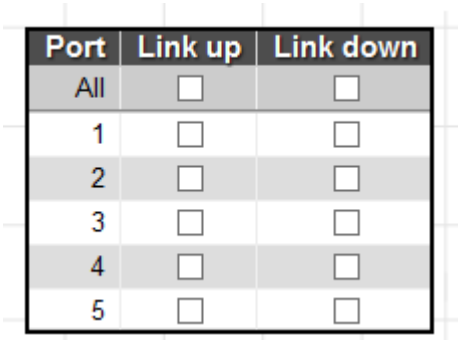
Interface: Indicates the Interface group's traps. Possible traps are:

Link Up: none/specific/all switches Link up trap.

Link Down: none/specific/all switches Link down trap.

LLDP: none/specific/all switches LLDP (Link Layer Discovery Protocol) trap.

When the "specific" radio button is selected, a popup graphic with port checkboxes allows selection specific ports.



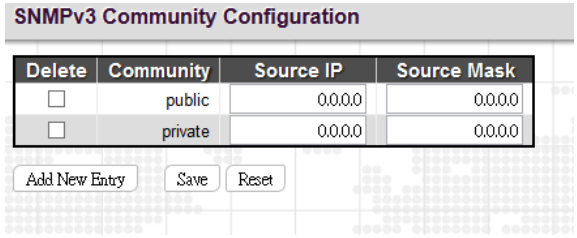
AAA: AAA stands for Authentication, Authorization and Accounting. A trap will be issued at any authentication failure.

Switch: Indicates that the Switch group's traps. Possible traps are:

RMON: Select the checkbox to enable RMON trap. Clear to disable RMON trap.

4.4.1.7.3 SNMPv3 Community Configuration

Configure SNMPv3 community table on this page. The entry index key is Community.



Delete: Check to delete the entry. It will be deleted during the next save.

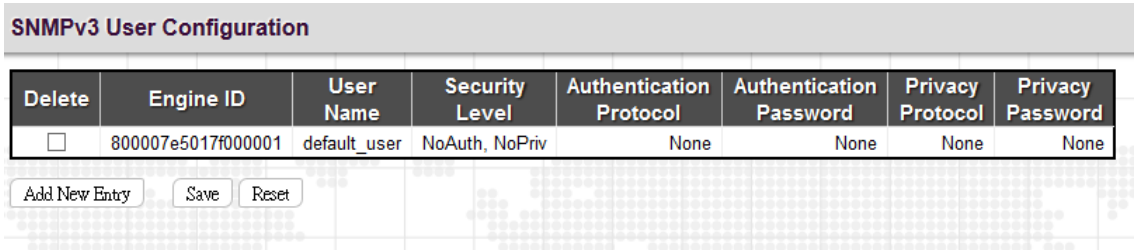
Community: Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string. This string is case 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.

4.4.1.7.4 SNMPv3 User Configuration

Configure SNMPv3 user table on this page. The entry index keys are Engine ID and User Name.



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 0x21 to 0x7E.

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.

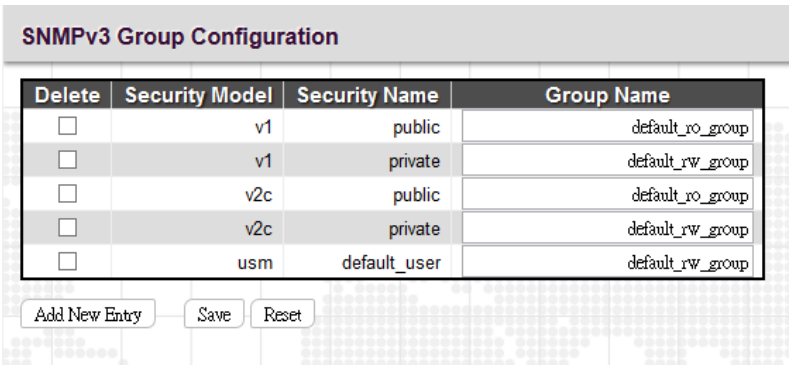
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.4.1.7.5 SNMPv3 Group Configuration

Configure SNMPv3 group table on this page. The entry index keys are Security Model and Security Name.



Security Model: Indicates the security model that this entry should belong to. Possible security models are:

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

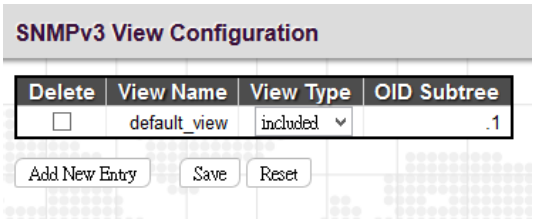
usm: User-based Security Model (USM) for SNMPv3.

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: 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.

4.4.1.7.6 SNMPv3 View Configuration

Configure SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.



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:

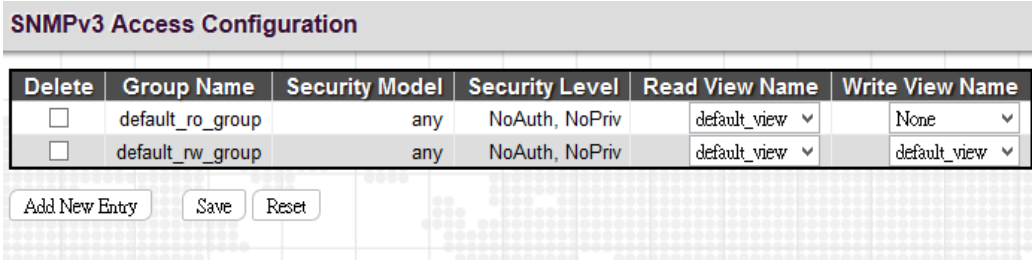
included: An optional flag to indicate that this view subtree should be included.

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 it's 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 (*).

4.4.1.7.7 SNMPv3 Access Configuration

Configure SNMPv3 access table on this page. The entry index keys are Group Name, Security Model and Security Level.



Delete: Check to delete the entry. It will be deleted during the next save.

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 level 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.

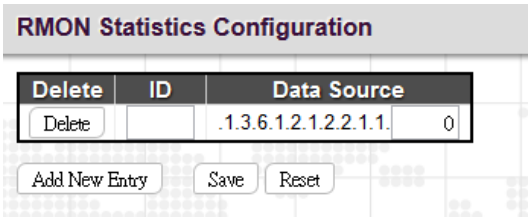
Read View Name: The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

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.

4.4.1.8 RMON

4.4.1.8.1 Statistics Configuration

Configure RMON Statistics table on this page. The entry index key is ID.



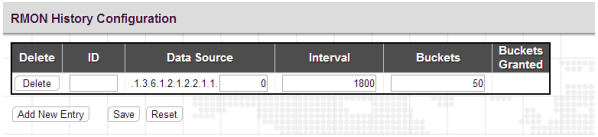
Delete: Check to delete the entry. It will be deleted during the next save.

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.

4.4.1.8.1.1 History 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.



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.

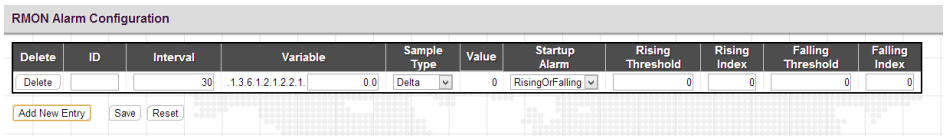
Click the "Delete" button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the "Save" button to save settings or changes.

Click the "Reset" button to restore changed settings to the default settings.

4.4.1.8.1.2 Alarm 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.



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.

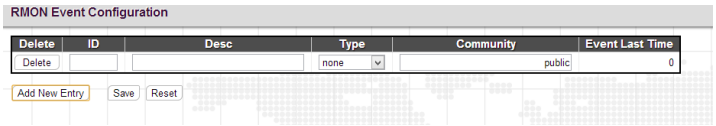
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.4.1.8.1.3 Event Configuration

RMON Event Configuration page is used to set an action taken when an alarm is triggered.



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.

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.

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.

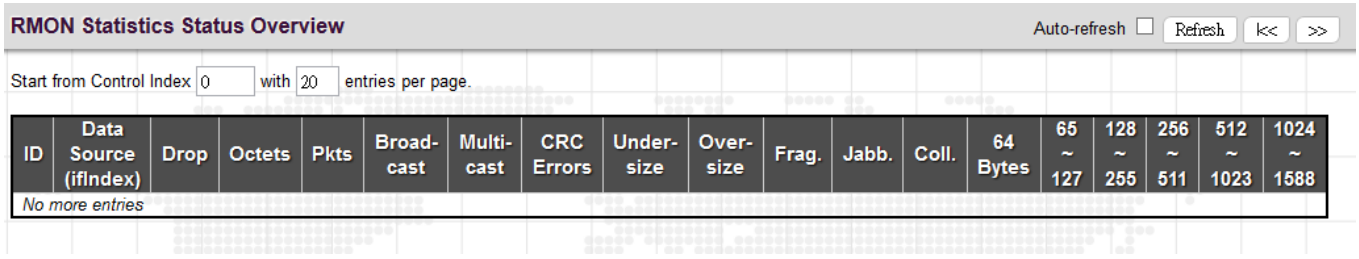
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.4.1.8.1.4 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.



ID: Display 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.

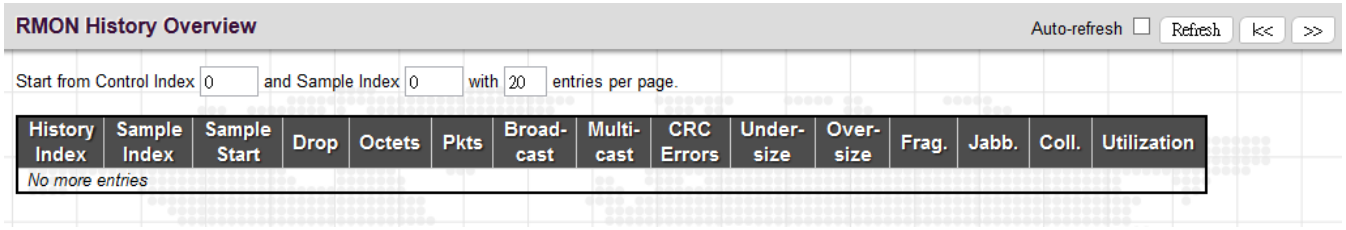
Jabb.: The number of frames which size is larger than 64 octets received with invalid CRC.

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.

4.4.1.8.2 History Overview



History Index: Display Index of History control entry.

Sample Index: Display 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.

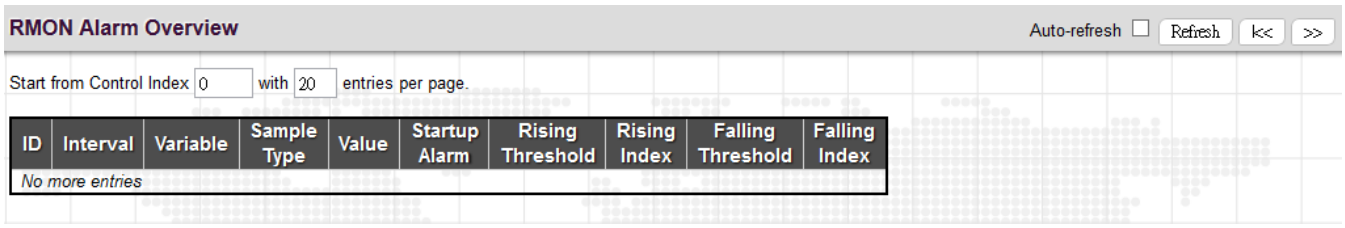
Frag.: The number of frames which size is less than 64 octets received with invalid CRC.

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.

4.4.1.8.3 Alarm Overview



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.

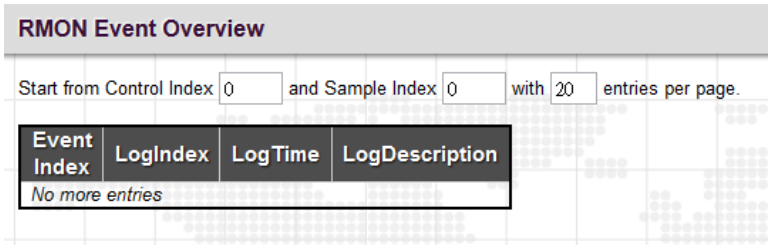
Rising Threshold: If the current value is greater than the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated.

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.

4.4.1.8.4 Event Overview



Event Index: Display the event entry index.

Log Index: Display the log entry index.

Log Time: Display Event log time.

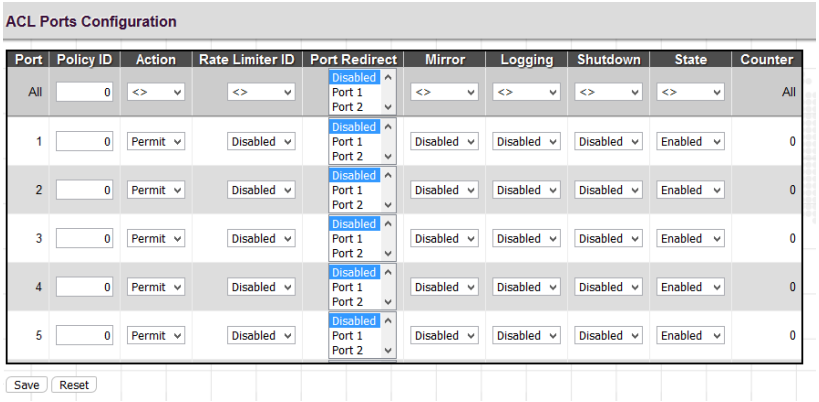
Log Description: Display Event description.

4.4.2 Network

4.4.2.1 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.

4.4.2.1.1 Ports



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.

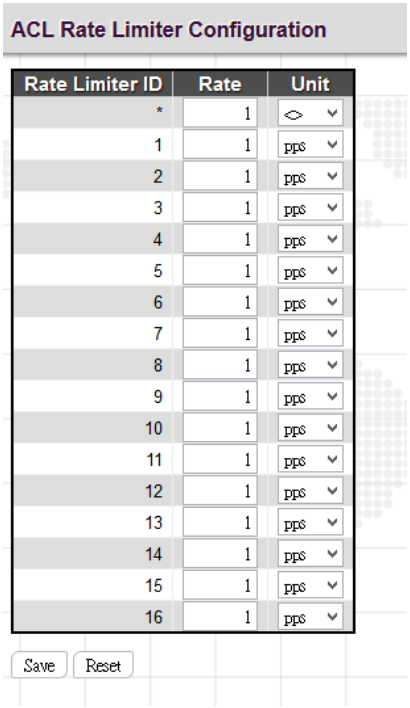
State: Select a port state.

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.

4.4.2.1.2 Rate Limiters



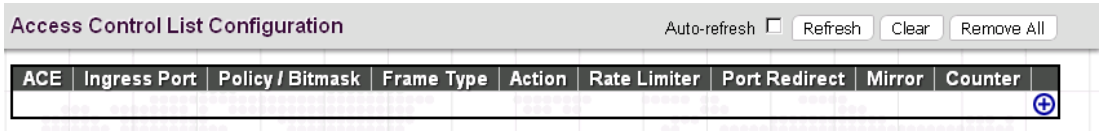
Rate Limiter ID: Display every rate limiter ID.

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.

4.4.2.1.3 Access Control List

Access Control List is to establish filtering rules for an ACL policy, for a particular port or for all ports. Rules applied to a port take effect immediately.



Ingress Port: The ingress port of the access control entry. Select “All” to apply to all ports or select a particular port.

Policy Bitmask: The policy number and bitmask of the ACE.

Frame Type: The type of frame that matches to this rule.

Action: Display the action type, either to permit or deny.

Rate Limiter: Display rate limiter is enabled or disabled when matched frames are found.

Port Redirect: Display port redirect is enabled or disabled.

Mirror: Display mirror function is enabled or disabled.

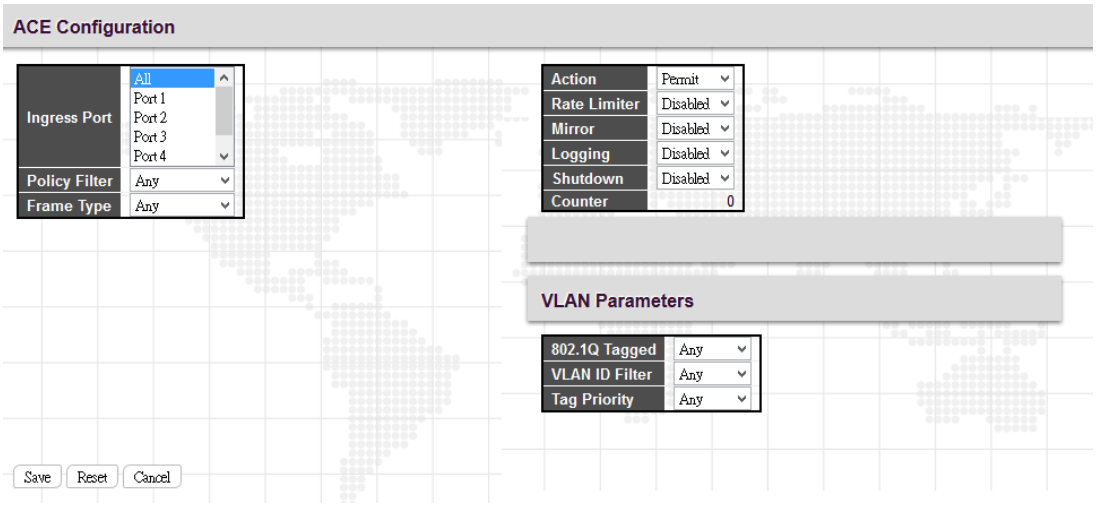
Counter: Display the number of frames that have matched any of the rules defined for this ACL.

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



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 Any 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.

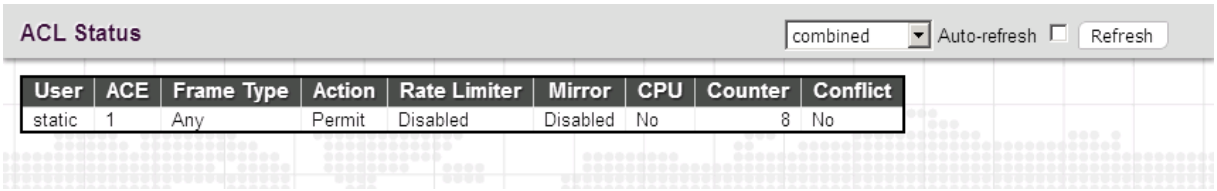
IPv6 Parameters

Next Header Filter: Select next header filter option. Available options include ICMP, UDP, TCP, Other.

SIP Filter: Select a source IP filter. “Any” denotes that any SIP filter is allowed. Select “Specific” to enter self-define SIP filter.

Hop Limit: Select “Any” to allow any values in this field. Select” “0” if IPv6 frames with a hop limit field greater than zero must not be able to match this entry. “1” denotes that IPv6 frames with a hop limit field greater than zero must be able to match this entry.

4.4.2.1.4 ACL Status



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: This field displays the number of ACL rule.

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.

IPv6: The ACE will match all IPv6 standard frames.

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.

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".

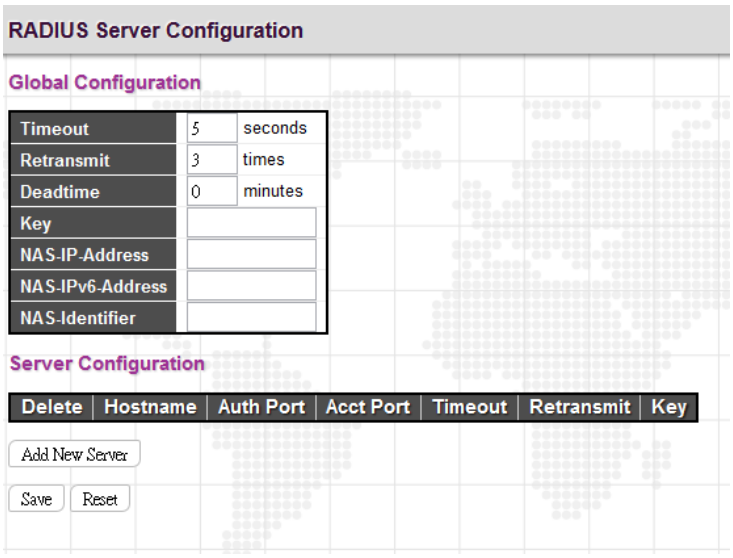
CPU: Forward packet that matched the specific ACE to CPU.

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.

4.4.3 RADIUS

4.4.3.1 Configuration



Global Configuration

Timeout: The time the switch waits for a reply from an authentication server before it retransmits the request.

Retransmit: Specify 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.

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 1440 minutes.

Key: Specify the secret key up to 64 characters. This is shared between the RADIUS sever and the switch.

NAS-IP-Address: The IPv4 address is 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: The IPv6 address is 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: The identifier, up to 256 characters long, is used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Sever Configuration

Hostname: The hostname or IP address for the RADIUS server.

Auth Port: The UDP port to be used on the RADIUS server for authentication.

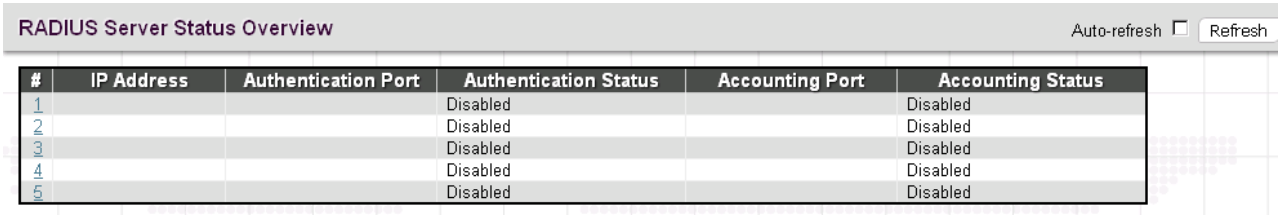
Acct Port: The UDP port to be used on the RADIUS server for accounting.

Timeout: 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: 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: 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.

4.4.3.2 RADIUS Overview



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:

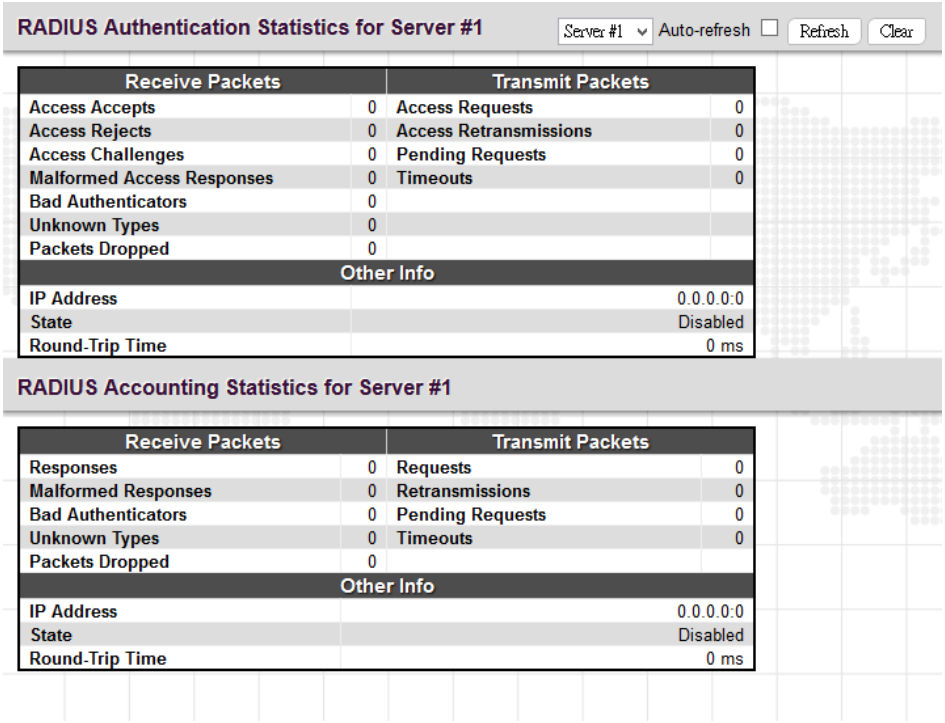
Disabled: The server is disabled.

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.

4.4.3.3 RADIUS Details



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.

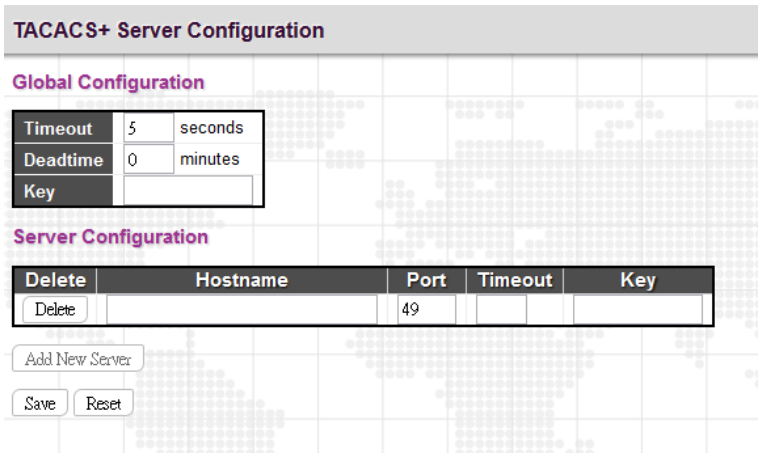
Not Ready: The server is enabled, but IP communication is not yet up and running.

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.

4.4.3.4 TACACS+



Global Configuration

Timeout: The time the switch waits for a reply from a TACACS+ server before it retransmits the request.

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..

Key: Specify the secret key up to 63 characters. This is shared between a TACACS+ sever and the switch.

Server Configuration

Hostname: The hostname or IP address for a TACACS+ server.

Port: The TCP port number to be used on a TACACS+ server for authentication.

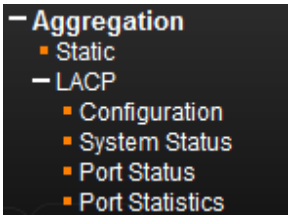
Timeout: If timeout value is specified here, it will replace the global timeout value. If you prefer to use the global value, leave this field blank.

Key: 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.

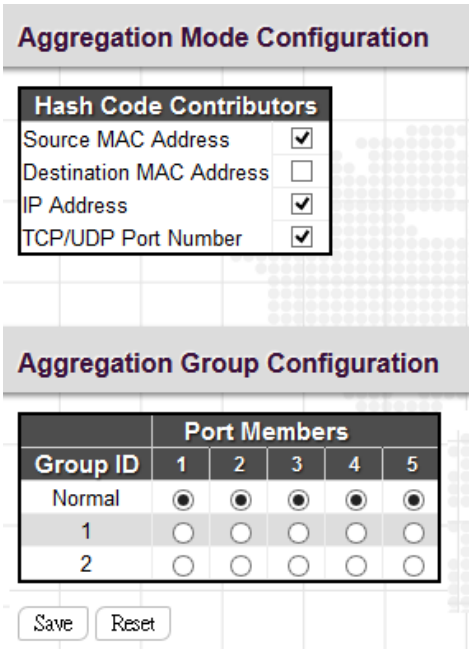
4.5 Aggregation

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.



4.5.1 Static



Aggregation Mode Configuration

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.

Aggregation Group Configuration

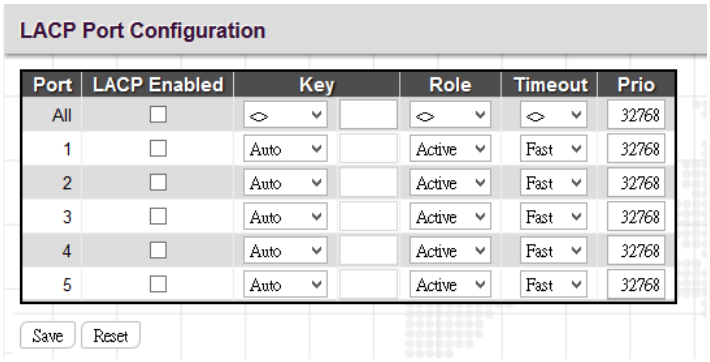
Group ID: By default, all ports belong to Normal group which means no aggregation group. Each group contains at least 2 to 5 links (ports). Please note that each port can only be used once in each group.

Port Members: Select ports to belong to a certain trunk.

4.5.2 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.

4.5.2.1 Port Configuration



Port: The port number. “Port *” settings apply to all ports.

LACP Enabled: Enable LACP on a switch port.

Key: The “Auto” setting sets the key as appropriate by the physical link speed. Select “Specific” if you want a user-defined key value. The allowed key value range is 1~65535. Ports in an aggregated link group must have the same LACP port Key. In order to allow a port to join an aggregated group, the port Key must be set to the same value.

Role: The user can select either “Active” or “Passive” role depending on the device’s capability of negotiating and sending LACP control packets.

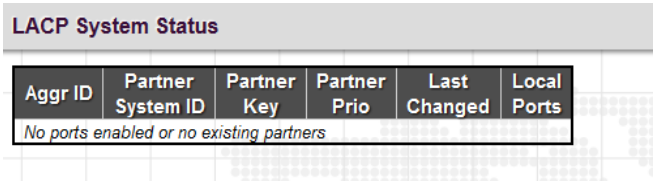
Ports that are designated as “Active” are able to process and send LACP control frames. Hence, this allows LACP compliant devices to negotiate the aggregated like so that the group may be changed dynamically as required. In order to add or remove ports from the group, at least one of the participating devices must set to “Active” LACP ports.

On the other hand, LACP ports that are set to “Passive” cannot send LACP control frames. In order to allow LACP-enabled devices to form a LACP group, one end of the connection must designate as “Passive” LACP ports.

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.

4.5.2.2 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).

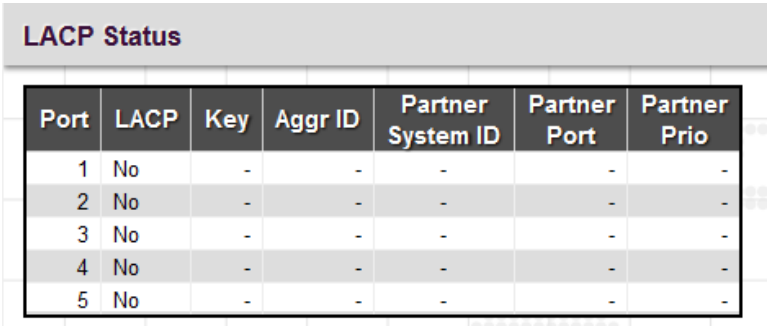
Partner Key: The partner key assigned to this LAG.

Partner Prio: The priority value of the partner.

Last Changed: The time since this LAG changed.

Local Ports: The local ports that are a port of this LAG.

4.5.2.3 Port Status



Port: The port number.

LACP: Show LACP status on a port.

Yes: LACP is enabled and the port link is up.

No: LACP is not enabled or the port link is down.

Backup: The port is in a backup role. When other ports leave LAG group, this port will join LAG.

Key: The aggregation key value on a port.

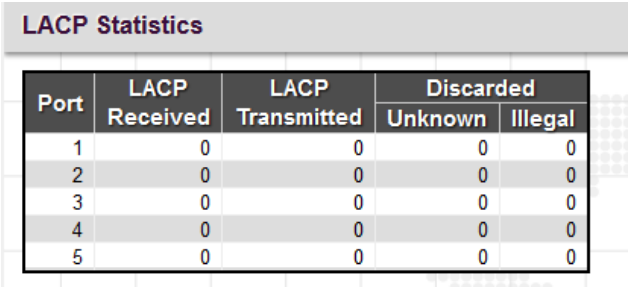
Aggr ID: Display the aggregation ID active on a port.

Partner System ID: LAG partner's system ID.

Partner Port: The partner port connected to this local port.

Partner Prio: The priority value of the partner.

4.5.2.4 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	0	0	0
5	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.

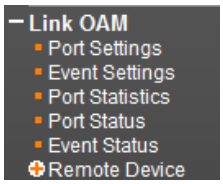
4.6 Link OAM

The Ethernet Operation, Administration, and Maintenance (OAM; IEEE 802.3ah) protocol for monitoring, and troubleshooting Metro Ethernet networks and Ethernet WANs relies on an optional sub-layer in the data link layer of the Normal link operation. Ethernet OAM can be implemented on any full-duplex point-to-point or emulated point-to-point Ethernet link for a network or part of a network.

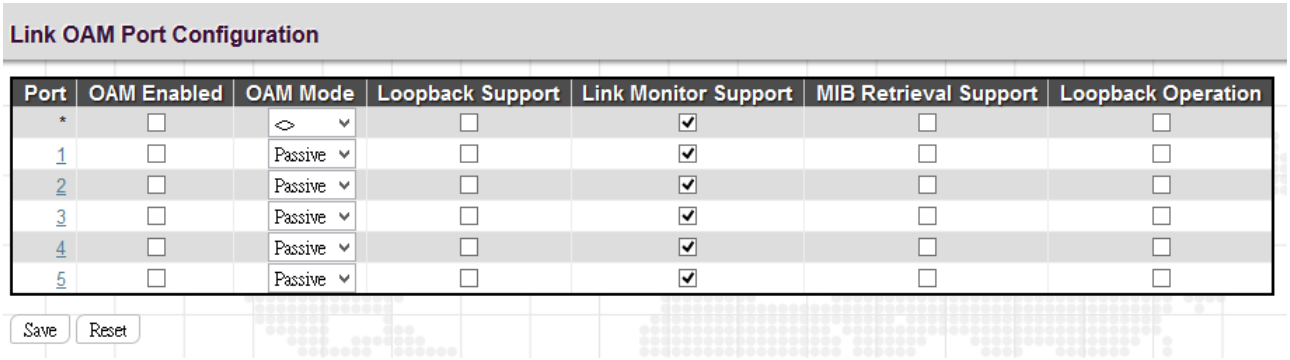
IEEE 802.3ah provides the following features:

Auto-discovery: IEEE 802.3ah provides a mechanism to detect the presence of an 802.3ah-capable Network Device (ND) on the other end of the Ethernet link. To this end, the 802.3ah-capable ND sends specified OAMPDUs in a periodic fashion, normally once a second. During the OAM Discovery process, the 802.3ah-capable ND monitors received OAMPDUs from the remote ND and allows 802.3ah OAM functionality to be enabled on the link based upon local and remote state and configuration settings. In other words, it supports OAM capability discovery function and hence eliminates the need for operators‟ configurations.

Remote loopback: IEEE 802.3ah provides a mechanism to support a data link layer frame-level loopback mode. With this function, the operator may test the performance of the link prior to placing a link in service. Once the Ethernet physical link is verified to be operational and error-free, the operator takes the link out of remote loopback and places it in service.



4.6.1 Port Settings



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.

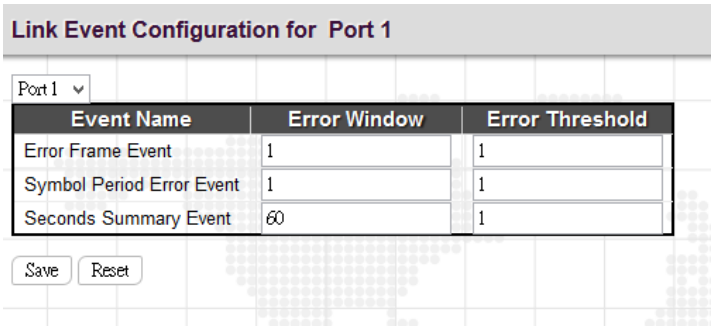
Loopback Support: Select the checkbox to enable loopback support on a port. Link OAM remote loopback support can be used for fault localization and link performance testing. Enabling the loopback support will allow the DTE to execute the remote loopback command that helps in the fault detection.

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.

4.6.2 Event Settings



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'.

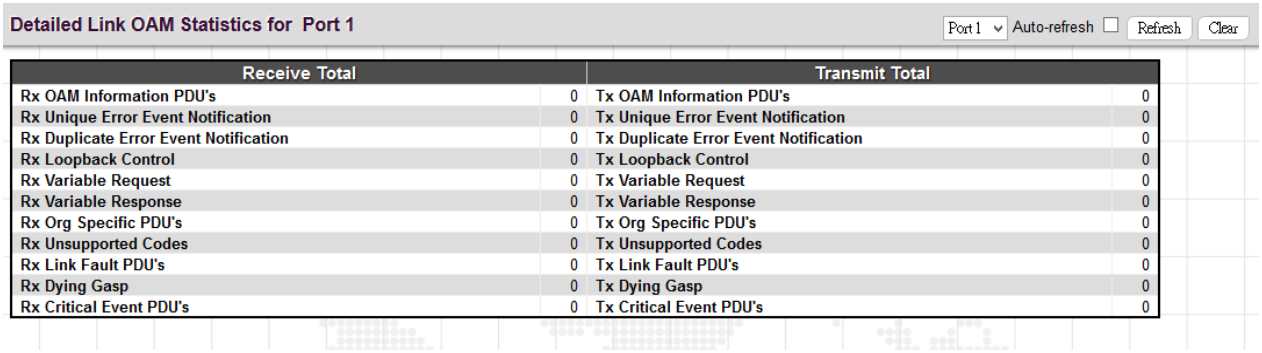
Symbol Period Error Event: The Errored Symbol Period Event counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error 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.

4.6.3 Port Statistics



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.

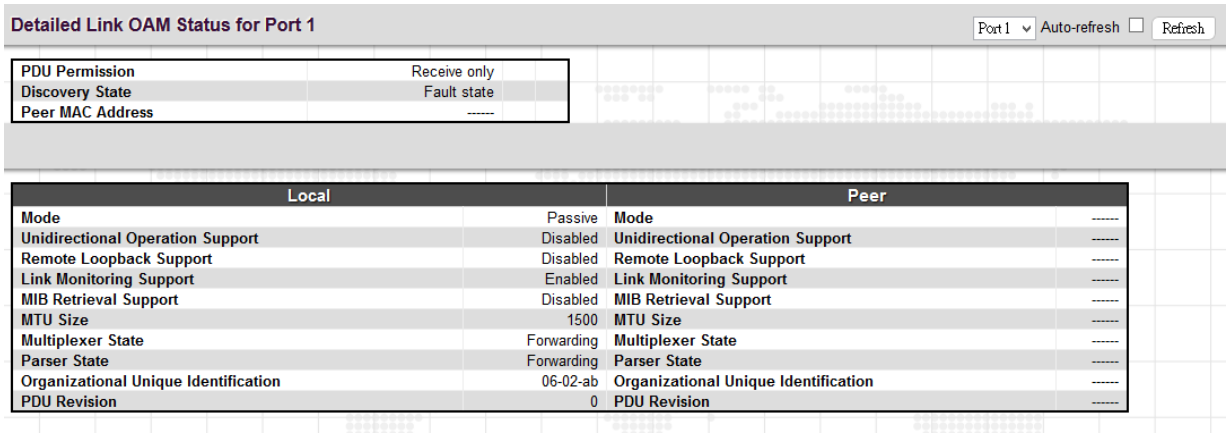
Rx & Tx Unsupported Codes: The number of OAMPDUs transmitted on this interface with an unsupported op-code.

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.

4.6.4 Port Status



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.

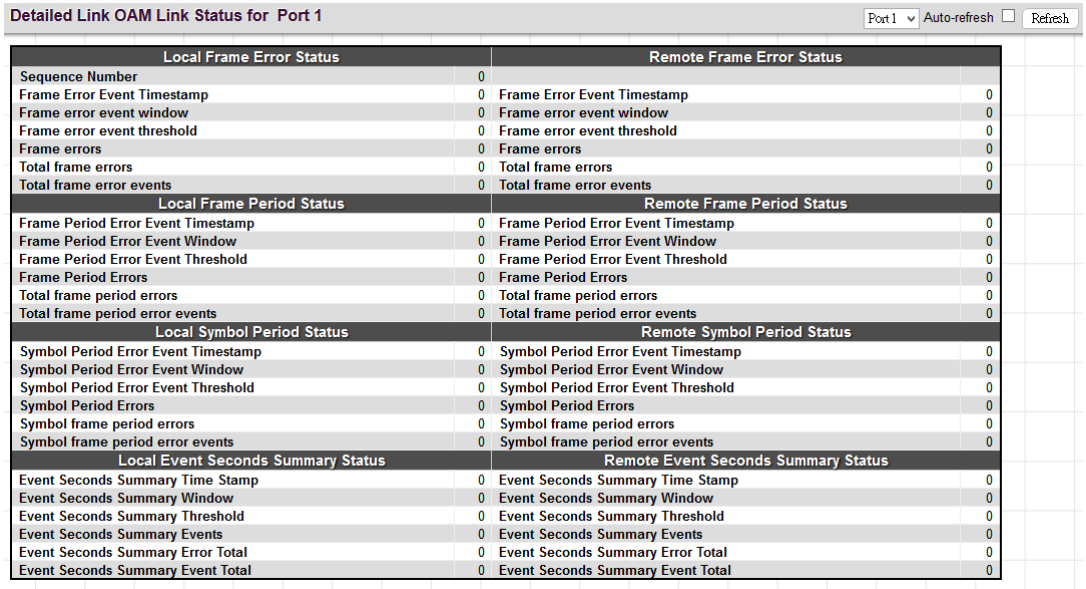
Multiplexer State: When in forwarding state, the device is forwarding non-OAMPDUs to the lower sub-layer. In case of discarding, the device discards all the non-OAMPDU's.

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).

4.6.5 Event Status



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.

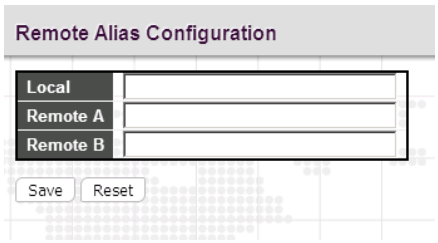
Event Seconds Summary Events: This two-octet field indicates the number of errored frame seconds in the period, encoded as a 16-bit unsigned integer.

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.

4.6.6 Remote Device

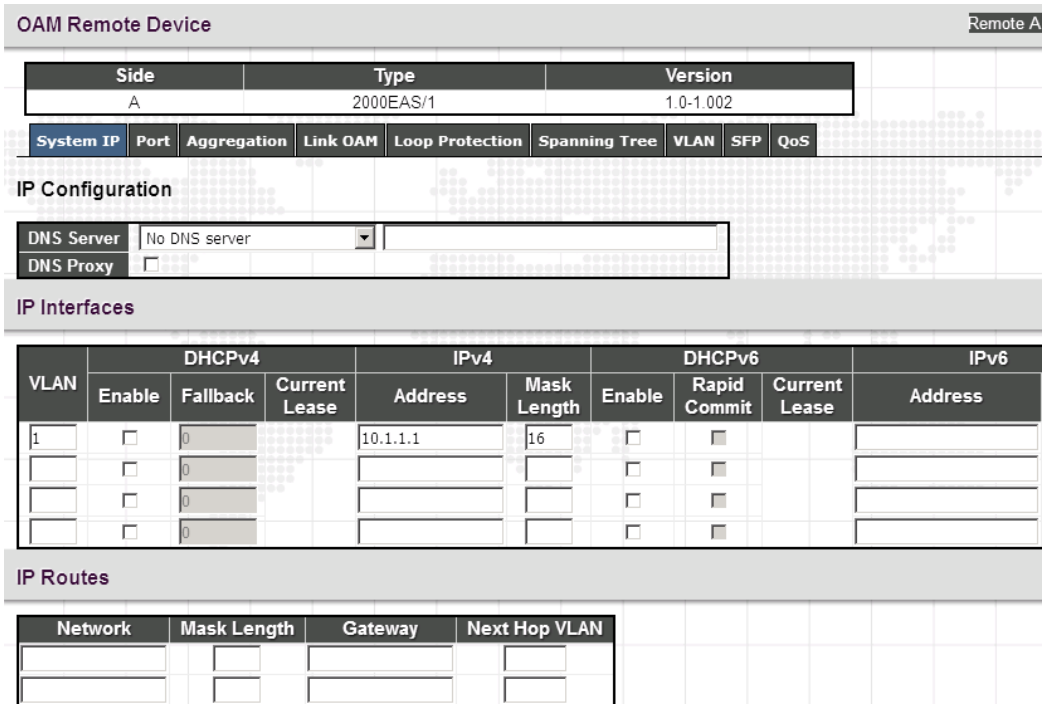
4.6.6.1 Alias



Provide an alias name for Local, Remote A & Remote B switch card.

4.6.6.2 Remote Devices

This device enables users to configure features of the remote devices using proprietary in-band management protocol. To do so, the local device must be set to “Active” mode. The remote device can be set to either “Active” or “Passive” mode. Once two devices are successfully connected, click on the “Remote" options on the left function menu in local device. Then, the screen same as below will appear.

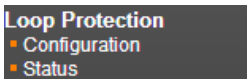


NOTE: *Apart from the method described above to manage the remote device in local side, both local and remote devices can also be managed via NMC card in FRM220A chassis. However, using this method only enables the NMC to manage remote devices that are connected to the slide-in local device via fiber optical cables. For detailed descriptions about proprietary in-band management via FRM 220A chassis, please refer to FRM220A user manual.*

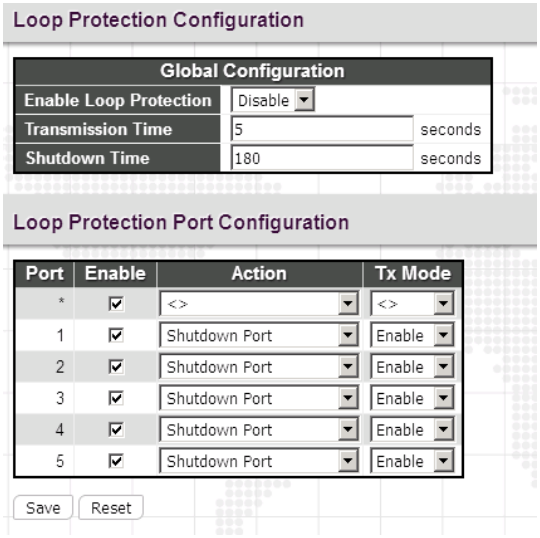
4.7 Loop Protection

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.



4.7.1 Configuration



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".

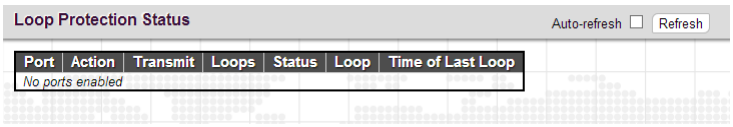
Shutdown Port: A loop-detected port is shutdown for a period of time configured in "Shutdown Time".

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.

4.7.2 Status



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.

4.8 Spanning Tree

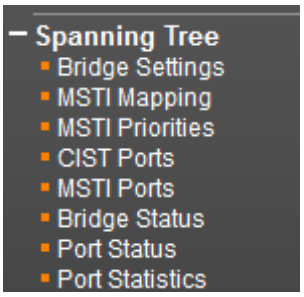
For some networking services, always-on connections are required to ensure that end users' online related activities are not interrupted due to unexpected disconnections. In these circumstances, multiple active paths between network nodes are established to prevent disconnections from happening. However, 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.

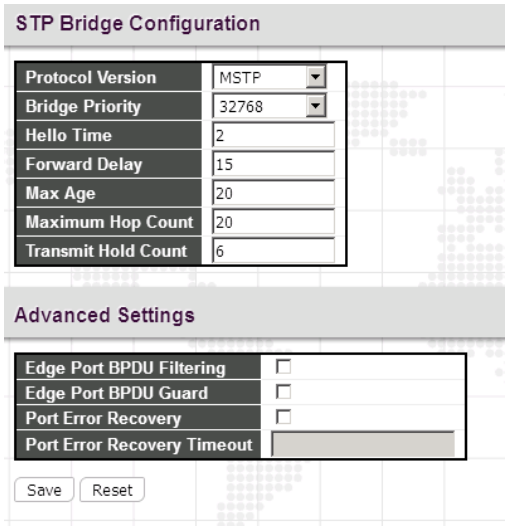
The Spanning Tree Protocol (STP), defined in the IEEE Standard 802.1s, can create a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches) and disable the links which are not part of that tree, leaving a single active path between any two network nodes.

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.



4.8.1 Bridge Settings



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.

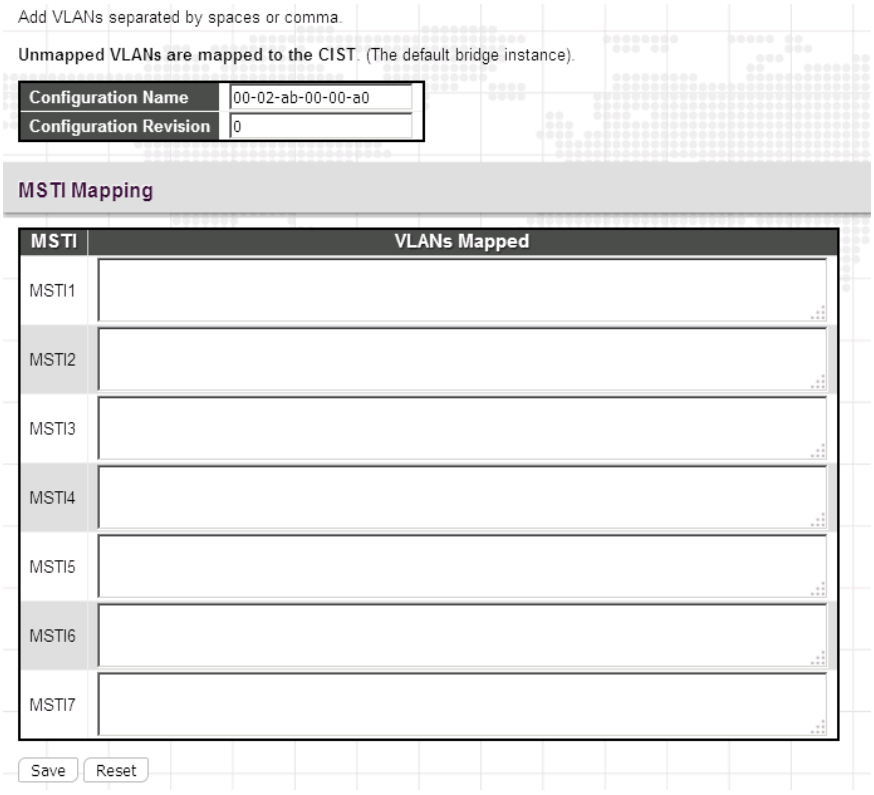
Edge Port BPDU Guard: Edge ports generally connect directly to PC, file servers or printers. Therefore, edge ports are configured to allow rapid transition. Under normal situations, edge ports should not receive configuration BPDUs. However, if they do, this probably is due to malicious attacks or mis-settings. 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.

4.8.2 MSTI Mapping



Configuration Identification

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.

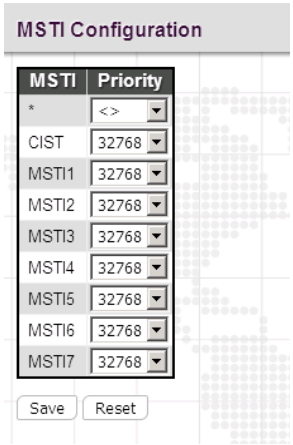
Configuration Revision: The revision number for this MSTI. The allowed range is 0~65535.

MSTI Mapping

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.

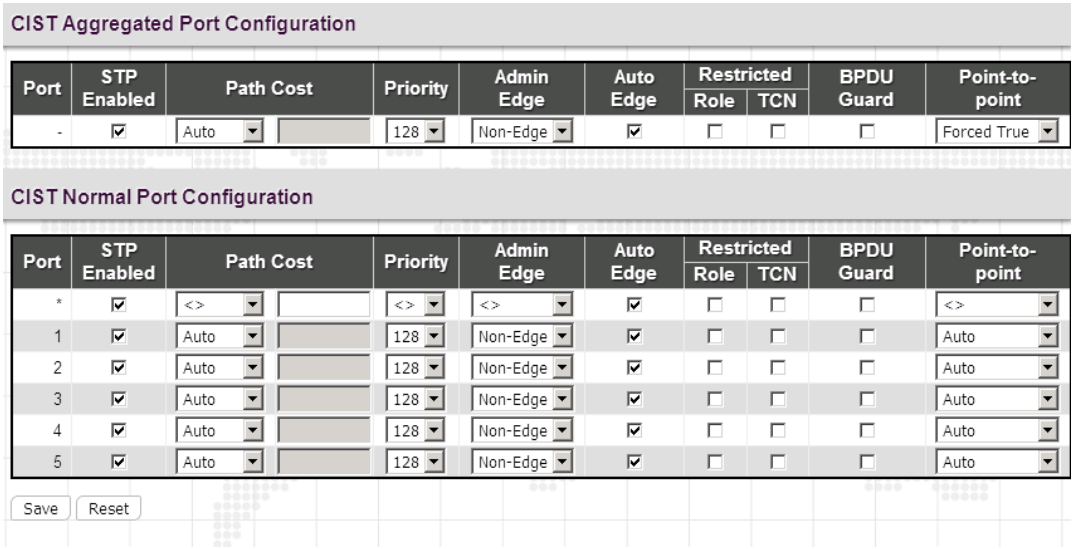
4.8.3 MSTI Priorities



MSTI: Display MSTI instance number. "MSTI *" 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.

4.8.4 CIST Ports



CIST Aggregated Port Configuration

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.

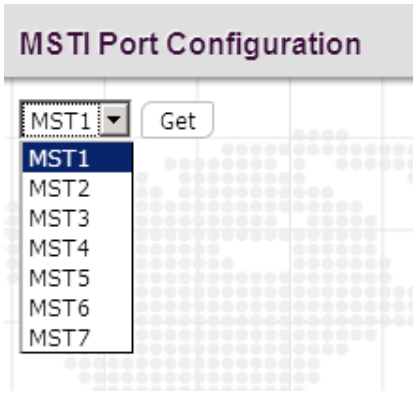
Point-to-Point: Select the link type attached to an interface.

Auto: The switch automatically determines whether the interface is attached to a point-to-point link or shared medium.

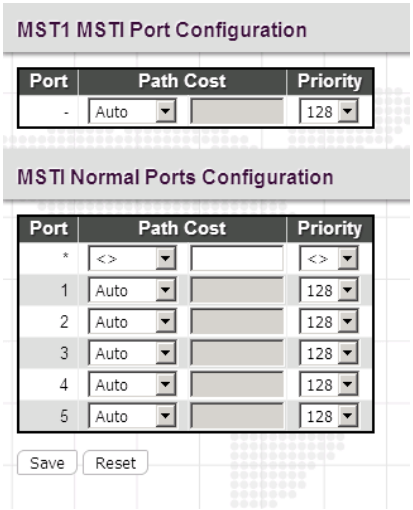
Forced True: It is a point-to-point connection.

Forced False: It is a shared medium connection.

4.8.5 MSTI Ports



Select a specific MSTI that you want to configure and then click the “Get” button.

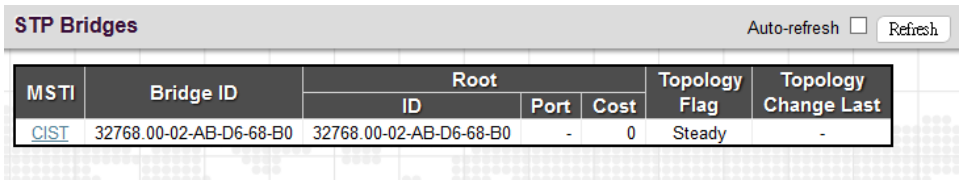


Port: The port number.

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.

4.8.6 Bridge Status



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.

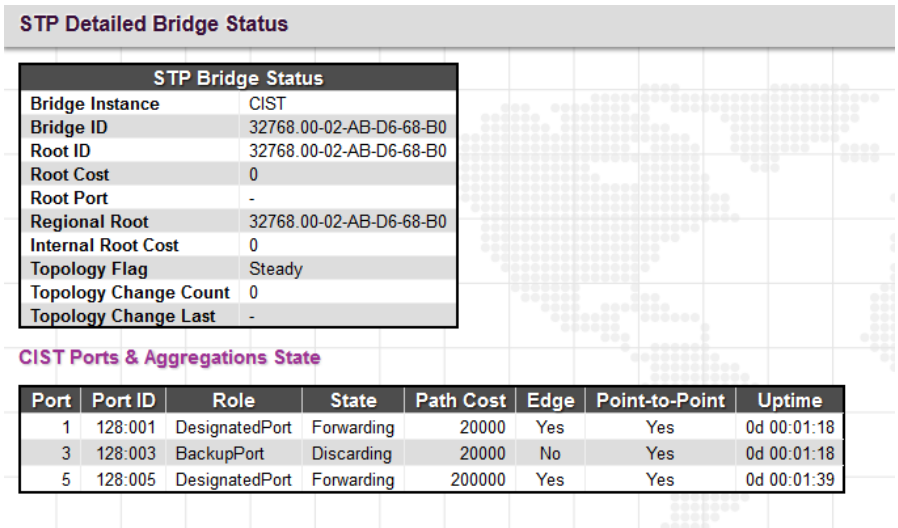
Root Port: The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.

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.

Click the MSTI instance to view STP detailed bridge status.



STP Detailed Bridge Status

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

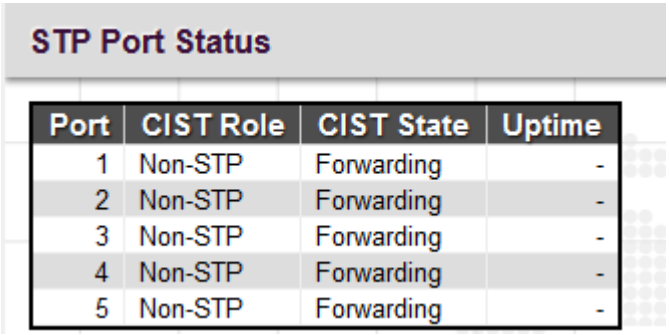
Forwarding: Ports forward packets and continue to learn addresses.

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.

4.8.7 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	-

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:

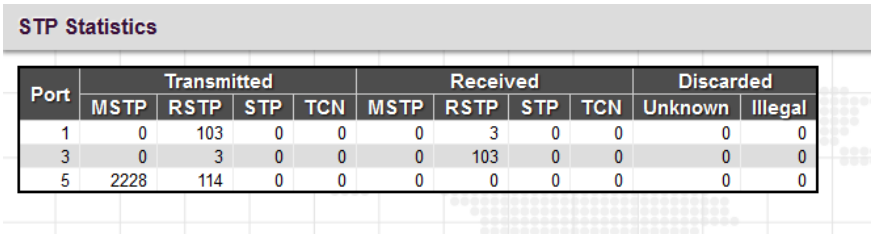
Blocking: Ports only receive BPDU messages but do not forward them.

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.

Uptime: The time since the bridge port was last initialized.

4.8.8 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.

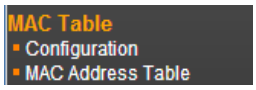
Transmitted & Received MSTP/RSTP/STP: The number of MSTP/RSTP/STP configuration BPDU messages transmitted and received on a port.

Transmitted & Received TCN: The number of TCN messages transmitted and received on a port.

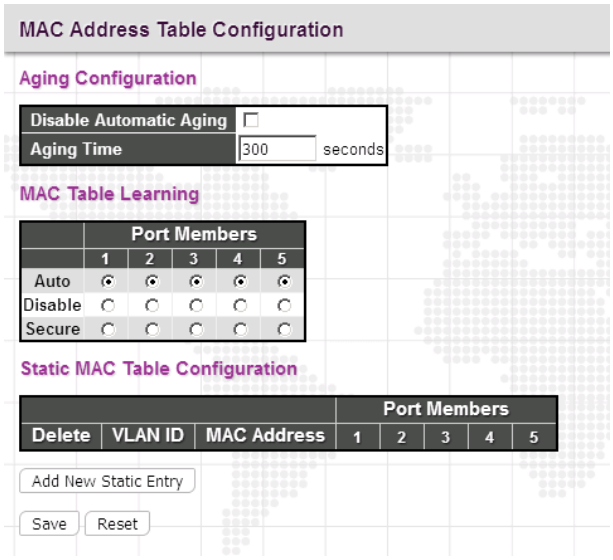
Discarded Unknown/Illegal: The number of unknown and illegal packets discarded on a port.

4.9 MAC Table

The “MAC Table” menu contains configuration and status sub menu. Select the configuration page to set up detailed configuration



4.9.1 Configuration



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.*

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.

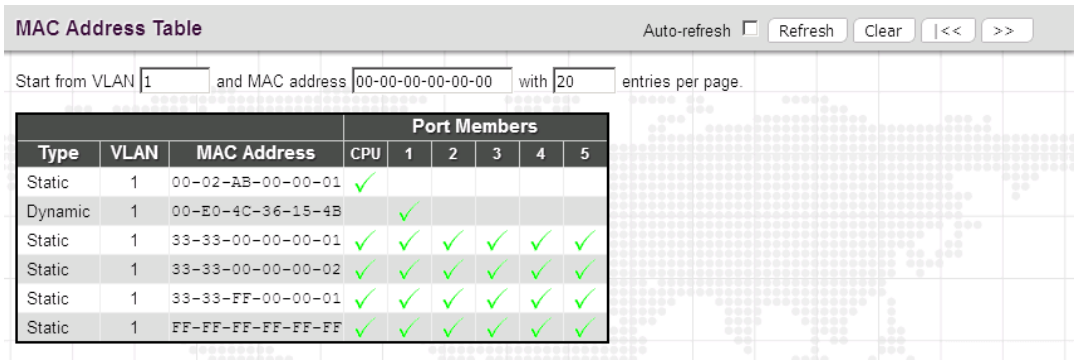
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

4.9.2 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

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.

4.10 VLANs

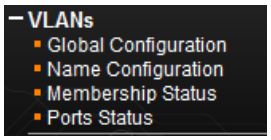
IEEE 802.1Q VLAN (Virtual Local Area Network) is a popular and cost-effectively way to segment your networking deployment by logically grouping devices with similar attributes irrespective of their physical connections. VLANs also segment the network into different broadcast domains so that packets are 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.

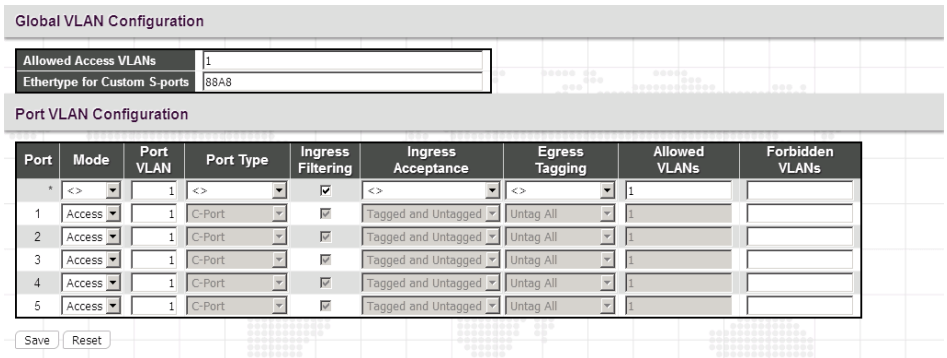
VLANs help control traffic: Traditionally, when networks are not segmented into VLANs, congestion can be easily caused by broadcast traffic that is directed to all devices. To minimize the possibility of broadcast traffic damaging the entire network, VLANs can help group devices that communicate frequently 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 set up the detailed configurations.



4.10.1 Global Configuration



Global VLAN Configuration

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.

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, 3. If the tagged frame with TPID=0x8100, it becomes a double-tag frame and is forwarded. 4. 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, 3. If a tagged frame with TIPID=0x8100, it is forwarded. 4. 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, 3. If a tagged frame with TPID=0x88A8, it is forwarded. 4. 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, 3. If a tagged frame with TPID=0x88A8, it is forwarded. 4. 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.	

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.

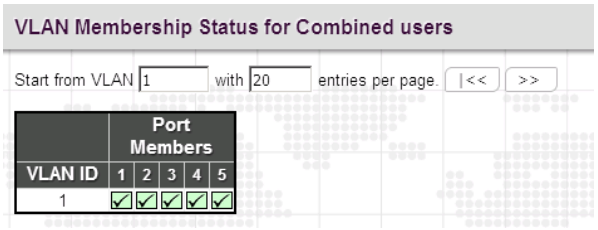
Tag All: Frames are transmitted with a tag.

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.

4.10.2 Membership Status

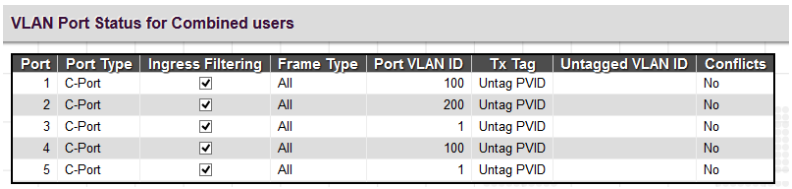


This page shows the current VLAN membership saved on the Switch.

VLAN ID: VLANs that are already created.

Port members: Display member ports on the configured VLANs.

4.10.3 Port Status



This page shows the current VLAN settings on a per-port basis saved on the Switch.

Port: The port number.

Port Type: Displays the selected port type of each port.

Ingress Filtering: Displays whether Ingress Filtering function of each port is enabled or not. When the checkbox is selected, it indicates that Ingress Filtering is enabled.

Frame Type: Displays the accepted Ingress frame type.

Port VLAN ID: Display the Port VLAN ID (PVID).

Tx Tag: Displays the Egress action on a port.

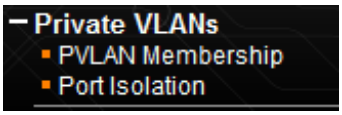
Untagged VLAN ID: Display the untagged VLAN ID. A port's UVID determines the packet's behavior at the egress side. If the VID of Ethernet frames leaving a port match the UVID, these frames will be sent untagged.

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:

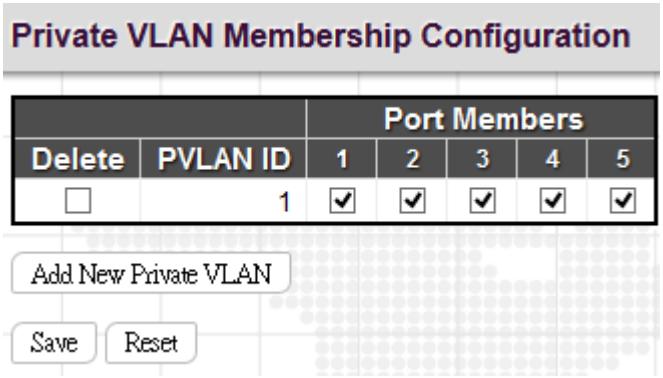
*Functional conflicts between features.
*Conflicts due to hardware limitations.
*Direct conflicts between user modules.

4.11 Private VLANs

The “Private VLANs” menu contains the following sub menus. Select the appropriate one to configure its detailed settings.



4.11.1 PVLAN Membership



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 11.

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.

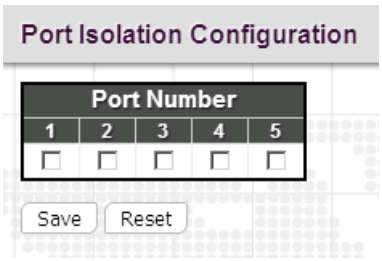
Delete: Delete this VLAN membership entry.

Add New VLAN: Click the button once to add a new VLAN entry.

Save: VLAN membership changes will be saved and new VLANs are enabled after clicking “Save” button.

Reset: Click “Reset” button to clear all unsaved VLAN settings and changes.

4.11.2 Port Isolation

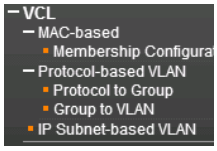


Private VLAN is used to group ports together so as to prevent communications within PVLAN. Port Isolation is used to prevent communications between customer ports in a same Private VLAN. The port that is isolated from others cannot forward any unicast, multicast or broadcast traffic to any other ports in the same PVLAN.

Port Number: Select the checkbox if you want a port or ports to be isolated from other ports.

4.12 VCL

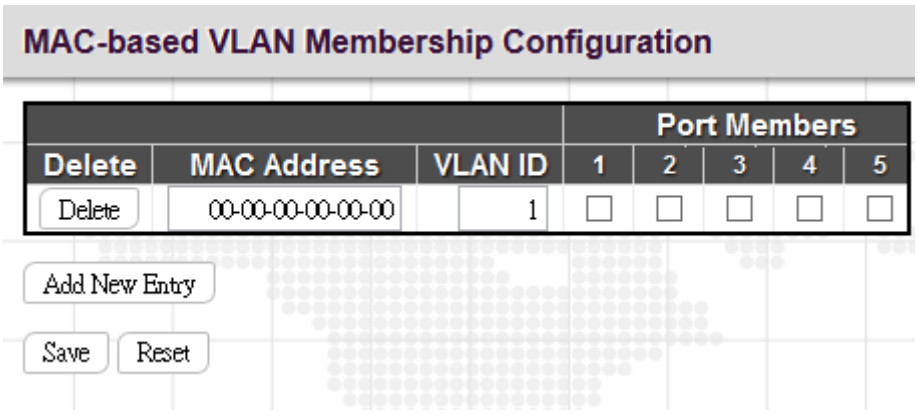
The "VCL" menu contains the following sub menus.



4.12.1 MAC-based

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 does not match the rules created, untagged frames are assigned to the receiving port's native VLAN ID (PVID).

3.12.1.1 Membership Configuration



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.

Save: Changes will be saved and newly entered rules are enabled after clicking “Save” button.

Click “Add New Entry” to create a new rule.

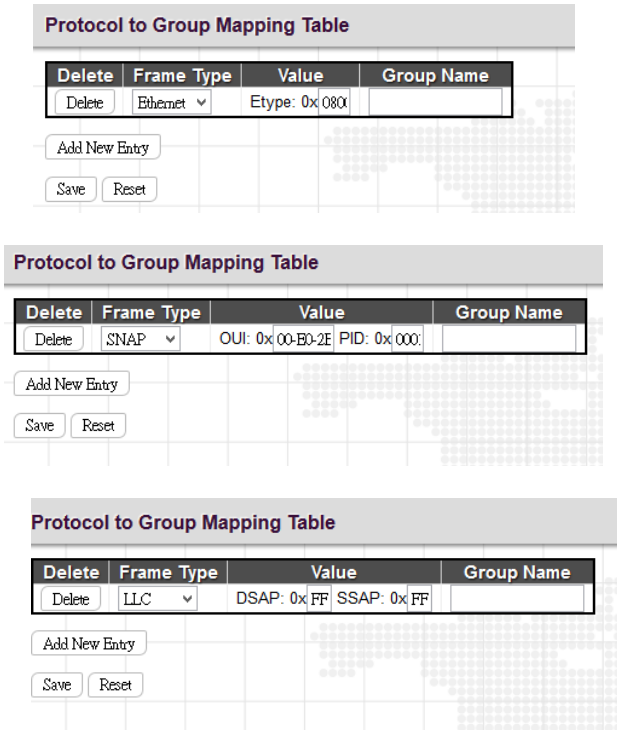
Delete: Click “Delete” to remove this entry.

4.12.2 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.

4.12.2.1 Protocol to Group



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.

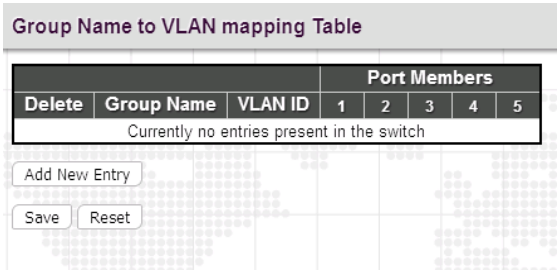
OUI: A value in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value in the ranges of 0x00-0xff.

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).

4.12.2.2 Group to VLAN



Group Name: Indicate the descriptive name for this entry. This field only allows 16 alphabet characters (a-z; A-Z) or integers (0-9).

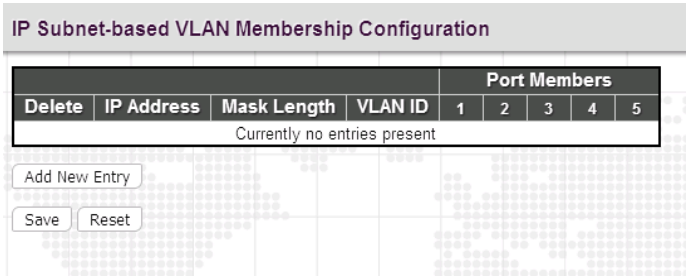
VLAN ID: Indicate the VLAN ID.

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.

4.12.3 IP Subnet-based VLAN



VCE ID: Index of the entry. Valid range is 0-128.

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.

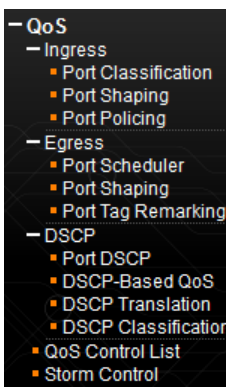
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

4.13 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.

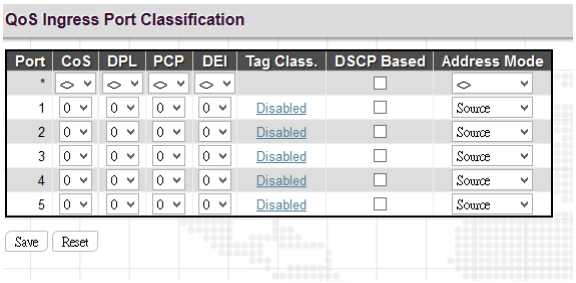
QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic. To set up the priority of packets in this switch, go to “Port Classification” page.

The “QoS” menu contains the following sub menus.



4.13.1 Ingress

4.13.1.1 Port Classification



Port: List of the number of each port. "Port *" rules will apply to all ports.

CoS: Indicate the Class of Service level. A CoS class of 0 has the lowest priority. By Default, 0 is used.

DPL: 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.

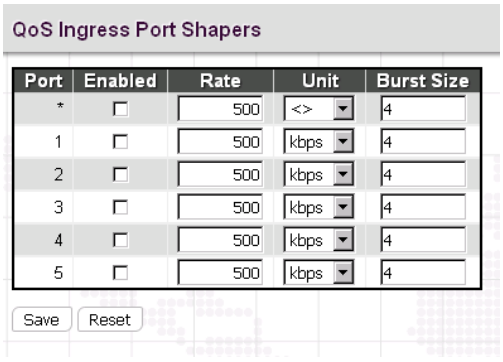
DSCP Based: Select the checkbox to enable DSCP based QoS (Ingress Port).

Address Mode: The IP/MAC address mode specifying whether the QCL destination must be based on source or destination addresses on this port. The allowed values are:

Source: Enable source IP/MAC matching.

Destination: Enable destination IP/MAC matching.

4.13.1.2 Port Shaping



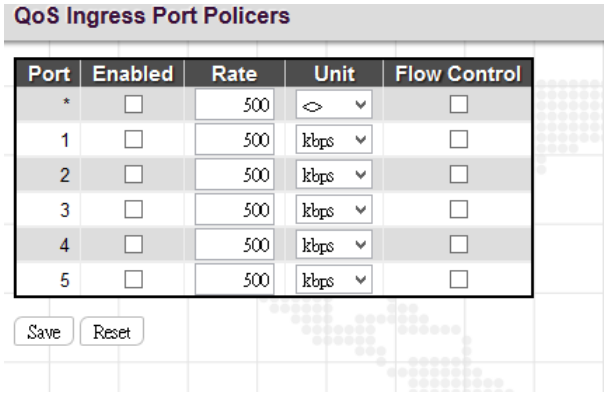
Enabled: Select the checkbox to enable port shaping function on a port.

Rate: Indicate the rate for the port shaping. 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 port shaping.

Burst Size: Indicate in bits (or bytes) per burst how much traffic can be sent within a given unit of time to not create scheduling concerns.

4.13.1.3 Port Policing



This page allows users to set each port's allowed bandwidth.

Port: The port number. "Port *" settings apply to all ports.

Enabled: Select the checkbox to enable port policing function on a port.

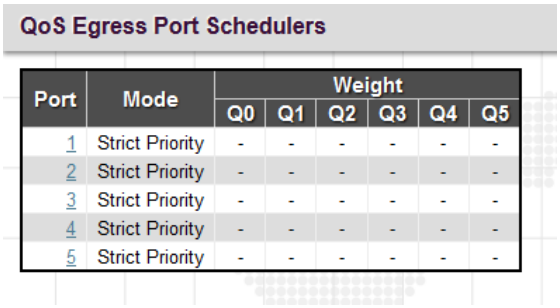
Rate: Indicate the rate for the policer. By default, 500kbps is used. The allowed range for kbps and fps is 100 to 1000000. The allowed range for Mbps and kfps is 1 to 3300Mbps.

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.

4.13.2 Egress

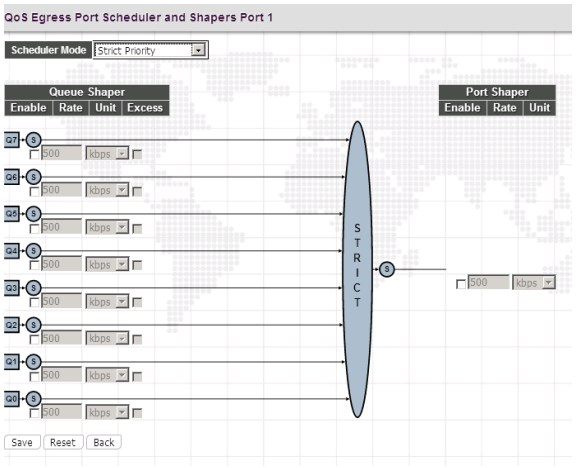
4.13.2.1 Port Scheduler

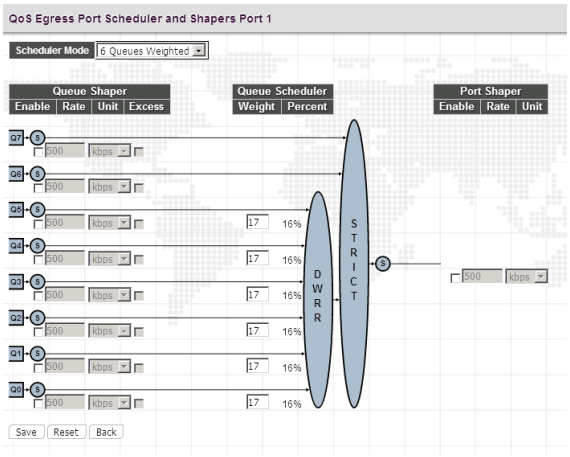


Port: Click the port to set up detailed settings for port scheduler.

Mode: Display scheduler mode selected.

Weight: Display the weight in percentage assigned to Q0~Q5.





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

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.

Queue Schedule

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.

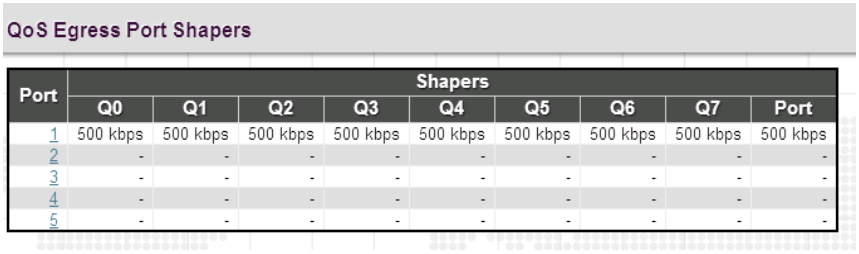
Port Shaper: Set the rate at which traffic can egress this queue.

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

4.13.2.2 Port Shaping

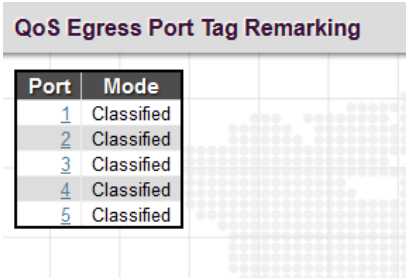

QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	500 kbps	500 kbps	500 kbps	500 kbps	500 kbps	500 kbps	500 kbps	500 kbps	500 kbps
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-

This table displays each port's queue shaper and port shaper's rate.

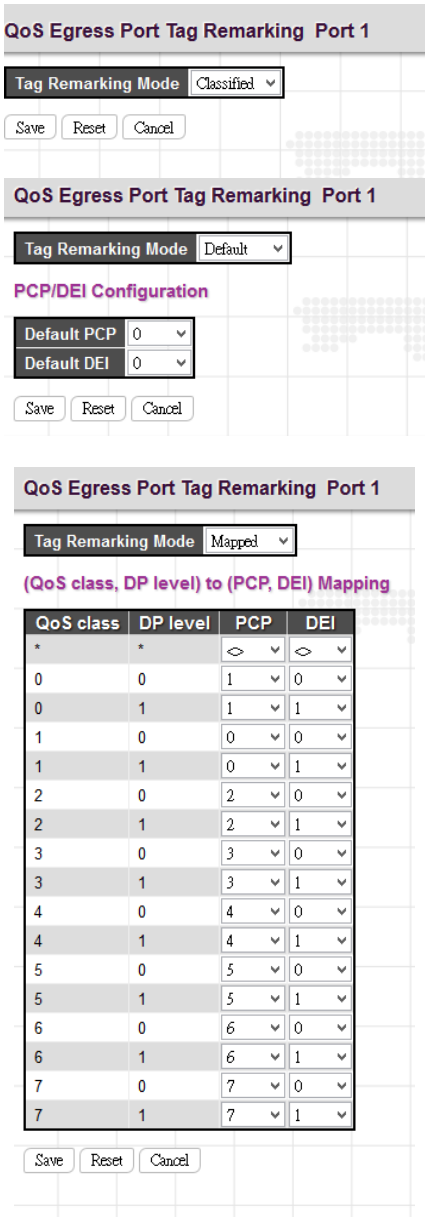
Click the port number to modify or reset queue shaper and port shaper's rates. See "Port Scheduler" for detailed explanation on each configuration option.

4.13.2.3 Port Tag Remarking


QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified

Click on the port number to configure its' QoS Egress Port Tag Remarking.



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.

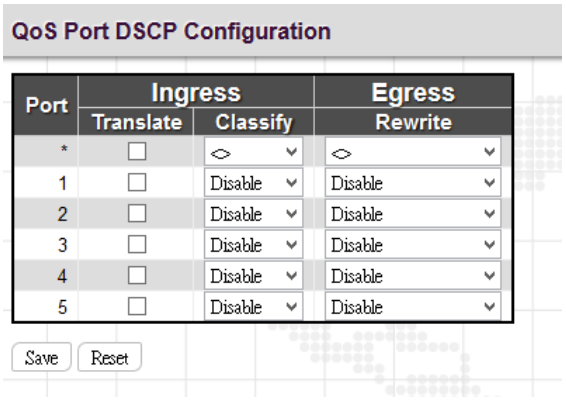
QoS class/DP level: Show the mapping options for QoS class values and DP levels (drop precedence).

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)

4.13.3 DSCP

4.13.3.1 Port DSCP



Port: The port number. "Port *" 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.

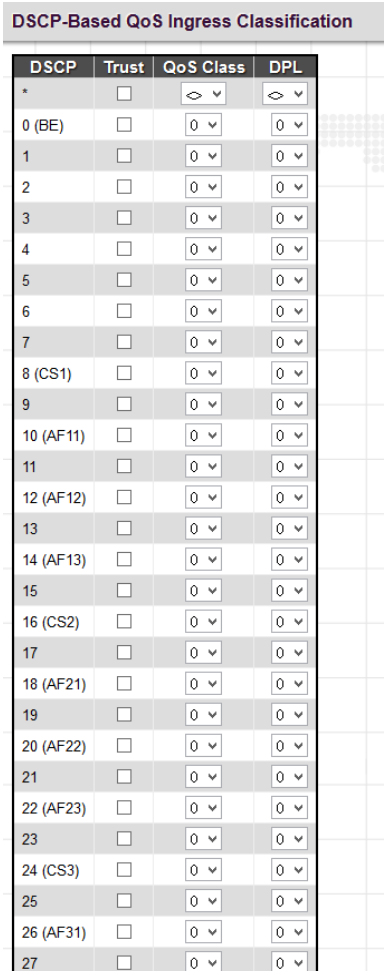
Disable: Egress rewriting is disabled.

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.

4.13.3.2 DSCP-Based QoS



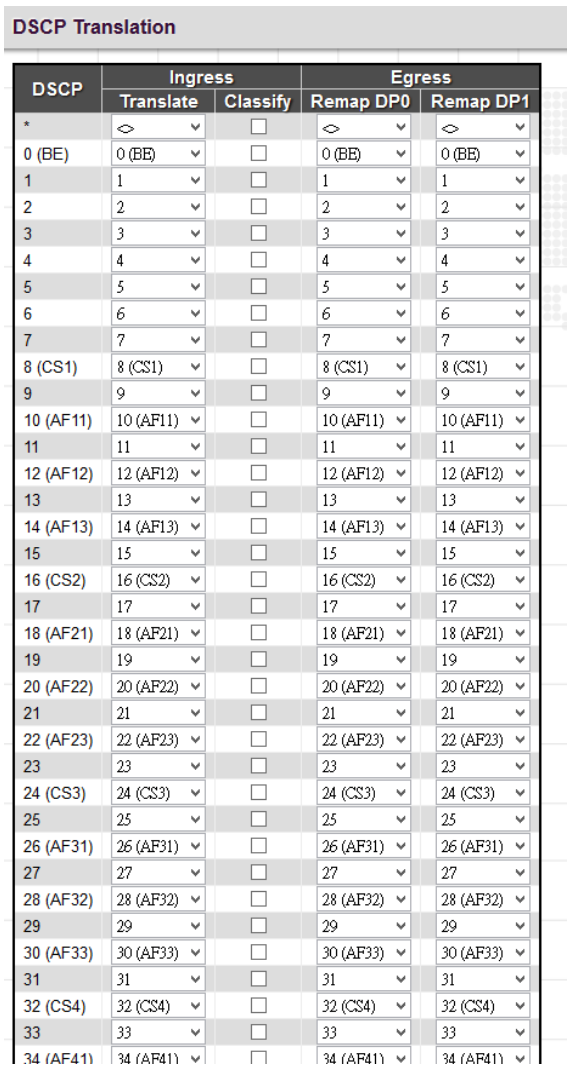
DSCP: DSCP value in ingress packet. DSCP range is from 0 to 63.

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.

4.13.3.3 DSCP Translation



DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	☐	<>	<>
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
28 (AF32)	28 (AF32)	☐	28 (AF32)	28 (AF32)
29	29	☐	29	29
30 (AF33)	30 (AF33)	☐	30 (AF33)	30 (AF33)
31	31	☐	31	31
32 (CS4)	32 (CS4)	☐	32 (CS4)	32 (CS4)
33	33	☐	33	33
34 (AF41)	34 (AF41)	☐	34 (AF41)	34 (AF41)

DSCP: DSCP value in ingress packet. DSCP range is from 0 to 63.

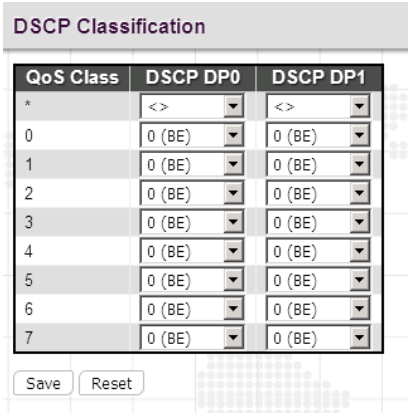
Ingress Translate: Enable Ingress Translation of DSCP values based on the specified classification method.

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.

4.13.3.4 DSCP Classification



Map DSCP values to QoS class and DPL value.

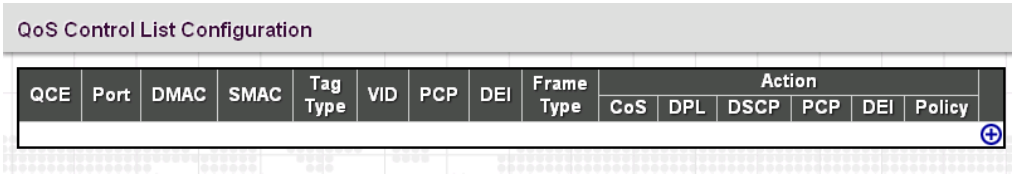
QoS Class: List of actual QoS class values.

DSCP DP0: Select the classified DSCP value (0~63) for Drop Precedence Level 0.

DSCP DP1: Select the classified DSCP value (0~63) for Drop Precedence Level 1.

4.13.4 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.



This page displays rules created in QoS control list (QCL) only. The maximum number of QCL is 256 on this device. Click ⊕ to insert a new QCL to the list.

QCE#: Display Quality Control Entry index.

Port: Display the port number that uses this QCL.

DMAC: Destination MAC address. Possible values are Any, Broadcast, Multicast, Unicast.

SMAC: Source MAC address.

Tag Type: Display whether it is tagged or untagged frames.

VID: Display VLAN ID (1~4095)

PCP: Display PCP value.

DEI: Display DEI value.

Frame Type: Display the frame type selected.

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.

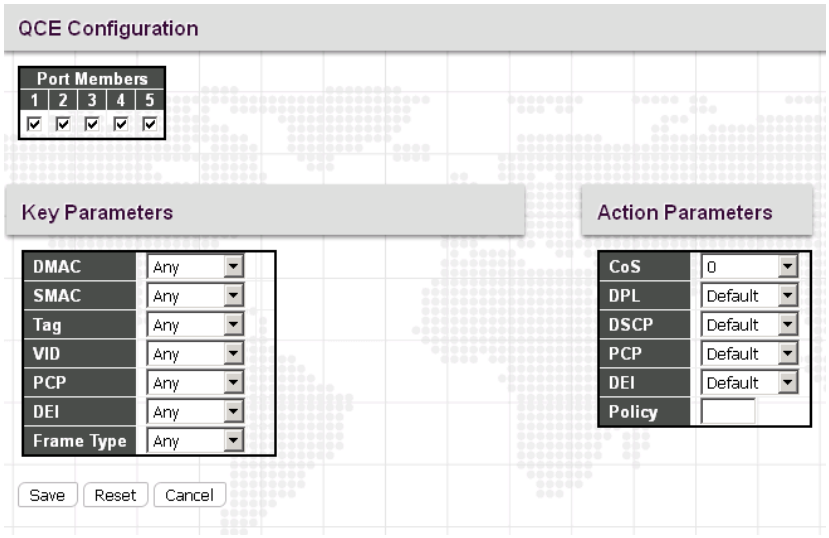
Class: If a frame matches the QCL, it will be put in the queue corresponding to the specified QoS class.

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:
: Insert a new QCE before the current row.
: Edit the QCE entry.
: Move the QCE up the list.
: Move the QCE down the list.
: Delete the QCE.
: The lowest plus sign add 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: Select ports that use this rule.

Key Parameters

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.

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).

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.

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.

Ether Type: 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).

SIP 32 LSB: 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:

CoS: 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.

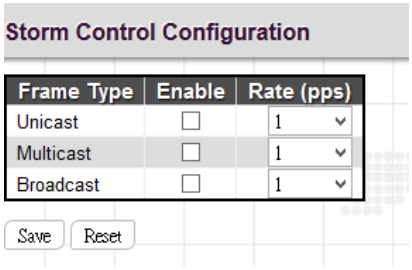
PCP: If a frame matches the QCE, the PCP value will be set to the selected one.

DEI: If a frame matches the QCE, the DEI value will be set to the selected one.

Policy: If a frame matches the QCE, it will follow the specified ACL policy.

4.13.5 Storm Control

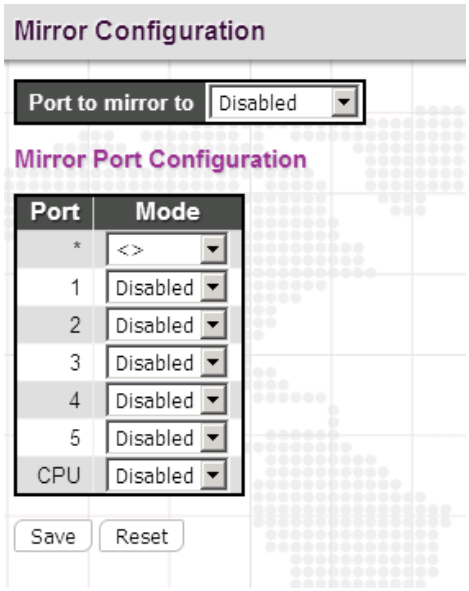
Storm Control is used to keep a network from downgraded performance or a complete halt by setting up a threshold for traffic like broadcast, unicast and multicast. When a device on the network is malfunctioning or application programs are not well designed or properly configured, storms may occur and 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.



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.

4.14 Mirroring



Port to mirror: This is also known as Mirror Port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Select "Disabled" to disable mirroring function.

Mode: There are four modes that can be used on each port.

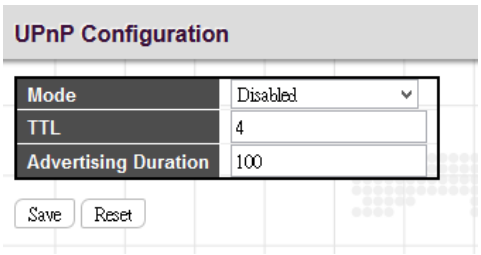
Disabled: Disable the port mirroring function on a given port.

Rx only: Only frames received on this port are mirrored on the mirror port.

Tx only: Only frames transmitted on this port are mirrored on the mirror port.

Enable: Both frames received and transmitted re mirrored on the mirror port.

4.15 UPnP



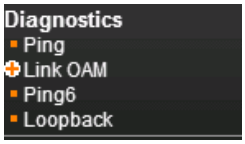
Mode: Enable or disable UPnP operation.

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.

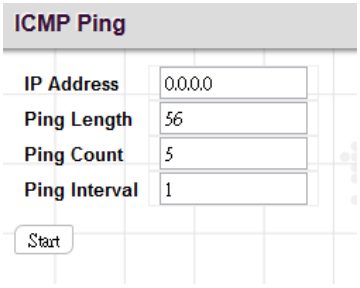
4.16 Diagnostics

The “Diagnostics” menu provides ping function to test the connectivity of a certain IP.



4.16.1 Ping

This Ping function is for ICMPv4 packets.



IP Address: Enter the IP address that you wish to ping.

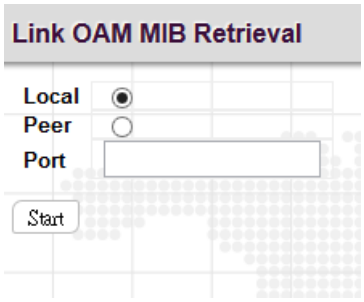
Ping Length: The size or length of echo packets.

Ping Count: The number of echo packets will be sent.

Ping Interval: The time interval between each ping request.

4.16.2 Link OAM

4.16.2.1 MIB Retrieval

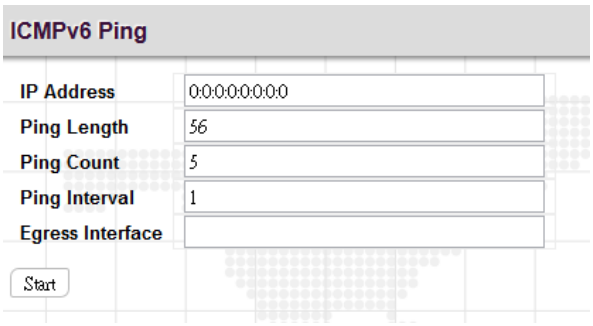


Local or Peer: Click on the radio button to select the location of MIB to be polled.

Port: The port on the device that is used for OAM MIB retrieval.

4.16.3 Ping6

This Ping function is for ICMPv6 packets.



IP Address: Enter the IP address that you wish to ping.

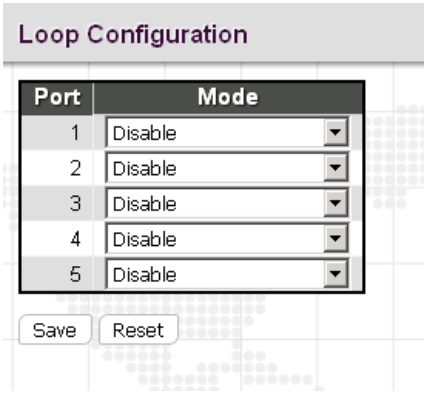
Ping Length: The size or length of echo packets.

Ping Count: The number of echo packets will be sent.

Ping Interval: The time interval between each ping request.

Egress Interface: The VLAN ID of the specific egress IPv6 interface which ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, Ping6 finds the best match interface for destination. Please note that do not specify egress interface for loopback address. Do specify egress interface for link-local or multicast address.

4.16.4 Loopback



Mode: There are two types of loopback modes available.

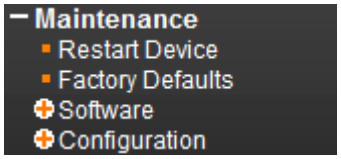
Disabled: Loopback function is not used.

Near-End: Near-End loopback provides the ability to loop the transmitted data back to the receiver.

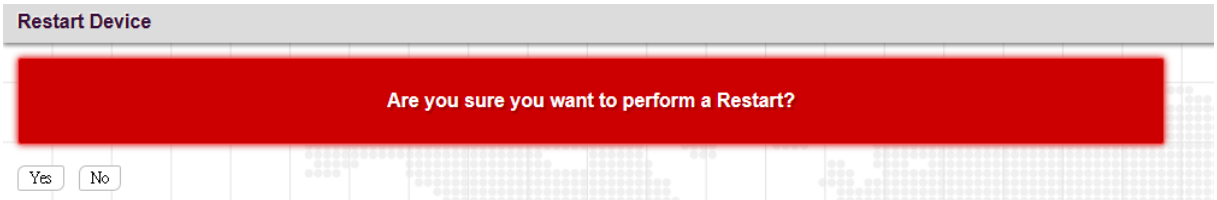
Far-End: Far-End loopback is to allow testing the PHY from the link partner side. In Far-End mode, data is received from the link partner through the PHY's receiver.

4.17 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.



4.17.1 Restart Device



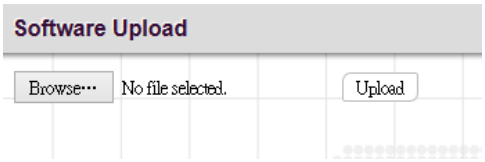
Click "Yes" button to reboot the switch.

4.17.2 Factory Defaults

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.

4.17.3 Software

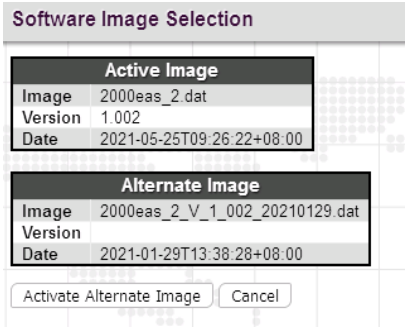
4.17.3.1 Upload



Update the latest Firmware file.

Select a Firmware file from your local device and then click “Upload” to start updating.

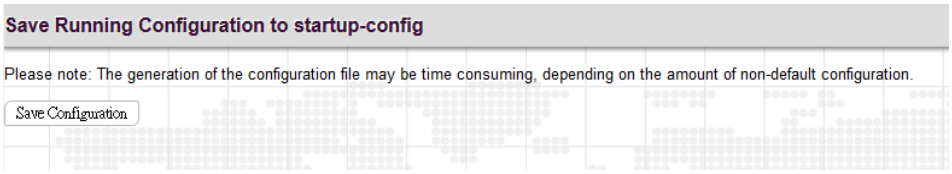
4.17.3.2 Image Select



Select the image file to be used in this device.

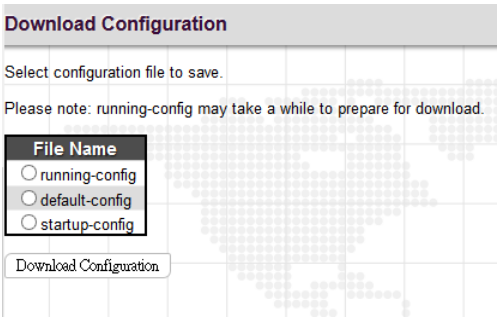
4.17.4 Configuration

4.17.4.1 Save



Click on the “Save Configuration” button to save current running configurations to startup configurations.

4.17.4.2 Download

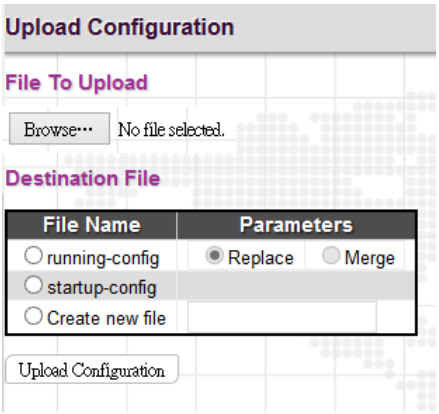


running-config: Download a copy of the current running configurations to your local device.

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.

4.17.4.3 Upload

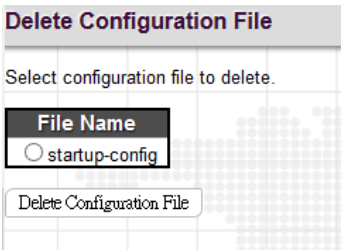


Select a file and then click “Upload Configuration” to start uploading the file.

4.17.4.4 Activate

Select the file that you would like to use. Click on the “Activate Configuration” to replace configurations to the selected one.

4.17.4.5 Delete



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.

CTC union®

www.ctcu.com

T +886-2 2659-1021 F +886-2 2659-0237 E sales@ctcu.com